



Informatica® Intelligent Cloud Services
Fall 2020 October

管理者

Informatica Intelligent Cloud Services 管理者
Fall 2020 October
2020 年 10 月

© 著作権 Informatica LLC 2006, 2020

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（電子的複製、写真複製、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: 2020-12-01

目次

序文	9
Informatica のリソース	9
Informatica マニュアル	9
Informatica Intelligent Cloud Services Web サイト	9
Informatica Intelligent Cloud Services コミュニティ	9
Informatica Intelligent Cloud Services マーケットプレイス	10
データ統合コネクタのドキュメント	10
Informatica ナレッジベース	10
Informatica Intelligent Cloud Services Trust Center	10
Informatica グローバルカスタマサポート	10
第 1 章 : 管理者について	11
ユーザープロファイルの編集	13
第 2 章 : 組織	14
組織の設定	14
組織のプロパティ	15
組織の全般プロパティ	15
認証プロパティ	16
接続プロパティの保存場所	17
データ統合サービスのプロパティ	18
CLAIRE の推奨設定	19
Enterprise Data Catalog 統合プロパティ	19
サブ組織	20
サブ組織の追加または削除	21
サブ組織の無効化または有効化	22
別の組織への切り替え	23
サブ組織への親組織のアクセスを拒否	23
サブ組織のアドオンコネクタ	23
サブ組織でのアセットのエクスポートとインポート	23
第 3 章 : ライセンス	24
ライセンスのカテゴリ	24
ライセンスのタイプ	24
サブ組織のライセンス	25
サブ組織のライセンスの編集	26
親組織とのライセンスの同期	26
ライセンスの有効期限	26
第 4 章 : エコシステムのシングルサインオン	27

第 5 章 : SAML のシングルサインオン	29
SAML のシングルサインオンの要件	30
シングルサインオンの制限	30
SAML のシングルサインオンによるユーザー管理	30
Informatica Intelligent Cloud Services の SAML シングルサインオン設定	31
プロバイダ設定とマッピング属性の設定	31
ID プロバイダのプロパティ	32
サービスプロバイダのプロパティ	33
SAML 属性マッピングのプロパティ	34
SAML ロールマッピングのプロパティ	35
サービスプロバイダメタデータのダウンロード	35
第 6 章 : メータリング	36
ライセンスメトリックの表示	36
メーター定義	37
メータリングの使用状況レポート	39
使用状況の詳細の表示	40
第 7 章 : ソース管理およびサービスアップグレード設定	41
ソース管理設定	41
サブ組織のソース管理設定	42
OAuth を使用したリポジトリアクセス	42
組織のソース管理の有効化	43
ソース管理リポジトリ URL の変更	43
組織のソース管理の無効化	44
リポジトリアクセスの設定	44
ソース管理のベストプラクティス	45
別のユーザーのチェックアウトの取り消し	46
Secure Agent サービスのローリングアップグレード	47
ローリングアップグレードエラーの処理	48
Secure Agent サービスの再開スケジュールの設定	48
第 8 章 : ユーザーとユーザーグループ	49
ユーザー	49
ユーザー認証	50
アプリケーションの統合の匿名ユーザー	51
ユーザー統計	51
ユーザーの詳細	52
ユーザーの作成	55
サービスの割り当ておよび割り当て解除	55
ユーザーの無効化	56
ユーザーのリセット	56

ユーザーのスケジュール済みジョブの再割り当て.	57
ユーザーの削除.	57
ユーザグループ.	58
ユーザーグループの詳細.	59
ユーザーグループの作成.	59
ユーザーグループの名前変更.	60
ユーザーグループの削除.	60
ユーザー設定の例.	60
第 9 章 : ユーザーロール.	63
ロールの詳細.	64
アプリケーションの統合機能特権.	66
Data Quality の機能特権.	67
システム定義のロール.	68
クロスサービスロール.	68
クロスサービスロールのアクセス特権.	69
サービス固有のロール.	73
アプリケーション統合ロールのアクセス特権.	73
データ統合ロールのアクセス特権.	74
MDM - Reference 360 ロールのアクセス特権.	75
カスタムロール.	75
カスタムロールの作成.	75
カスタムロールの削除.	76
B2B パートナーポータルของผู้utzerロール.	76
第 10 章 : 権限.	77
権限のルールおよびガイドライン.	78
権限の設定.	79
第 11 章 : ランタイム環境.	81
Hosted Agent.	81
Secure Agent グループ.	83
複数のエージェントを含む Secure Agent グループ.	84
Secure Agent グループへのサービス割り当て.	84
Secure Agent グループの共有.	87
Secure Agent グループの操作.	87
Secure Agent グループの依存関係の表示.	91
Secure Agent.	91
Secure Agent の操作.	92
Secure Agent でのサービスの停止と開始.	94
エージェントのブラックアウト期間の設定.	97
Secure Agent の名前変更.	99
Secure Agent の削除.	99

Secure Agent のアップグレード.	100
Secure Agent Manager.	100
非プロキシホストを除外するためのプロキシの設定.	100
Windows での Secure Agent の停止および再起動.	101
Linux での Secure Agent の起動および停止.	101
第 12 章 : サーバーレスランタイム環境.	103
サーバーレスコンピューティングユニット.	103
始める前に.	104
手順 1. NAT ゲートウェイの作成.	104
手順 2. 補足ファイル用の S3 フォルダの作成.	104
手順 3. IAM ロールの設定.	105
手順 4. セキュリティグループの作成.	106
サーバーレスランタイム環境のプロパティ.	107
サーバーレスランタイム環境の編集.	109
サーバーレスランタイム環境の再デプロイ.	109
サーバーレスランタイム環境のクローン作成.	110
ルールおよびガイドライン.	110
ディザスタリカバリ.	110
サーバーレスランタイム環境でのコネクタ.	111
第 13 章 : Secure Agent サービス.	113
API マイクロゲートウェイサービス.	115
API Microgateway Service のプロパティ.	116
CMI ストリーミングエージェント.	117
CMI ストリーミングエージェントのプロパティ.	117
共通統合コンポーネント.	119
共通統合コンポーネントプロパティ.	119
データベース取り込みサービス.	121
データベース取り込みサービスのプロパティ.	121
データベース取り込みエージェントの環境変数.	122
データ統合サーバー.	123
データ統合サーバーの回復機能.	123
データ統合サーバーのプロパティ.	124
エラスティックサーバー.	125
エラスティックサーバーのプロパティ.	125
ファイル統合サービス.	126
一括取り込み（ファイル）.	127
プロセスサーバー.	128
プロセスサーバーのプロパティ.	129
プロセスサーバーのサイズ決定に関する推奨事項.	135
Secure Agent との通信.	136
プロセスサーバーのための Secure Agent の設定.	137

Windows での PostgreSQL データベースの管理.	140
Linux での PostgreSQL データベースの管理.	143
Secure Agent サービスプロパティの設定.	146
第 14 章 : Secure Agent のインストール.	147
Windows での Secure Agent のインストール.	147
Windows での Secure Agent の要件.	147
Windows での Secure Agent のダウンロードおよびインストール.	148
Windows でのプロキシ設定.	150
Windows Secure Agent サービスへのログインの設定.	150
Windows での Secure Agent のアンインストール.	151
Linux での Secure Agent のインストール.	151
Linux での Secure Agent の要件.	152
Linux での Secure Agent のダウンロードおよびインストール.	153
Linux でのプロキシ設定.	153
Linux での Secure Agent のアンインストール.	154
第 15 章 : スケジュール.	155
ブラックアウト期間の設定.	156
繰り返し頻度.	156
タイムゾーンとスケジュール.	157
夏時間への移行とスケジュール.	157
スケジュールの設定.	158
スケジュールのエクスポート.	159
第 16 章 : バンドル管理.	160
バンドルのインストール.	160
バンドルのコピー.	161
バンドルのアップグレード.	162
バンドルのアンインストール.	162
第 17 章 : イベント監視.	163
第 18 章 : ファイル転送.	165
ファイルサーバーの設定プロセス.	166
始める前に.	167
ファイルサーバー.	167
ファイルサーバーの設定.	167
AS2 サーバーの設定プロパティ.	168
HTTPS サーバー設定プロパティ.	172
SFTP サーバー設定プロパティ.	174
プロキシサーバー設定プロパティ.	177
ファイル統合プロキシサーバーのインストール.	178

ファイルサーバー.....	179
ファイルサーバーのユーザー.....	180
ファイルサーバーユーザーの設定.....	180
ファイルサーバーユーザーのプロパティ.....	180
ファイルサーバーユーザーの削除.....	183
ファイル転送タスク.....	183
グローバル設定.....	184
第 19 章: トラブルシューティング.....	186
Secure Agent のトラブルシューティング.....	186
Secure Agent のエラー.....	186
AWS 上のエラスティッククラスタのトラブルシューティング.....	187
Microsoft Azure 上のエラスティッククラスタのトラブルシューティング.....	191
スケジュール済みタスクのトラブルシューティング.....	193
セキュリティのトラブルシューティング.....	194
索引.....	195

序文

*Administrator*を使用して、Informatica Intelligent Cloud ServicesSM組織とサブ組織の設定および管理方法を学習します。ライセンスの管理、エコシステムおよび SAML シングルサインオンの設定、ソース管理の設定、ユーザーの管理、オブジェクト権限の設定、ランタイム環境および Secure Agent サービスの設定、スケジュールの作成、バンドルの管理、イベントの監視、エラスティッククラスタの設定、ファイルサーバーの設定の方法について学習します。

Informatica のリソース

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

Informatica マニュアル

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

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

Informatica Intelligent Cloud Services Web サイト

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

Informatica Intelligent Cloud Services コミュニティ

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

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

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

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

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

Informatica Intelligent Cloud Services マーケットプレイス

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/>

データ統合コネクタのドキュメント

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

Informatica ナレッジベース

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

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

Informatica Intelligent Cloud Services Trust Center

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

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

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

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

Informatica グローバルカスタマサポート

電話またはオンラインでカスタマサポートセンターに連絡できます。

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

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

第 1 章

管理者について

管理者は、Informatica Intelligent Cloud Services にわたる組織管理機能を提供します。

管理者を使用して、組織の以下の側面を管理します。

組織とサブ組織

パスワードの要件、信頼される IP アドレス、接続プロパティの保存、データ統合タスクのタイムゾーンおよび電子メール通知の設定、CLAIRE™推奨の設定、Enterprise Data Catalog の設定など、組織およびサブ組織の設定を行います。サブ組織を作成し、管理します。

組織およびサブ組織の詳細については、[第 2 章、「組織」 \(ページ 14\)](#)を参照してください。

ライセンス

組織のライセンス表示、サブ組織のライセンス管理、およびジョブの制限数や使用状況に関する情報を含むメータリング情報の表示を行います。

ライセンスおよびメータリングの詳細については、[第 3 章、「ライセンス」 \(ページ 24\)](#)を参照してください。

エコシステムと SAML のシングルサインオン

Microsoft Azure のシングルサインオン設定を行います。SAML のサードパーティ ID プロバイダのシングルサインオン機能を有効にします。

Microsoft Azure のシングルサインオン設定に関する詳細については、[第 4 章、「エコシステムのシングルサインオン」 \(ページ 27\)](#)を参照してください。SAML シングルサインオンの有効化および設定の詳細については、[第 5 章、「SAML のシングルサインオン」 \(ページ 29\)](#)を参照してください。

ソース管理および Secure Agent サービスのアップグレード設定

プロジェクト、フォルダ、およびアセットのバージョン管理を有効にするためのソース管理を設定します。

一部の Secure Agent サービス用にアップグレードエラー処理とアップグレード再起動スケジュールを設定します。

ソース管理と Secure Agent サービスのアップグレード設定の詳細については、[第 7 章、「ソース管理およびサービスアップグレード設定」 \(ページ 41\)](#)を参照してください。

ユーザー、ユーザーグループ、およびユーザーロール

ユーザーアカウントを個別に作成および設定して、組織にアクセスできるようにします。同じタスクを実行できるユーザーグループを作成します。ロールを作成および設定して、ユーザーとユーザーグループの特権を定義します。

ユーザーとユーザーグループの詳細については、[第 8 章、「ユーザーとユーザーグループ」 \(ページ 49\)](#)を参照してください。ユーザーロールの詳細については、[第 9 章、「ユーザーロール」 \(ページ 63\)](#)を参照してください。

許可

ユーザーとユーザーグループが Secure Agent、Secure Agent グループ、接続、およびスケジュールなどのオブジェクトに対して持つ事のできるアクセス権限を設定します。

権限および権限の設定に関する詳細については、[第 10 章、「権限」 \(ページ 77\)](#)を参照してください。

ランタイム環境

Secure Agent をダウンロードし、インストールします。Secure Agent グループを作成し、設定します。

Secure Agent および Secure Agent グループの詳細については、[第 11 章、「ランタイム環境」 \(ページ 81\)](#)を参照してください。Secure Agent のダウンロードおよびインストールに関する詳細については、[第 14 章、「Secure Agent のインストール」 \(ページ 147\)](#)を参照してください。

サーバーレスランタイム環境

メンテナンスのオーバーヘッドを削減するために、データ統合によって管理されるランタイム環境を使用します。サーバーレスランタイム環境では、マッピングまたはエラスティックマッピングに基づいたマッピングタスクを実行できます。

注: サーバーレスランタイム環境を使用するには、AWS クラウドプラットフォームでプライベートクラウドを使用する必要があります。

サーバーレスランタイム環境について詳しくは、[第 12 章、「サーバーレスランタイム環境」 \(ページ 103\)](#)を参照してください。

Secure Agent サービス

エラスティックサーバー、CIH プロセッサ、データ統合サーバー、EDC 検索エージェント、プロセスサーバーなど、Secure Agent がデータ処理に使用するマイクロサービスを設定します。

Secure Agent サービスおよびその設定に関する詳細については、[第 13 章、「Secure Agent サービス」 \(ページ 113\)](#)を参照してください。

エラスティッククラスタ

サーバーレス Spark エンジンでのデータ統合ジョブを処理するために組織で利用できる一時クラスタを管理します。

エラスティッククラスタの詳細については、Data Integration Elastic の管理に関する項目を参照してください。

スケジュール

タスクまたはタスクフローを、指定した時間または一定の間隔で実行するようにスケジュールを作成します。組織でスケジュールされたタスクやジョブが実行出来なくなるブラックアウト期間を定義します。

スケジュールおよび組織のブラックアウト期間に関する詳細については、[第 15 章、「スケジュール」 \(ページ 155\)](#)を参照してください。

アドオンバンドル

データ統合ユーザーがデータ統合プロジェクトで使用する関連マッピング、マッピングタスク、マップレット、および Visio テンプレートのセットをインストール、コピー、アップグレード、およびアンインストールします。

アドオンバンドルの管理に関する詳細については、[第 16 章、「バンドル管理」 \(ページ 160\)](#)を参照してください。

イベント監視

アセットおよびセキュリティログを使用して、組織内のアセット、ライセンス、ユーザー、および Secure Agent のイベントを監視します。

アセットおよびセキュリティログの詳細については、[第 17 章, 「イベント監視」 \(ページ 163\)](#)を参照してください。

ファイル転送

組織のファイルサーバーを設定して、ビジネスパートナーのリモートサーバーからファイルを安全に送受信します。接続を設定してから Informatica Intelligent Cloud Services の REST API を使用してパートナーにファイルを送信します。

ファイルサーバーおよびファイル転送の詳細については、[第 18 章, 「ファイル転送」 \(ページ 165\)](#)を参照してください。

ユーザープロファイルの編集

ユーザープロファイルには Informatica Intelligent Cloud Services のユーザーアカウントの詳細が含まれます。

プロファイル内の次の情報を更新できます。

- 電子メールアドレス
- タイムゾーン ([すべてのジョブ]、[実行中のジョブ]、[マイジョブ]、[インポート/エクスポートログ]、[マイインポート/エクスポートログ] ページのジョブ実行のタイムスタンプで使用)
- パスワード
- セキュリティの質問

ユーザープロファイルを編集するには:

1. Informatica Intelligent Cloud Services ウィンドウ右上隅にある **【ユーザー】** アイコンをクリックして、**【プロファイル】** を選択します。
2. **【プロファイル】** ページで、氏名、役職、電話番号、電子メールアドレス、タイムゾーンなどの個人情報を追加または編集します。
3. 必要に応じて、パスワードまたはセキュリティの質問を変更します。
4. **【保存】** をクリックします。

第 2 章

組織

組織は、ライセンス、ユーザーアカウント、マッピングやタスクなどのデータ統合アセット、およびジョブとセキュリティに関する情報を格納する Informatica Intelligent Cloud Services リポジトリ内の安全な領域です。ライセンスに基づいて、1 つの組織または親組織と 1 つ以上のサブ組織にアクセスできます。

組織の管理者は、組織とサブ組織を保持します。

Informatica Intelligent Cloud Services に管理者としてログインし、組織の設定、スケジュールの作成と管理、およびアセットとセキュリティに関連するアクティビティの監視を行います。

組織の設定

組織を構成するときは、組織のプロパティ、サブ組織、ライセンス、ランタイム環境、およびユーザーアカウントを設定します。

会社の組織を設定するには、次の手順を実行します。

1. 組織名や住所、認証情報、通知を受ける電子メールアドレスなどの組織のプロパティを構成します。
2. 必要に応じて、1 つ以上のサブ組織を作成します。
3. 組織に適切なライセンスがあることを確認し、サブ組織のライセンスを設定します。
4. ランタイム環境と Secure Agents を設定します。
5. ユーザー、ユーザーグループ、およびロールを設定します。

また、組織用に非ネイティブコネクタをダウンロードしてインストールする必要がある場合もあります。例えば、組織内のユーザーが Teradata テーブルからデータを読み取るタスクを作成する場合は、Teradata のアドオンコネクタをダウンロードしてインストールする必要があります。アドオンコネクタのダウンロードとインストールの詳細については、「[接続](#)」を参照してください。

組織のプロパティ

【組織】 ページの組織またはサブ組織のプロパティを構成します。【組織】 ページにアクセスするには、管理者で【組織】 を選択します。

次の図は、【組織】 ページを示しています。

The screenshot shows the Informatica Administrator interface for the 'InfoProd' organization. The left sidebar lists various settings categories like SAML Setup, Licenses, Users, User Groups, User Roles, Runtime Environments, Connections, Add-On Connectors, Schedules, Add-On Bundles, Swagger Files, and Logs. The main content area is titled 'InfoProd' and 'Sub-Organizations'. It has tabs for 'Settings' and 'Sub-Organizations'. The 'Settings' tab is active, showing the 'Overview' section with fields for Name, ID, Environment Type, Description, and Number of Employees. The 'Address' section contains fields for Address 1, Address 2, Address 3, City, State, Zip Code, and Country. The 'History' section shows a table with Created By, Created On, Updated By, and Updated On. The 'Authentication' section contains fields for Minimum Password Length, Minimum Character Mix, Password Reuse, and Password Expires, along with a checkbox for Use Trusted IP Ranges.

次のプロパティを設定することができます。

- 組織名、説明、従業員数、住所情報などの全般的なプロパティ。
- 認証情報と接続プロパティの保存場所。
- 電子メール通知に使用するタイムゾーンや電子メールアドレスなどのデータ統合サービスのプロパティ。
- CLAIRE™の推奨設定。有効にすると、収集されたメタデータに基づいて CLAIRE で推奨する設計時間が指定されます。
- Enterprise Data Catalog サービスの URL、Enterprise Data Catalog からデータを読み取るランタイム環境、Enterprise Data Catalog のユーザー名とパスワードなどの Enterprise Data Catalog 統合プロパティ。

組織の全般プロパティ

組織およびサブ組織の全般的なプロパティを構成できます。全般プロパティには、組織名、ID、説明、住所、従業員の数などの情報が含まれます。組織の履歴情報も全般プロパティに表示されます。

全般プロパティには次のような情報があります。

概要情報

以下の表で、概要プロパティについて説明します。

プロパティ	説明
名前	組織の名前。 組織名を変更した場合、ログアウトしてログインし直すと【組織】メニューに新しい名前が表示されます。
ID	組織の作成時に組織に割り当てられた ID。組織 ID を変更することはできません。
親組織 ID	サブ組織を表示すると、このプロパティには、親組織に割り当てられた ID が表示されます。組織 ID を変更することはできません。
環境タイプ	開発、プロダクション、QA、またはサンドボックスのいずれか。
説明	組織の説明（省略可能）。
従業員数	組織の従業員数。
このサブ組織への親組織のアクセスを拒否	<p>このオプションをオンにすると、親組織のユーザーは、親組織からサブ組織に切り替えられません。適切な権限を所有する親組織のユーザーは、サブ組織に次の変更のみを加えることができます。</p> <ul style="list-style-type: none">- サブ組織の有効化および無効化- サブ組織のライセンスの更新- 組織の説明や CLAIRE の推奨設定などのサブ組織のプロパティの編集 <p>このオプションはサブ組織の【組織】ページに表示されます。このオプションは、サブ組織の管理者がサブ組織にログインすると変更できます。このオプションは、親組織の管理者がサブ組織の組織のプロパティを表示するときは読み取り専用です。</p> <p>このオプションはデフォルトでオフになっています。</p>

住所情報

住所プロパティを使用して、組織の住所を指定します。

履歴情報

組織の履歴情報には、組織が作成された日時、組織を作成したユーザー、組織が最後に更新された日時、および組織を最後に更新したユーザーが表示されます。組織に変更を加えると、Informatica Intelligent Cloud Services で履歴情報が更新されます。

認証プロパティ

組織およびサブ組織の認証プロパティを構成できます。認証プロパティは、パスワード制限および IP アドレスフィルタリングを制御します。

ユーザーが匿名ユーザーのパスワードを作成または変更する場合は、パスワード制限が適用されます。パスワードの有効期限日を「Never（なし）」からある日数に変更すると、その日数より古いパスワードを持つユーザーは、次回 Informatica Intelligent Cloud Services にログインするときにパスワードを変更する必要があります。

次の表に、認証プロパティを示します。

プロパティ	説明
パスワードの最小文字数	有効なパスワードに必要なパスワードの最小文字数。4 から 12 文字の範囲でなければなりません。
最小混合文字数	有効なパスワードに必要な文字タイプの最小数。 パスワードには、次の文字セットを混在させることができます。 <ul style="list-style-type: none">- 小文字の英字- 大文字の英字- 数字- 特殊文字 例えば、 【最小混合文字数】 オプションを 1 に設定した場合、パスワードには 1 つ以上の文字セットが含まれている必要があります。 【最小混合文字数】 を 2 に設定した場合は、パスワードに 2 つ以上の文字セットが含まれている必要があります。
パスワードの再利用	ユーザーがパスワードを再利用できるかどうかを制御します。
パスワードの有効期限が切れる	ユーザーがパスワードをリセットしなければならない頻度を設定します。
信頼済み IP 範囲を使用	IP アドレスフィルタリングを有効にします。 IP アドレスフィルタリングは、信頼済み IP アドレス範囲とアカウントパスワードを使用し、未認証のユーザーが組織にアクセスできないようにします。IP アドレスフィルタリングを有効にすると、有効なログインのあるユーザーに、信頼済み IP アドレス範囲内の IP アドレスも必要になります。そうでない場合、そのユーザーは組織にログインできなくなります。 このオプションを有効にした場合は、1 つ以上の信頼済み IP アドレス範囲も入力する必要があります。
許可された信頼済み IP 範囲	組織にアクセスするためのログインに使用可能な信頼済み IP アドレス範囲。Informatica Intelligent Cloud Services では、IP version 4 (IPv4) と IP version 6 (IPv6) での IP アドレス形式がサポートされています。 IP アドレスフィルタリングを有効にすると、信頼済み IP アドレス範囲のフィールドが表示されます。追加のアドレス範囲を入力するには、 [+] をクリックします。 注: 無効な IP アドレス範囲を入力した場合、ユーザーは組織にアクセスできません。有効な IP アドレス範囲については、ネットワーク管理者にお問い合わせください。

接続プロパティの保存場所

組織およびサブ組織の接続プロパティを保存する場所を設定できます。接続プロパティの保存場所を指定するには、**【組織】** ページで **【接続の資格情報】** を設定します。

接続プロパティは、次のいずれかの場所に保存できます。

Informatica Cloud

Informatica Intelligent Cloud Services を使用して接続プロパティを保存した場合は、接続プロパティをいつでも利用できます。Informatica Intelligent Cloud Services では、標準のバックアップ手順の一環として、接続プロパティを定期的にバックアップします。

ローカルの Secure Agent

ファイアウォール内に存在する接続プロパティが必要な場合は、ローカルな Secure Agent を使用して接続プロパティを格納できます。ローカルな Secure Agent を使用して接続プロパティを格納する場合、組織には Externalize Connections ライセンスが必要です。

ローカルな Secure Agent を使用してプロパティを格納する場合は、タスクを実行し、ユーザーが接続を操作できるように、Secure Agent を実行する必要があります。データの損失を回避するために、接続プロパティを定期的にバックアップします。ベストプラクティスとして、接続プロパティの場所または暗号化キーを変更した後に接続プロパティをバックアップすることをお勧めします。

接続プロパティは次のディレクトリに格納されます。

<Secure Agent のインストールディレクトリ>/apps/Data_Integration_Server/data

Informatica Intelligent Cloud Services では、暗号化キーを生成して、Secure Agent を使用して格納された接続プロパティの安全性を確保します。ランダムに生成されたパスワードを使用することも、暗号化キーの基盤としてカスタムパスワードを入力することもできます。

暗号化キーを定期的に更新する場合は、カスタムパスワードを使用します。暗号化キーを更新するときに、カスタムパスワードを変更できます。

接続プロパティを格納する場所を変更できます。これにより、Informatica Intelligent Cloud Services は、接続プロパティを適切な場所に移動します。例えば、ライセンスの有効期限が切れるため、クラウドに接続を格納するように組織を設定するとします。Informatica Intelligent Cloud Services は、ローカルな Secure Agent から Informatica Intelligent Cloud Services へ接続プロパティを移動します。

データ統合サービスのプロパティ

データ統合サービスプロパティはデータ統合で使用されます。次のプロパティを設定して、ジョブの通知に使用するタイムゾーンと電子メールアドレスを設定します。

以下のデータ統合サービスのプロパティを設定できます。

ジョブのプロパティ

次の表に、ジョブのプロパティを示します。

プロパティ	説明
スケジュールオフセット	標準の予定開始時刻でのサーバーのオーバーロードを防ぐために、予定開始時刻に追加されるわずかな時間。組織には、すべてのスケジュールに適用される単一のスケジュールオフセットがあります。スケジュールオフセットは、手動で開始されたタスクまたはタスクフローの開始時刻には影響しません。スケジュールオフセットは変更できません。スケジュールの詳細には表示されませんが、組織のスケジュールオフセットはすべてのスケジュールに設定した時間範囲に追加されます。これにより、スケジュール済みのタスクが想定どおりの頻度で実行されるようになります。例えば、8:00 a.m.から 12:00 p.m. まで毎時間タスクを実行するようにスケジュールを設定し、組織のスケジュールオフセットを 15 秒とすると、そのスケジュールで、8:00:15、9:00:15、10:00:15、11:00:15、および 12:00:15 にタスクが実行されます。
時間帯	電子メール通知でのジョブ実行タイムスタンプの表示に使用するタイムゾーン。

電子メール通知のプロパティ

ジョブの失敗、警告、および成功メッセージに使用するデフォルトの電子メールアドレスを設定する電子メール通知プロパティを構成します。有効な電子メールアドレスを 1 つ以上入力します。カンマ (,) またはセミコロン (;) を使用して電子メールアドレスを区切ります。

また、タスクレベルで電子メール通知のプロパティを設定することもできます。タスクまたはタスクフローで電子メール通知を設定すると、Informatica Intelligent Cloud Services は、組織に対して設定されたアドレスではなく、タスクまたはタスクフローのアドレスに電子メールを送信します。

CLAIRE の推奨設定

CLAIRE の推奨を有効にすると、ご自身の会社のアセットまたはその他の Informatica Intelligent Cloud Services 組織のアセットのメタデータの分析に基づいたマッピングデザインに対する製品内の推奨事項が許可されます。CLAIRE エンジンによって収集され処理されたメタデータは匿名です。

CLAIRE の推奨はデフォルトで「有効」に設定されています。CLAIRE の推奨を無効にすると、会社内のすべてのユーザーに対して推奨が無効になります。会社では推奨をいつでも有効または無効にする事ができます。

下位組織の CLAIRE の推奨は、下位組織内から有効および無効にします。

CLAIRE の推奨を有効にすると、データ統合ユーザーは個々のマッピングの推奨をマッピングデザイナーで無効にできます。

エラスティックマッピングに基づくマッピングタスクを作成する場合は、CLAIRE の推奨を有効にして CLAIRE チューニングを使用できます。

Enterprise Data Catalog 統合プロパティ

Azure のデータアクセラレータを使用している場合、またはデータ統合でデータカタログ検出を使用している場合、組織およびサブ組織に Enterprise Data Catalog 統合プロパティを設定できます。ユーザーがマッピング、同期タスク、ファイル取り込みタスク、および Azure のデータ同期タスクでカタログアセットを使用できるように、Enterprise Data Catalog 統合プロパティを設定します。

組織に設定する Enterprise Data Catalog 統合プロパティは、組織の全ユーザーが実行するデータカタログ検索に適用されます。組織にサブ組織が含まれる場合は、親組織と各サブ組織に異なる Enterprise Data Catalog 統合プロパティを設定できます。

以下の表に、Enterprise Data Catalog 統合プロパティを示します。

プロパティ	説明
カタログ URL	Enterprise Data Catalog サービスの URL。次の形式を使用します。 <code>http://<完全修飾ホスト名>:<ポート></code> URL の最後に「/ldmcatalog」を追加しないでください。
ランタイム環境	Enterprise Data Catalog からのデータの読み取りに使用する Secure Agent グループの名前。 選択したグループのエージェントは、Enterprise Data Catalog と通信できる必要があります。このため、Enterprise Data Catalog ホストがエージェントマシンと同じネットワーク内に存在するか、通信用の適切なポートが開かれている必要があります。
ユーザー名	Secure Agent が Enterprise Data Catalog にアクセスするために使用する Enterprise Data Catalog ユーザーアカウント。 このユーザーアカウントは、Enterprise Data Catalog 内のオブジェクトを表示および検索し、Enterprise Data Catalog REST API を使用して機能を実行する権限を持っている必要があります。
パスワード	Enterprise Data Catalog ユーザーアカウントのパスワード。
データカタログを表示	データ統合 のデータ統合ページを表示および非表示にします。

サブ組織

組織に組織階層ライセンスがある場合は、組織内に 1 つ以上のサブ組織を作成できます。企業内のさまざまなビジネス環境を表すサブ組織を作成します。例えば、開発、テスト、およびプロダクション環境を表す個別のサブ組織を作成することができます。

サブ組織を作成すると、サブ組織を作成するために使用する組織が親組織になります。各サブ組織の親組織は 1 つのみで、別のサブ組織を含めることはできません。

組織階層ライセンスで、作成できるサブ組織の数を制御します。この数を増やすには、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。

サブ組織の作成には、次の利点があります。

サブ組織のライセンスは、個別に管理するか、親組織のライセンスと自動的に同期できます。

各サブ組織が、組織階層ライセンスおよびバンドルライセンスを除く、親組織からのすべての機能、コネクタ、およびカスタムライセンスを継承します。

ライセンスを個別に管理すると、親組織の管理者は、サブ組織が継承するライセンスの有効期限の無効化、有効化、および変更を行うことができます。各サブ組織のライセンスを個別に設定します。したがって、あるサブ組織でライセンスを無効にしても、他のサブ組織のライセンスは無効になりません。

または、適切なライセンスを所有している場合、サブ組織のライセンスを親組織と自動的に同期できます。このライセンスを有効にすると、ライセンスが親組織で変更されるたびに、すべてのサブ組織はライセンスの変更を継承します。

ユーザーとアセットを個別に管理できます。

各サブ組織には、ユーザーとアセットの独自のセットがあります。

サブ組織で作成するユーザーは、サブ組織に固有のものです。親組織や他のサブ組織にはログインできません。親組織の管理者と、サブ組織のアクセス特権を持つ親組織のユーザーのみが、親組織およびすべてのサブ組織にアクセスできます。

マッピングやタスクなどのアセットも組織内で固有のものです。アセットは、サブ組織間、または親組織と任意のサブ組織間では共有されません。組織間でアセットを移行する場合は、片方の組織からアセットをエクスポートし、別の組織にインポートします。

ランタイム環境を共有できます。

親組織の管理者は、Secure Agent グループをサブ組織と共有できます。Secure Agent グループを共有すると、サブ組織のユーザーは、グループ内の Secure Agent でタスクを実行できます。

ログインせずに組織間を切り替えることができます。

サブ組織を表示する特権を持つ親組織のユーザーは、ログアウトせずに組織間を切り替えたり、Informatica Intelligent Cloud Services にログインし直したりすることができます。

サブ組織の例

同期タスクの開発、テスト、およびプロダクションのための個別の環境が必要であり、タスクはプロダクション環境で実行される前に必ずテストを行います。

管理者として親組織にログインし、タスク開発用のサブ組織、テスト用のサブ組織、およびプロダクション用のサブ組織を作成します。サブ組織にユーザーを追加し、組織ごとにデータ同期ライセンスが有効になっていることを確認します。

タスクの開発が完了したら、開発サブ組織からタスクをエクスポートし、テスト用のサブ組織にログインしてタスクをインポートします。テストが完了したら、テスト用のサブ組織からタスクをエクスポートし、プロダクション用のサブ組織にログインしてタスクをインポートします。

サブ組織の追加または削除

サブ組織を追加するには、新しいサブ組織を作成するか、既存の組織をリンクします。サブ組織を削除するには、組織のリンクを解除するか、サブ組織を削除します。

次のいずれかの方法でサブ組織を追加できます。

- サブ組織の作成。親組織にする組織にログインして、サブ組織を作成します。
- 既存の組織のリンク。リンク元の組織が親組織になり、リンク先の組織がサブ組織になります。

次のいずれかの方法でサブ組織を削除できます。

- 親組織からの既存サブ組織のリンク解除。
- サブ組織の削除。組織を削除すると、その組織に関連付けられたすべてのデータが削除されます。

サブ組織の作成

親組織の管理者はサブ組織を作成できます。

1. 親組織にする組織にログインします。
2. 管理者を開いて **【組織】** を選択します。
3. **【サブ組織】** ページを開き、**【新しいサブ組織】** をクリックします。
4. サブ組織のプロパティを入力し、**【保存】** をクリックします。

サブ組織を作成したら、ライセンスを確認し、他の人が使用できるようにランタイム環境、ユーザーアカウント、および接続を構成します。

組織のリンク

既存の組織をリンクすることで、サブ組織を作成できます。リンク元の組織が親組織になり、リンク先の組織がサブ組織になります。

組織をリンクするには、リンクする組織の組織 ID が必要になります。この情報は、**【組織】** ページで確認できます。

注: 親組織が持っていないライセンスを持つサブ組織をリンクすると、サブ組織はそのライセンスを失います。

次のすべての条件が該当する場合に、組織をリンクできます。

- ユーザーアカウントと組織があること。
- 組織は別の組織の親でもサブ組織でもありません。
- 組織階層ライセンスのある親組織の管理者であること。
- サブ組織としてリンクする組織には、組織階層ライセンスがありません。

後から組織をリンク解除できます。

組織をリンクするには:

1. 親組織にする組織にログインします。
2. 管理者を開いて **【組織】** を選択します。
3. **【サブ組織】** ページを開き、**【サブ組織をリンク】** をクリックします。
4. **【サブ組織をリンク】** ダイアログボックスで、次の情報を入力します。
 - リンクする組織の組織 ID。

- サブ組織として設定する組織の管理者のユーザー名とパスワード。
5. 組織をリンクするには、**【サブ組織をリンク】** をクリックします。
組織が **【サブ組織】** ページに表示されます。

サブ組織のリンク解除

親組織からサブ組織のリンクを解除することができます。組織のリンクを解除してから、必要なライセンスでリンクされていない組織を更新します。

次の条件が該当する場合、サブ組織のリンクを解除できます。

- リンク解除するサブ組織に対する管理者アカウントを持っていること。
- 組織階層ライセンスのある親組織の管理者であること。
- リンクを解除するサブ組織内のアセットは、Secure Agent グループの共有をランタイム環境として使用しません。サブ組織内の任意のアセットが Secure Agent グループの共有をランタイム環境として使用している場合は、サブ組織のリンクを解除する前に、別のランタイム環境を使用するようにアセットを更新します。

サブ組織のリンクを解除するには:

1. 親組織にログインします。
2. 管理者を開いて **【組織】** を選択します。
3. **【サブ組織】** ページを開きます。
4. リンクを解除するサブ組織の **【アクション】** メニューを展開し、**【リンク解除】** を選択します。
5. **【リンク解除】** ダイアログボックスで、管理者ロールを持つサブ組織内のユーザーのユーザー名とパスワードを入力します。
6. **【リンク解除】** をクリックします。
組織がリンク解除されます。

サブ組織の削除

サブ組織を削除できます。サブ組織を削除すると、関連付けられたすべてのデータが削除されます。

親組織の管理者であれば、サブ組織を削除できます。

1. 親組織にログインします。
2. 管理者を開いて **【組織】** を選択します。
3. **【サブ組織】** ページを開きます。
4. リンクを解除するサブ組織の **【アクション】** メニューを展開し、**【削除】** を選択します。

サブ組織の無効化または有効化

親組織の管理者である場合は、サブ組織を無効または有効にできます。

サブ組織の作成時に、デフォルトでサブ組織は有効化されます。サブ組織と別個の使用許諾契約がある場合や、使用許諾契約の有効期限が切れた場合、サブ組織を無効にすることがあります。サブ組織は、無効化後に再度有効にできます。

サブ組織は、サブ組織の管理者がサブ組織への親組織のアクセスをブロックしている場合も、無効または有効にできます。

次のアクションを実行できます。

サブ組織の無効化

サブ組織を無効にすると、その組織は残りますが、サブ組織のユーザーはサブ組織にログインできない、または REST API を介してサブ組織にアクセスします。サブ組織内のスケジュールされたジョブは実行されません。

サブ組織の有効化

サブ組織を有効にすると、サブ組織のユーザーはサブ組織にログインでき、自分のユーザーロールに基づいてアセットにアクセスし、タスクを実行できます。適切な権限を持つユーザーは、REST API を介してサブ組織にアクセスできます。スケジュールされたジョブは、スケジュールに従って再開されます。

サブ組織を【組織】 ページの【サブ組織】 タブで無効または有効にします。サブ組織の【アクション】 メニューで、【無効】 または【有効】 を選択します。

別の組織への切り替え

親組織の管理者またはサブ組織の表示権限を持つ親組織のユーザーの場合は、これらの組織間で切り替えることができます。Informatica Intelligent Cloud Services をログアウトして、もう一度ログインする必要はありません。

別の組織に切り替えるには:

- ▶ 右上隅の【組織】メニューから、表示する組織を選択します。

サブ組織への親組織のアクセスを拒否

サブ組織の管理者である場合は、サブ組織への親組織のアクセスを拒否できます。

サブ組織へのアクセスを拒否すると、親組織のユーザーは、親組織からサブ組織に切り替えられません。適切な権限を所有する親組織のユーザーは、サブ組織に次の変更のみを加えることができます。

- サブ組織の有効化および無効化
- サブ組織のライセンスの更新
- 組織の説明や CLAIRE の推奨設定などのサブ組織のプロパティの編集

親組織のサブ組織へのアクセスを拒否するには、管理者としてサブ組織にログインします。【組織】 ページで、【このサブ組織への親組織のアクセスを拒否】 オプションを有効にします。

サブ組織のアドオンコネクタ

サブ組織でアドオンコネクタを使用するには、親組織にコネクタをインストールする必要があります。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。

サブ組織は、親組織からすべてのコネクタライセンスを継承します。サブ組織で特定のコネクタを使用しない場合は、サブ組織でそのコネクタライセンスを無効にします。

サブ組織でのアセットのエクスポートとインポート

サブ組織では、次の方法でアセットをエクスポートおよびインポートします。

- サブ組織にログインして、サブ組織からアセットをエクスポートおよびインポートします。
- 親組織の管理者は親組織にログインし、サブ組織に切り替えて、データ統合アセットをインポートまたはエクスポートできます。

第 3 章

ライセンス

ライセンスによって組織の Informatica Intelligent Cloud Services サブスクリプションレベルが決まり、Informatica Intelligent Cloud Services の機能、コネクタ、およびバンドルへアクセスできるようになります。

管理者は、組織に対して設定されているライセンス、ライセンスの有効期限、およびジョブの制限と使用状況を確認できます。また、サブ組織のライセンスを管理し、サブ組織のジョブの制限と使用状況を表示することもできます。

ライセンスのカテゴリ

ライセンスは、エディションライセンス、コネクタライセンス、およびカスタムライセンスに分類されます。次のライセンスカテゴリを利用できます。

エディションライセンス

エディションライセンスは、使用できる Informatica Intelligent Cloud Services の機能を制御します。機能ライセンスを使用すると、マッピングタスク、レプリケーションタスク、同期タスクなどのデータ統合タスクへアクセスできます。また、ビジネスサービスや保存されたクエリなどのコンポーネントへのアクセスや、ファイングレインセキュリティおよび Salesforce 接続などの機能も提供します。

コネクタライセンス

コネクタライセンスは、Amazon Redshift、Microsoft SQL Server、Oracle などのエンティティへの接続を提供します。

カスタムライセンス

カスタムライセンスは、エディションに含まれていないライセンスです。機能、パッケージ、またはバンドルへのアクセスを提供します。エディションライセンスにも含まれている機能へのアクセスを提供するカスタムライセンスを組織で使用している場合、カスタムライセンスの使用条件は、エディションライセンスの条件を上書きします。

ライセンスのタイプ

組織を作成すると、Informatica Intelligent Cloud Services でライセンスされている各エディションのライセンスタイプを組織に割り当てます。

Informatica Intelligent Cloud Services では、以下のタイプのライセンスを使用します。

トライアル

30 日間無料でエディションを使用できます。トライアル期間の終了時に、エディションをサブスクライブできます。トライアルサブスクリプションでは、ライセンスに関連付けられている機能、コネクタ、およびパッケージへのアクセスが制限される場合があります。

サブスクリプション

契約期間中は、ライセンスされているエディションを使用することができます。契約期間の終わりに近づくと、Informatica Intelligent Cloud Services から契約が間もなく終了することが通知されます。エディションの使用を続けるには、契約を更新します。

無料サブスクリプション

同期タスクは、無料で使用できます。無料サブスクリプションでは、同期タスクの機能へのアクセスが制限される場合があります。

サブ組織のライセンス

サブ組織には、親組織によって保持されるライセンスがあります。親組織に属していないライセンスをサブ組織が必要とする場合は、Informatica グローバルカスタマサポートに連絡して、親組織のライセンスを取得します。

サブ組織を作成すると、各サブ組織は親組織からカスタムライセンスとしてライセンスを継承します。サブ組織は、次のライセンスを除くすべてのライセンスを継承します。

- 組織階層ライセンス
- バンドルライセンスサブ組織でバンドルを使用するには、サブ組織のユーザーがバンドルをインストールする必要があります。

サブ組織のライセンスは、次の方法で管理できます。

ライセンスの個別管理

ライセンスを個別に管理すると、親組織の管理者は、継承されたライセンスの有効期限の無効化、有効化、および短縮を行うことができます。各サブ組織のライセンスを個別に管理します。サブ組織の管理者はライセンスを表示できますが、変更はできません。

これがデフォルトのオプションです。

サブ組織のライセンスの親組織との自動同期

適切なライセンスを所有している場合、サブ組織のライセンスを親組織と自動的に同期できます。このライセンスを有効にすると、ライセンスが親組織で変更されるたびに、すべてのサブ組織はライセンスの変更を継承します。

ライセンスの同期は、組織に多数のサブ組織があり、サブ組織が同じライセンスを所有しているときに有効にすることがあります。

ライセンスの同期が組織に対して有効でない場合、サブ組織のライセンスを個別に管理する必要があります。

注: 親組織が持っていないライセンスを持つサブ組織をリンクすると、サブ組織はそのライセンスを失います。

サブ組織のライセンスの編集

親組織の管理者であり、親組織とサブ組織との間のライセンス同期が有効でない場合、サブ組織のライセンスを編集できます。サブ組織のライセンスは、親組織内またはサブ組織内から編集できます。

1. 親組織にログインします。
2. 親組織内からライセンスを編集するには:
 - a. 管理者を開いて【組織】を選択します。
 - b. 【サブ組織】をクリックします。
 - c. ライセンスを編集するサブ組織を選択します。
 - d. 【ライセンス】をクリックします。
3. サブ組織内からライセンスを編集するには:
 - a. 右上隅の【組織】メニューから、ライセンスを編集するサブ組織を選択します。
 - b. 管理者を開いて【ライセンス】を選択します。
4. 機能を有効にするにはライセンスを選択し、機能を無効にするにはライセンスの選択を解除します。
5. 必要に応じて、有効期限を変更します。
サブ組織のライセンス有効期限を短縮することはできますが、延長することはできません。
6. 【保存】をクリックします。

親組織とのライセンスの同期

サブ組織のライセンスを親組織と自動的に同期できます。ライセンスが親組織で変更されるたびに、すべてのサブ組織はライセンスの変更を継承します。

ライセンスの同期を有効にするには、Informatica グローバルカスタマサポートに問い合わせ、この機能のライセンスを要求してください。ライセンスが親組織に対して有効になると、ライセンスのサブ組織との同期が自動的に発生します。親組織の管理者は、ライセンスを同期させるために、何か操作をする必要はありません。

注: この機能のライセンスが有効になると、サブ組織のライセンスを個別に編集することはできません。

この機能のライセンスが有効になり、サブ組織を無効にすると、サブ組織はライセンス設定を失います。サブ組織を再度有効にした場合、サブ組織はすべてのライセンス設定を親組織から継承します。

親組織とサブ組織との間のライセンス同期は、サブ組織のライセンスメーターカウントには影響しません。

ライセンスの有効期限

ライセンスの有効期限が切れると、ライセンスに関連付けられている機能、コネクタ、またはパッケージにアクセスできなくなります。ライセンスに関連付けられているスケジュール済みのジョブも無効になります。組織のすべてのライセンスの有効期限が切れると、Informatica Intelligent Cloud Services にログインできなくなります。

管理者の【ライセンス】ページでライセンスの有効期限を確認することができます。ライセンスを延長するには、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。ライセンスを延長すると、関連付けられている機能、コネクタ、およびパッケージにアクセスし、スケジュール済みのジョブの処理を再開できます。

第 4 章

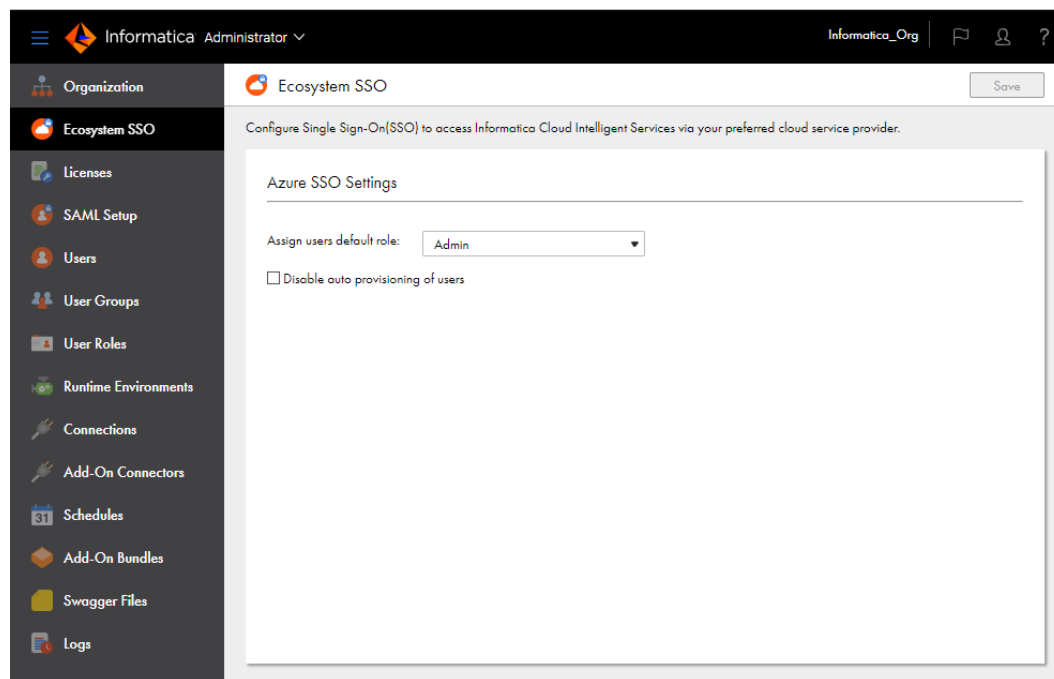
エコシステムのシングルサインオン

Informatica Intelligent Cloud Services で、Microsoft Azure ユーザーのシングルサインオン機能を有効にします。これにより、Microsoft Azure ユーザーはログイン情報を入力し直すことなく Informatica Intelligent Cloud Services にサインインできます。

Microsoft Azure で組織を作成する場合、Microsoft Azure ユーザー向けの一部のシングルサインオンプロパティを **[Ecosystem SSO (エコシステムの SSO)]** ページで設定できます。

注: Microsoft Azure 用に設定するエコシステムのシングルサインオンプロパティは、サードパーティの ID プロバイダからシングルサインオンを有効にするために設定する SAML のシングルサインオンプロパティとは異なります。組織の SAML シングルサインオンを設定するには、[第 5 章, 「SAML のシングルサインオン」 \(ページ 29\)](#)を参照してください。

次の図は、**[Ecosystem SSO (エコシステムの SSO)]** ページを示しています。



Microsoft Azure ユーザーに対して次のプロパティを設定できます。

Assign users default role (ユーザーにデフォルトロールを割り当て)

Microsoft Azure ユーザーが組織に初めてサインインしたときに、Informatica Intelligent Cloud Services によってユーザーが組織に追加され、ユーザーにデフォルトロールが割り当てられます。デフォルトでは、Informatica Intelligent Cloud Services によってユーザーに管理者ロールが割り当てられます。

デフォルトロールは、デザイナロールなどの別のロールに変更できます。デフォルトのユーザーロールを変更するには、**[Assign users default role (ユーザーにデフォルトロールを割り当て)]** リストで別のロールを選択します。

注: Microsoft Azure ユーザーが Secure Agent のダウンロード、インストール、登録を行えるようにする場合は、管理者ロールまたはデザイナロールを割り当てます。Secure Agent の作成、読み取り、および更新を行える特権を持つカスタムロールをユーザーに割り当てすることもできます。

ユーザーの自動プロビジョニングの無効化

デフォルトでは、Microsoft Azure ユーザーが Azure のデータアクセラレータに初めてサインインしたときに、Informatica Intelligent Cloud Services によってユーザーが組織に追加されます。このプロセスを自動プロビジョニングと呼びます。

Microsoft Azure ユーザーの自動プロビジョニングは有効化または無効化できます。これを行うには、**[ユーザーの自動プロビジョニングの無効化]** オプションを有効または無効にします。

注: 自動プロビジョニングを無効にした場合、**[ユーザー]** ページで各ユーザーを作成する必要があります。ユーザーが Microsoft Azure からシングルサインオンを使用できるようにする場合は、**[ユーザーの詳細]** ページの**【認証】** フィールドを**【Azure SSO】** に設定する必要があります。

第 5 章

SAML のシングルサインオン

ユーザーがログイン情報を入力せずに組織にアクセスできるように、シングルサインオン（SSO）機能を有効にできます。

Informatica Intelligent Cloud Services へのシングルサインオンは、Security Assertion Markup Language (SAML) 2.0 Web ブラウザシングルサインオンプロファイルに基づいています。SAML Web ブラウザシングルサインオンプロファイルは、次のエンティティで構成されています。

ID プロバイダ

認証情報を管理し、セキュリティトークンを使用して認証サービスを提供するエンティティ。

サービスプロバイダ

Web サービスをプリンシパルに提供するエンティティ（Web アプリケーションをホストするエンティティなど）。Informatica Intelligent Cloud Services はサービスプロバイダです。

プリンシパル

HTTP ユーザーエージェントを介して対話するエンドユーザー。

SAML 2.0 は、セキュリティトークンを使用する XML ベースのプロトコルです。セキュリティトークンには、ID プロバイダとサービスプロバイダ間でプリンシパルに関する情報を渡すアサーションが含まれます。アサーションは、SAML オーソリティによって作成されるステートメントを提供する情報のパッケージです。

ユーザーがブラウザで Informatica Intelligent Cloud Services シングルサインオン URL を入力すると、次のプロセスが開始されます。

1. Informatica Intelligent Cloud Services は、SAML 認証要求を組織の ID プロバイダに送信します。
2. ID プロバイダは、ユーザーの ID を確認し、SAML 認証応答を Informatica Intelligent Cloud Services に送信します。
3. Informatica Intelligent Cloud Services は、ID プロバイダから SAML 認証応答を受信すると、Informatica Intelligent Cloud Services ユーザーセッションを確立し、ユーザーを Informatica Intelligent Cloud Services にログインさせます。
4. ユーザーが Informatica Intelligent Cloud Services からログアウトするか、セッションがタイムアウトすると、Informatica Intelligent Cloud Services は SAML ログアウト要求を ID プロバイダに送信します。
5. ID プロバイダは、ID プロバイダ側でユーザーセッションを終了します。

SAML の詳細については、Oasis Web サイト (<https://www.oasis-open.org>) を参照してください。

SAML のシングルサインオンの要件

Informatica Intelligent Cloud Services 組織の SAML シングルサインオンをセットアップするには、システムに適した ID プロバイダを使用する必要があります。また、適切なライセンスを使用する必要があります。

組織の SAML シングルサインオンをセットアップするには、次の要件が満たされていることを確認します。

- システムでは SAML 2.0 ベースの ID プロバイダを使用する必要があります。
共通の ID プロバイダには、Microsoft Active Directory フェデレーションサービス (AD FS)、Okta、SSOCircle、OpenLDAP および Shibboleth が含まれています。ID プロバイダは、DSA-SHA1 または RSA-SHA1 のいずれかのアルゴリズムを使用して署名を生成するように設定する必要があります。
- Informatica Intelligent Cloud Services の組織は SAML ベースのシングルサインオンライセンスを使用する必要があります。
- シングルサインオンを設定するために組織の管理者として組織にアクセスできる。

シングルサインオンの制限

Informatica Intelligent Cloud Services への SAML シングルサインオンアクセスにはいくつかの制限があります。

SAML シングルサインオンアクセスには、次の制限が適用されます。

- ID プロバイダのライセンスの有効期限が切れると、シングルサインオンを使用して Informatica Intelligent Cloud Services にアクセスできなくなります。
- ID プロバイダがダウンしている場合、または Informatica Intelligent Cloud Services のサーバーが ID プロバイダにアクセスできない場合、ユーザーはシングルサインオンを使用して Informatica Intelligent Cloud Services にログインすることができません。
- Informatica Intelligent Cloud Services への SAML シングルサインオンで使用される ID プロバイダ証明書の有効期限が切れると、ユーザーはシングルサインオンを使用して Informatica Intelligent Cloud Services にアクセスできなくなります。
- 組織で信頼済み IP アドレス範囲を使用する場合、ユーザーは信頼済み IP アドレス範囲外の IP アドレスで Informatica Intelligent Cloud Services にログインすることができません。

SAML のシングルサインオンによるユーザー管理

Informatica Intelligent Cloud Services の SAML シングルサインオンを有効にすると、次のルールがユーザーおよびユーザーアカウントに適用されます。

- Informatica Intelligent Cloud Services は、名や電子メールアドレスなど、ID プロバイダから転送されるユーザー情報を Informatica Intelligent Cloud Services リポジトリに保存します。
- 組織でシングルサインオンを有効にすると、Informatica Intelligent Cloud Services 内の資格情報を使用して通常ユーザーアカウントを作成できます。ユーザー資格情報は Informatica Intelligent Cloud Services リポジトリに保存されます。ただし、ユーザーはシングルサインオンを使用せずに Informatica Intelligent Cloud Services に直接ログインする必要があります。

- Informatica Intelligent Cloud Services からユーザーを削除すると、このユーザーは Informatica Intelligent Cloud Services リポジトリからも削除されます。ID プロバイダからユーザーは削除されません。

Informatica Intelligent Cloud Services の SAML シングルサインオン設定

Informatica Intelligent Cloud Services と ID プロバイダは、シングルサインオンの設定時に設定情報を交換します。

認証要求を ID プロバイダに送信するには、Informatica Intelligent Cloud Services に ID プロバイダメタデータが必要です。認証応答を Informatica Intelligent Cloud Services に送信するには、ID プロバイダに Informatica Intelligent Cloud Services のサービスプロバイダメタデータが必要です。

認証応答で渡されるデータを Informatica Intelligent Cloud Services でコンシュームできるように、SAML と Informatica Intelligent Cloud Services の属性（ユーザーロールなど）をマッピングする必要があります。Informatica Intelligent Cloud Services でシングルサインオンを設定したら、Informatica Intelligent Cloud Services サービスプロバイダメタデータを ID プロバイダに渡します。

Informatica Intelligent Cloud Services のシングルサインオンを設定するには、次のタスクを実行します。

1. SAML ID プロバイダおよびサービスプロバイダを設定し、Informatica Intelligent Cloud Services で SAML の属性とユーザーロールを Informatica Intelligent Cloud Services の属性とユーザーロールにマッピングします。
2. Informatica Intelligent Cloud Services から Informatica Intelligent Cloud Services サービスプロバイダメタデータをダウンロードし、組織のメタデータおよび Informatica Intelligent Cloud Services シングルサインオン URL を SAML の ID プロバイダ管理者に配信します。

プロバイダ設定とマッピング属性の設定

[SAML セットアップ] ページで、SAML のシングルサインオンを設定して SAML の属性をマップします。

1. 組織の管理者として Informatica Intelligent Cloud Services にログインします。
2. 管理者で、**[SAML セットアップ]** を選択します。
3. **[SAML セットアップ]** ページで、次のプロパティを設定します。
 - ID プロバイダのプロパティ
 - サービスプロバイダのプロパティ
 - SAML 属性マッピングのプロパティ
 - SAML ロールマッピングのプロパティ

4. **【保存】** をクリックします。

Informatica Intelligent Cloud Services はサービスプロバイダメタデータファイルを生成します。また、Informatica Intelligent Cloud Services は組織固有のトークンを生成し、このトークンを Informatica Intelligent Cloud Services リポジトリに保存します。組織のシングルサインオン URL にトークンが含まれます。例:

`https://dm-us.informaticacloud.com/ma/sso/<組織のトークン>`

【SAML セットアップ】 ページに変更を保存した後、サービスプロバイダメタデータをダウンロードし、Informatica Intelligent Cloud Services シングルサインオン URL と共にこのデータを ID プロバイダに送信します。

ID プロバイダのプロパティ

【SAML セットアップ】 ページで SAML ID プロバイダプロパティを定義します。

ID プロバイダ XML ファイルがある場合、そのファイルをアップロードして、一部のプロパティを取り込むことができます。Informatica Intelligent Cloud Services は、XML ファイルから大部分のデータを解析して抽出できます。ただし、名前識別子の形式などの特定のフィールドを手動で入力することが必要になる場合もあります。

次の表に、ID プロバイダ設定のプロパティを示します。

プロパティ	説明
ID プロバイダファイルを使用	ID プロバイダ XML ファイルでは、 【SAML セットアップ】 ページの多くのプロパティが取り込まれます。 ID プロバイダ XML ファイルを使用して ID プロバイダのプロパティを定義するには、 【参照】 をクリックし、ID プロバイダ XML ファイルに移動します。
ユーザーの自動プロビジョニングの無効化	SAML ユーザーの自動プロビジョニングを無効にします。新規 SAML ユーザーが初めて Informatica Intelligent Cloud Services にログインするとき、ユーザーは Informatica Intelligent Cloud Services 内の組織に追加されません。
発行者	ID プロバイダのエンティティ ID。これは、一意の識別子です。 ID プロバイダから Informatica Intelligent Cloud Services へのすべてのメッセージの発行者の値は、この値と一致する必要があります。例: <code><saml:Issuer>http://idp.example.com</saml:Issuer></code>
シングルサインオンサービス URL	SingleSignOnService に対する ID プロバイダの HTTP-POST SAML バインディング URL。これは、SingleSignOnService 要素の場所属性です。Informatica Intelligent Cloud Services はこの URL にログイン要求を送信します。
シングルログアウトサービス URL	SingleLogoutService に対する ID プロバイダの HTTP-POST SAML バインディング URL。これは、SingleLogoutService 要素の場所属性です。Informatica Intelligent Cloud Services はこの URL にログアウト要求を送信します。
署名証明書	Informatica Intelligent Cloud Services が ID プロバイダからの署名済み SAML メッセージの検証に使用する、Base64 でエンコードされた PEM 形式の ID プロバイダ証明書です。 注: ID プロバイダ署名アルゴリズムが DSA-SHA1 または RSA-SHA1 のいずれかである必要があります。
暗号化に署名証明書を使用します	署名証明書のパブリックキーを使用して、ユーザーが Informatica Intelligent Cloud Services からログアウトするときに ID プロバイダに送信されるログアウト要求を暗号化できます。

プロパティ	説明
暗号化証明書	Informatica Intelligent Cloud Services が ID プロバイダに送信された SAML メッセージの暗号化に使用する、Base64 でエンコードされた PEM 形式の ID プロバイダ証明書です。 署名証明書を使用して暗号化しない場合に適用できます。
名前識別子の形式	ID プロバイダが Informatica Intelligent Cloud Services に返す認証要求の名前識別子の形式。Informatica Intelligent Cloud Services は、名前識別子の値を Informatica Intelligent Cloud Services のユーザー名として使用します。 名前識別子は、ログインごとに変更される可能性のある一時的な値にすることはできません。特定のユーザーの Informatica Intelligent Cloud Services への各シングルサインオンログインには、同じ名前識別子の値が含まれている必要があります。 名前識別子が電子メールアドレスになるように指定する場合、名前識別子の形式は次のようになります。 <code>urn:oasis:names:tc:SAML:1.1:nameidformat:emailAddress</code>
ログアウトサービス URL (SOAP バインディング)	シングルログアウトサービスの ID プロバイダの SAML SOAP バインディング URL。Informatica Intelligent Cloud Services はこの URL にログアウト要求を送信します。
ログアウトページ URL	ユーザーが Informatica Intelligent Cloud Services からログアウトした後にリダイレクトされるランディングページです。 Informatica Intelligent Cloud Services では、次の方法でログアウトしたユーザーをランディングページにリダイレクトします。 <ul style="list-style-type: none"> - ログアウトページ URL を指定した場合、ログアウト後に Informatica Intelligent Cloud Services はユーザーをこの URL にリダイレクトします。 - ログアウトページ URL を指定していない場合、Informatica Intelligent Cloud Services はユーザーをデフォルトログアウトページにリダイレクトします。

サービスプロバイダのプロパティ

[SAML セットアップ] ページで Informatica Intelligent Cloud Services のサービスプロバイダのプロパティを定義します。

次の表に、サービスプロバイダのプロパティを示します。

プロパティ	説明
Informatica Cloud プラットフォーム SSO	組織のシングルサインオン URL を表示します。この URL は Informatica Intelligent Cloud Services によって自動的に生成されます。
クロックスキュー	ID プロバイダからの SAML 応答のタイムスタンプと Informatica Intelligent Cloud Services のクロック間の最大許容時間を指定します。
名前識別子の値は、ユーザーの電子メールアドレスを表します	選択すると、Informatica Intelligent Cloud Services は、電子メールアドレスを名前識別子として使用します。
認証要求への署名	選択すると、Informatica Intelligent Cloud Services は、ID プロバイダへの認証要求を署名します。

プロパティ	説明
SOAP バインディングを使用して送信したログアウト要求に署名	選択すると、Informatica Intelligent Cloud Services は、ID プロバイダに送信されるログアウト要求を署名します。
ログアウト要求の名前 ID を暗号化	選択すると、Informatica Intelligent Cloud Services は、ログアウト要求の名前識別子を暗号化します。 注: ID プロバイダが名前識別子の復号化をサポートしていることを確認します。

SAML 属性マッピングのプロパティ

名前、電子メールアドレス、ユーザーロールなどのユーザーログイン属性は、ID プロバイダから Informatica Intelligent Cloud Services への認証応答に含まれます。Informatica Intelligent Cloud Services のユーザーフィールドを **[SAML セットアップ]** ページで対応する SAML 属性にマップします。

次の表に、SAML 属性マッピングのプロパティを示します。

プロパティ	説明
わかりやすい SAML 属性名を使用します	選択されている場合は、SAML 属性名のわかりやすい形式が使用されます。これは、OID や UUID など、属性名が複雑な場合やわかりにくい場合に役立つことがあります。
名	ユーザーの名を渡すために使用される SAML 属性。
姓	ユーザーの姓を渡すために使用される SAML 属性。
役職	ユーザーの役職を渡すために使用される SAML 属性。
電子メールアドレス	ユーザーの電子メールアドレスを渡すために使用される SAML 属性。
電子メール区切り文字	複数の電子メールアドレスが渡される場合に電子メールアドレスを区切る区切り文字。
電話番号	ユーザーの電話番号を渡すために使用される SAML 属性。
タイムゾーン	ユーザーの時間帯を渡すために使用される SAML 属性。
ユーザーロール	ユーザーに割り当てられているユーザーロールを渡すために使用される SAML 属性。
ロール区切り文字	複数のロールが渡される場合にロールを区切る区切り文字。

SAML ロールマッピングのプロパティ

SAML ロール名を Informatica Intelligent Cloud Services ロール名にマッピングします。複数の SAML ロール名を 1 つの Informatica Intelligent Cloud Services ロールにマッピングできます。**[SAML セットアップ]** ページで、SAML ロールマッピングのプロパティを定義します。

次の表に、SAML ロールマッピングのプロパティを示します。

プロパティ	説明
Informatica Intelligent Cloud Services のロール	Informatica Intelligent Cloud Services のロールに相当する SAML ロール。複数のロールを入力する必要がある場合、カンマを使用してロールを区切ります。
デフォルトロール	SAML 認証応答に SAML ユーザーロール属性が含まれていない場合に使用されるデフォルトロール。
デフォルトユーザーグループ	シングルサインオンユーザーのデフォルトユーザーグループ。

サービスプロバイダメタデータのダウンロード

SAML シングルサインオンの設定プロセスを完了するには、ID プロバイダに SAML SAML サービスプロバイダメタデータおよび Informatica Intelligent Cloud Services URL が必要です。Informatica Intelligent Cloud Services がサービスプロバイダメタデータファイルを生成したら、ファイルおよび Informatica Intelligent Cloud Services URL を ID プロバイダに配信します。

1. **[SAML セットアップ]** ページで、**[サービスプロバイダメタデータのダウンロード]** をクリックします。
サービスプロバイダのメタデータファイルがマシンにダウンロードされます。
2. **[情報]** ダイアログボックスで、シングルサインオンアクセスの URL を Informatica Intelligent Cloud Services 組織に記録します。
3. **[OK]** をクリックして、**[情報]** ダイアログボックスを閉じます。
4. メタデータファイルおよび Informatica Intelligent Cloud Services シングルサインオン URL を ID プロバイダ管理者に送信します。

第 6 章

メータリング

組織およびサブ組織のメータリング情報を表示できます。メータリング情報は【メータリング】ページに表示されます。

メーターには、一括取り込みストリーミングの合計データボリュームなど、組織が使用するコンピューティングリソースの量が表示されます。また、組織のライセンス数で設定されるジョブの制限数も表示されます。

【メータリング】ページには、組織のライセンスに基づいて次のビューに情報が表示されます。

ダッシュボードビュー

適切なライセンスがある場合、【メータリング】ページのダッシュボードビューに情報が表示されます。

ダッシュボードビューのサマリ領域には、該当月の残りコンピューティングリソースに関するサマリが表示されます。組織に適用されるすべてのメーターのテーブルを表示することもできます。組織に適用されるメーターは、組織のエディションによって異なります。

詳細領域には、一括取り込みストリーミングデータボリューム使用状況に関する月次の使用統計が表示されます。データボリューム使用状況に関する詳細なチャートを表示することもできます。

ライセンスメトリックビュー

ダッシュボードビューの表示に必要なライセンスがない場合は、【メータリング】ページにはライセンスメトリックのテーブルが表示されます。テーブルには、組織に適用されるすべてのメーターが表示されます。組織に適用されるメーターは、組織のエディションによって異なります。

ライセンスメトリックの表示

組織で使用しているすべてのメーターのテーブルを表示し、メータリング使用状況を示すレポートをダウンロードできます。【メータリング】ページのライセンスメトリックビューからテーブルを表示し、レポートをダウンロードします。

ダッシュボードビューからライセンスメトリックビューを開くには、[メトリックサマリ - 今月] 領域の【すべてのメーター】をクリックします。ダッシュボードビューの表示に必要なライセンスがない場合は、【メータリング】ページを開くとライセンスメトリックビューが表示されます。

ライセンスメトリックビューに表示されるメーターは、組織が使用しているエディションによって決まります。また、組織にはカスタムメーターも割り当てられる場合があります。メータリング情報はすべてのエディションで使用できない場合があります。

組織で複数のエディションを使用している場合、またはカスタムメーターを使用している場合、1つのメーターが異なる制限で複数回表示されることがあります。この場合、最新の制限が適用されます。例えば、あるエディションの同期ジョブが1日500個に制限され、別のエディションの同期ジョブが1日に100個に制限されている場合、1日のジョブは500個に制限されます。【有効】カラムに適用した制限が表示されます。

ライセンスメトリックビューには、メーターごとに以下の情報が表示されます。

プロパティ	説明
エディション	メーターに関連付けられているエディションの名前。
サービス	メーターが適用されるサービス。
メータリング	メーターの名前。例えば、1日あたりの同期ジョブの数、1か月あたりのマッピングジョブによって処理する行数、またはレプリケーションジョブの合計数です。
制限	ジョブまたは処理した行の最大数などの制限数。 この制限は親組織と各サブ組織に適用されます。例えば、1日あたりのジョブが100個に制限された場合、親組織が実行できるジョブは1日100個、各サブ組織が実行できるジョブも1日100個になります。 このフィールドに-1が表示された場合、制限はありません。
使用中	使用された実際のユニット数。組織またはサブ組織でメータリング期間に実行されるジョブ数または使用される計算時間などがあります。
使用済みの割合	組織またはサブ組織でメータリング期間に使用されたユニットの割合。
有効	組織またはサブ組織でメーターが有効かどうかを示します。

メーター定義

【メータリング】 ページの「ライセンスメトリック」ビューに表示されるメーターは、組織が使用しているエディションによって決まります。

次の表に、エディションに基づいて効力がある可能性があるメーターについて説明します。

メーター	定義
エージェントの総数	停止したエージェントを含む、Secure Agents の合計数。 Informatica Cloud Hosted Agent は含みません。
接続の総数	接続の総数。
プロジェクトの総数	プロジェクトの総数。
フォルダの総数	フォルダの総数。
日次/月間受信 API 要求最大	日次または月間の API アクセス要求の数。
日次/月間のマッピングジョブの数	日次または月間のマッピングジョブの数。*
マッピングジョブの総数	マッピングジョブの総数。*
日次/月間のマッピングジョブが処理した行数	日次または月間のマッピングジョブが処理した行数。*
マッピングジョブが処理した行の総数	マッピングジョブが処理した行の総数。*

メーター	定義
日次/月間のマスキングジョブの数	日次または月間のマスキングジョブの数。
マスキングジョブの総数	マスキングジョブの総数。
日次/月間のマスキングジョブが処理した行数	日次または月間のマスキングジョブが処理した行数。
マスキングジョブが処理した行の総数	マスキングジョブが処理した行の総数。
日次/月間の PowerCenter ジョブの数	日次または月間の PowerCenter ジョブの数。
PowerCenter ジョブの総数	PowerCenter ジョブの総数。
日次/月間の PowerCenter ジョブが処理した行数	日次または月間の PowerCenter ジョブが処理した行数。
PowerCenter ジョブが処理した行の総数	PowerCenter ジョブが処理した行の総数。
日次/月間のレプリケーションジョブの数	日次または月間のレプリケーションジョブの数。
レプリケーションジョブの総数	レプリケーションジョブの総数。
日次/月間のレプリケーションジョブが処理した行数	日次または月間のレプリケーションジョブが処理した行数。
レプリケーションジョブが処理した行の総数	レプリケーションジョブが処理した行の総数。
月間のストリーミング取り込みタスクが処理したデータ数 (GB 単位)。	月間のストリーミング統合ジョブが処理したギガバイト数。
日次/月間の同期ジョブの数	日次または月間の同期ジョブの数。
同期ジョブの総数	同期ジョブの総数。
日次/月間の同期ジョブが処理した行数	日次または月間の同期ジョブが処理した行数。
同期ジョブが処理した行の総数	同期ジョブが処理した行の総数。
サブ組織の数	サブ組織の数。
日次の状態同期ジョブの数	日次の状態同期ジョブの数。 状態同期ジョブには、REST API を介して実行する fetchState ジョブおよび loadState ジョブが含まれます。
ユーザー管理作成要求数	ユーザー管理作成要求数。 ユーザー管理作成要求には、ユーザー、ユーザーグループ、カスタムロールの作成のための要求が含まれます。

メーター	定義
エラスティッククラスタのノードが使用した計算時間の合計	エラスティッククラスタのノードが使用した計算時間の合計。 注: 組織で Data Integration Elastic を使用している場合、各ノードがエラスティッククラスタで提供する処理能力または計算時間に基づいて、メータリングが計算されます。メータリングは、ノードがクラスタに追加されると開始します。メータリングは、ノードがクラスタから削除されるかクラスタが停止すると終了します。
使用されたサーバーレスユニットの総数	タスクの実行に使用されたサーバーレスコンピューティングユニットの総数。

* 組織が Azure のデータアクセラレータを使用する場合、このメーターには Azure のデータ同期ジョブが含まれます。これは、各 Azure のデータ同期ジョブは基盤マッピングを実行するためです。

メータリングの使用状況レポート

組織で Data Integration Elastic、一括取り込みサービス、またはサーバーレスランタイム環境を使用する場合、メータリングの使用状況レポートをダウンロードできます。

メータリングの使用状況レポートには、次の情報が含まれます。

- Data Integration Elastic の場合、レポートには、エラスティッククラスタ内のノードの計算時間に関する詳細が含まれます。この詳細を CSV ファイルにエクスポートできます。
- 一括取り込みの場合、レポートには、一括取り込みストリーミングジョブによって取り込まれたデータの量に関する詳細が含まれます。
- サーバーレスランタイム環境の場合、レポートには、タスクを実行するために要求および使用されたサーバーレスコンピューティングユニットの数に関する詳細が含まれます。

組織で Data Integration Elastic、一括取り込みストリーミング、またはサーバーレスランタイム環境を使用していない場合、メータリングの使用状況レポートは使用できません。

メータリングの使用状況レポートのダウンロード

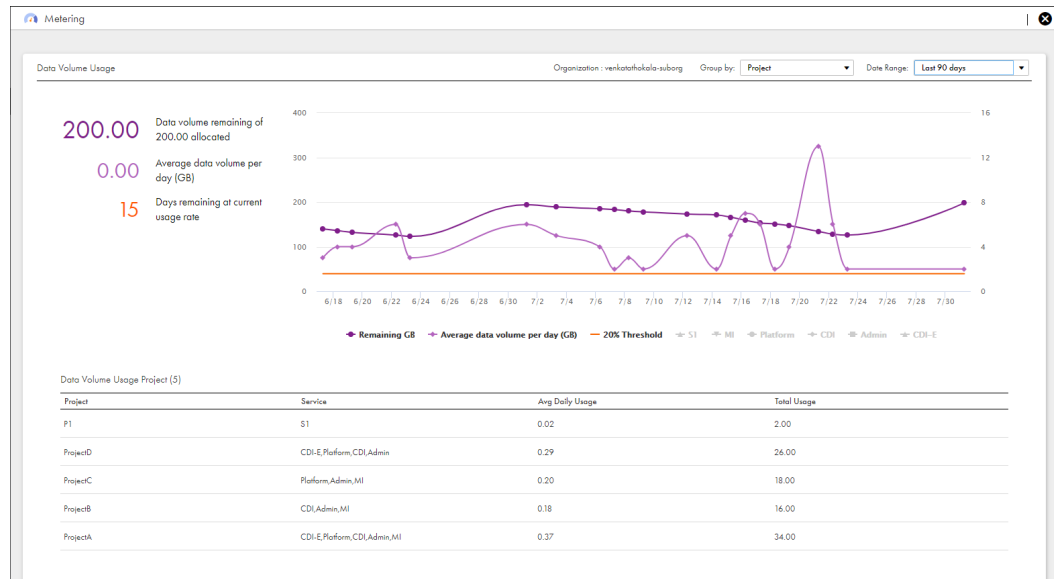
【メータリング】 ページの **【ライセンスメトリック】** ビューからメータリングの使用状況レポートをダウンロードします。

1. 管理者で **【メータリング】** を選択します。
2. ダッシュボードビューが表示された場合は、**【メトリックサマリ - 今月】** 領域で **【すべてのメーター】** をクリックして、**【ライセンスメトリック】** ビューを開きます。
3. **【ファイルへエクスポート】** をクリックして、**【メータリングの使用状況の詳細】** を選択します。
4. サービス機能または製品機能と、表示する日付範囲を選択して、**【エクスポート】** をクリックします。

使用状況の詳細の表示

一括取り込みストリーミングデータボリューム使用状況に関する詳細な統計を表示できます。詳細な統計を表示するには、**【メータリング】** ページのダッシュボードビューで、**【詳細なチャート】** をクリックするか、**【データボリューム使用状況 - 今月】** 領域のグラフをクリックします。

次の図は、過去 90 日間のデータボリューム使用状況の詳細ページの例を示しています。



ページは、次の方法でカスタマイズできます。

- 組織にサブ組織がある場合は、親組織またはサブ組織の使用状況の詳細を表示できます。
- グループ化は変更できます。例えば、使用状況の詳細をプロジェクト別、ランタイム環境別、またはその両方で表示できます。
- 日付範囲は変更できます。
- 使用状況の詳細が複数のサービスに適用される場合は、各サービスのリソース使用状況を表示するようグラフを更新できます。あるサービスのリソース使用状況を表示するようグラフを更新するには、グラフの下にあるそのサービス名を選択します。

注: 一括取り込みストリーミングで、実行状態であるストリーミング統合ジョブのランタイム環境名またはプロジェクトを変更すると、引き続きメータリング情報は古いランタイム環境名で表示されたり、ジョブの古いプロジェクトに表示されたりします。ストリーミング統合ジョブを再デプロイすると、それぞれのメータリング情報が新しいランタイム環境名またはプロジェクトで表示されます。

第 7 章

ソース管理およびサービスアップグレード設定

Secure Agent サービスのソース管理およびアップグレード設定は、**【設定】** ページで設定できます。

以下の設定項目を設定することができます。

ソース管理設定

組織に適切なライセンスがある場合は、組織のソース管理を設定できます。プロジェクト、フォルダ、およびアセットのバージョン管理を有効にするためのソース管理を設定します。ソース管理を設定するには、**【ソース管理の有効化】** オプションを有効にし、リポジトリアクセスのタイプを設定してから、ソース管理リポジトリへの接続を設定します。

ソース管理リポジトリへの読み取り/書き込み、または読み取り専用アクセスを設定できます。読み取り/書き込みアクセスを設定するには、**【Git リポジトリへのプッシュを許可】** オプションを有効にします。読み取り専用アクセスを設定するには、**【Git リポジトリへのプッシュを許可】** オプションを無効にします。

Secure Agent サービスのアップグレード設定

ローリングアップグレードをサポートするサービスのアップグレード中にエラーが発生した場合、そのサービスのアップグレードを続行するか停止するかを指定できます。

マイナーアップグレード後に再起動する必要があるサービスの再起動スケジュールを設定できます。再起動スケジュールの再開を設定するには、アップグレードを実行する曜日と時刻を選択します。

ソース管理設定

プロジェクト、フォルダ、およびアセットのバージョン管理を有効にするために、組織のソース管理を設定できます。ソース管理を設定するときに、Git リポジトリ内にオブジェクトのバージョンを保存できます。ソース管理は **【設定】** ページで設定します。

組織のソース管理を設定すると、ユーザーはソース管理をオブジェクトに適用できます。オブジェクトは自動的にチェックインされません。ユーザーは、ソース管理を個別のアセットまたはプロジェクトまたはフォルダ内のすべてのアセットに適用できます。ソース管理のプロジェクト、フォルダ、およびアセットへの適用の詳細については、該当する Informatica Intelligent Cloud Services サービスのヘルプシステムを参照してください。

組織のソース管理を設定するには、適切なライセンスを所有している必要があります。

組織のソース管理は、次の方法で設定できます。

ソース管理リポジトリへの読み取り/書き込みアクセスを設定します。

読み取り/書き込みアクセスを設定すると、組織内のユーザーは、オブジェクトのチェックインおよびチェックアウト、オブジェクトのバージョンのプル、オブジェクトを前のバージョンに戻すことができます。ユーザーは、ソース管理オブジェクトを変更するには、それらをチェックアウトする必要があります。ユーザーはオブジェクトを排他的にチェックアウトするため、ユーザーは別のユーザーによってチェックアウトされているオブジェクトを変更することはできません。ユーザーは、ソース管理されていないオブジェクトはチェックアウトせずに変更できます。

読み取り/書き込みアクセスは、プロジェクトおよびアセットを開発する組織用に設定することがあります。

ソース管理リポジトリへの読み取り専用アクセスを設定します。

読み取り専用アクセスを設定すると、組織内のユーザーは、ソース管理オブジェクトのバージョンをリポジトリからプルできます。しかし、ユーザーはオブジェクトのチェックアウトまたはチェックインをすることはできません。ユーザーは、組織内のプロジェクト、フォルダ、およびアセットをチェックアウトせずに、それらに変更を加えることができます。

読み取り専用アクセスは、テストまたは本番組織に設定し、ユーザーがアセットの最新バージョンをテストまたは実行できるようにすることがあります。

警告: 読み取り専用アクセスを設定すると、ユーザーは、ソース管理オブジェクトを上書きできます。例えば、ユーザー John が最新バージョンのソース管理マッピングをプルし、変更するとします。別のユーザーが後でこのマッピングの任意のバージョンをプルした場合、John の変更は失われます。オブジェクトの権限およびユーザー権限は、ユーザーが誤って組織内のソース管理アセットを上書きするのを防止するように、注意深く設定します。

リポジトリアクセスタイプを変更できます。しかし、読み取り/書き込みから読み取り専用に変更するには、まずオブジェクトがチェックアウトされていないことを確認する必要があります。Informatica Intelligent Cloud Services は、チェックアウトされているオブジェクトがある場合、リポジトリアクセスタイプの読み取り/書き込みから読み取り専用への変更を許可しません。

リポジトリ URL も変更できます。これを実行するには、まずすべてのソース管理アセットのリンクを解除します。Informatica Intelligent Cloud Services は、ソース管理アセットがある場合、リポジトリ URL の変更を許可しません。

設定した後でソース管理を無効にする場合、ソース管理からすべてのオブジェクトのリンクを解除してから、組織のソース管理を無効にします。

サブ組織のソース管理設定

サブ組織のソース管理は、サブ組織の【設定】ページで設定します。ベストプラクティスとして、各サブ組織は、その組織用のソース管理リポジトリを使用する必要があります。さらに、サブ組織用のソース管理リポジトリは、その親組織のソース管理リポジトリと別である必要があります。

個別のソース管理リポジトリを管理することで、1 つの組織内のユーザーが、別の組織のアセットを誤って上書きしたり変更したりすること起きないようにします。

親組織の管理者がサブ組織のソース管理操作を実行できるようにする場合、親組織の管理者の Git ユーザーアカウントが、サブ組織のソース管理リポジトリへのアクセス権を持つように設定します。

OAuth を使用したリポジトリアクセス

ソース管理リポジトリへのアクセスを提供するために、個人のアクセストークンではなく OAuth 認証を使用するように組織を設定できます。OAuth 認証は【設定】ページで設定します。

GitHub リポジトリを使用する場合は、Informatica Intelligent Cloud Services が組織の GitHub リポジトリに対してソース管理操作を実行できるようにする GitHub アクセスタブアプリケーションがリポジトリにインストール

ルされている必要があります。このアプリケーションがリポジトリにインストールされていない場合は、**【設定】** ページからインストールできます。

組織のソース管理の有効化

組織のソース管理を有効にする場合、**【設定】** ページでソース管理リポジトリへのアクセスタイプと接続を設定します。選択するソース管理リポジトリには、「master」という名前のブランチを含める必要があります。

1. 管理者の **【設定】** ページで、[ソース管理] 領域の **【編集】** をクリックします。
2. **【ソース管理の有効化】** オプションを有効にします。
3. ソース管理リポジトリへのアクセスタイプを設定します。
 - 読み取り/書き込みアクセスを設定するには、**【Git リポジトリへのプッシュを許可】** オプションを有効にします。
 - 読み取り専用アクセスを設定するには、**【Git リポジトリへのプッシュを許可】** オプションを無効にします。
4. 次のように、リポジトリ URL を入力します。

`https://github.com/MyGitUser/MyRepositoryName.git`

リポジトリ URL は HTTPS プロトコルを使用する必要があります。

5. 必要に応じて、OAuth を使用してリポジトリにアクセスするには、**【Git への OAuth のアクセスを許可】** を有効にします

GitHub リポジトリを使用する場合は、Informatica Intelligent Cloud Services のアクセスを許可する Git アクセスアプリケーションをリポジトリにインストールする必要があります。このアプリケーションをインストールするには、**【Git アクセスアプリケーションのインストール】** をクリックします。

6. **【保存】** をクリックします。

Informatica Intelligent Cloud Services は、リポジトリ接続を確認するためのソース管理資格情報の入力を求めるプロンプトを表示します。Informatica Intelligent Cloud Services はこの情報を保存しません。

接続が有効であり、リポジトリへの読み取り/書き込みアクセスを設定した場合、Informatica Intelligent Cloud Services はこのリポジトリに小さな readme ファイルを書き込み、これがリポジトリにオブジェクトをプッシュできることを確認します。

ソース管理の有効化後、ソース管理を使用するすべてのユーザーは、ユーザー設定で自分のソース管理資格情報を入力する必要があります。ユーザーは、自分の資格情報を入力するまでは、**【参照】** ページのソース管理コラムを表示できず、ソース管理アクションを実行できません。ソース管理資格情報を入力するには、**【ユーザー】** アイコンを Informatica Intelligent Cloud Services ウィンドウの右上隅でクリックし、**【設定】** を選択します。

ソース管理リポジトリ URL の変更

ソース管理リポジトリ URL を変更するには、まず組織内のすべてのオブジェクトをリンク解除し、新規リポジトリ URL を管理者の **【設定】** ページで入力します。URL の変更後、ソース管理を使用するすべてのユーザーは、ユーザー設定で自分のソース管理資格情報を更新する必要があります。

1. そのリポジトリを使用する各 Informatica Intelligent Cloud Services サービスで、すべてのオブジェクトをソース管理からリンク解除します。
2. 管理者で、**【設定】** ページを開き、[ソース管理] 領域の **【編集】** をクリックします。
3. **【ソース管理の有効化】** オプションが有効になっていることを確認します。
4. ソース管理リポジトリへのアクセスタイプを設定します。

- 読み取り/書き込みアクセスを設定するには、**【Git リポジトリへのプッシュを許可】** オプションを有効にします。
 - 読み取り専用アクセスを設定するには、**【Git リポジトリへのプッシュを許可】** オプションを無効にします。
5. 新規リポジトリ URL を次のように入力します。
- ```
https://github.com/MyGitUser/MyRepositoryName.git
```
- ヒント:** GitHub で、リポジトリ URL を検索できます。これには、リポジトリを開き、**【Clone or download (クローンまたはダウンロード)】** > **【Clone with HTTPS (HTTPS でのクローン)】** を選択します。
- リポジトリ URL は HTTPS プロトコルを使用する必要があります。
6. **【保存】** をクリックします。
- Informatica Intelligent Cloud Services は、リポジトリ接続を確認するためのソース管理資格情報の入力を求めるプロンプトを表示します。Informatica Intelligent Cloud Services はこの情報を保存しません。
- 接続が有効であり、リポジトリへの読み取り/書き込みアクセスを設定した場合、Informatica Intelligent Cloud Services はこのリポジトリに小さな readme ファイルを書き込み、これがリポジトリにオブジェクトをプッシュできることを確認します。
- ソース管理リポジトリ URL の変更後、ソース管理を使用するすべてのユーザーは、ユーザー設定で自分のソース管理資格情報を更新する必要があります。ソース管理資格情報を更新するには、**【ユーザー】** アイコンを Informatica Intelligent Cloud Services ウィンドウの右上隅でクリックし、**【設定】** を選択します。

## 組織のソース管理の無効化

組織のソース管理を無効にできます。ソース管理を無効にすると、組織とソース管理リポジトリの間のリンクが解除されます。ソース管理リポジトリ内のオブジェクトは削除されません。

読み取り書き込みに関する組織のソース管理を無効にする前に、すべてのアセットをリンク解除する必要があります。

1. そのリポジトリを使用する各 Informatica Intelligent Cloud Services サービスで、すべてのオブジェクトをソース管理からリンク解除します。
2. 管理者で、ソース管理を無効にします。
  - a. 管理者で、**【設定】** ページを開きます。
  - b. **【ソース管理】** 領域の **【編集】** をクリックします。
  - c. **【ソース管理の有効化】** オプションを無効にします。
  - d. **【保存】** をクリックします。
3. オプションとして、組織内のユーザーがユーザー設定で自分のソース管理資格情報を削除できるようにします。
  - a. Informatica Intelligent Cloud Services ウィンドウの右上隅で、**【ユーザー】** アイコンをクリックし、**【設定】** を選択します。
  - b. ソース管理資格情報をクリアします。
  - c. **【保存】** をクリックします。

## リポジトリアクセスの設定

ソース制御オブジェクトを操作するには、Informatica Intelligent Cloud Services で GitHub または Azure DevOps Git リポジトリの認証情報を指定します。

資格情報には、ユーザー名とパーソナルアクセストークンを含めることができます。

管理者が組織のリポジトリを OAuth アクセス用に設定している場合は、パーソナルアクセストークンを提供する代わりに OAuth アクセスを有効化することができます。

パーソナルアクセストークンは、プライベートリポジトリを完全に制御できるように設定する必要があります。パーソナルアクセストークンの生成については、GitHub または Azure DevOps Git のヘルプを参照してください。

Informatica Intelligent Cloud Services で次のステップを実行して、リポジトリへのアクセスを設定します。

1. Informatica Intelligent Cloud Services ウィンドウ右上隅にある **【ユーザー】** アイコンをクリックして、**【設定】** を選択します。
2. 次のいずれかの手順に従います。
  - リポジトリの資格情報を入力します。GitHub の場合は、ユーザー名とパーソナルアクセストークンを入力します。Azure DevOps Git の場合は、パーソナルアクセストークンを入力します。
  - リポジトリへの OAuth アクセスを有効にします。アクセスを許可していない場合は、Git アクセスアプリが表示されます。Informatica Intelligent Cloud Services へのアクセスを承認する場合に選択します。
3. **【保存】** をクリックします。

## ソース管理のベストプラクティス

組織がソース管理を効果的に設定して使用できるようにするには、次のガイドラインをベストプラクティスとして使用します。

### 設定のガイドライン

組織のソース管理を設定するときは、次のガイドラインに従います。

- 開発、テスト、ステージング、本番には別々の組織を使用します。

異なる組織を管理するときは、環境間を独立させ、1つの環境に対する変更が、他の環境に影響しないようにします。例えば、テスト環境内のアセットへの変更が、誤って本番環境にデプロイされることがないようにします。
- ソース管理リポジトリへの読み取り/書き込みアクセスを持つ開発組織を設定し、ソース管理リポジトリへの読み取り専用アクセスを持つ非開発組織を設定します。

そうすることで、開発組織内のユーザーのみが、アセットに変更を加えられます。また、非開発環境内のユーザーが、誤って変更をソース管理リポジトリにプッシュすることを防止できます。
- 1つの開発組織のみが、特定のソース管理リポジトリを使用することを保証します。

独立したリポジトリを管理することで、1つの組織内のユーザーが別の組織のアセットを誤って変更したり上書きしたりする事故が起きないことを保証します。
- 組織のソース管理を有効にするときは、空のリポジトリを選択します。

Informatica Intelligent Cloud Services はアセットを Git リポジトリ内の Explore フォルダに保存するため、リポジトリに Explore という名前のフォルダが含まれないようにします。
- ソース管理の資格情報を、複数の Informatica Intelligent Cloud Services ユーザー間で共有しないようにします。

個別の資格情報によってセキュリティが維持され、特定の変更を加えたユーザーが誰かを追跡するのが簡単になります。さらに、各ユーザーは、GitHub 内に自分の制限を持ちます。

### 開発ガイドライン

アセットを開発し操作するときは、次のガイドラインに従います。

## 依存関係の管理に関するガイドライン

依存関係を持つアセットを管理するには、次のガイドラインに従います。

- アセットをリポジトリからプルする前に、接続およびランタイム環境を作成します。  
必要な接続およびランタイム環境がターゲット組織内にあるときは、タスクをリポジトリからプルした直後に実行できます。
- マッピングやコンポーネントなどの再利用可能なアセットが、使用前にリポジトリ内にあることを確認します。  
Informatica Intelligent Cloud Services は、マッピングタスクなどのアセットが依存するマッピングが組織内にはない場合、アセットの保存を許可しません。
- 他のアセットが使用するソース管理アセットの移動や名前の変更を避けます。  
ソース管理アセットを移動または名前を変更した場合、そのアセットへの参照は切断されます。

## アセットのチェックインおよびチェックアウトに関するガイドライン

アセットをチェックインおよびチェックアウトするときは、次のガイドラインに従います。

- マッピング、マップレット、およびユーザー定義の関数などの再利用可能なアセットをチェックアウトする前に、すべての依存関係を特定します。  
チェックアウト、チェックイン、およびプルなどのソース管理操作には、依存アセットは自動的に含まれません。
- マッピングまたはコンポーネントなどの再利用可能なアセットを更新する必要があるときは、そのアセットとすべての依存アセットをチェックアウトします。  
例えば、マッピングを更新する必要があるときは、そのマッピングと、それを使用するすべてのマッピングタスクをチェックアウトし、マッピングへの変更が、それらのマッピングタスクにプロパゲートされることを保証します。
- 1つの操作内で再利用可能なアセットとすべての依存アセットをチェックインします。  
これにより、そのアセットと依存アセットへの変更が、ソース管理リポジトリに同時にコミットされることが保証されます。また、ユーザーがアセットをプルするときに、最新バージョンの依存アセットをユーザーが取得することが保証されます。
- アセットのチェックイン時にコメントを入力します。  
アセットのチェックイン時に、リリースタグ名を【サマリ】フィールドに入力し、より説明的なコメントを【説明】フィールドに入力することがあります。これを実行すると、Informatica Intelligent Cloud Services の【Git Summary (Git サマリ)】フィールドに、アセットに関連付けられたリリースタグが表示されます。
- 複数のアセットを同時にチェックインするときは、アセット数を 1000 件以下に制限します。  
1000 件を超えるアセットを同時にチェックインすると、Informatica Intelligent Cloud Services と GitHub リポジトリサービスとの間のパフォーマンスが低下する可能性があります。

# 別のユーザーのチェックアウトの取り消し

管理者ロールがある場合、またはユーザーロールに管理者サービスへのチェックアウトの取り消しを強制する機能がある場合、別のユーザーがチェックアウトしたオブジェクトのチェックアウトを取り消すことができます。



す。ユーザーがオブジェクトをチェックアウトして、休暇を取る場合、または組織を離れる場合、別のユーザーによりチェックアウトされたオブジェクトのチェックアウトを取り消す必要がある場合があります。

チェックアウトを取り消すと、オブジェクトはソース管理リポジトリにある最後のバージョンに戻ります。オブジェクトのバージョン履歴には、チェックアウトやチェックアウトアクションを取り消した記録は残りません。後で変更したバージョンが必要になる可能性がある場合、チェックアウトを取り消す前にオブジェクトのコピーを作成します。

取り消しアクションは元に戻せません。プロジェクトまたはフォルダのチェックアウトを取り消すと、そのプロジェクトまたはフォルダのロックは解除されますが、プロジェクトまたはフォルダ内にあるオブジェクトはロックされたままになります。

1. ユーザーがオブジェクトをチェックアウトしたサービスを開きます。
2. **【エクスプローラ】** ページで、オブジェクトに移動します。
3. オブジェクトが含まれている行で、**【アクション】** をクリックし、**【チェックアウトの取り消し】** を選択します。

取り消しアクションによってロックが解除されるため、オブジェクトはチェックアウトできる状態になります。

**注:** オブジェクトがチェックアウトされた後に移動または名前が変更された場合、チェックアウトを取り消すとオブジェクトの名前と場所はチェックアウトされる前の名前と場所に戻されます。

## Secure Agent サービスのローリングアップグレード

一部の Secure Agent サービスは、ローリングアップグレードをサポートしています。ローリングアップグレードでは、Secure Agent グループ内のエージェントで実行されているサービスは、順次アップグレードされます。そのため、あるエージェント上でサービスがアップグレードされる間、そのサービスはグループ内の他のエージェント上で使用可能であり続けます。

次の Secure Agent サービスは、ローリングアップグレードをサポートしています。

- プロセスサーバー

Secure Agent グループ内のエージェントで実行されているその他のサービスは、各エージェント上で同時にアップグレードされます。そのため、そのグループ内のエージェントがアップグレードされている間は、サービスを使用できません。グループ内のすべてのエージェントが正常にアップグレードされると、使用できるようになります。

### 例

組織では、次のランタイム環境を使用しています。

- Secure Agent グループ A:

エージェント A1 はデータ統合サーバーおよびプロセスサーバーを実行します。

エージェント A2 はデータ統合サーバー、一括取り込み、およびプロセスサーバーを実行します。

- Secure Agent グループ B:

エージェント B1 はデータ統合サーバー、一括取り込み、およびプロセスサーバーを実行します。

エージェント B2 はデータ統合サーバー、一括取り込み、およびプロセスサーバーを実行します。

組織がアップグレードされるときに、Secure Agent グループ A および B は同時にアップグレードされます。各 Secure Agent グループ内で、プロセスサーバーは順次アップグレードされます。そのため、プロセスサーバーがエージェント A1 および B1 でアップグレードされる間、エージェント A2 および B2 で実行され続けま

す。エージェント A1 および B1 でのアップグレードが完了すると、プロセスサーバーはエージェント A2 および B2 でアップグレードされます。

データ統合サーバーと一括取り込みはローリングアップグレードをサポートしていません。グループ A および B で、データ統合サーバーは各エージェントで同時にアップグレードされます。グループ B で、一括取り込みはエージェント B1 および B2 で同時にアップグレードされます。

## ローリングアップグレードエラーの処理

ローリングアップグレードをサポートするサービスのアップグレード中にエラーが発生した場合、そのサービスのアップグレードを続行するか停止するかを指定できます。エラー処理動作を **【設定】** ページで設定します。

以下のいずれかのオプションを選択することができます。

### エラーが発生した場合、エラーにフラグを設定して、アップグレードを続行する

サービスのアップグレード中にエラーが発生した場合、サービスはエラーが発生したエージェントのエラーで停止します。そのアップグレードは、グループ内の別のエージェント上で続行されます。

**警告:** このオプションを有効にし、グループ内のすべてのエージェント上でエラーが発生した場合、そのサービスは Secure Agent グループでの実行を停止します。これがジョブの中断の原因になる場合があります。

### エラーが発生した場合、アップグレードを停止する

サービスのアップグレード中にエラーが発生した場合、サービスはエラーが発生したエージェントのエラーで停止します。まだアップグレードされていないグループ内の他のすべてのエージェントに対してサービスのアップグレードが停止します。まだアップグレードされていないエージェントは、そのサービスの以前のバージョンで実行し続けます。

これがデフォルトのオプションです。

エラー処理動作を設定するには、**【編集】** を [Secure Agent サービスのアップグレード設定] 領域でクリックし、適切なオプションを選択し、**【保存】** をクリックします。

## Secure Agent サービスの再開スケジュールの設定

プロセスサーバーなどの一部の Secure Agent サービスには、アップグレード後に再開する必要があるものがあります。これらのサービスは、月間アップグレードやパッチリリースなどのマイナーアップグレード後に再開スケジュールを設定できます。再開スケジュールを **【設定】** ページで設定します。

再開スケジュールを設定するときは、サービスを再開する曜日と時刻を選択します。例えば、毎週日曜日の 00:00 GMT の再開をスケジュールできます。

再開スケジュールは、次の Secure Agent サービスに対して設定できます。

- プロセスサーバー

スケジュールを設定するには、**【編集】** を [Secure Agent サービスのアップグレード設定] 領域でクリックし、日時を選択し、**【保存】** をクリックします。



## 第 8 章

# ユーザーとユーザーグループ

組織とアセットへのアクセスを許可するようにユーザーとユーザーグループを設定します。

ユーザーは、組織への安全なアクセスを可能にする Informatica Intelligent Cloud Services の個別アカウントです。

ユーザーグループは、グループのすべてのメンバが同じタスクを実行し、さまざまなタイプのアセットに対して同じアクセス権を持つことができるユーザーアカウントのグループです。

ユーザーとグループは割り当てられているロールに基づいて、タスクを実行し、アセットにアクセスすることができます。ユーザーロールの詳細については、[第 9 章、「ユーザーロール」 \(ページ 63\)](#) を参照してください。

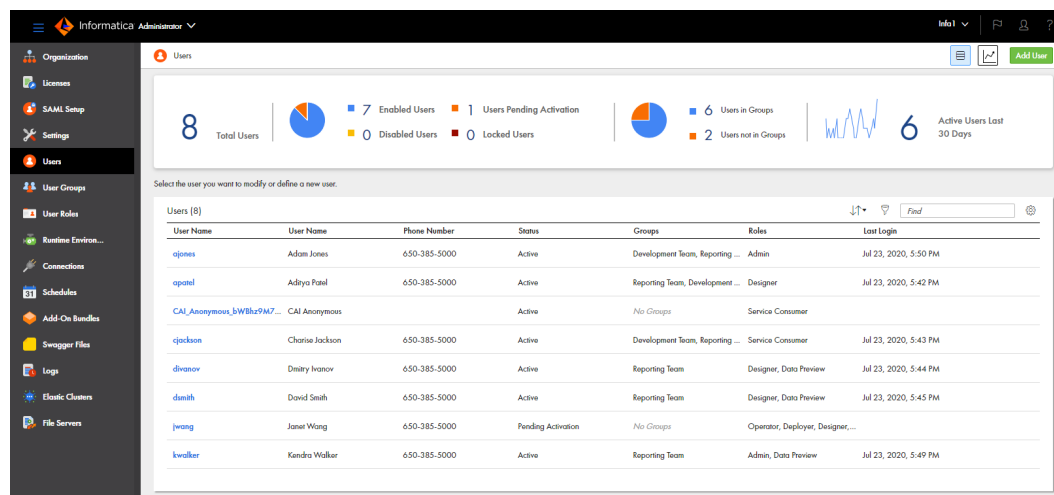
## ユーザー

ユーザーは、組織への安全なアクセスを可能にする個別の Informatica Intelligent Cloud Services アカウントです。ユーザーは、そのユーザーに割り当てられたロールに基づいてタスクを実行し、アセットにアクセスできます。ロールは、ユーザーまたはユーザーが所属するグループに直接割り当てることができます。

管理者は、組織のユーザーアカウントを作成して設定できます。

[ユーザー] ページには組織のすべてのユーザーが一覧表示されます。[ユーザー] ページにアクセスするには、管理者で [ユーザー] を選択します。

次の図は、[ユーザー] ページを示しています。



【ユーザー】 ページには、組織のユーザー統計が表示され、各ユーザーがリストされます。アプリケーションの統合を使用している場合、このページにはアプリケーションの統合の匿名ユーザーとその状態も一覧表示されます。ユーザーの詳細情報を表示するには、ユーザー名をクリックします。

ユーザーに対して次のタスクを実行できます。

- ユーザーの詳細を表示および編集します。
- ユーザーを作成する。
- サービスを割り当ておよび割り当て解除する。
- ユーザーを無効にする。
- ユーザーをリセットする。
- ユーザーのスケジュール済みジョブを別のユーザーに再割り当てする。
- ユーザーを削除する。

## ユーザー認証

Informatica Intelligent Cloud Services はさまざまなタイプのユーザー認証を使用します。ネイティブユーザーは Informatica Intelligent Cloud Services によって認証されます。Salesforce、Microsoft Azure、および SAML ユーザーは、それぞれの ID プロバイダによって認証されます。

Informatica Intelligent Cloud Services では、以下のタイプのユーザー認証を使用できます。

### Native

ネイティブユーザーは、ユーザー名およびパスワードを使用して Informatica Intelligent Cloud Services のログインページから Informatica Intelligent Cloud Services にログインします。ユーザーは Informatica Intelligent Cloud Services によって認証されます。

### Salesforce

Salesforce ユーザーは、Salesforce または Salesforce アプリケーションから Informatica Intelligent Cloud Services にサインインします。ユーザーは Salesforce によって認証されます。

Salesforce 認証の詳細については、データ統合のヘルプの Salesforce コネクタのヘルプを参照してください。

### Microsoft Azure

Microsoft Azure ユーザーは Microsoft Azure から Informatica Intelligent Cloud Services にサインインします。ユーザーは Microsoft Azure によって認証されます。

Microsoft Azure 認証の詳細については、[第 4 章, 「エコシステムのシングルサインオン」 \(ページ 27\)](#)を参照してください。

### SAML

SAML ユーザーは ID プロバイダから Informatica Intelligent Cloud Services にサインインします。ユーザーは ID プロバイダによって認証されます。

SAML シングルサインオンの設定の詳細については、[第 5 章, 「SAML のシングルサインオン」 \(ページ 29\)](#)を参照してください。

## アプリケーションの統合の匿名ユーザー

ライセンスされているアプリケーションの統合を保有している場合、Informatica Intelligent Cloud Services は CAI\_Anonymous\_<Organization\_ID> というシステムユーザーを作成します。アプリケーションの統合では、データ統合タスクを呼び出す匿名プロセスを開始する場合にこのユーザーを必要とします。

**重要:** データ統合タスクを呼び出す匿名プロセスを開始する必要がある場合は、アプリケーションの統合の匿名ユーザーを編集または削除しないでください。

データ統合タスクにカスタム権限を割り当てて、アプリケーション統合プロセスまたはガイドを介してデータ統合タスクを呼び出す場合は、次のいずれかのタスクを実行する必要があります。

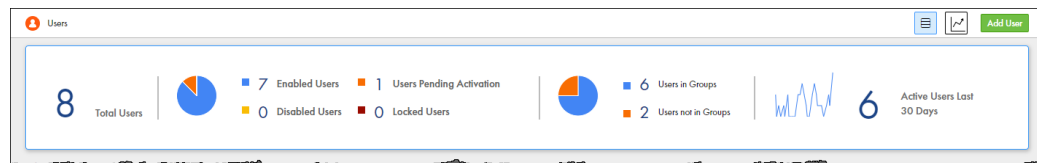
- アプリケーション統合の匿名ユーザーに、関連するデータ統合アセットの実行権限を付与します。
- アプリケーション統合の匿名ユーザーを、関連するデータ統合アセットの実行権限を持つユーザーグループに追加します。

## ユーザー統計

管理者ロールを持つか、または「読み取りユーザー」および「監査ログ - 表示」特権を持つ場合、組織のユーザー統計を表示できます。

**[ユーザー]** ページの統計領域には、組織内のユーザー数、ステータスごとのユーザー数、特定期間内のアクティブなユーザー数といった統計が表示されます。

次の図は、統計領域を示しています。



統計領域を使用して、**[ユーザー]** ページ上のユーザーをフィルタできます。例えば、ステータスが「アクティベーション保留」であるユーザーのみを表示するには、**[アクティベーション保留ユーザー]** をクリックします。すべてのユーザーをリストするには、**[合計ユーザー]** をクリックします。

管理者ロールを持つか、または「ユーザーの作成」および「監査ログ - 表示」特権を持つ場合、過去 7 日間、30 日間、または 90 日間の 1 日あたりのアクティブなユーザー数のグラフを表示できます。グラフを表示するには、**[チャートビュー]** をクリックし、適切な期間を選択します。その期間における各ユーザーのログイン日時がリストされたレポートをダウンロードすることもできます。

**[ユーザー]** ページのリストビューに戻るには、**[リストビュー]** をクリックします。

# ユーザーの詳細

ユーザー名、電子メール、ログイン設定、割り当てられたユーザーグループとロールなどのユーザーの詳細を [ユーザーの詳細] ページで設定できます。[ユーザーの詳細] ページを表示するには、管理者で [ユーザー] を選択し、ユーザー名をクリックします。

次の図は、[ユーザーの詳細] ページを示しています。

opatel

Save

Define the user account settings, including group and role assignments.

User Information

First Name: \*

Aditya

Last Name: \*

Patel

Job Title: \*

Reporter

Phone Number: \*

555-456-2301

Email: \*

apatel@info.com

Description:

Login Settings

Authentication: \*

Native

User Name: \*

opatel

Max Login Attempts:

10

Account Status:

Active

☐ Force password reset on next login

Assigned User Groups and Roles

| Enabled                             | Group Name       | Description                | Enabled                             | Role Name                            | Description                                                         |
|-------------------------------------|------------------|----------------------------|-------------------------------------|--------------------------------------|---------------------------------------------------------------------|
| <input type="checkbox"/>            | Development team | Group for development team | <input type="checkbox"/>            | Admin                                | Role for performing administrative tasks for an organization. Ha... |
| <input checked="" type="checkbox"/> | Reporting team   | Group for reporting team   | <input type="checkbox"/>            | Application Integration Business ... | Role used for business managers                                     |
|                                     |                  |                            | <input type="checkbox"/>            | Application Integration Data Vie...  | Role used for granting access for data                              |
|                                     |                  |                            | <input type="checkbox"/>            | Data Integration Data Previewer      | Role to preview data                                                |
|                                     |                  |                            | <input type="checkbox"/>            | Data Integration Task Executor       | Role to run Data Integration tasks                                  |
|                                     |                  |                            | <input type="checkbox"/>            | Deployer                             | Role used by deployer                                               |
|                                     |                  |                            | <input type="checkbox"/>            | Designer                             | Role for creating assets, tasks, and processes. Can configure co... |
|                                     |                  |                            | <input type="checkbox"/>            | Developer                            | Role for development team                                           |
|                                     |                  |                            | <input type="checkbox"/>            | Monitor                              | Role used for application monitor                                   |
|                                     |                  |                            | <input type="checkbox"/>            | Operator                             | Role used for monitoring execution environments                     |
|                                     |                  |                            | <input checked="" type="checkbox"/> | Reporter                             | Role for reporting team                                             |
|                                     |                  |                            | <input type="checkbox"/>            | Service Consumer                     | Role for running tasks, taskflows, and processes.                   |

ユーザーに対して次の詳細を構成できます。

## ユーザー情報

以下の表に、ユーザー情報を示します。

| プロパティ | 説明                                                                                                 |
|-------|----------------------------------------------------------------------------------------------------|
| 名     | ユーザーの下の名前。                                                                                         |
| 姓     | ユーザーの姓。                                                                                            |
| 役職    | ユーザーの役職。                                                                                           |
| 電話番号  | ユーザーの電話番号。                                                                                         |
| 電子メール | ユーザーの電子メールアドレス。<br>次の形式で有効な電子メールアドレスを指定する必要があります: <local_part>@<domain><br>例: jsmith@mycompany.com |
| 説明    | ユーザーの説明（省略可能）。                                                                                     |

## ログイン設定

以下の表に、ログイン設定を示します。

| プロパティ                                         | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 認証                                            | <p>認証方法。次のいずれかの値を指定できます。</p> <ul style="list-style-type: none"> <li>- ネイティブ。ユーザーは Informatica Intelligent Cloud Services によって認証されます。ユーザーは Informatica Intelligent Cloud Services の URL からログインします。</li> <li>- Salesforce。ユーザーは Salesforce または Salesforce アプリケーションからサインインし、Salesforce によって認証されます。</li> <li>- Azure SSO。ユーザーは Microsoft Azure からサインインし、Microsoft Azure によって認証されます。</li> <li>- IDP と SAML。ユーザーは SAML ID プロバイダからサインインし、SAML ID プロバイダによって認証されます。</li> </ul>                                                                                                                                                                                                                      |
| 検証コード使用のアクティブ化/<br>Salesforce OAuth 使用のアクティブ化 | <p>Salesforce ユーザーのアカウントのアクティブ化方法。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"> <li>- 検証コード使用のアクティブ化。ユーザーが Salesforce アプリケーションから Informatica Intelligent Cloud Services にサインインする場合は、このオプションを選択します。</li> </ul> <p>このオプションを選択すると、ユーザーは検証コードが含まれる電子メールを受信します。このユーザーが Salesforce にログインするとユーザーアカウントがアクティブ化され、Salesforce アプリが開くので、検証コードを入力します。</p> <ul style="list-style-type: none"> <li>- Salesforce OAuth 使用のアクティブ化。Salesforce OAuth を使用してユーザーアカウントをアクティブ化するには、このオプションを選択します。</li> </ul> <p>このオプションを選択すると、ユーザーは【アカウントの確認】リンクが含まれる電子メールを受信します。このユーザーが【アカウントの確認】リンクをクリックして Salesforce のユーザー名およびパスワードを入力すると、ユーザーアカウントがアクティブ化されます。</p> <p>これらのオプションは認証方法が Salesforce の場合に表示されます。</p> |
| 環境                                            | <p>Salesforce 組織環境。プロダクションまたはサンドボックスです。</p> <p>このオプションは、ユーザーのアクティブ化方法が Salesforce OAuth の場合に表示されます。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| ユーザー名                                         | <p>Informatica Intelligent Cloud Services のユーザー名。Informatica Intelligent Cloud Services の組織内で一意である必要があります。ユーザーの保存後に名前を変更する事は出来ません。</p> <p>このプロパティは、認証方法がネイティブである場合に表示されます。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Salesforce のユーザー名                             | <p>Salesforce のユーザー名。Informatica Intelligent Cloud Services の組織内で一意である必要があります。ユーザーの保存後に名前を変更する事は出来ません。</p> <p>Salesforce ユーザーの場合、Informatica Intelligent Cloud Services ユーザー名は、Informatica Intelligent Cloud Services の組織内でこの名前がすでに使用されていない限り、Salesforce ユーザー名と同じです。名前がすでに使用されている場合、Informatica Intelligent Cloud Services は、「Salesforce」、「Salesforce1」、「Salesforce2」などの文字列を Salesforce ユーザー名の最後に追加し、Informatica Intelligent Cloud Services の一意のユーザー名を形成します。</p> <p>このプロパティは、認証方法が Salesforce である場合に表示されます。</p>                                                                                                                                                                            |

| プロパティ                 | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Azure ユーザー名           | <p>Microsoft Azure ユーザー名 Informatica Intelligent Cloud Services の組織内で一意である必要があります。ユーザーの保存後に名前を変更する事は出来ません。</p> <p>Microsoft Azure ユーザーの場合、Informatica Intelligent Cloud Services ユーザー名は、Informatica Intelligent Cloud Services の組織内でこの名前がすでに使用されていない限り、Azure ユーザー名と同じです。名前がすでに使用されている場合、Informatica Intelligent Cloud Services は、「.Azure」、「.Azure1」、「.Azure2」などの文字列を Azure ユーザー名の最後に追加し、Informatica Intelligent Cloud Services の一意のユーザー名を形成します。</p> <p>このプロパティは、認証方法が Azure SSO である場合に表示されます。</p>                                                      |
| SAML ユーザー名            | <p>SAML ユーザー名。Informatica Intelligent Cloud Services の組織内で一意である必要があります。ユーザーの保存後に名前を変更する事は出来ません。</p> <p>SAML ユーザーの場合、Informatica Intelligent Cloud Services ユーザー名は、Informatica Intelligent Cloud Services の組織内でこの名前がすでに使用されていない限り、SAML 名前識別子と同じです。名前がすでに使用されている場合、Informatica Intelligent Cloud Services は、「.SAML」、「.SAML1」、「.SAML2」などの文字列を SAML 名前識別子の最後に追加し、Informatica Intelligent Cloud Services の一意のユーザー名を形成します。</p> <p>このプロパティは、認証方法が SAML の IDP である場合に表示されます。</p>                                                                                |
| 最大ログイン試行回数            | <p>ロックアウトされるまでにユーザーが試行できるログインの最大試行回数。数値または「制限なし」を選択します。</p> <p>ロックアウトされている場合、ユーザーが [ログイン] ページの <b>【パスワードを忘れた場合】</b> リンクをクリックするか、組織管理者が <b>【ユーザー】</b> ページでユーザーをリセットすることができます。</p> <p>このプロパティは、認証方法がネイティブである場合に表示されます。</p>                                                                                                                                                                                                                                                                                                                               |
| アカウントステータス            | <p>アカウントのステータス。次のいずれかを指定します。</p> <ul style="list-style-type: none"> <li>- アクティベーション保留。ユーザーアカウントは作成またはリセットされていますが、ユーザーがまだアカウントをアクティブ化していません。</li> <li>- アクティブ。ユーザーアカウントが作成および検証されており、ユーザーは Informatica Intelligent Cloud Services にログインできます。</li> <li>- ロック状態。ネイティブユーザーアカウントに適用されます。ログイン試行の最大数を超えたため、アカウントがロックされています。ユーザーのロックを解除するには、ユーザーが [ログイン] ページの <b>【パスワードを忘れた場合】</b> リンクをクリックするか、管理者が <b>【ユーザー】</b> ページでユーザーをリセットすることができます。</li> <li>- 利用不可状態。ユーザーアカウントは管理者によって無効にされています。ユーザーは Informatica Intelligent Cloud Services にログインする事が出来ません。</li> </ul> |
| 次のログイン時にパスワードのリセットを強制 | <p>ユーザーが次回ログインしようとしたときに、ユーザーにパスワードのリセットを強制します。</p> <p>このプロパティは、認証方法がネイティブである場合に表示されます。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

### 割り当て済みのユーザーグループおよびロール

各ユーザーには、少なくとも 1 つのユーザーグループまたはロールを割り当てる必要があります。ユーザーグループまたはロールを割り当てるか、または削除するには、グループまたはロールを有効または無効にしてから、**【保存】** をクリックします。

グループをユーザーに割り当てると、そのグループに関連付けられているすべてのロールが有効になります。これらのロールを個別に削除することはできません。ロールを削除するには、グループを削除する必要があります。

## ユーザーの作成

【ユーザー】 ページでユーザーを作成します。ユーザーを作成すると、ユーザーステータスが認証方法に基づいて [アクティベーション保留] または [アクティブ] に設定されます。

1. 管理者で 【ユーザー】 を選択します。
2. 【ユーザーの追加】 をクリックします。
3. ユーザー情報を入力します。
4. 以下の手順でログイン設定を入力します。
  - a. 認証方法を選択します。
  - b. Salesforce ユーザーの場合は、検証コードまたは Salesforce OAuth を使用してユーザーアカウントをアクティブにするかどうかを指定します。
  - c. Informatica Intelligent Cloud Services のユーザー名、またはサードパーティの ID プロバイダシステムのユーザー名を入力します。

ネイティブユーザーの場合は、Informatica Intelligent Cloud Services のユーザー名を入力して下さい。Salesforce、Microsoft Azure、SAML のユーザーの場合は、サードパーティの ID プロバイダシステムのユーザー名を入力して下さい。

ユーザー名は、Informatica Intelligent Cloud Services 組織内で一意にする必要があります。ユーザーの作成後にユーザー名を変更する事は出来ません。
  - d. ネイティブユーザーの場合は、最大ログイン試行回数を選択します。
5. 【割り当て済みのユーザーグループおよびロール】 セクションで、ユーザーに割り当てるユーザーグループとロールを選択します。

ユーザーにシステム定義およびカスタムロールを割り当てることができます。グループを割り当てると、そのグループに関連付けられているすべてのロールがユーザーに継承されます。
6. 【保存】 をクリックします。

ユーザーを作成すると、ユーザーステータスが認証方法に基づいて次のように設定されます。

- ネイティブユーザーは [アクティベーション保留] に設定されます。ユーザーは、アカウントを確認するための電子メールを受信します。ユーザーが電子メール内の 【アカウントの確認】 リンクをクリックすると、パスワードとセキュリティの質問を設定するように求められます。設定が完了するとステータスが [アクティブ] に変わり、ユーザーは Informatica Intelligent Cloud Services にログイン出来るようになります。
- Salesforce ユーザーは [アクティベーション保留] に設定されます。

検証コードを使用してユーザーをアクティブ化すると、ユーザーは検証コードを使用して電子メールを受信します。このユーザーが Salesforce にログインするとユーザーアカウントがアクティブ化され、Salesforce アプリが開くので、検証コードを入力します。

Salesforce OAuth を使用してユーザーをアクティブ化すると、ユーザーは 【アカウントの確認】 リンクを使用して電子メールを受信します。このユーザーが 【アカウントの確認】 リンクをクリックして Salesforce のユーザー名およびパスワードを入力すると、ユーザーアカウントがアクティブ化されます。
- Microsoft Azure および SAML ユーザーは [アクティブ] に設定されます。ユーザーは、ユーザーの ID プロバイダを介してサインイン出来ます。

## サービスの割り当ておよび割り当て解除

ユーザーを作成すると、そのユーザーは組織のライセンスおよびユーザーのロールに基づいてサービスにアクセス出来るようになります。これらのサービスに対するユーザーのアクセスを制限出来ます。

ユーザーによる特定のサービスへのアクセスを許可または拒否するには、ユーザーに対してサービスを割り当てまたは割り当て解除します。【ユーザー】 ページで、ユーザーに対してサービスを割り当ておよび割り当て解除します。



サービスをユーザーに割り当てると、割り当てられたサービスが【**マイサービス**】ページに表示されます。ユーザーのロールでこのサービスが許可されていれば、このサービスにアクセスして使用出来ます。

サービスを割り当て解除すると、ユーザーの【**マイサービス**】ページにはサービスが表示されなくなります。ユーザーのロールに関係なく、ユーザーはサービスにアクセス出来ず使用する事も出来ません。

例えば、サービスコンシューマロールを持つアプリケーション開発者に対し、API ポータルは使用出来るがデータ統合やアプリケーションの統合は使用出来ないようにします。API ポータルサービスをユーザーに割り当て、データ統合サービスおよびアプリケーションの統合サービスを割り当て解除します。これにより、アプリケーション開発者の【**マイサービス**】ページには、データ統合サービスおよびアプリケーションの統合サービスが表示されなくなります。サービスコンシューマロールには上記サービスに関連する特権がありますが、アプリケーション開発者はこれらのサービスを使用出来ません。

1. 管理者で【**ユーザー**】を選択します。
2. ユーザーを含む行で【**アクション**】をクリックし、【**サービスの割り当て**】を選択します。
3. 【**サービスの割り当て**】ダイアログボックスでユーザーに割り当てるサービスを選択し、割り当て解除するサービスの選択を解除します。
4. 【**保存**】をクリックします。

## ユーザーの無効化

【**ユーザー**】ページでユーザーを無効にします。ユーザーを無効にすると、そのユーザーは Informatica Intelligent Cloud Services にログイン出来なくなります。

ユーザーを無効にする前に、そのユーザーがタスクまたはタスクフローをスケジュールしていない事を確認して下さい。タスクまたはタスクフローをスケジュールしているユーザーを無効にすると、スケジュール済みのジョブが失敗します。

ユーザーを無効にしても、そのユーザーは組織および Informatica Intelligent Cloud Services リポジトリに残ります。ユーザーの詳細を表示出来ませんが、編集する事は出来ません。ユーザーが作成または更新したアセットも、組織に残ります。【参照】ページの【作成者】および【更新者】列にユーザーが無効化されている事が表示されます。

1. 管理者で【**ユーザー**】を選択します。
2. 無効にするユーザーを含む行で【**アクション**】をクリックし、【**無効化**】を選択します。

## ユーザーのリセット

【**ユーザー**】ページでユーザーをリセットします。アカウントが無効になっているユーザーやアカウントがロックされているユーザーをリセット出来ます。ユーザーをリセットすると、ユーザーステータスが認証方法に基づいて【**アクティベーション保留**】または【**アクティブ**】に設定されます。

1. 管理者で【**ユーザー**】を選択します。
2. ユーザーを含む行で【**アクション**】をクリックし、【**リセット**】を選択します。

ユーザーをリセットすると、ユーザーステータスが認証方法に基づいて次のようにリセットされます。

- ネイティブユーザーは【**アクティベーション保留**】に設定されます。ユーザーは、アカウントを確認するための電子メールを受信します。ユーザーが電子メール内の【**アカウントの確認**】リンクをクリックすると、パスワードとセキュリティの質問をリセットするように求められます。これで、ユーザーが Informatica Intelligent Cloud Services にログイン出来るようになります。
- Salesforce ユーザーは【**アクティベーション保留**】に設定されます。



検証コードを使用してユーザーをアクティブ化すると、ユーザーは検証コードを使用して電子メールを受信します。このユーザーが Salesforce にログインするとユーザーアカウントがアクティブ化され、Salesforce アプリが開くので、検証コードを入力します。

Salesforce OAuth を使用してユーザーをアクティブ化すると、ユーザーは **【アカウントの確認】** リンクを使用して電子メールを受信します。このユーザーが **【アカウントの確認】** リンクをクリックして Salesforce のユーザー名およびパスワードを入力すると、ユーザーアカウントがアクティブ化されます。

- Microsoft Azure および SAML ユーザーは **【アクティブ】** に設定されます。ユーザーは、ユーザーの ID プロバイダを介してサインイン出来ます。

## ユーザーのスケジュール済みジョブの再割り当て

**【ユーザー】** ページでユーザーのスケジュール済みジョブを再割り当てします。スケジュール済みタスクまたはタスクフローのあるユーザーが組織を離れるときに、スケジュール済みジョブを再割り当てする必要がある場合があります。ユーザーを削除する前に、ユーザーのスケジュール済みジョブを再割り当てする必要があります。

スケジュール済みジョブの所有者は、スケジュール済みタスクまたはタスクフローを最後に保存した人です。例えば、組織でユーザー Arun がスケジュールを作成し、ユーザー Beth がマッピングタスクを作成し、スケジュールをタスクに割り当ててから、Chandra がタスクを更新して保存したとします。Chandra がこのスケジュール済みジョブの所有者になります。Chandra が組織を離れる場合、彼女のユーザーアカウントを削除する前に、彼女のスケジュール済みジョブを他のユーザーに再割り当てする必要があります。

1. 管理者で **【ユーザー】** を選択します。
2. ユーザーを含む行で **【アクション】** をクリックし、**【スケジュール済みジョブの再割り当て】** を選択します。
3. スケジュール済みジョブを再割り当てするユーザーを選択します。  
選択するユーザーはアクティブユーザーである必要があります。
4. **【再割り当て】** をクリックします。

## ユーザーの削除

**【ユーザー】** ページでユーザーを削除します。ユーザーを削除すると、そのユーザーは組織および Informatica Intelligent Cloud Services リポジトリから削除されます。

ユーザーを削除する前に、ユーザーのスケジュール済みジョブを別のユーザーに再割り当てする必要があります。

**注:** 削除したユーザーをリセットする事は出来ません。ユーザーアカウントを再びアクティブにする可能性がある場合は、ユーザーを削除するのではなく無効にしてください。

1. 管理者で **【ユーザー】** を選択します。
2. 削除するユーザーを含む行で **【アクション】** をクリックし、**【削除】** を選択します。
3. ユーザーがスケジュール済みタスクまたはタスクフローの所有者である場合、管理者によって、ジョブを別のユーザーに再割り当てするよう求めるプロンプトが表示されます。ジョブを再割り当てするユーザーを選択し、**【再割り当てして削除】** をクリックします。

ユーザーがスケジュール済みタスクまたはタスクフローを所有していない場合、管理者によってそのユーザーが削除されます。ユーザーがスケジュール済みタスクまたはタスクフローの所有者である場合、管理者によってジョブが再割り当てされ、そのユーザーが削除されます。

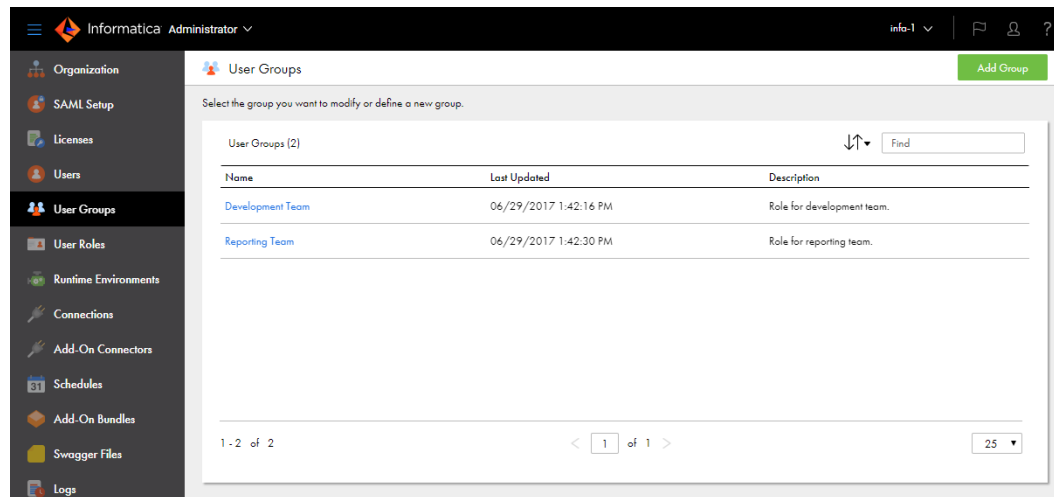
# ユーザグループ

ユーザグループは、すべてのメンバが同じタスクを実行し、さまざまなタイプのアセットに対して同じアクセス権を持つことができるユーザーのグループです。グループのメンバは、そのグループに割り当てたロールに基づいてタスクを実行し、アセットにアクセスできます。

管理者は、組織のユーザグループを構成できます。

[ユーザグループ] ページには、組織のすべてのユーザグループが一覧表示されます。[ユーザグループ] ページにアクセスするには、管理者で [ユーザグループ] を選択します。

次の図は、[ユーザグループ] ページを示しています。



ユーザグループに対して次のタスクを実行できます。

- グループの詳細を表示および編集する。
- グループを作成する。
- グループの名前を変更する。
- グループを削除する。

# ユーザーグループの詳細

グループ情報、割り当てられたロール、グループメンバなどユーザーグループに関する詳細を「グループの詳細」ページで設定できます。「グループの詳細」ページを表示するには、管理者で「ユーザーグループ」をクリックし、グループ名をクリックします。

次の図は、「グループの詳細」ページを示しています。

Reporting Team

Save

Select group members, and assign roles to define the application privileges.

Group Information

Name\*

Reporting Team

Description

Role for reporting team.

Assigned Roles

| Role Name                                    | Description                                                               |
|----------------------------------------------|---------------------------------------------------------------------------|
| <input type="checkbox"/> Admin               | Role that has ability to perform administrative tasks for an organization |
| <input type="checkbox"/> Designer            | Role that has ability to design data service tasks                        |
| <input type="checkbox"/> Developer           | Role that defines privileges for the development team.                    |
| <input checked="" type="checkbox"/> Reporter | Role that defines privileges for members of the reporting team.           |
| <input type="checkbox"/> Service Consumer    | Role that has ability to run tasks.                                       |

Group Members

Available Users

ajones  
cjackson  
dhoang  
dcusero  
janer  
jwang  
lroy

>

<

>>

<<

Assigned Users

apatel  
damith  
lsmith

ユーザーグループに対して次の詳細を構成できます。

| プロパティ       | 説明                                                                                                                                                                                                                                                                                    |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前          | 必須。ユーザーグループの名前。組織内で一意である必要があります。<br>グループ名は、作成後に変更できます。                                                                                                                                                                                                                                |
| 説明          | ユーザーグループの説明（省略可能）。                                                                                                                                                                                                                                                                    |
| 割り当て<br>ロール | グループのすべてのメンバに割り当てられているロール。各グループには、少なくとも 1 つの<br>ロールを割り当てる必要があります。<br>ロールを割り当てるか、または削除するには、グループまたはロールを有効または無効にして<br>から、 <b>保存</b> をクリックします。                                                                                                                                            |
| グループ<br>メンバ | グループに割り当てられているユーザー。<br>ユーザーをグループに割り当てるには、 <b>利用可能なユーザー</b> の一覧から <b>割り当てユーザー</b><br>の一覧にユーザーを移動し、 <b>保存</b> をクリックします。ユーザーをグループから削除す<br>るには、 <b>割り当てユーザー</b> の一覧から <b>利用可能なユーザー</b> の一覧にユーザーを移動し、<br><b>保存</b> をクリックします。<br>ユーザーをグループに割り当てると、そのグループに割り当てられているすべてのロールが自<br>動的に割り当てられます。 |

# ユーザーグループの作成

組織内の複数のユーザーが同じタスクを実行し、さまざまな種類のアセットに対して同じアクセス権を必要とする場合は、ユーザーグループを作成します。グループメンバは、そのグループに割り当てたロールに基づいてタスクを実行し、アセットにアクセスできます。「ユーザーグループ」ページでユーザーグループを作成します。

1. 管理者で、「ユーザーグループ」を選択します。

2. **【グループの追加】** をクリックします。
3. グループの名前を入力し、必要に応じて説明を入力します。  
グループ名は、組織内で一意である必要があります。
4. **【割り当てロール】** セクションで、グループに割り当てるロールを選択します。  
グループにシステム定義およびカスタムロールを割り当てることができます。ロールは、グループのすべてのメンバに適用されます。
5. 必要に応じて、ユーザーをグループに割り当てます。  
ユーザーをグループに割り当てするには、**【利用可能なユーザー】** の一覧から **【割り当てユーザー】** の一覧にユーザーを移動します。  
ユーザーを作成または編集するときに、ユーザーをグループに割り当てすることもできます。
6. **【保存】** をクリックします。

## ユーザーグループの名前変更

**【ユーザーグループ】** ページでユーザーグループの名前を変更します。また、ユーザーグループを編集したり、**【グループの詳細】** ページでグループ名を変更したりすることもできます。

1. 管理者で、**【ユーザーグループ】** を選択します。
2. ユーザーグループを含む行で **【アクション】** をクリックし、**【名前の変更】** を選択します。
3. 新しい名前を入力し、**【保存】** をクリックします。

## ユーザーグループの削除

**【ユーザーグループ】** ページでユーザーグループを削除します。

**ヒント:** Informatica Intelligent Cloud Services を中断なく継続して使用できるように、ユーザーグループを削除する前に、すべてのグループメンバが適切なロールを持っているか、または他のグループに割り当てられていることを確認します。

1. 管理者で、**【ユーザーグループ】** を選択します。
2. ユーザーグループを含む行で **【アクション】** をクリックし、**【削除】** を選択します。

## ユーザー設定の例

次の例は、ビジネスニーズに応じて Informatica Intelligent Cloud Services へのアクセスを制御するユーザーおよびユーザーグループを構成する方法を示しています。

ユーザーロールの詳細については、[第 9 章, 「ユーザーロール」 \(ページ 63\)](#) を参照してください。

開発チームにデータ統合でタスクとタスクフローの作成を依頼するとします。開発チームは、開発環境のサンプルデータを表示できるようにする必要がありますが、プロダクションデータへのアクセスは制限したいと考えています。

1. 開発チームの開発者ロールを作成します。タスクおよび関連アセットのすべての権限を持つロールを構成しますが、接続に対しては読み取り特権のみを設定します。
2. 開発チームのユーザーグループを作成し、開発チームのすべてのメンバをそのグループに追加します。

3. 開発チームグループに開発者ロールを割り当てます。
4. 可能であれば、サンプルデータへの開発接続を作成します。開発とプロダクションの両方の接続がある場合は、開発チームグループがこれらの接続に対する読み取り権限を持たないように、プロダクション接続を構成します。これにより、開発チームグループのユーザーが、タスクのプロダクション接続を使用できないようにします。
5. テストが完了し、タスクをプロダクション環境に移行する準備ができたなら、管理者または他の資格あるユーザーによって、プロダクション接続を使用するようにタスクが設定されるようにします。
6. 開発者ロールを編集し、タスクを実行する特権を削除します。タスクのタイプに対して開発が完了した場合は、タスクを読み取りおよび更新するための特権を削除することもできます。読み取り特権を削除すると、開発者ロールを持つユーザーが、プロダクションタスクに関する情報にアクセスできなくなります。

データ統合でタスクを実行する必要があるとしても、タスクを安全に設定する技術的な知識を持っていないレポートチームも存在します。

1. レポートチームのレポーターロールを作成します。タスクおよびタスクフローの読み取りと実行、およびスケジュールの読み取り、作成、および更新を行う特権を持つロールを構成します。組織内のアセットに対する特権を作成、更新、削除、または設定する権限を有効にしないでください。
2. レポートチームのユーザーグループを作成し、レポートチームのすべてのメンバをそのグループに追加します。
3. レポートチームグループにレポーターロールを割り当てます。

ロールとユーザーグループの割り当てやアクセス制御の設定を行うことができて、タスクを作成、編集、または実行できないセキュリティ管理者を指定するとします。

1. Security Administrator（セキュリティ管理者）という名前のカスタムロールを作成します。
2. Security Administrator（セキュリティ管理者）ロールを編集し、タスク、接続、およびスケジュールを作成、更新、削除、実行するための特権を除くすべての特権を付与します。
3. Security Administrator（セキュリティ管理者）ロールをセキュリティ管理者に割り当てます。

組織の管理者を簡単に追跡したいとします。

「組織の管理者」というユーザーグループを作成し、このグループに管理者ロールを割り当てます。組織のすべての管理者を、このグループに追加します。

組織では、OrderProcessing API を使用して大規模なサプライヤへの注文を管理します。この API は、CreateOrder、ApproveOrder、GetOrder を含むアプリケーションの統合のプロセスからなります。管理者は、ApproveOrder プロセスにアクセスできるユーザーを少数に制限する必要があります。

1. 承認者という名前のカスタムロールを作成します。承認者ロールのアプリケーション統合アセットに実行特権を設定します。
2. 注文承認者という名前のユーザーグループを作成します。
3. 承認者ロールを注文承認者グループに割り当てます。
4. サービスコンシューマロールを注文承認者グループに割り当てます。サービスコンシューマロールでプロセスにアクセスして呼び出すことができるように割り当てする必要があります。
5. ApproveOrder を呼び出すことができるユーザーを注文承認者グループに割り当てます。
6. ApproveOrder プロセスの許可ロールフィールドで、承認者を入力します。

ApproveOrder プロセスを呼び出すことができるのは、注文承認者グループのメンバだけです。

アプリケーションの統合開発者がアプリケーション統合コンソールの詳細なプロセスログの表示以外のすべての機能を実行できるようにしたいとします。

1. Custom\_Dev というロールを作成し、そのロールに次の特権を設定します。
  - a. アプリケーションの統合サービスを選択し、**【アセット】** タブに移動して、**【アプリケーション統合アセット】** のすべての CRUD 特権を有効にします。
  - b. **【機能】** タブに移動し、ロールに、開発、コンソール管理、アプリケーション統合アセットのパブリッシュ、アプリケーション統合コンソールの表示、アプリケーション統合デザイナの表示の各特権を追加します。
  - c. データ統合サービスを選択し、**【アセット】** タブに移動して、**【プロジェクト】** と **【フォルダ】** アセットのすべての CRUD 特権を有効にします。
2. Custom\_Dev ロールを開発者に割り当てます。

## 第 9 章

# ユーザーロール

ロールとは、ユーザーおよびグループへの割り当ての可能な特権の集まりです。すべてのユーザーがアセットにアクセスして組織内のタスクを実行できるようにするには、各ユーザーまたはユーザーグループに 1 つ以上のロールを割り当てます。

ロールは、さまざまなタイプのアセットとサービス特権に対する特権を定義します。例えば、デザイナーロールを持つユーザーは、ほとんどのタイプのデータ統合アセットに対する権限を作成、読み取り、更新、削除、および設定できます。ただし、サブ組織や監査ログなど、特定の管理者サービス機能にはアクセスできません。

管理者は、組織のロールを構成および割り当てることができます。

ユーザーによる割り当ての可能なロールには、次の種類があります。

### システム定義

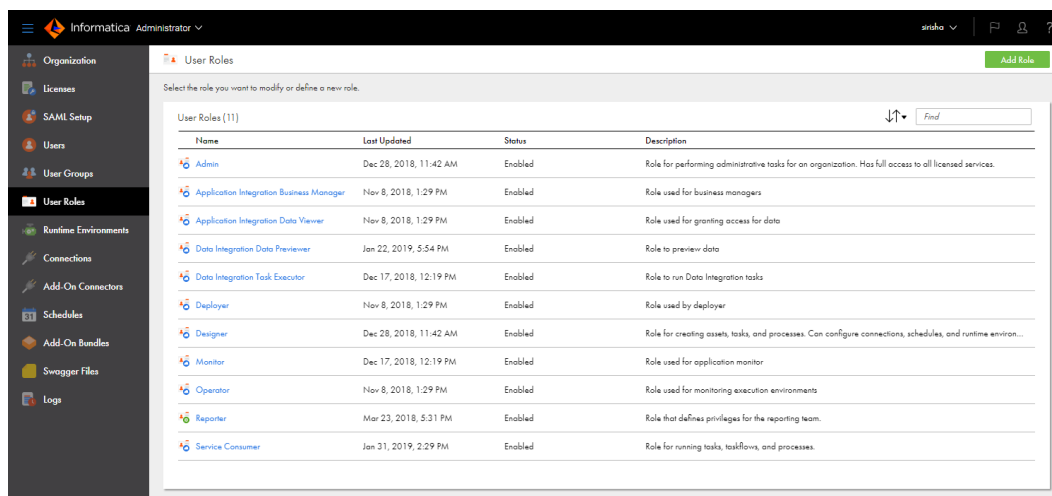
システム定義ロールは、組織で使用するサービスのアクセス特権を定義した定義済みのロールです。ユーザーおよびグループに割り当てることのできるシステム定義ロールは、組織のライセンスによって異なります。これらのシステム定義ロールを編集したり削除したりすることはできません。

### カスタムロール

カスタムロールは特権を個別に設定するために作成するロールです。カスタムロールを作成するには、適切なライセンスが必要です。カスタムロールは、ユーザーによる編集および削除が可能です。

**[ユーザーロール]** ページでは、システム定義のロールおよびカスタムロールの両方を表示できます。**[ユーザーロール]** ページには、組織内のすべてのロールの一覧が表示されます。**[ユーザーロール]** ページにアクセスするには、管理者で **[ユーザーロール]** を選択します。

次の図は、**[ユーザーロール]** ページを示しています。



| Name                                     | Last Updated           | Status  | Description                                                                                                  |
|------------------------------------------|------------------------|---------|--------------------------------------------------------------------------------------------------------------|
| Admin                                    | Dec 28, 2018, 11:42 AM | Enabled | Role for performing administrative tasks for an organization. Has full access to all licensed services.      |
| Application Integration Business Manager | Nov 8, 2018, 1:29 PM   | Enabled | Role used for business managers                                                                              |
| Application Integration Data Viewer      | Nov 8, 2018, 1:29 PM   | Enabled | Role used for granting access for data                                                                       |
| Data Integration Data Previewer          | Jan 22, 2019, 5:54 PM  | Enabled | Role to preview data                                                                                         |
| Data Integration Task Executor           | Dec 17, 2018, 12:19 PM | Enabled | Role to run Data Integration tasks                                                                           |
| Deployer                                 | Nov 8, 2018, 1:29 PM   | Enabled | Role used by deployer                                                                                        |
| Designer                                 | Dec 28, 2018, 11:42 AM | Enabled | Role for creating assets, tasks, and processes. Can configure connections, schedules, and runtime environ... |
| Monitor                                  | Dec 17, 2018, 12:19 PM | Enabled | Role used for application monitor                                                                            |
| Operator                                 | Nov 8, 2018, 1:29 PM   | Enabled | Role used for monitoring execution environments                                                              |
| Reporter                                 | Mar 23, 2018, 5:31 PM  | Enabled | Role that defines privileges for the reporting team.                                                         |
| Service Consumer                         | Jan 31, 2019, 2:29 PM  | Enabled | Role for running tasks, workflows, and processes.                                                            |

[ステータス] 列は、組織に対してロールが有効か無効かを示します。ライセンスの有効期限が切れると、ロールは無効になります。

複数のロールをユーザーまたはユーザーグループに割り当てることができます。複数のロールを割り当てる場合、そのユーザーまたはグループはそれらのロールすべてに関連付けられたアクセス特権を継承します。

## ロールの詳細

[ロールの詳細] ページには、ロールに関連付けられているアセットや機能特権など、ロールに関する情報が表示されます。システム定義ロールの場合、ロール情報や特権を表示出来ます。カスタムロールの場合、ロール情報および割り当てられているアセットや機能特権を表示および変更出来ます。

[ロールの詳細] ページを表示するには、管理者で **[ユーザーロール]** を選択し、ロール名をクリックします。次の図に、[ロールの詳細] ページを示します。

Reporter

Save

Set the privileges for users and groups assigned to the role. Configure privileges separately for each service.

Role Information

Role Name: \* Reporter

Description: Role that defines privileges for the reporting team.

Services: Data Integration

Assets Features

| Asset Type                  | Create                   | Read                                | Update                   | Delete                   | Run                                 | Set Permission           |
|-----------------------------|--------------------------|-------------------------------------|--------------------------|--------------------------|-------------------------------------|--------------------------|
| Business Service Definition | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> |
| Cloud Content               | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> |
| Connection                  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> |
| Data Masking Task           | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Fixed-Width File Format     | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> |
| Folder                      | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> |
| Hierarchical Schema         | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Intelligent Structure Task  | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Linear Taskflow             | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

各ロールには、次のプロパティがあります。

### 役割名

ロールの名前。カスタムロールの場合、ロール名を変更出来ます。

### 説明

ロールの説明。カスタムロールの場合、ロールの説明を変更出来ます。

### サービス

特権が有効または無効になっているサービスの名前。サービスを選択して、そのサービスに関連付けられているアセットや機能特権を表示します。



サービスのライセンスが期限切れの場合、そのサービスは無効とマークされます。無効なサービスに関連付けられているアセットや機能特権は表示出来ません。

## アセット

選択したサービスのアセット特権。アセット特権は、さまざまなタイプのアセットへのアクセスを制御します。例えば、サービスコンシューマロールを持つユーザーは、データ統合のマッピングを表示および実行することは出来ませんが、マッピングに対する権限を作成、更新、削除、または設定することはできません。

以下の表に、アセット特権を示します。

| 特権    | 説明                                                                                                                                                                         |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 作成    | 選択したタイプのアセットを作成します。Secure Agent の場合、この特権により、ユーザーは Secure Agent をダウンロードしてインストールできます。<br>自動的に付与される読み取りおよび更新の特権が必要です。                                                         |
| 読み取り  | 選択したタイプのアセットを開きます。タスクの場合、この特権によって、ユーザーはタスク内の接続またはスケジュールを使用することもできます。                                                                                                       |
| 更新    | 選択したタイプのアセットを編集します。<br>自動的に付与される読み取り特権が必要です。                                                                                                                               |
| 削除    | 選択したタイプのアセットを削除します。                                                                                                                                                        |
| 実行    | 選択したタイプのアセットを実行します。<br>データ統合サービスでは、ユーザーはマッピング、タスク、またはタスクフローを実行出来ます。また、ユーザーはマッピング、タスク、またはタスクフローのインスタンスを監視、停止、および再起動出来ます。<br>Hub の統合サービスでは、ユーザーはパブリケーションまたはサブスクリプションを実行出来ます。 |
| 権限の設定 | 選択したタイプのアセットの権限を構成します。例えば、この特権をプロジェクトに付与すると、そのロールを持つユーザーはプロジェクトを選択し、選択したプロジェクトの権限を他のユーザーとグループが読み取り、更新、削除、または変更できるようにすることが出来ます。<br>この特権を設定するには、組織に適したライセンスが必要です。            |

特権がアセットタイプに適用されない場合、その特権は無効になります。例えば、フォルダに対する実行特権は無効になっています。

カスタムロールの場合、サービスが無効になっていない限り、そのサービスのアセット特権を有効または無効にすることが出来ます。

## 機能

選択したサービスの機能特権。機能特権は、サービスの機能を使用する権限を制御する一般的な特権です。例えば、デザイナロールを持つユーザーは、データ統合でデータカタログ検出を実行することは出来ませんが、データをプレビューすることはできません。

カスタムロールの場合、サービスが無効になっていない限り、そのサービスの機能特権を有効または無効にすることが出来ます。

## アプリケーションの統合機能特権

カスタムロールを作成するにはアプリケーションの統合機能特権を使用します。

**重要:** ユーザーのロールにフォルダとプロジェクトのアセット特権を割り当てる必要があります。これを行うには、データ統合サービスを選択し、フォルダアセットとプロジェクトアセットの CRUD オプションを選択します。

カスタムロールを作成する場合は、次のアプリケーションの統合機能特権を有効化できます。

### 管理

ユーザーにアプリケーションの統合とアプリケーション統合コンソールへの完全な設計時およびランタイム管理者アクセスを提供したい場合は、ロールに管理特権を割り当てます。

管理特権を持つユーザーは次のタスクを実行できます。

- すべてのアプリケーションの統合アセットの表示、作成、更新、削除。
- サービスの管理と開始。
- 実行中のサービスの停止。
- デプロイされたプロセスのインスタンスとログの表示。
- アプリケーション統合コンソールへのプロセス開発者 BPR ファイルのデプロイ。
- デプロイされたカタログの管理。
- 複数のシステム全体のデプロイされた WSDL ファイルの表示。
- プロセスサーバーのメトリックの表示。

**注:** アプリケーションの統合管理特権は、ユーザーに Informatica Intelligent Cloud Services 全体の管理特権を付与するものではありません。例えば、アプリケーションの統合管理特権のみを持つユーザーは、サブ組織を作成することはできません。

### コンソール管理

ユーザーにアプリケーション統合コンソールへのほぼ完全なアクセスを提供したい場合は、ロールにコンソール管理特権を割り当てます。

コンソール管理特権を持つユーザーは次のタスクを実行できます。

- デプロイされたプロセスのインスタンスの表示。
- 実行中のサービスの停止。
- デプロイされたプロセス開発者 BPR とカタログの表示。
- 複数のシステム全体のデプロイされた WSDL ファイルの表示。
- プロセスサーバーのメトリックの表示。

コンソール管理特権を持つユーザーは BPR ファイルをデプロイできません。

### データビューア

アプリケーション統合コンソールで詳細なログにアクセスする必要があるユーザーにはデータビューア特権を割り当てます。

例えば、組織全体のログを参照する必要があるユーザーにこの特権を割り当てることができます。開発者にこのロールを普段から割り当てないほうがよいでしょう。

**注:** 詳細なログを取得するには、プロセスログレベルを [詳細] に設定する必要があります。

### 開発

場合によってプロセスをデバッグする必要がある開発者には開発特権を割り当てます。

開発特権を持つユーザーは次のタスクを実行できます。

- すべてのアプリケーションの統合アセットの表示、作成、更新、削除。
- サービスの開始。
- アプリケーション統合コンソールの [Detailed Process Instance (プロセスインスタンス詳細)] ページの表示。
- プロセスインスタンスの管理。

## 監視

アプリケーション統合コンソールの詳細なログ以外のすべての部分を表示する必要があるユーザーには、監視特権を割り当てます。

## アプリケーション統合アセットのパブリッシュ

アプリケーションの統合プロセス、ガイド、接続、サービスコネクタをパブリッシュする必要があるユーザーには、アプリケーション統合アセットのパブリッシュ特権を割り当てます。

## アプリケーション統合コンソールの表示

アプリケーション統合コンソールサービスにアクセスする必要があるユーザーには、アプリケーション統合コンソールの表示特権を割り当てます。アプリケーション統合コンソールの操作を含む特権を持つロールには、この特権を割り当てる必要があります。

例えば、開発特権と共にこの特権を割り当てる必要があります。

## アプリケーション統合デザイナの表示

アプリケーションの統合サービスにアクセスする必要があるユーザーには、アプリケーション統合デザイナの表示特権を割り当てます。アプリケーション統合コンソールの操作を含む特権を持つロールには、この特権を割り当てる必要があります。

例えば、アプリケーション統合アセットのパブリッシュ特権と共にこの特権を割り当てる必要があります。

# Data Quality の機能特権

ユーザーにデータ品質アセットでのプレビュー機能へのアクセス権を付与するには、Data Quality の機能特権を使用します。カスタムロールを作成するときに、この機能特権を有効化できます。

Data Quality の次の機能特権を有効にできます。

## データプレビュー - デクシヨナリ

次の場合にユーザーがデクシヨナリのコンテンツを表示できるようにするには、ロールのデータプレビュー - デクシヨナリ特権を有効にします。

- ユーザーが [エクスプローラ] ページからデクシヨナリを開いたとき。
- ユーザーが Data Quality アセットでデクシヨナリを選択したとき。

## データプレビュー - テストパネル

ユーザーが Data Quality アセットのテストパネルでデータを表示できるようにするには、ロールのデータプレビュー - テストパネル特権を有効にします。

管理者ロールとデザイナロールでは、Data Quality の機能特権がデフォルトで有効になっています。

**注:** デクシヨナリアセットのデータプレビュー - デクシヨナリ機能特権と読み取り特権は、互いに独立して機能します。読み取り特権があると、[エクスプローラ] ページからデクシヨナリを開くことができます。データプレビュー - デクシヨナリ特権があると、デクシヨナリデータを表示できます。

データプレビュー - デクシヨナリ特権なしでデクシヨナリを開くと、Data Quality によりデータを表示するための十分な権限がないことを通知するメッセージが表示されます。

# システム定義のロール

Informatica Intelligent Cloud Services には、ユーザーまたはユーザーグループに割り当てることができるシステム定義のロールが用意されています。システム定義のロールを変更または削除することはできません。

ユーザーおよびグループに割り当てることができるシステム定義ロールは、組織のライセンスによって異なります。例えば、組織にアプリケーションの統合または API Manager へのアクセス権がない場合、デプロイ、アプリケーション統合ビジネスマネージャ、アプリケーション統合データビューア、またはオペレータロールを組織のユーザーまたはグループに割り当てすることはできません。

実行する必要があるタスクに基づいて、ユーザーおよびグループにシステム定義ロールを割り当てます。

システム定義のロールには、次の 2 つのタイプがあります。

- クロスサービスロールは複数のサービスにまたがるアクセス特権を定義します。
- サービス固有のロールは、1 つのサービス、または密接な関連のあるサービスのグループのアクセス特権を定義します。

## クロスサービスロール

クロスサービスロールは、複数のサービスにまたがるアクセス権限を定義するシステム定義ロールです。

例えば、デザイナーロールを持つユーザーはデータ統合でアセットとタスクを作成し、Cloud Integration Hub でアセットを作成し、アプリケーションの統合でプロセスを作成できます。また、アプリケーション統合コンソールにもアクセスできます。モニタロールを持つユーザーは、データ統合ジョブ、Cloud Integration Hub アセット、およびアプリケーションの統合プロセスインスタンスを監視できます。

次のロールがクロスサービスロールです。

- 管理
- データ統合プレビューア
- デプロイ
- デザイナー
- モニタ
- 演算子
- サービスコンシューマ

以下の表に、各クロスサービスロールでアクセスできるサービスを示します。

|             | 管理者ロール | データ統合データプレビューアロール* | デプロイロール | デザイナーロール | モニタロール | オペレータロール | サービスコンシューマロール |
|-------------|--------|--------------------|---------|----------|--------|----------|---------------|
| 管理者         | X      | -                  | -       | X        | X      | -        | X             |
| API Manager | X      | -                  | X       | -        | -      | -        | X             |
| API Portal  | X      | -                  | -       | -        | -      | -        | X             |
| アプリケーションの統合 | X      | -                  | X       | X        | X      | X        | X             |

|                                                                                                                                                      | 管理者ロール | データ統合データプレビューアロール* | デプロイヤロール | デザイナーロール | モニターロール | オペレーターロール | サービスコンシューマロール |
|------------------------------------------------------------------------------------------------------------------------------------------------------|--------|--------------------|----------|----------|---------|-----------|---------------|
| アプリケーション統合コンソール                                                                                                                                      | X      | -                  | X        | X        | X       | X         | X             |
| B2B Gateway                                                                                                                                          | X      | -                  | -        | X        | X       | -         | -             |
| B2B パートナーポータル                                                                                                                                        | X      | -                  | -        | -        | -       | -         | -             |
| データ統合                                                                                                                                                | X      | -                  | -        | X        | X       | -         | X             |
| Data Quality                                                                                                                                         | X      | -                  | X        | X        | X       | X         | X             |
| データプロファイリング                                                                                                                                          | X      | -                  | -        | X        | X       | X         | -             |
| Integration Hub                                                                                                                                      | X      | -                  | -        | X        | X       | -         | -             |
| モニタ                                                                                                                                                  | X      | -                  | -        | X        | X       | -         | -             |
| オペレーションインサイト                                                                                                                                         | X      | -                  | -        | -        | -       | X         | -             |
| * データ統合プレビューアロールは、ユーザーがデータ統合およびデータプロファイリングでデータをプレビューできるようにする補足ロールです。サービスに対するアクセスは提供しません。このロールを、ユーザーがデータ統合またはデータプロファイリングにアクセスできるようにする別のロールと一緒に割り当てます。 |        |                    |          |          |         |           |               |

上記の表で「X」は当該ロールを持つユーザーがサービスにアクセスできる事を意味します。例えば、管理者ロールを持つユーザーは、すべてのサービスにアクセスできます。

## クロスサービスロールのアクセス特権

Informatica Intelligent Cloud Services のさまざまなサービスへの特権アクセスが必要なユーザーにはクロスサービスロールを割り当てます。各クロスサービスロールは異なるアクセス特権を提供します。

クロスサービスロールには次のアクセス特権があります。

### 管理者

管理者ロールを持つユーザーは、ライセンス供与されたすべてのサービスにフルアクセスできます。管理者ロールとサービスコンシューマロールの両方が割り当てられている場合は、組織内のすべてのタスクを実行できます。

ベストプラクティスは、1 つまたは 2 つの信頼されたユーザーに管理者ロールを割り当て、すべてのアセットタイプに対する完全な権限を持つ管理ユーザーグループにそのユーザーを割り当てることです。これらのユーザーは代替の組織の管理者として活動し、アクセス制御や組織のセキュリティの問題のトラブルシューティングを支援することができます。

**注:** OAuth 2.0 クライアント管理のためのすべての特権を含めて、API Manager サービスへのフルアクセスを提供するには、ユーザーに管理者ロールとサービスコンシューマロールの両方を割り当てます。

## データ統合プレビューア

データ統合プレビューアロールを持つユーザーは、マッピングまたはタスクで使用するソース、ターゲット、またはルックアップオブジェクトを選択したときに、データをプレビューできます。データ統合また、プロファイルを作成するとき、またはプロファイル結果をデータプロファイリングで表示するときに、ソースオブジェクトデータを表示することもできます。

データ統合プレビューアロールは補足的なロールです。ユーザーがデータ統合およびデータプロファイリングにアクセスできるようにするために、このロールは、デザイナロールなどの別のロールと一緒に割り当てます。

## デプロイヤ

デプロイヤロールを持つユーザーはアプリケーションの統合アセットをデプロイでき、API Manager から API を管理できます。このロールはデプロイアクセスが一般的に禁止されているプロダクション環境で割り当ててください。

デプロイヤ特権を持つユーザーは、Data Quality でアセットを表示できます。

**注:** OAuth 2.0 クライアント管理のためのすべての特権を含めて、API Manager サービスへのフルアクセスを提供するには、ユーザーにデプロイヤロールとサービスコンシューマロールの両方を割り当てます。

以下の表に、デプロイヤロールを持つユーザーがアクセスできるサービスと、各サービスに関連付けられているアクセス特権の一覧を示します。

| サービス            | アクセス特権                                                                                                                     |
|-----------------|----------------------------------------------------------------------------------------------------------------------------|
| API Manager     | サービスコンシューマロールも割り当てられている場合、このサービスにフルアクセスでき、OAuth 2.0 クライアント管理特権を持ちます。                                                       |
| アプリケーションの統合     | アセットの詳細を表示できます。                                                                                                            |
| アプリケーション統合コンソール | [プロセス]、[ログ]、[サーバー設定]、[デプロイ済みアセット]、[リソース] の各ページでアセットをデプロイし、設定を表示できます。プロセス開発者が生成したオーケストレーションアーティファクト（BPR）をアップロードおよびデプロイできます。 |
| Data Quality    | アセットの詳細を表示できます。                                                                                                            |

## デザイナ

デザイナロールを持つユーザーは、アセット、タスク、およびプロセスを作成できます。接続、スケジュール、およびランタイム環境を設定できます。また、組織のジョブおよびエラスティッククラスタを監視できます。

以下の表に、デザイナロールを持つユーザーがアクセスできるサービスと、各サービスに関連付けられているアクセス特権の一覧を示します。

| サービス            | アクセス特権                                                                                                                                                                                                    |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 管理者             | 接続、ランタイム環境、スケジュール、Swagger ファイル、およびエラスティック構成を設定できます。アドオンコネクタをインストールすること、およびアドオンバンドルをアンインストールすることができます。Secure Agent サービスのアップグレード設定を表示できます。ファイルサーバーを開始および停止すること、プロキシサーバーを設定すること、および他のファイルサーバー設定を表示することができます。 |
| アプリケーションの統合     | このサービスにフルアクセスできます。                                                                                                                                                                                        |
| アプリケーション統合コンソール | サーバー設定プロパティを除くすべての設定を表示および編集できます。                                                                                                                                                                         |
| B2B Gateway     | このサービスにフルアクセスできます。                                                                                                                                                                                        |
| データ統合           | このサービスにフルアクセスできます。                                                                                                                                                                                        |
| Data Quality    | このサービスにフルアクセスできます。                                                                                                                                                                                        |
| Data Profiling  | このサービスにフルアクセスできます。                                                                                                                                                                                        |
| Integration Hub | このサービスにフルアクセスできます。                                                                                                                                                                                        |
| モニタ             | このサービスにフルアクセスできます。                                                                                                                                                                                        |

## モニタ

モニタロールを持つユーザーは、組織のデータ統合ジョブ、Cloud Integration Hub アセット、Data Quality アセット、およびアプリケーションの統合プロセスインスタンスを監視できます。

以下の表に、モニタロールを持つユーザーがアクセスできるサービスと、各サービスに関連付けられているアクセス特権の一覧を示します。

| サービス            | アクセス特権                                                                                                        |
|-----------------|---------------------------------------------------------------------------------------------------------------|
| 管理者             | Secure Agent サービスのスケジュールおよびアップグレード設定を表示できます。ファイルサーバーを開始および停止すること、プロキシサーバーを設定すること、および他のファイルサーバー設定を表示することができます。 |
| アプリケーションの統合     | アセットの詳細を表示できます。                                                                                               |
| アプリケーション統合コンソール | 設定を表示できます。                                                                                                    |
| B2B Gateway     | アセットの詳細を表示できます。                                                                                               |
| データ統合           | アセットの詳細を表示できます。                                                                                               |
| Data Quality    | アセットの詳細を表示できます。                                                                                               |

| サービス            | アクセス特権                                             |
|-----------------|----------------------------------------------------|
| Data Profiling  | アセットの詳細を表示できます。                                    |
| Integration Hub | アセットの詳細を表示できます。                                    |
| モニタ             | データ統合ジョブとジョブの詳細を表示できます。エクスポートジョブとインポートジョブは表示できません。 |

## オペレータ

オペレータはプロセスの実行管理とプロセスサーバーの設定更新を担当します。オペレータロールを持つユーザーはアセットの詳細を表示できますが、それらを変更することはできません。プロセスインスタンスの管理と一部の運用サーバーパラメータの変更を行うことができます。

以下の表に、オペレータロールを持つユーザーがアクセスできるサービスと、各サービスに関連付けられているアクセス特権の一覧を示します。

| サービス            | アクセス特権                                                                                                                 |
|-----------------|------------------------------------------------------------------------------------------------------------------------|
| アプリケーションの統合     | アセットの詳細を表示できます。                                                                                                        |
| アプリケーション統合コンソール | プロセスサーバーの設定と一部のクラウドサーバーの設定を表示および編集できます。例えば、オペレータロールを持つユーザーは警告サービスを作成できますが、テナントの詳細は表示できません。                             |
| Data Quality    | アセットの詳細を表示できます。                                                                                                        |
| Data Profiling  | アセットの詳細を表示できます。                                                                                                        |
| オペレーションインサイト    | クラウドおよびドメインインフラストラクチャを表示できます。ドメインおよびインフラストラクチャである <i>Secure Agent</i> のアラート設定を編集できます。ドメインインフラストラクチャを編集できます（ドメインの登録など）。 |

## サービスコンシューマ

サービスコンシューマロールを持つユーザーはタスク、タスクフロー、プロセスを実行できますが、アセットの作成と編集はできません。API を通してデータ統合ジョブとアプリケーションの統合プロセスを実行する必要があるユーザーにこのロールを割り当てます。

**注:** API Manager サービスへのフルアクセスを提供するには、ユーザーにサービスコンシューマロールとデプロイヤロールの両方を割り当てるか、ユーザーにサービスコンシューマロールと管理者ロールの両方を割り当てます。



以下の表に、サービスコンシューマロールを持つユーザーがアクセスできるサービスと、各サービスに関連付けられているアクセス特権の一覧を示します。

| サービス         | アクセス特権                                                                                                                      |
|--------------|-----------------------------------------------------------------------------------------------------------------------------|
| 管理者          | Secure Agent サービスのスケジュール、Swagger ファイル、およびアップグレード設定を表示できます。ファイルサーバーを開始および停止すること、プロキシサーバーを設定すること、および他のファイルサーバー設定を表示することができます。 |
| API Manager  | デプロイヤロールまたは管理者ロールも割り当てられている場合は、このサービスにフルアクセスできます。                                                                           |
| API Portal   | このサービスにフルアクセスできます。                                                                                                          |
| アプリケーションの統合  | アプリケーションの統合プロセスを呼び出すことができます。                                                                                                |
| データ統合        | タスクの表示、タスクの実行、マッピングのテスト実行、タスクフローの実行、およびワークフロー XML のダウンロードを行うことができます。                                                        |
| Data Quality | アセットの詳細を表示できます。                                                                                                             |

## サービス固有のロール

サービス固有のロールは、1つのサービス、または密接な関連のあるサービスのグループのアクセス特権を定義するシステム定義ロールです。例えば、アプリケーションの統合のサービス固有のロールでは、アプリケーションの統合とアプリケーション統合コンソールの両方へのアクセスが提供されます。

複数のサービスにアクセスする必要がないユーザーにはサービス固有のロールを割り当てます。サービス固有のロールには、特権が適用されるサービスに基づいてさまざまなアクセス特権があります。

次の表に、ロールを使用するサービスごとのサービス固有のロールを示します。

| サービス                | サービス固有のロール                                                                                               |
|---------------------|----------------------------------------------------------------------------------------------------------|
| アプリケーションの統合         | アプリケーション統合ビジネスマネージャ<br>アプリケーション統合データビューア                                                                 |
| データ統合               | データ統合タスク実行者                                                                                              |
| MDM - Reference 360 | Reference 360 ビジネスアナリスト<br>Reference 360 ビジネススチュワード<br>Reference 360 プライマリオーナー<br>Reference 360 ステークホルダー |

## アプリケーション統合ロールのアクセス特権

アプリケーションの統合およびアプリケーション統合コンソールのアクセス特権が必要なユーザーには、アプリケーションの統合ロールを割り当てます。各ロールは異なるアクセス特権を提供します。

次のサービス固有のロールは、アプリケーションの統合およびアプリケーション統合コンソールのアクセス特権を定義します。

## アプリケーション統合ビジネスマネージャ

アプリケーション統合ビジネスマネージャはビジネスアクティビティを監視します。アプリケーション統合ビジネスマネージャロールを持つユーザーは、アセットとプロセスインスタンスに関する情報を表示できますが、それらを変更することはできません。

以下の表に、アプリケーション統合ビジネスマネージャロールを持つユーザーがアクセスできるサービスと、各サービスに関連付けられているアクセス特権の一覧を示します。

| サービス            | アクセス特権                        |
|-----------------|-------------------------------|
| アプリケーションの統合     | フォルダとアセットのリスト、アセットの詳細を表示できます。 |
| アプリケーション統合コンソール | [プロセス] ページにアクセスできます。          |

## アプリケーション統合データビューア

アプリケーション統合データビューアロールを持つユーザーは、アプリケーション統合コンソールサービスで詳細なログを表示できます。

**注:** 詳細ログを表示するユーザーのアーティファクトのログレベルは、詳細に設定する必要があります。

アプリケーション統合データビューアロールは補足的なロールです。このロールは、他の 1 つ以上のロールと共に割り当てます。例えば、デザイナーロールを持つユーザーが詳細なプロセスサーバーログを表示する場合は、このユーザーにアプリケーション統合データビューアとデザイナーのロールを割り当て、プロセスサーバーのログレベルを詳細に設定します。

## データ統合ロールのアクセス特権

データ統合タスク実行者ロールによって、データ統合のアクセス権限が決まります。データ統合タスク実行者ロールを持つユーザーは、データ統合のタスクおよびタスクフローの実行、マッピングのテスト実行を行うことができます。データ統合ジョブを監視することもできます。

以下の表に、データ統合タスク実行者ロールを持つユーザーがアクセスできるサービスと、各サービスに関連付けられているアクセス特権の一覧を示します。

| サービス  | アクセス特権                                                                                                                                                    |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 管理者   | Secure Agent サービスのスケジュールおよびアップグレード設定を表示できます。ファイルサーバーを開始および停止すること、プロキシサーバーを設定すること、および他のファイルサーバー設定を表示することができます。                                             |
| データ統合 | アセットおよびアセット詳細の表示、タスクおよびタスクフローの実行、マッピングのテスト実行を行うことができます。ユーザー独自のデータ統合ジョブおよびジョブ詳細の表示、ユーザー独自のジョブの開始および停止、セッションログのダウンロードを行うことができます。エクスポートジョブとインポートジョブは表示できません。 |
| モニタ   | データ統合ジョブおよびジョブ詳細の表示、データ統合ジョブの開始および停止、セッションログのダウンロードを行うことができます。エクスポートジョブとインポートジョブは表示できません。                                                                 |

## MDM - Reference 360 ロールのアクセス特権

MDM - Reference 360 のアクセス特権を必要とするユーザーに Reference 360 ロールを割り当てます。各ロールは異なるアクセス特権を提供します。

次のサービス固有のロールで Reference 360 のアクセス特権を定義します。

### Reference 360 ビジネスアナリスト

Reference 360 ビジネスアナリストロールを持つユーザーは、参照データ値とクロスワークを表示およびエクスポート出来ます。すべてのアセットを表示出来ますが、変更する事は出来ません。

### Reference 360 ビジネススチュワード

Reference 360 ビジネススチュワードロールを持つユーザーは、参照データ値と値のマッピングを作成および管理出来ます。Reference 360 ビジネススチュワードロールを持つユーザーは、参照データ値に対する独自の変更を、承認を得ずにパブリッシュ出来ます。他のユーザーが提案した参照データ値に対する変更を確認および承認します。

### Reference 360 プライマリオーナー

Reference 360 プライマリオーナーロールを持つユーザーは、参照データセットとコードリストを作成および定義出来ます。また、参照データ値に対する変更を提案する事も出来ます。提案された変更はすべて、ビジネススチュワードによって承認される必要があります。

### Reference 360 ステークホルダー

Reference 360 ステークホルダーロールを持つユーザーは、参照データ値に対する変更を提案出来ます。提案された変更はすべて、ビジネススチュワードによって承認される必要があります。

上記ロールの詳細については、MDM - Reference 360 のヘルプを参照して下さい。

## カスタムロール

カスタムロールは、組織のニーズに基づいて作成するロールです。例えば、ロール、ユーザーグループ、およびアクセス制御を構成できるが、データ統合タスクを作成、編集、または実行できないカスタム管理ロールを作成する場合があります。

カスタムロールを作成するには、組織が適切なライセンスを持っている必要があります。

カスタムロールは、作成後に編集および削除できます。

組織が新しいライセンスを取得した場合は、カスタムロールを編集できます。ロールを編集して、新しいアセットタイプと機能へのアクセス権限を付与します。組織が新しいライセンスを取得したときに、Informatica Intelligent Cloud Services はカスタムロールに追加の権限を付与しません。

## カスタムロールの作成

**【ユーザーロール】** ページでカスタムロールを作成します。ロールを作成する場合は、ロールに関連付けられている特権を構成します。特権は、サービスごとに別途構成します。

1. 管理者で、**【ユーザーロール】** を選択します。
2. **【ロールの追加】** をクリックします。
3. ロールの名前を入力し、必要に応じて説明を入力します。
4. **【サービス】** フィールドで、特権を構成するサービスを選択します。

例えば、データ統合の特権を構成するには、**【データ統合】**を選択します。管理者特権を構成するには、**【管理者】**を選択します。

5. アセット特権を構成するには、**【アセット】**を選択し、各アセットタイプに対して適切な特権を有効にします。

例えば、ロールを持つユーザーがフォルダを作成できるようにするには、**【フォルダ】**の横にある**【作成】**を有効にします。

アセット特権を取り消すには、特権を無効にします。

6. 機能特権を構成するには、**【機能】**を選択し、各アセットタイプに対して適切な特権を有効にします。

例えば、ロールを持つユーザーがアセットをインポートできるようにするには、**【アセット - インポート】**を有効にします。

機能特権を取り消すには、特権を無効にします。

7. 各サービスに対して、[4](#) から [6](#) の手順を繰り返します。

8. **【保存】**をクリックします。

ロールを作成した後、ユーザーまたはユーザーグループに割り当てることができます。ユーザーまたはグループにロールを割り当てるには、ユーザーまたはグループを編集します。

## カスタムロールの削除

**【ユーザーロール】** ページでカスタムロールを削除します。ユーザーまたはユーザーグループに割り当てられているカスタムロールを削除することはできません。システム定義のロールを削除することはできません。

1. 管理者で、**【ユーザーロール】**を選択します。
2. 削除するロールが含まれている行で**【アクション】**をクリックし、**【削除】**を選択します。

## B2B パートナーポータルユーザーロール

組織で B2B Gateway を使用する場合、外部の取引パートナーのために B2B パートナーポータルへのアクセスを有効にする必要がある場合があります。B2B パートナーポータルへのアクセス権を取引パートナーに付与するには、カスタムロールを作成し、それをパートナーユーザーに割り当てます。

パートナーユーザーのカスタムロールを作成する場合、ロールには、B2B パートナーポータルのユーザー用のロールであるような名前を付けます。例えば、ロールには「B2B パートナーポータルのユーザー」などの名前を付けます。

オプションとして、ロールに説明を付与できます。パートナー会社のユーザー用のロールであるような明確な説明を付与します。例えば、ロールには「パートナー会社のユーザーが B2B パートナーポータルサービスにアクセスできるようにするためのロール」などの説明を付与します。

B2B パートナーポータルのユーザー用のカスタムロールを作成する場合、B2B パートナーポータルサービスのパートナーポータル機能特権を有効にします。カスタムロールの作成について詳しくは、[「カスタムロールの作成」 \(ページ 75\)](#)を参照してください。

パートナー会社のユーザーにカスタムロールを割り当てます。B2B パートナーポータルのユーザー用のロールは 1 つだけ作成すれば済みます。同じロールを B2B パートナーポータルのすべての外部ユーザーに割り当てます。

## 第 10 章

# 権限

権限によって、Secure Agent、Secure Agent グループ、接続、スケジュール、またはアセットに対するユーザーのアクセス権が決まります。また、オブジェクトに対する追加またはカスタムのセキュリティを追加します。権限によって、オブジェクトに対する権限の読み取り、更新、削除、実行、および変更が可能なユーザーおよびグループが定義されます。

オブジェクトの権限を構成するには、次のライセンスと特権が必要です。

- プロジェクト内のすべてのアセットについてプロジェクトレベルで権限を構成するには、プロジェクトレベルでセキュリティ権限の設定または設定解除を行うためのライセンスが組織に必要です。
- プロジェクト内のすべてのアセットについてフォルダレベルで権限を構成するには、フォルダレベルでセキュリティ権限の設定または設定解除を行うためのライセンスが組織に必要です。
- 個々のアセットの権限を構成するには、セキュリティを詳細に設定するためのライセンスが組織に必要です。
- ユーザーアカウント、または管理者がメンバとなっているグループに割り当てられたロールには、オブジェクトタイプに対する権限の設定特権が必要です。例えば、Secure Agent の権限を構成するには、Secure Agent に対する権限の設定特権を持つロールが割り当てられる必要があります。

オブジェクトの権限を構成するには、オブジェクトに移動して適切な権限を設定します。例えば、開発チームのユーザーグループのユーザーだけが開発データフォルダのアセットにアクセスできるようにします。フォルダに移動し、権限を編集し、フォルダに開発チームのユーザーグループの権限を付与します。

権限は、オブジェクトのコピーではなく、権限を構成するオブジェクトに適用します。したがって、アセットをコピーまたはエクスポートする場合、その権限はアセットと一緒にコピーまたはエクスポートされません。例えば、ユーザー rjones が実行権限を持っているマッピングタスクをエクスポートします。マッピングタスクをインポートすると、インポートされたマッピングには割り当てられた権限がありません。したがって、マッピングタスクを実行する特権を持つユーザーは、インポートされたタスクを実行できます。

オブジェクトに対して次の権限を構成できます。

| 権限   | 説明                                                                                                                                                                |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 読み取り | オブジェクトを開いて表示します。<br>オブジェクトがソース管理されている場合、この権限によって、ユーザーまたはグループはオブジェクトをソース管理リポジトリからプルまたはチェックアウトできます。<br>タスクを選択すると、この権限によって、ユーザーまたはグループがタスク内の接続またはスケジュールを使用することもできます。 |
| 更新   | オブジェクトを編集します。<br>オブジェクトがソース管理されている場合、この権限によって、ユーザーまたはグループは、オブジェクトをチェックイン、チェックアウト、プル、リンク解除、またはロールバックできます。<br>読み取り権限が必要です（自動的に付与される）。                               |

| 権限    | 説明                                                                                  |
|-------|-------------------------------------------------------------------------------------|
| 削除    | オブジェクトを削除します。                                                                       |
| 実行    | オブジェクトを実行します。マッピング、タスク、およびタスクフローに適用されます。マッピング、タスク、またはタスクフローのインスタンスを監視、停止、および再起動します。 |
| 権限の変更 | オブジェクトに割り当てられている権限を変更します。                                                           |

**注:** これらの権限は、Informatica Intelligent Cloud Services 内で制御されます。Windows や Linux で Secure Agent を起動、停止、または設定する場合の権限のような、オペレーティングシステムの権限を制御するものではありません。

## 権限のルールおよびガイドライン

権限には、次の規則とガイドラインを使用します。

- オブジェクトの権限を構成するときに、権限を付与するユーザーまたはグループに、そのオブジェクトタイプに対する適切な特権を持つロールが割り当てられていることを確認します。例えば、ユーザーに特定のフォルダに対するサービスコンシューマロールの更新特権があっても、サービスコンシューマロールにはフォルダの更新特権がないため、ユーザーはフォルダを更新できません。
- アセットを編集するには、アセット内で使用されているすべてのアセットに対する読み取り権限がユーザーに与えられている必要があります。例えば、同期タスクに対する読み取りおよび更新の権限をユーザーに割り当てた場合、そのユーザーにタスクで使用されている接続、マップレット、スケジュール、および保存されたクエリに対する読み取り権限もあることを確認します。
- ユーザーがタスクを編集すると、読み取り権限のないアセットは表示されません。予期しない結果を回避するには、ユーザーが適切な読み取り権限を付与されるまで、すべての変更をキャンセルし、タスクの編集を回避する必要があります。
- タスクフローを構成する場合、ユーザーは、タスクフローに追加するすべてのタスクに対する実行権限を必要とします。
- タスクフローを編集するには、タスクフローのすべてのタスクに対して実行権限が必要です。すべてのタスクに対して実行権限がない場合、ユーザーはタスクフローに変更を保存できません。
- タスクフローを実行するには、ユーザーにタスクフローに対する読み取り権限と実行権限が必要です。
- ジョブを監視したり、実行中のジョブを停止したりするには、ユーザーはマッピング、タスク、またはタスクフローの実行権限を必要とします。
- データ統合タスクにカスタム権限を割り当てて、アプリケーション統合プロセスまたはガイドを介してデータ統合タスクを呼び出す場合は、次のいずれかのタスクを実行する必要があります。
  - アプリケーション統合の匿名ユーザーに、関連するデータ統合アセットの実行権限を付与します。
  - アプリケーション統合の匿名ユーザーを、関連するデータ統合アセットの実行権限を持つユーザーグループに追加します。

# 権限の設定

オブジェクトタイプに対する権限の設定特権を持つロールが割り当てられている場合は、オブジェクトの権限を構成できます。例えば、フォルダの権限を構成するには、フォルダの権限の設定特権を持つロールが割り当てられている必要があります。

1. 権限を構成するオブジェクトに移動します。

例:

- Secure Agent または Secure Agent グループの権限を構成するには、管理者で **【ランタイム環境】** を選択します。
- 接続の権限を構成するには、管理者で **【接続】** を選択します。
- マッピングの権限を構成するには、データ統合でマッピングを含むプロジェクトとフォルダを開きます。

2. オブジェクトを含む行で、**【アクション】** をクリックして **【権限】** を選択するか、**【権限の変更】** アイコンをクリックします。

**【権限】** ダイアログボックスには、オブジェクトに対する権限を持つユーザーとグループが一覧表示されます。

**【権限】** ダイアログボックスにユーザーまたはグループが一覧表示されない場合は、そのオブジェクトに対して権限が構成されていません。オブジェクトタイプに対して適切な特権を持つユーザーは、オブジェクトにアクセスできます。

次の図は、マッピングの **【権限】** ダイアログボックスを示しています。

| <input type="checkbox"/> | User Name | First Name | Last Name | Read                                | Update                              | Delete                              | Execute                             | Change Permissions                  |
|--------------------------|-----------|------------|-----------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> | mclark    | Melissa    | Clark     | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> | ajones    | Adam       | Jones     | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> | dsmith    | David      | Smith     | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |

3. オブジェクトに対するユーザー権限を構成するには:

- a. **【ユーザー】** を選択します。
- b. ユーザーが **【ユーザー】** の一覧に表示されていない場合は、**【追加】** をクリックし、ユーザーを選択します。
- c. ユーザーに対する適切な権限を有効または無効にします。

**注:** オブジェクトに対するユーザー権限を付与すると、Informatica Intelligent Cloud Services によって管理者もオブジェクトに対するアクセス権限を持つユーザーとして追加されます。これにより、権限を構成するときにオブジェクトへのアクセスが失われるのを防ぎます。

4. オブジェクトに対するユーザーグループの権限を構成するには:
  - a. **【グループ】** を選択します。
  - b. グループが **【グループ】** の一覧に表示されていない場合は、**【追加】** をクリックし、グループを選択します。
  - c. グループに対する適切な権限を有効または無効にします。

**注:** オブジェクトに対するグループの権限を付与すると、Informatica Intelligent Cloud Services によって管理者もオブジェクトに対するアクセス権限を持つユーザーとして追加されます。これにより、権限を構成するときにオブジェクトへのアクセスが失われるのを防ぎます。

5. オブジェクトの権限の制限をすべて削除するには、**【権限】** ダイアログボックスからすべてのユーザーとグループを削除します。

すべてのユーザーとグループを削除すると、そのオブジェクトタイプに対して適切な特権を持つすべてのユーザーがオブジェクトにアクセスできるようになります。
6. **【保存】** をクリックします。



## 第 11 章

# ランタイム環境

ランタイム環境は、データ統合またはアプリケーション統合タスクを実行する実行プラットフォームです。組織内のユーザーがタスクを実行できるように、各組織に少なくとも 1 つのランタイム環境が必要です。

ランタイム環境は、1 つ以上の Secure Agent で構成されます。Secure Agent は、すべてのタスクを実行し、組織と Informatica Intelligent Cloud Services 間でのファイアウォールを越えた安全な通信を可能にする軽量プログラムです。

ランタイム環境は、次の方法で設定できます。

**Informatica Cloud Hosted Agent のライセンスを取得します。**

Hosted Agent のライセンスを取得する場合は、Informatica Cloud ホスティングファシリティ内でタスクを実行します。Informatica は、Hosted Agent のランタイム環境とエージェントを保持します。

**1 つ以上の Secure Agent グループを作成します。**

1 つ以上の Secure Agent をダウンロードしてインストールし、ネットワーク内または Amazon Web Services や Microsoft Azure などのクラウドコンピューティングサービス環境で実行することができます。1 つの Secure Agent を物理マシンまたは仮想マシンにそれぞれインストールできます。

Secure Agent をインストールすると、デフォルトでは独自のグループに追加されます。Secure Agent クラスタライセンスを持っている場合は、1 つの Secure Agent グループに複数のエージェントを追加できます。

接続または一部のタイプのタスクを構成するときは、使用するランタイム環境を指定します。ランタイム環境により、実行時にタスクを実行するエージェントが決まります。ランタイム環境が Hosted Agent である場合は、Hosted Agent がタスクを実行します。ランタイム環境が Secure Agent グループである場合、グループ内の使用可能なすべてのエージェントがタスクを実行できます。

ランタイム環境を使用して、エラスティックマッピングに基づくマッピングタスクを実行するには、ランタイム環境がエラスティック構成と関連付けられている必要があります。Secure Agent で、設定を使用してエラスティッククラスタにデータ処理をプッシュします。

## Hosted Agent

組織に Cloud Runtime ライセンスがある場合は、Hosted Agent を使用してタスクを実行できます。Hosted Agent は、特定のコネクタを使用する同期タスクおよびマッピングタスクを実行できます。

エラスティックマッピングに基づくマッピングタスクを実行するために、Hosted Agent は使用できません。

データ統合で Hosted Agent のランタイム環境が管理されるため、Hosted Agent を追加、削除、または構成することはできません。

Hosted Agent は、特定のコネクタを使用する同期タスク、マッピングタスク、およびレプリケーションタスクを実行できます。

- Amazon Athena コネクタ
- Amazon Aurora コネクタ
- Amazon DynamoDB コネクタ
- Amazon Redshift コネクタ
- Amazon Redshift V2 コネクタ
- Amazon S3 コネクタ
- Amazon S3 V2 コネクタ
- Box コネクタ
- Box OAuth コネクタ
- CDM フォルダコネクタ
- Cloud Integration Hub
- Concur V2 コネクタ
- Coupa V2 コネクタ
- DB2 Warehouse on Cloud コネクタ
- Eloqua Bulk API コネクタ
- Google Analytics コネクタ
- Google Big Query コネクタ
- Google Big Query V2 コネクタ
- Google Cloud Spanner コネクタ
- Google Cloud Storage コネクタ
- Google Cloud Storage V2 コネクタ
- Marketo V3 コネクタ
- Microsoft Azure Blob コネクタ
- Microsoft Azure Blob ストレージ V2 コネクタ
- Microsoft Azure Blob Storage V3 コネクタ
- Microsoft Azure Cosmos DB SQL API コネクタ
- Microsoft Azure Data Lake コネクタ
- Microsoft Azure Data Lake Store Gen2 コネクタ
- Microsoft Azure Data Lake Store V2 コネクタ
- Microsoft Azure Data Lake Store V3 コネクタ
- Microsoft Azure Data Warehouse コネクタ
- Microsoft Azure SQL Data Warehouse V2 コネクタ
- Microsoft Azure SQL Data Warehouse V3 コネクタ
- Microsoft Dynamics 365 for Operations コネクタ
- Microsoft Dynamics 365 for Sales コネクタ
- Microsoft SQL Server コネクタ

- Mock コネクタ
- MongoDB コネクタ
- MySQL コネクタ
- NetSuite コネクタ
- NetSuite V2 コネクタ
- Oracle コネクタ
- PostgreSQL コネクタ
- REST V2 コネクタ
- Salesforce コネクタ
- Salesforce Marketing Cloud コネクタ
- Salesforce Oauth コネクタ
- ServiceNow コネクタ
- Snowflake Cloud Data Warehouse V2 コネクタ
- Snowflake コネクタ
- SuccessFactors ODATA コネクタ
- SuccessFactors SOAP コネクタ
- SugarCRM REST コネクタ
- UltiPro コネクタ
- Workday V2 コネクタ
- Zendesk コネクタ
- Zendesk V2 コネクタ

**注:** Hosted Agent のサポートはコネクタ固有です。詳細については、関連するコネクタのヘルプを参照してください。

## Secure Agent グループ

オンプレミスのデータにアクセスする必要がある場合や、Hosted Agent を使用せずにクラウドコンピューティングサービス環境内のデータにアクセスする場合は、Secure Agent をランタイム環境として使用します。接続またはタスクのランタイム環境として Secure Agent グループを選択すると、グループ内の Secure Agent エージェントがタスクを実行します。

次の目標を達成するために、Secure Agent エージェントグループを作成します。

**ある部門の活動が別の部門に影響を与えないようにします。**

ある部門の活動が別の部門に影響を与えないようにするため、部門ごとに別々の Secure Agent グループを作成します。例えば、営業部門のユーザーが、財務部門のユーザーと同じ数のタスクを 10 回実行するとしても、財務タスクは時間が非常に重要です。営業タスクが財務タスクに影響を与えないようにするため、部門ごとに別々の Secure Agent エージェントグループを作成します。次に、一方のランタイム環境に営業タスクを割り当て、もう一方のランタイム環境に対して財務タスクを実行します。

### 環境ごとにタスクを分離する。

テストおよび運用環境では、異なる Secure Agent グループを作成できます。接続を構成するとき、ランタイム環境として適切な Secure Agent グループを選択することで、その接続をテスト用または本稼働用のデータベースに関連付けることができます。

Secure Agent グループを作成すると、組織内のすべてのユーザーが、ランタイム環境として Secure Agent グループを選択できます。

グループから Secure Agent を追加および削除できます。ライセンスに基づいて、次の操作を実行することもできます。

- Secure Agent クラスタライセンスを持っている場合は、1 つの Secure Agent グループに複数のエージェントを追加できます。
- 組織階層ライセンスがある場合は、Secure Agent グループをサブ組織と共有できます。

**注:** ランタイム環境を使用して、エラスティックマッピングに基づくマッピングタスクを実行するには、Secure Agent グループに 1 つの Secure Agent のみ含まれている必要があります。

Secure Agent マシン上の出力ファイルにアクセスする必要がある場合は、モニタで **【すべてのジョブ】** ページを表示するか、データ統合で **【マイジョブ】** ページを表示してタスクの実行場所を決定します。

## 複数のエージェントを含む Secure Agent グループ

Secure Agent を作成すると、デフォルトでは独自のグループに追加されます。Secure Agent クラスタライセンスを持っている場合は、1 つの Secure Agent グループに複数のエージェントを追加できます。グループ内のすべてのエージェントは、ネットワーク内で実行されるすべてのエージェントや Amazon EC2 マシンで実行されるすべてのエージェントなど、同じ種類である必要があります。

グループに複数のエージェントを追加して、次の目標を達成します。

### 負荷をマシン間で分散する。

複数のエージェントをグループに追加して、マシン間のタスクの分散を調整します。ランタイム環境が複数のエージェントを持つ Secure Agent グループである場合、グループは、ラウンドロビン方式で使用可能なエージェントにタスクをディスパッチします。

### 接続とタスクの拡張性を向上させる。

接続またはタスクを作成するときは、使用するランタイム環境を選択します。ランタイム環境が複数のエージェントを持つ Secure Agent グループである場合、グループ内に稼働している Secure Agent があれば、そのタスクを実行できます。エージェントを追加または削除するとき、またはグループ内のエージェントが実行を停止したときに、接続またはタスクのプロパティを変更する必要はありません。

グループに複数のエージェントを追加する場合は、すべての Secure Agent が同じタイプであることを確認します。例えば、組織で、ネットワーク内の物理マシンに 4 つの Secure Agent、Amazon EC2 マシン上に 2 つの Secure Agent をインストールしているとします。ローカルエージェントの一部またはすべてを含む Secure Agent グループ、および EC2 エージェントを含む別のグループを作成できます。ローカルエージェントと EC2 エージェントの両方を含むグループを作成しないでください。

Secure Agent マシン上の出力ファイルにアクセスする必要がある場合は、ジョブの詳細を表示して、どの Secure Agent がタスクを実行したかを確認できます。ジョブの詳細を表示するには、モニタを開いて **【すべてのジョブ】** を選択し、ジョブ名をクリックします。

## Secure Agent グループへのサービス割り当て

デフォルトでは、Secure Agent グループを作成した場合、組織で使用するすべてのサービスがこのグループを使用できます。組織が複数のサービスを使用する場合、Secure Agent グループに対する需要は高くなります。

Secure Agent グループに対する潜在的な需要を減らすために、グループに対して特定の Secure Agent サービスを有効または無効にできます。

Secure Agent グループに対して有効または無効にするサービスは Secure Agent サービスで、Informatica Intelligent Cloud Services とは異なります。例えば、グループのエージェントをオペレーションインサイトでのみ使用する場合は、グループに対して OI データコレクタサービスを有効にして、他のすべてのサービスを無効にします。Secure Agent サービスの詳細については、[第 13 章、「Secure Agent サービス」 \(ページ 113\)](#)を参照してください。

次のアクションを実行できます。

Secure Agent **グループに対してサービスを有効にする。**

グループのエージェントに、サービスまたはサービスセットに関連付けられている接続、タスク、プロセス、または製品機能を実行させる場合は、サービスを有効にします。サービスを有効にすると、Secure Agent グループの各エージェントでサービスが起動します。

Secure Agent **グループに対してサービスを無効にする。**

グループのエージェントに、サービスまたはサービスセットに関連付けられている接続、タスク、プロセス、または製品機能を実行させない場合は、サービスを無効にします。サービスを無効にすると、Secure Agent グループの各エージェントでサービスが停止します。Secure Agent グループをランタイム環境として使用する接続、タスク、プロセス、または製品機能は実行されなくなります。

**[ランタイム環境]** ページで、Secure Agent グループに対してサービスを有効または無効にします。

次の図は、**[ランタイム環境]** ページを示しています。

| Actions | Environment Name               | Status           | Enabled Services                         | Host Name    | Platform  | Version | Upgrade Status | Last Upgrade Check      | Last Status Change      |
|---------|--------------------------------|------------------|------------------------------------------|--------------|-----------|---------|----------------|-------------------------|-------------------------|
|         | Informatica Cloud Hosted Agent | Up and Running   | EDC_Search_Agent_Data_Integration_Server |              |           |         |                |                         |                         |
|         | CAW184178 (1)                  |                  |                                          |              |           |         |                |                         |                         |
|         | CAW184178                      | Up and Running   | Data_Integration_Server                  | CAW184178    | Windows64 | 54.1    | Up-to-date     | Feb 5, 2020 11:06:30 AM | Feb 5, 2020 10:42:11 AM |
|         | TMS26W0864 (1) (shared)        |                  |                                          |              |           |         |                |                         |                         |
|         | TMS26W0864                     | Stopped          | Data_Integration_Server                  | TMS26W0864   | Windows64 | 53.1    | Out-of-date    | Jan 3, 2020 1:24:37 PM  | Jan 3, 2020 3:30:01 PM  |
|         | USW1PF0UFLSJ (1)               |                  |                                          |              |           |         |                |                         |                         |
|         | USW1PF0UFLSJ                   | Up and Running   | EDC_Search_Agent_Data_Integration_Server | USW1PF0UFLSJ | Windows64 | 54.1    | Up-to-date     | Feb 5, 2020 11:06:30 AM | Feb 5, 2020 10:42:11 AM |
|         | USW1PF0WZ3NF                   | No Secure Agents | EDC_Search_Agent_Data_Integration_Server |              |           |         |                |                         |                         |
|         | USW1PF10EL71 (1)               |                  |                                          |              |           |         |                |                         |                         |
|         | USW1PF10EL71                   | Up and Running   | EDC_Search_Agent_Data_Integration_Server | USW1PF10EL71 | Windows64 | 54.1    | Up-to-date     | Feb 5, 2020 11:06:55 AM | Feb 5, 2020 10:03:53 AM |

[有効なサービス] 列に、Secure Agent グループに対して有効になっているサービスが示されます。Hosted Agent の [有効なサービス] 列には、組織が使用ライセンスを持っているすべての Secure Agent サービスが一覧表示されます。サービスを有効または無効にするには、Secure Agent グループの **[アクション]** メニューを展開して、**[サービスの有効化または無効化]** を選択します。

Secure Agent グループにサービス割り当てを行った後、エージェントを追加または削除できます。グループに Secure Agent を追加すると、エージェントは追加先グループのサービス割り当てを継承します。

## 例

組織はデータ統合を使用しており、一括取り込みおよび Enterprise Data Catalog データ検出のライセンスを持っています。組織では、次の Secure Agent グループを使用しています。

- グループ 1: Secure Agent 1、Secure Agent 2、Secure Agent 3
- グループ 2: Secure Agent 4

- グループ 3: Secure Agent 5

デフォルトでは、組織のユーザーは任意のグループを接続またはタスク（ファイル取り込みタスクを含む）のランタイム環境として選択できます。管理者は、任意のグループを Enterprise Data Catalog との統合のランタイム環境として選択することもできます。

Secure Agent グループ間の負荷を分散するために、グループ 1 をファイル取り込みタスクを除くデータ統合タスクに予約し、グループ 2 をファイル取り込みタスクに予約し、グループ 3 をデータカタログ検出に予約することができます。

そのために、次の Secure Agent サービスを有効または無効にすることができます。

| Secure Agent グループ | 有効なサービス      | 無効なサービス                |
|-------------------|--------------|------------------------|
| グループ 1            | データ統合サーバー    | 一括取り込み、EDC 検索エージェント    |
| グループ 2            | 一括取り込み       | データ統合サーバー、EDC 検索エージェント |
| グループ 3            | EDC 検索エージェント | データ統合サーバー、一括取り込み       |

タスクおよび機能の失敗を回避するために、次の設定も確認する必要があります。

- データ統合タスクを除くすべてのファイル取り込みタスクが、グループ 1 をランタイム環境として使用している。これらのタスクで使用する接続もすべて、グループ 1 をランタイム環境として使用している。
- すべてのファイル取り込みタスクが、グループ 2 をランタイム環境として使用している。これらのタスクで使用する接続もすべて、グループ 2 をランタイム環境として使用している。
- 管理者の【組織】ページで、Enterprise Data Catalog 統合プロパティがグループ 3 をランタイム環境として使用している。

## サービス割り当てのガイドライン

Secure Agent グループに対してサービスを有効または無効にする際は、次のガイドラインを使用します。

- サービスを無効にする前に、グループをランタイム環境として使用する接続、タスク、またはプロセスがサービスを必要としていないことを確認します。

接続、タスク、またはプロセスで Secure Agent グループがランタイム環境として選択されている場合、必要なサービスを無効にすると、そのタスクまたはプロセスは実行できません。例えば、マッピングソースの接続でランタイム環境 RuntimeEnv1 を使用しているとします。RuntimeEnv1 でデータ統合サーバーを無効にすると、マッピングタスクは実行時に失敗します。

- サービスを無効にする前に、グループをランタイム環境として使用する機能がサービスを必要としていないことを確認します。

機能で Secure Agent グループがランタイム環境として選択されている場合、必要なサービスを無効にすると、その機能は使用できません。例えば、Enterprise Data Catalog 統合のランタイム環境が RuntimeEnv2 に設定されているとします。RuntimeEnv2 で EDC 検索サービスを無効にすると、データカタログ検索を実行できなくなります。

- 接続を作成する際は、必要なサービスが有効化されているランタイム環境を選択します。

例えば、ファイル取り込みタスクターゲットに高度な SFTP 接続を作成するとします。接続を作成する際は、一括取り込みサービスが有効化されているランタイム環境を選択します。

- Secure Agent では、サービスを無効にして一時的に停止する事はしないでください。Secure Agent でのサービスの一時的な停止に関する詳細については、[「Secure Agent でのサービスの停止と開始」](#)（ページ 94）を参照してください。

## Secure Agent グループの共有

親組織の管理者は、Secure Agent グループをサブ組織と共有できます。Secure Agent グループを共有すると、すべてのサブ組織がグループ内の Secure Agent でデータ統合ジョブを実行出来るようになります。

**注:** グループ内のすべてのエージェントでデータ統合サーバーのサービスのみを実行する場合は、Secure Agent グループを共有します。Secure Agent グループの共有で非データ統合ジョブを実行する事は出来ません。

Secure Agent グループを共有すると、使用可能な Secure Agent リソースを最大限に活用できます。例えば、タイムゾーンが異なる部門の別々のサブ組織が組織に含まれているとします。各サブ組織は、1 日の中の異なる時間にデータ統合タスクを実行します。サブ組織ごとに 1 つの Secure Agent グループを作成すると、時間帯によっては、使用負荷が高い Secure Agent グループと、アイドル状態の Secure Agent グループが混在する場合があります。タスクをより均等に分散するには、Secure Agent を Secure Agent グループに追加して、その Secure Agent グループをサブ組織と共有します。

Secure Agent グループを共有するには、適切なライセンスが必要です。

Secure Agent グループを共有すると、そのグループがすべてのサブ組織の **【ランタイム環境】** ページに表示されます。サブ組織の管理者が、グループ内の Secure Agent を表示することはできません。また、Secure Agent の追加や削除、グループの名前変更、削除、共有解除、グループ権限の変更などのグループ管理タスクを行うこともできません。

サブ組織のユーザーが接続またはタスクを作成すると、そのユーザーはランタイム環境に Secure Agent グループの共有を選択出来ます。

### 共有された Secure Agent グループでのフラットファイル接続

共有された Secure Agent グループに複数の Secure Agent が含まれている場合、このグループをフラットファイル接続用のランタイム環境として使用するときは、グループ内のすべての Secure Agent が、接続で使われるディレクトリにアクセスできる必要があります。

すべての Secure Agent がこのディレクトリにアクセスできない場合は、Secure Agent に割り当てられている、その接続を使用するタスクが失敗します。

## Secure Agent グループの操作

**【ランタイム環境】** ページで Secure Agent グループを作成します。Secure Agent グループの作成後は、グループの名前変更または削除、Secure Agent の追加と削除、およびグループ権限の変更を行うことができます。

次のタスクを実行できます。

**Secure Agent グループを作成する。**

Secure Agent グループを作成するには、**【新しいランタイム環境】** をクリックし、グループの名前を入力します。グループを作成した後、グループに Secure Agent を追加できます。

**Secure Agent グループの名前を変更する。**

Secure Agent グループの名前を変更するには、**【アクション】** メニューを展開して **【Secure Agent グループの名前変更】** を選択し、グループの新しい名前を入力します。Informatica Intelligent Cloud Services は、そのグループを使用するすべてのサービスでグループ名を更新します。

**Secure Agent グループに対してサービスを有効または無効にする。**

Secure Agent グループに対してサービスを有効または無効にするには、**【アクション】** メニューを展開して **【サービスの有効化または無効化】** を選択し、有効または無効にするサービスを選択します。組織が使用ライセンスを持っているサービスを有効または無効に出来ます。



**注:** サービスを無効にする前に、グループをランタイム環境として使用する接続、タスク、またはプロセスがサービスを必要としていないことを確認します。接続、タスク、またはプロセスで Secure Agent グループがランタイム環境として選択されている場合、必要なサービスを無効にすると、そのタスクまたはプロセスは実行できません。同様に、機能で Secure Agent グループがランタイム環境として選択されている場合、必要なサービスを無効にすると、その機能は使用できません。

#### Secure Agent をグループに追加する。

Secure Agent をグループに追加するには、[アクション] メニューを展開し、**[Secure Agent の追加または削除]** を選択します。**[ランタイム環境]** ページの [未割り当て状態のエージェント] グループにある任意のエージェントを追加出来ます。

または、エージェントを登録する前に infaagent.ini ファイルの InfaAgent.GroupName プロパティを設定することで、既存のグループに新しい Secure Agent を追加出来ます。

Secure Agent グループに複数の Secure Agent を追加する場合、すべてのエージェントは次の要件を満たしている必要があります。

- すべてのエージェントは、すべてローカルエージェントである、またはすべて Amazon EC2 マシンで実行されているなど、同じ種類である必要がある。
- 各 Secure Agent は、同じ外部システムに接続し、ライブラリ、初期化ファイル、および JAR ファイルなどのファイルへのアクセス権を持つように設定されている。
- 各 Secure Agent は、タスクで使用するファイルにアクセスできる必要がある。タスクで使用するファイルが共有場所でも使用可能なことを確認する。

#### Secure Agent をグループから削除する。

Secure Agent をグループから削除するには、[アクション] メニューを展開し、**[Secure Agent の追加または削除]** を選択します。グループからエージェントを削除すると、Informatica Intelligent Cloud Services で「Unassigned Agents (未割り当て状態のエージェント)」という名前のグループにエージェントが追加されます。

グループが接続またはタスクでランタイム環境として使用されていない場合は、Secure Agent グループからエージェントを削除できます。グループが使用されている場合、そのグループ内の唯一のエージェントでない場合は、エージェントを削除できます。

#### Secure Agent グループを削除する。

Secure Agent グループを削除するには、[アクション] メニューを展開し、**[Secure Agent グループの削除]** を選択します。Secure Agent グループは、Secure Agent が含まれていない場合には削除できます。

Secure Agent グループがエラスティック構成と関連付けられ、エラスティッククラスタが実行されると、クラスタを停止し、グループ削除前にこの構成を別のランタイム環境と関連付ける必要があります。

#### Secure Agent グループを共有または共有解除する。

親組織の管理者が Secure Agent グループを共有すると、サブ組織は、その Secure Agent グループを使用出来るようになります。接続またはタスクで使用されていないグループは、共有解除出来ます。グループに関連付けられている [アクション] メニューから、**[Secure Agent グループの共有]** または **[Secure Agent グループの共有解除]** を選択します。

#### Secure Agent グループの権限を変更する。

Secure Agent グループの権限を変更するには、[アクション] メニューを展開し、**[権限の変更]** を選択します。組織のユーザーグループごとに Secure Agent グループの権限を定義できます。



次の権限を設定することができます。

| 権限   | 説明                                                        |
|------|-----------------------------------------------------------|
| 読み取り | Secure Agent グループに関する詳細を表示し、タスクで Secure Agent グループを使用します。 |
| 更新   | Secure Agent グループを編集します。                                  |
| 削除   | Secure Agent グループを削除します。                                  |
| 変更   | Secure Agent グループの権限を変更します。                               |

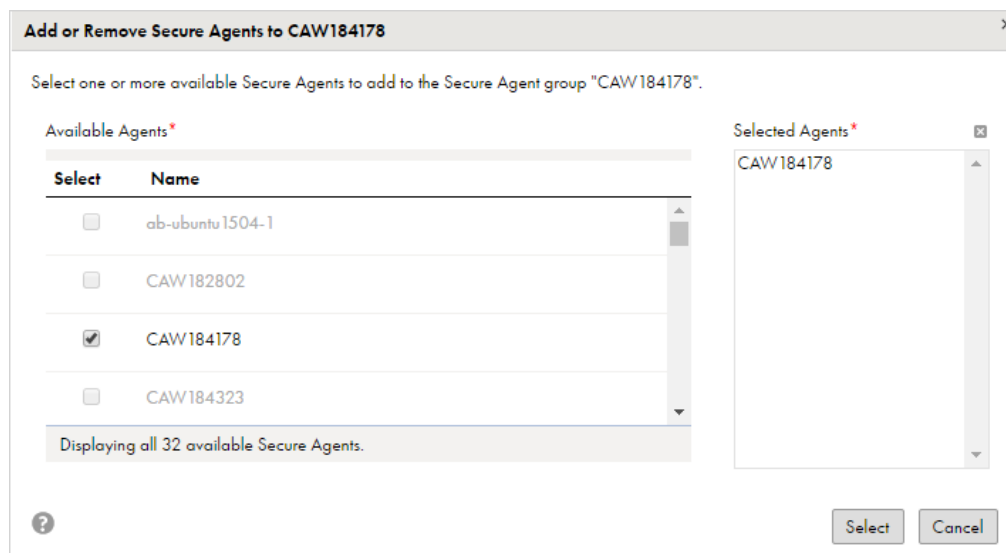
## グループへの Secure Agent の追加

Secure Agent グループに、使用可能な任意の Secure Agent を追加できます。使用可能なエージェントは、**【ランタイム環境】** ページの「未割り当て状態のエージェント」グループに表示されます。Secure Agent がすでに別のグループに追加されている場合は、グループにエージェントを追加することはできません。

1. 管理者で、**【ランタイム環境】** を選択します。
2. Secure Agent グループの **【アクション】** メニューを展開し、**【Secure Agent の追加または削除】** を選択します。
3. **【使用可能なエージェント】** リストで、グループに追加する Secure Agent のチェックボックスをオンにします。

**【使用可能なエージェント】** リストでエージェント名が有効になっていない場合は、すべてのエージェントが他のグループに追加されます。エージェントを別のグループに追加するには、まずはグループからエージェントを削除する必要があります。

チェックボックスを有効にすると、次の図に示すように、Secure Agent が **【選択したエージェント】** リストに示されます。



4. **【選択】** をクリックします。

## 既存のグループへの新規 Secure Agent の追加

エージェントをインストールしている場合、Secure Agent グループに Secure Agent を追加できます。既存のグループに Secure Agent を追加するには、エージェントを登録する前に infaagent.ini ファイルに InfaAgent.GroupName プロパティを追加します。

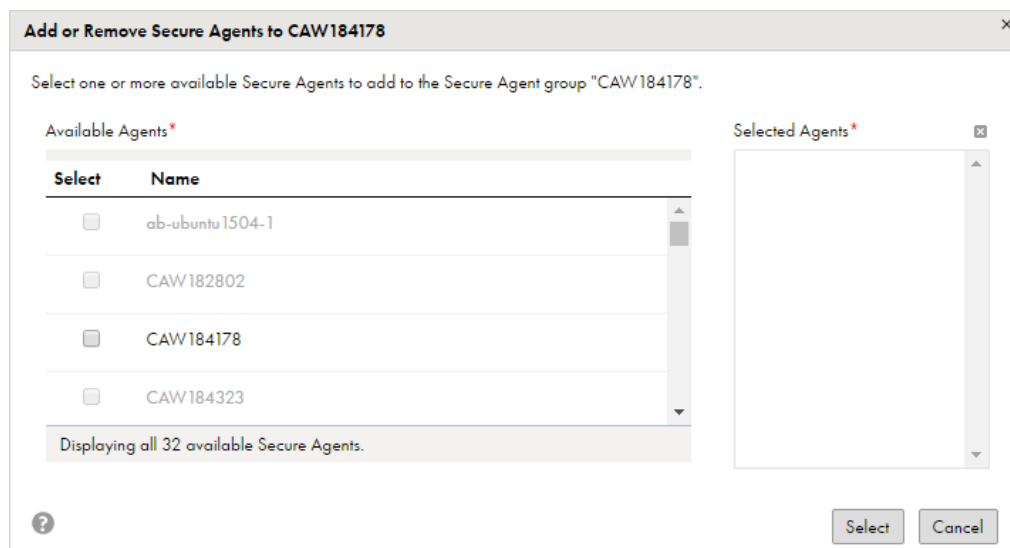
1. Secure Agent をインストールします。
2. Windows では、エージェントの登録を求められたときに Windows の[サービス]を開き、エージェントを停止します。  
Linux では、インストールプログラムが完了したときに、エージェントを起動しないようにします。
3. テキストエディタで<Secure Agent インストールディレクトリ>/apps/agentcore/conf/infaagent.ini を開きます。
4. 次のプロパティを追加してファイルを保存します。  
InfaAgent.GroupName=<Secure Agent グループ名>
5. エージェントを開始します。
6. エージェントを登録します。  
Informatica Intelligent Cloud Services によって、新規グループではなく InfaAgent.GroupName プロパティで指定したグループに Secure Agent が追加されます。

## グループからの Secure Agent の削除

グループが接続またはタスクで使用されていない場合は、Secure Agent グループからエージェントを削除できます。グループが接続またはタスクで使用されている場合、そのグループ内の唯一のエージェントでない場合は、エージェントを削除できます。グループから Secure Agent を削除すると、Informatica Intelligent Cloud Services によって Secure Agent が「未割り当て状態のエージェント」という名前のグループに追加されます。

1. 管理者で、**ランタイム環境** を選択します。
2. Secure Agent グループの [アクション] メニューを展開し、**Secure Agent の追加または削除** を選択します。
3. **選択したエージェント** の一覧で、グループから削除するエージェントを選択し、[X] をクリックします。

次の図に示すように、削除した各エージェントのチェックボックスは無効になり、Secure Agent は**選択したエージェント** の一覧に表示されなくなります。



4. **【選択】** をクリックします。

**【ランタイム環境】** ページの「未割り当て状態のエージェント」グループに、Secure Agent が表示されます。

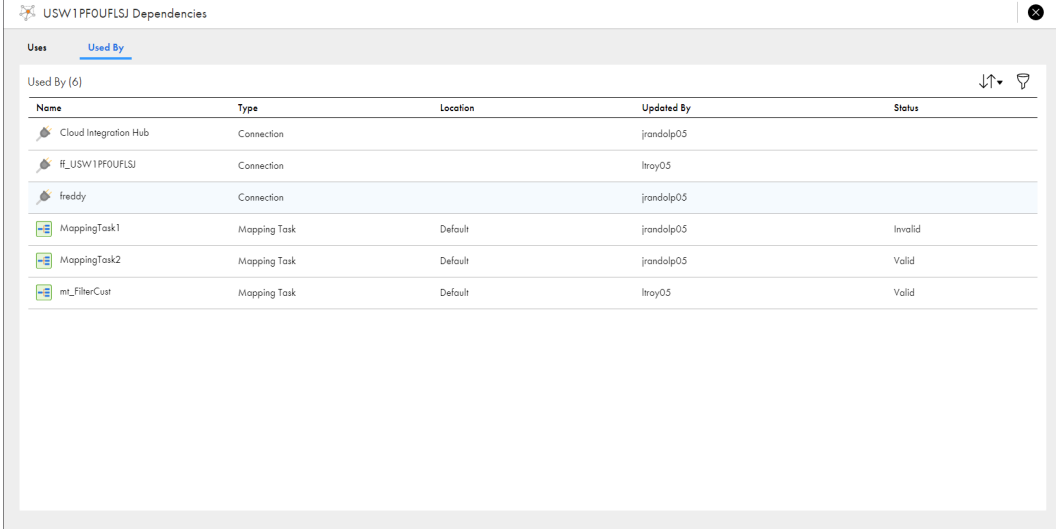
## Secure Agent グループの依存関係の表示

Secure Agent グループのオブジェクトの依存関係を表示することができます。

Secure Agent グループの依存関係を表示する場合、管理者はランタイム環境としてグループを使用する各サービスの接続およびアセットのリストを表示します。

Secure Agent グループのオブジェクトの依存関係を表示するには、**【アクション】** メニューを展開し、**【依存関係の表示】** を選択します。

次の図に、Secure Agent グループの **【依存関係】** ページを示します。



| Name                  | Type         | Location | Updated By | Status  |
|-----------------------|--------------|----------|------------|---------|
| Cloud Integration Hub | Connection   |          | jrandolp05 |         |
| if_USW1PFOUFLSJ       | Connection   |          | ltroy05    |         |
| freddy                | Connection   |          | jrandolp05 |         |
| MappingTask1          | Mapping Task | Default  | jrandolp05 | Invalid |
| MappingTask2          | Mapping Task | Default  | jrandolp05 | Valid   |
| mt_FilterCut          | Mapping Task | Default  | ltroy05    | 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、ソート基準の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、Oracle の接続を名前で見つけるには、**【タイプ】** フィルタを追加し、**【接続】** を指定します。次に、**【名前】** フィルタを追加し、「Oracle」と入力します。

## Secure Agent

Informatica Cloud Secure Agent は、すべてのタスクを実行し、組織と Informatica Intelligent Cloud Services の間でファイアウォールを越えた安全な通信を可能にする軽量プログラムです。Secure Agent は、タスクを実行する場合、Informatica Cloud ホスティング機能に接続してタスク情報にアクセスします。ソースとターゲットに直接かつ安全に接続し、それらの間でデータを転送し、タスクのフローを調整し、プロセスを実行して、追加のタスク要件を実行します。

Secure Agent で Informatica Intelligent Cloud Services への接続が失われると、接続を再確立してタスクの継続を試みます。接続を再確立できない場合、タスクは失敗します。

Secure Agent は、データ処理にプラグブルサービスを使用します。例えば、データ統合サーバーはすべてのデータ統合ジョブを実行し、プロセスサーバーはアプリケーション統合を実行してオーケストレーションジョブを処理します。各サービスは、Tomcat 設定や Tomcat JRE 設定など、一連の設定プロパティを独自に備えています。Secure Agent サービスの詳細については、[第 13 章, 「Secure Agent サービス」 \(ページ 113\)](#)を参照してください。

1 つの Secure Agent を物理マシンまたは仮想マシンにそれぞれインストールして実行できます。Secure Agent をインストールすると、組織内のすべてのユーザーがその Secure Agent を共有します。Secure Agent のプロパティを設定し、別の Secure Agent グループに移動することができます。また、拡張性を向上させるために、Secure Agent グループに複数のエージェントを追加することもできます。

## Secure Agent の操作

Secure Agent を作成したら、エージェントのプロパティの表示および構成、ホスト情報の確認、監査ログの表示、エージェントの状態の更新などの管理タスクを実行する必要があります。また、Secure Agent が使用されなくなった場合は、削除できます。

Secure Agent のほとんどの管理タスクは、エージェントの詳細ページで実行します。エージェントの詳細ページにアクセスするには、**[ランタイム環境]** ページで Secure Agent をクリックします。

次の図に、エージェントの詳細ページを示します。

The screenshot displays the 'Details' tab for a Secure Agent named 'USW1PF0UFLSJ'. The interface includes a 'Refresh Status' button and an 'Edit' button. The agent's status is 'Up and Running'. Below this, a table lists the 'Agent Service Details'.

| Service Name            | Enabled/Disabled | Status         | Version   | Last Update Time         |
|-------------------------|------------------|----------------|-----------|--------------------------|
| Data Integration Server | Enabled          | Up and Running | 55.0.5    | May 29, 2019 10:15:41 AM |
| Process Server          | Enabled          | Up and Running | 8308017.1 | Jun 3, 2019 8:51:12 AM   |
| EDC Search Agent        | Enabled          | Up and Running | 2.0.2     | Jun 3, 2019 8:50:35 AM   |

Below the table, there is a section for 'Agent Service Start or Stop' with a dropdown menu set to 'Data Integration Server' and a 'Stop' button. Further down, there are expandable sections for 'Agent Package Details', 'System Configuration Details', and 'Agent Host | Updated: May 22, 2019 9:59:20 AM' with a 'Refresh' button.

次のタスクを実行できます。

Secure Agent の詳細を表示する。

ホスト名、現在のステータス、エージェントの最終更新日時、およびエージェントバージョンなどの詳細を表示します。

Secure Agent は、次のいずれかのステータスを持つことができます。

| ステータス                  | 説明                                            |
|------------------------|-----------------------------------------------|
| Agent Core は実行されていません。 | Secure Agent は使用できませんが、1 つ以上のサービスが実行されています。   |
| 実行されていないサービスがあります。     | Secure Agent は使用可能ですが、使用できないサービスが 1 つ以上あります。  |
| Agent Core のアップグレード中   | Secure Agent は新しいバージョンにアップグレード中です。            |
| 停止                     | Secure Agent を使用できません。                        |
| 稼働中                    | Secure Agent、およびそのエージェントが実行するすべてのサービスが使用可能です。 |

#### エージェントサービスの詳細を表示する。

サービス名、状態、バージョン、最終更新時刻など、Secure Agent で実行するサービスの詳細を表示します。

サービスは、次のいずれかのステータスを持つことができます。

| ステータス      | 説明                                                             |
|------------|----------------------------------------------------------------|
| エラー        | プロセスが失敗しました。                                                   |
| エラーによる再起動中 | サービスはエラーが発生したため起動中です。                                          |
| シャットダウン中   | サービスがシャットダウンしています。                                             |
| スタンバイ      | サービスは実行中ですが、Informatica Intelligent Cloud Services と互換性がありません。 |
| 起動中        | サービスは起動中です。                                                    |
| 停止         | サービスは使用できません。                                                  |
| 稼働中        | サービスは実行中です。                                                    |
| 警告         | サービスは実行中ですが、操作を受け付けることができません。                                  |

サービスを変更するたびにバージョン番号が変更されます。Secure Agent では、旧バージョンのサービスのディレクトリが 7 日間維持されます。例えば、バージョン 55.0.2 のデータ統合サーバーの NetworkTimeoutPeriod を更新すると、エージェントはバージョン番号を 55.0.3 に上げ、次のディレクトリを作成します。

<Secure Agent installation directory>/apps/Data\_Integration\_Server/55.0.3.1

7 日間後、<Secure Agent installation directory>/apps/Data\_Integration\_Server/55.0.2.x ディレクトリは削除されます。

Secure Agent で実行するサービスを停止および開始します。

Secure Agent で実行するサービスを停止および開始し、トラブルシューティングの実行、エージェントマシンでのリソースの最適化、またはサービス設定の変更を行います。サービスを停止または開始しても、エージェントで実行されている他のサービスは影響を受けません。

Secure Agent パッケージを表示する。

【エージェントパッケージの詳細】 セクションを展開して、Secure Agent で実行する各サービスのパッケージの名前とバージョン番号を確認します。サービスごとにパッケージをフィルタ処理できます。

Secure Agent サービスプロパティを表示および編集します。

【システム構成の詳細】 セクションを展開すると、Secure Agent サービスプロパティが表示されます。プロパティは、サービスとタイプでフィルタリングできます。

プロパティを構成するには、【編集】 をクリックします。Secure Agent で実行される各サービスのプロパティを設定できます。コネクタで使用するカスタムプロパティを追加および削除することもできます。Secure Agent サービスおよびサービスプロパティの詳細については、[第 13 章、「Secure Agent サービス」 \(ページ 113\)](#) を参照してください。カスタムプロパティの詳細については、該当するコネクタのヘルプを参照してください。

Secure Agent ホストのプロパティを表示する。

【エージェントホスト】 セクションを展開し、Secure Agent をホストするマシンに関する情報を表示します。例えば、マシン名、オペレーティングシステム、および使用可能なディスク領域を表示できます。

情報を更新するには、【更新】 をクリックします。情報が更新された最後の日時が、【エージェントホスト | 更新済み】 見出しの横に表示されます。

監査ログを表示する。

開始時間と終了時間、サーバー接続、およびアップグレードメッセージなどの監査情報を表示するには、【監査ログ】 をクリックします。

Secure Agent のステータスを更新する。

Secure Agent の状態を更新するには、ページの右上隅にある【状態の更新】 をクリックします。

Linux では、次のディレクトリに移動してステータスを表示することもできます。

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

次に、次のコマンドのいずれかを実行します。

- 。 consoleAgentManager.sh getstatus
- 。 consoleAgentManager.sh updatestatus

## Secure Agent でのサービスの停止と開始

デフォルトでは、組織内の各 Secure Agent は、組織内のデータ処理で使用するすべてのマイクロサービスを実行します。これらのサービスを停止および開始すると、トラブルシューティングの実行、エージェントマシンのリソースの最適化、または設定の変更を行う事ができます。Secure Agent サービスを停止または開始しても、エージェントで実行されている他のサービスは影響を受けません。

Secure Agent で停止および開始するサービスは Secure Agent サービスで、Informatica Intelligent Cloud Services とは異なります。例えば、オペレーションインサイトに関連するサービスを停止する場合、OI データコレクタサービスをエージェントで停止する必要があります。Secure Agent サービスの詳細については、[第 13 章、「Secure Agent サービス」 \(ページ 113\)](#) を参照してください。

次の状況での Secure Agent サービスの停止および再起動が必要になる場合があります。

**特定のサービスの問題をトラブルシューティングする必要があります。**

サービスでエラー状態が表示された場合は、サービスを停止し、問題をトラブルシューティングしてから、サービスを再起動する事ができます。

**メモリまたは CPU 負荷の高いジョブを実行する場合、Secure Agent マシンの計算リソースを最適化します。**

例えば、組織でデータ統合ジョブおよびアプリケーションの統合ジョブを実行します。データ統合ジョブを昼間に、アプリケーションの統合ジョブを夜間に行うように、計算リソースを最適化します。このためには、プロセスサーバーを昼間停止し、夜間に再起動して、データ統合サーバーを夜間に停止し、早朝再起動します。

**ファイル統合サービスのサービス設定プロパティを更新します。**

ファイル統合サービスの設定プロパティを変更すると、サービスを再起動する必要があります。Secure Agent が他のサービスを実行している場合、他のサービスに影響を与えずにファイル統合サービスを停止および再起動できます。

Secure Agent のサービスを開始または停止するには、Secure Agent で権限を更新しておく必要があります。

下位組織の管理者である場合は、下位組織のエージェントでサービスを開始および停止できます。ただし、Secure Agent 共有グループ内の Secure Agent でサービスを開始および停止する事は出来ません。

サービスを開始および再起動するたびに、Secure Agent はサービス関連ファイルの新しいサブディレクトリを作成します。例えば、Secure Agent がバージョン 12.1 の B2B Processor Service を使用する場合、Secure Agent のインストールディレクトリには次のサブディレクトリが含まれます。

<Secure Agent インストールディレクトリ>/apps/B2BProcessor/12.1.1

B2B Processor Service を停止および再起動すると、Secure Agent は次のディレクトリを作成します。

<Secure Agent インストールディレクトリ>/apps/B2BProcessor/12.1.2

Secure Agent はディレクトリ.../12.1.1 を削除しません。

## 例

組織でデータ統合を使用し、Enterprise Data Catalog 統合、ファイル統合、および一括取り込みのライセンスを使用します。

Secure Agent は次のサービスを実行します。

- データ統合サーバー
- EDC 検索エージェント
- ファイル統合サービス
- 一括取り込み

Enterprise Data Catalog 検索に問題がある場合、トラブルシューティングを実行しながら EDC Search Agent サービスを停止する事ができます。EDC Search Agent サービスを停止すると、データ統合でデータカタログ検索を実行出来ません。ただし、マッピング、タスク、タスクフローなど、このエージェントの他のサービスで処理されるジョブ、および AS2 ファイルの転送は継続されます。

## サービスを停止および開始する際のガイドライン

Secure Agent でサービスを停止および開始する際は、次のガイドラインを使用します。

- サービスを停止する事でジョブが失敗する可能性があるため、Secure Agent でサービスを停止する際は慎重に行ってください。  
サービスを停止すると、そのサービスを必要とするジョブ、およびエージェント上で現在実行中のジョブがすべて停止します。グループ内に他のエージェントがない場合、ジョブを実行出来なくなります。グループ内に他のエージェントがある場合、そのジョブを再開すると別のエージェントで実行されるようになります。
- エージェントに接続プロパティを保存している場合は、そのエージェント上のデータ統合サーバーを停止しないでください。  
ローカルの Secure Agent に接続プロパティを保存している場合にそのエージェント上のデータ統合サーバーを停止すると、ユーザーが組織内の接続にアクセスする事もタスクを実行する事も出来なくなります。また、エージェント上で現在実行中のジョブも失敗します。
- 特定のタイプのジョブの Secure Agent グループを保持するためにサービスを開始したり停止したりしないでください。  
特定のタイプのジョブの Secure Agent グループを保持する場合は、Secure Agent グループで必要なサービスを有効にし、その他のサービスを無効に出来ます。Secure Agent グループのサービスの有効化および無効化に関する詳細については、[「Secure Agent グループへのサービス割り当て」 \(ページ 84\)](#)を参照してください。

## サービスの停止

「稼働中」または「エラー」状態のサービスを停止する事が出来ます。サービスを停止すると、稼働中のすべてのバージョンのサービスが停止します。サービスの停止後、最新バージョンのサービスを開始する事が出来ます。

**注:** サービスを停止してから Secure Agent を再起動した場合、サービスは開始するまで停止状態となります。

1. 管理者で、**ランタイム環境** を選択します。
2. **ランタイム環境** ページで、Secure Agent の名前をクリックします。  
**注:** Secure Agent グループ内の Secure Agent を一覧表示するには、Secure Agent グループの展開が必要になる場合があります。
3. **詳細** タブをクリックします。
4. **Agent Service の開始または停止** 領域で、停止するサービスを選択します。
5. **停止** をクリックします。

サービスが停止し、Informatica Intelligent Cloud Services はサービスがユーザーにより停止された事を示すエントリを監査ログに追加します。

## サービスの開始

「停止」状態のサービスを起動出来ます。サービスを起動すると、サービスの最新バージョンが起動します。

1. 管理者で、**ランタイム環境** を選択します。
2. **ランタイム環境** ページで、Secure Agent の名前をクリックします。  
**注:** Secure Agent グループ内の Secure Agent を一覧表示するには、Secure Agent グループの展開が必要になる場合があります。
3. **詳細** タブをクリックします。
4. **エージェントサービスの開始または停止** 領域で、起動するサービスを選択します。



5. **【開始】** をクリックします。

Informatica Intelligent Cloud Services でサービスの起動を試行します。サービスが起動すると、ステータスが「稼働中」に変わります。サービスの起動に失敗する場合は、監査ログを確認してエラーの原因を突き止めます。

## エージェントのブラックアウト期間の設定

Secure Agent のブラックアウト期間を設定出来ます。ブラックアウト期間によって、一定期間中にデータ統合ジョブがエージェント上で実行されないようにします。エージェントのブラックアウト期間を設定し、エージェント上でデータ統合ジョブを実行出来ないようにする具体的な時間、日数、または間隔を指定します。

エージェントのブラックアウト期間によって、データ統合サーバーサービスでは当該期間中の Secure Agent 上でのジョブの実行が停止します。エージェント上のその他のタイプのジョブが実行されなくなる事はありません。エージェントのブラックアウト期間は、以下のような状況の場合に設定します。

- データ統合サーバーがエージェント上で唯一有効になっているサービスであり、一定期間中のすべてのデータ統合ジョブの実行を停止する必要がある。
- Secure Agent で複数のサービスを実行しているが、一定期間データ統合ジョブの実行のみを停止する必要がある。

**注:** エージェントのブラックアウト期間は、組織のスケジュールブラックアウト期間とは異なります。組織のスケジュールブラックアウト期間中は、いずれのエージェント上でもジョブを実行する事は出来ません。スケジュールブラックアウト期間の詳細については、[「ブラックアウト期間の設定」 \(ページ 156\)](#)を参照して下さい。

Secure Agent 上でブラックアウト期間を設定するには、ブラックアウトファイルを作成する必要があります。ブラックアウトファイルは、各ブラックアウト期間の繰り返し頻度、および開始日と終了日を指定する XML ファイルです。

例えば、以下のブラックアウトファイルには、7 月 27 日午前 5 時～7 月 28 日午後 11 時というブラックアウト期間と、金曜日の午後 2 時～4 時に繰り返すというブラックアウト期間が含まれています。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<BlackoutWindows>
 <BlackoutWindow>
 <RepeatFrequency>OneTime</RepeatFrequency>
 <Start>2019-07-27 5:00:00</Start>
 <End>2019-07-28 23:00:00</End>
 </BlackoutWindow>
 <BlackoutWindow>
 <RepeatFrequency>Friday</RepeatFrequency>
 <Start>14:00:00</Start>
 <End>16:00:00</End>
 </BlackoutWindow>
</BlackoutWindows>
```

1 つ以上のブラックアウト期間を設定するには、次のディレクトリに「blackoutWindows.dat」という名前のファイルを作成します。

```
<Secure Agent Installation Directory>\apps\Data_Integration_Server\conf\
```

別のファイル名やディレクトリを使用する場合は、このファイル名とファイルパスを上書きして下さい。

ブラックアウトファイルを作成すると、Secure Agent 上のデータ統合サーバーサービスが再開され、ブラックアウト期間が有効になります。

## ブラックアウトファイル名およびディレクトリの上書き

ブラックアウトファイル名およびディレクトリを上書き出来ます。

上書きするには、エージェントの詳細ページでデータ統合サーバーの以下のカスタムプロパティを設定します。

サービス	タイプ	名前	値
データ統合サーバー	Tomcat	BlackoutWindowsFile	ブラックアウトファイルのファイルパスとファイル名。以下に例を示します。 C:/AgentBlackouts/Agent001Blackouts.dat 注: Secure Agent ではバックスラッシュ (\) をエスケープ文字と解釈するため、Windows マシンでも UNIX マシンでもファイルパスにはスラッシュ (/) を使用して下さい。 Secure Agent からアクセス出来るファイルパスにする必要があります。

Secure Agent サービスのカスタムプロパティを設定する方法に関する詳細については、[「Secure Agent サービスプロパティの設定」 \(ページ 146\)](#)を参照して下さい。

## ブラックアウトファイルの構造

ブラックアウトファイルは、各ブラックアウトの期間とその頻度、および各ブラックアウト期間の開始時刻と終了時刻を定義する要素が含まれた XML ファイルです。

ブラックアウトファイルの構造は次のとおりです。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<BlackoutWindows>
 <BlackoutWindow>
 <RepeatFrequency></RepeatFrequency>
 <Start></Start>
 <End></End>
 </BlackoutWindow>
 <BlackoutWindow>
 <RepeatFrequency></RepeatFrequency>
 <Start></Start>
 <End></End>
 </BlackoutWindow>
 ...
</BlackoutWindows>
```

ファイルには、以下の要素が含まれます。

要素	必須/オプション	説明
BlackoutWindows	必須	ブラックアウト期間ごとに BlackoutWindow 要素が含まれています。BlackoutWindow 要素は 1 つ以上含まれている必要があります。
BlackoutWindow	必須	ブラックアウト期間を 1 つ定義します。RepeatFrequency 要素、Start 要素、End 要素を 1 つずつ含める必要があります。

要素	必須/ オプション	説明
RepeatFrequency	必須	ブラックアウト期間の繰り返し頻度。 次のいずれかの値を含める必要があります。 - 1 回 - 日次 - 平日 - 日曜日 - 月曜日 - 火曜日 - 水曜日 - 木曜日 - 金曜日 - 土曜日
Start	必須	yyyy-mm-dd hh24:mi:ss 形式によるブラックアウト期間の開始時刻。例: 2019-07-25 10:26:55。 タイムゾーンは Secure Agent ゾーンです。
End	必須	yyyy-mm-dd hh24:mi:ss 形式によるブラックアウト期間の終了時刻。例: 2019/07/26 11:45:00。 タイムゾーンは Secure Agent ゾーンです。

要素値は引用符で囲まないで下さい。

## Secure Agent の名前変更

デフォルトでは、Secure Agent の名前はエージェントをインストールしたマシンの名前と同じです。エージェント名は変更できます。

1. **【ランタイム環境】** ページで、Secure Agent の名前をクリックします。  
**注:** Secure Agent グループ内の Secure Agent を一覧表示するには、Secure Agent グループの展開が必要になる場合があります。
2. **【詳細】** タブをクリックします。
3. 右上隅の **【編集】** をクリックします。
4. **【エージェント名】** フィールドに新しい名前を入力します。
5. **【保存】** をクリックします。

## Secure Agent の削除

タスクを実行するのに必要ではなくなった場合は、Secure Agent を削除します。**【ランタイム環境】** ページで、Secure Agent を削除します。

**注:** 接続またはタスクで使用されている場合は、Secure Agent を削除することはできません。例えば、Secure Agent がグループ内の唯一のエージェントであり、そのグループが接続またはタスクの実行時環境として使用されている場合、エージェントを削除することはできません。

1. 管理者で **【ランタイム環境】** を選択します。

2. Secure Agent の [アクション] メニューを展開し、[Secure Agent の削除] を選択します。

Secure Agent が実行中の場合には、警告メッセージが表示されます。アクティブな Secure Agent を停止すると、その Secure Agent に関連付けられているスケジュール済みタスクの実行が阻まれます。Secure Agent が不要な場合は、警告を無視します。

Secure Agent が不要になった場合は、削除した後、Secure Agent をアンインストールします。

## Secure Agent のアップグレード

Secure Agent は、新しい Informatica Intelligent Cloud Services リリースに初めてアクセスしたときに自動でアップグレードされます。アップグレードプロセスは、Secure Agent の新しいバージョンをインストールし、コネクタパッケージを更新し、エージェント上で実行されるマイクロサービスの構成の変更を適用します。Secure Agent を手動でアップグレードする必要はありません。

ただし、アップグレードを準備するため、アップグレードに利用可能なディスク空き容量が各 Secure Agent マシンにあることを確認するなどのタスクを実行する必要があります。アップグレードの準備の詳細については、『*管理者の新機能*』を参照してください。

## Secure Agent Manager

Windows に Secure Agent をインストールするときには、Informatica Cloud Secure Agent Manager もインストールします。Secure Agent が Windows サービスとして実行されます。Secure Agent Manager は、Windows の [スタート] メニューまたはデスクトップアイコンから起動できます。

Secure Agent Manager を使用すると、次のタスクを実行できます。

- Secure Agent の状態と、Secure Agent で実行されるサービスを表示します。
- Secure Agent を停止および再起動します。
- プロキシ設定や Windows の Secure Agent サービスログインなどの Windows 設定を構成します。

Secure Agent Manager には、Secure Agent のステータスと、Secure Agent が実行するサービスのステータスが表示されます。Secure Agent、または Secure Agent が実行するいずれかのサービスが起動または稼働していない場合、Secure Agent Manager には、警告メッセージとリンクが表示されます。このリンクをクリックすると、詳細を確認できます。

Secure Agent Manager を閉じると、Windows タスクバーが最小化され、即座にアクセスできる状態で表示されます。Secure Agent Manager を閉じて、Secure Agent は停止しません。Secure Agent Manager を最小化する場合は、Secure Agent Manager アイコンにカーソルを合わせると Secure Agent の状態を表示できます。

## 非プロキシホストを除外するためのプロキシの設定

プロキシサーバーでは、セキュリティとパフォーマンス上の理由から、ネットワークサービスへの間接接続が許可されています。例えば、プロキシサーバーを使用してファイアウォールを通過できます。一部のプロキシではキャッシュメカニズムが提供されています。Informatica Cloud Secure Agent のプロキシサーバーを設定するときは、プロキシから特定の IP アドレスとホスト名を除外できます。

Informatica Cloud Secure Agent にプロキシサーバーを設定するときは、Secure Agent Manager で必要最低限の設定を定義します。Informatica Intelligent Cloud Services は、次のファイルを更新して、手動で編集できる他のプロパティを追加します。

```
<Secure Agent installation directory>/apps/agentcore/conf/proxy.ini
```

InfAgent.NonProxyHost プロパティを使用すると、IP アドレスまたはホスト名を除外できます。プロキシサーバーを最初に設定するとき、Informatica Intelligent Cloud Services はデフォルトで InfAgent.NonProxyHost の値として localhost を追加します。

```
InfAgent.ProxyPassword=ZU8KjIzgtVrVmFRMUPzPMw\=\n
InfAgent.ProxyNtDomain=
InfAgent.ProxyHost=foo.bar.com
InfAgent.ProxyPasswordEncrypted=true
InfAgent.NonProxyHost=localhost|127.*|[\:\:1]
InfAgent.ProxyUser=
InfAgent.ProxyPort=12345
InfAgent.AuthenticationOrder=
```

プロキシから特定の IP アドレスまたはホスト名を除外するには、次の手順を実行します。

1. <Secure Agent installation directory>/apps/agentcore/conf/proxy.ini を開きます。
2. 除外する IP アドレスまたはホスト名を指定して、InfAgent.NonProxyHost の値を更新します。

例:

- ローカル IP アドレス:

```
InfAgent.NonProxyHost=localhost|127.|[\:\:1]|123.432.
```

- ホスト名:

```
InfAgent.NonProxyHost=localhost|127.|[\:\:1]|.foo.com
```

**注:** 区切り文字としてパイプ文字 (|) を使用して、ホスト名と IP アドレスのリストを結合できます。ホスト名の左または IP アドレスの右に、ワイルドカードを入力することもできます。

3. 変更が有効になるように、Secure Agent を再起動します。

## Windows での Secure Agent の停止および再起動

Secure Agent Manager に Secure Agent のステータスが表示されます。Secure Agent Manager を使用して、Secure Agent を停止または再起動することができます。

Windows の **【スタート】** メニューから Secure Agent Manager を起動します。Secure Agent Manager がアクティブである場合は、Windows タスクバーの通知領域にある Informatica Cloud Secure Agent Manager のアイコンをクリックして Secure Agent Manager を開くことができます。

Secure Agent Manager から Secure Agent を停止するには、**【停止】** をクリックします。Secure Agent を再起動するには、**【再起動】** をクリックします。アクションが完了すると、Secure Agent Manager にメッセージが表示されます。

Secure Agent Manager を閉じると、Windows タスクバーの通知トレイが最小化されます。Secure Agent Manager を閉じて、Secure Agent は停止しません。

## Linux での Secure Agent の起動および停止

Linux マシンに Secure Agent プログラムをダウンロードした後は、Secure Agent を Linux プロセスとして実行できます。Linux で、Secure Agent プロセスを手動で起動します。

1. コマンドラインから次のディレクトリに移動します。  
<Secure Agent installation directory>/apps/agentcore
2. Secure Agent を起動するには、次のコマンドを入力します。  
./infaagent startup
3. Secure Agent を停止するには、次のコマンドを入力します。  
./infaagent shutdown

Secure Agent の状態は、Informatica Intelligent Cloud Services または Linux コマンドラインから確認できます。

## 第 12 章

# サーバーレスランタイム環境

サーバーレスランタイム環境は、Secure Agent や Secure Agent グループのダウンロード、インストール、設定、管理が必要ない高度なサーバーレスデプロイメントソリューションです。サーバーレスランタイム環境は、データ統合で接続や一部のタイプのタスクを設定するときにランタイム環境を使用する場合と同じ方法で使用できます。

Hosted Agent 上のマルチテナントモデルと比較して、サーバーレスランタイム環境は、分離されたシングルテナントモデルを使用します。このモデルでは、組織のタスクを実行する仮想マシンリソースを備えた専用サーバー 1 台があります。サーバーレスランタイム環境は、負荷の規模に合わせて自動スケールしますが、データはクラウド環境内に残ります。

サーバーレスランタイム環境は、AWS クラウドプラットフォームの Informatica の Amazon Virtual Private Cloud (VPC) にホストされます。サーバーレスランタイム環境は、アカウント間エラスティックネットワークインタフェース (ENI) を作成してクラウド環境に接続します。

**注:** サーバーレスランタイム環境を使用するには、クラウド環境が AWS クラウドプラットフォームにあり、VPC がデフォルトテナンシを使用する必要があります。サーバーレスランタイム環境は、専用インスタステナシを使用する VPC に接続できません。

サーバーレスランタイム環境を使用するには、組織に適切なライセンスが必要です。

### Data Integration Elastic 用にサーバーレスランタイム環境の使用

サーバーレスランタイム環境を Data Integration Elastic の高度なサーバーレスデプロイメントとして使用する場合、エラスティッククラスタの作成とクラスタでのエラスティックジョブの実行に必要な前提条件に従ってサーバーレスランタイム環境が設定されます。サーバーレスランタイム環境は、エラスティッククラスタを管理しますが、クラスタはリソースのプロビジョニングとプロビジョニング解除によって負荷の変化に適応します。

## サーバーレスコンピューティングユニット

サーバーレスコンピューティングユニットとは、サーバーレスランタイム環境でタスクを実行するために使用できる CPU とメモリを表します。Data Integration Elastic を使用する場合、コンピューティングユニットは、Spark エンジンがエラスティックジョブを実行するために作成する Spark Executor の最大数にも影響します。

サーバーレスランタイム環境を作成するときは、各タスクがサーバーレスランタイム環境から要求できるサーバーレスコンピューティングユニットの最大数を設定します。マッピングタスクを作成するときは、タスクが要求できるコンピューティングユニットの最大数を上書きできます。Monitor では、タスクが要求および使用したコンピューティングユニットの数を表示できます。

タスクが指定されたタスクタイムアウトよりも長く実行している場合、サーバーレスランタイム環境によってタスクが強制終了されます。

# 始める前に

サーバーレスランタイム環境を作成する前に、サーバーレスランタイム環境に接続するクラウド環境をセットアップする必要があります。

以下のタスクを完了させます。

1. 必要に応じて、サーバーレスランタイム環境が外部サービスに接続するために使用できる NAT ゲートウェイを作成します。
2. オプションとして、JAR ファイルや外部ライブラリなどの補助ファイル用の S3 フォルダを作成します。
3. ENI を作成するために使用できる IAM ロールをセットアップします。
4. サーバーレスランタイム環境が ENI にアタッチするセキュリティグループを作成します。

## 手順 1. NAT ゲートウェイの作成

オプションとして、サーバーレス環境に設定されたサブネットがインターネット経由で外部サービスに接続できる NAT ゲートウェイを作成します。

次の状況では、NAT ゲートウェイを作成する必要があります。

- タスクがアクセスする Amazon S3 ソースおよびターゲットが異なる AWS リージョンにある。
- タスクがアクセスするソースおよびターゲットが AWS 上にない。

NAT ゲートウェイを設定するときは、以下のタスクを実行し、インバウンドルールを持つサブネットに関連付けられた NACL（ネットワークアクセス制御リスト）を設定して、以下のポートですべてのトラフィックを許可します。

- 一時ポート範囲 1024-65535
- ポート 443

NAT ゲートウェイの作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。

## 手順 2. 補足ファイル用の S3 フォルダの作成

環境およびデータ統合ジョブで JAR ファイルおよび外部ライブラリが必要な場合、Amazon S3 にファイルを保存する専用の場所を確保し、ファイルタイプごとにフォルダを作成します。サーバーレスランタイム環境はその場所にアクセスし、ファイルを取得します。

Amazon S3 に次のファイル構造を作成します。

S3 location for supplementary files

```
graph LR
 S3[S3 location for supplementary files] --- ext[ext]
 S3 --- odbc[odbc]
 S3 --- jars[jars]
 S3 --- ctjars[ctjars]
 ext --- python[python]
 odbc --- lib[lib]
```

各場所に次のファイルのタイプを保存します。

場所	ファイル
<S3 location>/ext	JDBC JAR ファイル
<S3 location>/ext/python/	Python トランスフォーマーで使用される Python インストールおよびリソースファイル



場所	ファイル
<S3 location>/odbc	次のファイル - odbc.ini - odbcinst.ini - exports.ini
<S3 location>/odbc/lib	Linux オペレーティングシステム用の ODBC 共有ライブラリ
<S3 location>/jars/ctjars	Java トランスフォーメーションで使用する JAR ファイル

## 手順 3。IAM ロールの設定

サーバーレスランタイム環境が ENI を作成し、クラウド環境のデータソースに安全に接続できるように、AWS アカウントおよび Informatica AWS アカウント間に信頼を確立するための IAM ロールを作成します。

Informatica を信頼されているエンティティとして識別するアカウント間 IAM ロールを AWS アカウントに作成します。

1. 別の AWS アカウントのロールを作成します。
2. [信頼関係] に Informatica アカウント番号および外部 ID を指定します。

例えば、信頼関係に次のポリシーを指定します。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "AWS": "arn:aws:iam::<Informatica account>:root"
 },
 "Action": "sts:AssumeRole",
 "Condition": {
 "StringEquals": {
 "sts:ExternalId": "<External ID>"
 }
 }
 }
]
}
```

3. ロール権限を編集し、ポリシーを指定して、サーバーレスランタイム環境にアカウントでの最小限の権限のセットを付与します。

次のテンプレートをポリシー用に使用します。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "VisualEditor0",
 "Effect": "Allow",
 "Action": [
 "ec2:DetachNetworkInterface",
 "ec2:DeleteTags",
 "ec2:DescribeTags",
 "ec2:CreateTags",
 "ec2:DeleteNetworkInterface",
 "ec2:DescribeSecurityGroups",
 "ec2:CreateNetworkInterface",
 "ec2:DeleteNetworkInterfacePermission",
 "ec2:DescribeNetworkInterfaces",

```

```

 "ec2:DescribeAvailabilityZones",
 "ec2:CreateNetworkInterfacePermission",
 "ec2:AttachNetworkInterface",
 "ec2:DescribeNetworkInterfacePermissions",
 "ec2:DescribeSubnets",
 "ec2:DescribeNetworkAcls"
],
 "Resource": "*"
 },
 {
 "Sid": "VisualEditor1",
 "Effect": "Allow",
 "Action": [
 "s3:PutObject",
 "s3:GetObject",
 "s3:ListBucket",
 "s3:DeleteObject",
 "s3:GetBucketAcl"
],
 "Resource": [
 "arn:aws:s3:::<S3 location for supplementary files>",
 "arn:aws:s3:::<S3 location for supplementary files>/*"
]
 }
]
}

```

アカウント間 IAM ロールの設定方法の詳細については、AWS のドキュメントを参照してください。

## 手順 4。セキュリティグループの作成

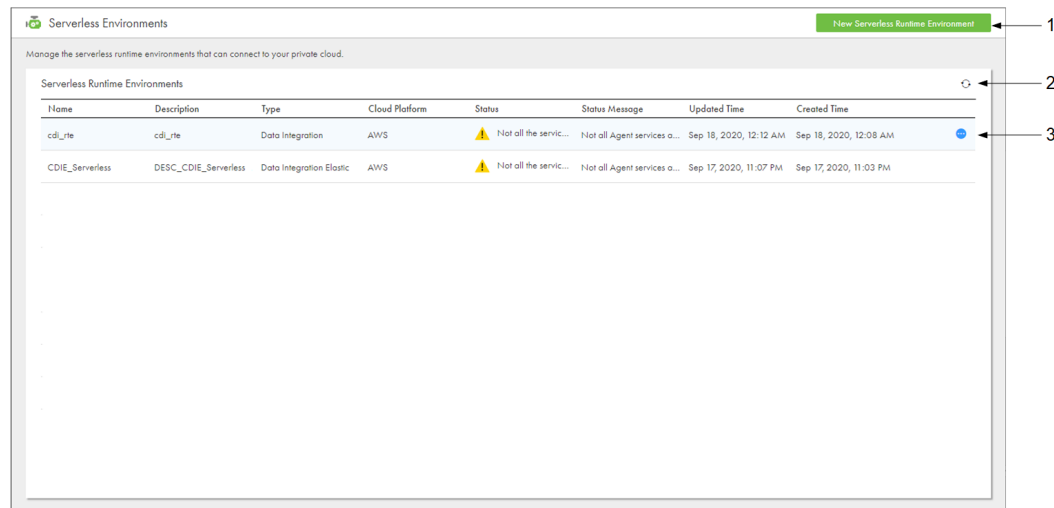
サーバーレスランタイム環境が ENI にアタッチするセキュリティグループを作成します。

セキュリティグループを作成する場合、セキュリティグループがすべてのインバウンドトラフィックを制限し、すべてのアウトバウンドトラフィックを許可することを確認します。

# サーバーレスランタイム環境のプロパティ

[サーバーレス環境] ページで、新しいサーバーレスランタイム環境を作成し、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パティを表示するには、環境の【アクション】メニューを展開し、【表示】を選択します。

次の図は、[サーバーレス環境] ページを示しています。



1. 新しいサーバーレスランタイム環境を作成するためのオプション
2. [更新] アイコン
3. アクション

## 基本設定

次の表は、サーバーレスランタイム環境に対して設定する基本プロパティの説明です。

プロパティ	説明
名前	サーバーレスランタイム環境の名前
説明	サーバーレスランタイム環境の説明。
タスクタイプ	サーバーレスランタイム環境で実行されるタスクのタイプ。 <ul style="list-style-type: none"><li>- データ統合を選択すると、データ統合を使用して作成されたタスクを実行します。</li><li>- Data Integration Elastic を選択すると、Data Integration Elastic を使用して作成されたタスクを実行します。</li></ul>
クラウドプラットフォーム	サーバーレスランタイム環境をホストするクラウドプラットフォーム。 使用できるのは Amazon Web Services (AWS) のみです。

プロパティ	説明
最大コンピューティングユニット	タスクが使用できる、マシンリソースに対応するサーバーレスコンピューティングユニットの最大数。
タスクのタイムアウト	タスクを終了する前に、タスクが完了するまで待機する時間の長さ。タイムアウトにより、タスクがハングしたときにサーバーレスコンピューティングユニットが無応答にならないようにします。 デフォルトでは、タイムアウトは 2880 分（48 時間）です。タイムアウトは 2880 分未満の値に設定できます。

## クラウドデータ統合設定

次の表は、サーバーレスランタイム環境の IAM ロールを作成するのに使用するプロパティの説明です。

プロパティ	説明
Informatica アカウント番号	サーバーレスランタイム環境が作成されるクラウドプラットフォームの Informatica のアカウント番号。アカウント番号は自動的に取り込まれます。
外部 ID	サーバーレスランタイム環境用に作成するロールに関連付ける外部 ID。生成された外部 ID を使用することも、固有の外部 ID を指定することもできます。

## AWS リソース設定

AWS リソース設定では、サーバーレスランタイム環境の、AWS アカウントと、マッピングで使用するソースおよびターゲットへの接続方法を指定します。

以下の表に、プロパティを示します。

プロパティ	説明
設定名	AWS リソース設定の名前。 名前は、最大 255 文字の ASCII 文字で構成される必要があります。
設定の説明	AWS リソース設定の説明。 説明は、最大 255 文字の ASCII 文字で構成される必要があります。
アカウント番号	クラウドプラットフォームでのアカウント番号。
リージョン	クラウドプラットフォームでのリージョン。マッピングで使用するソースおよびターゲットは、リージョンに存在するか、リージョンからアクセスできる必要があります。
AZ ID	可用性ゾーンの識別子。マッピングで使用するソースおよびターゲットは、リージョンに存在するか、可用性ゾーンからアクセスできる必要があります。
VPC ID	Amazon Virtual Private Cloud (VPC) の ID。VPC ではマッピングで使用するソースおよびターゲットにアクセスするためのエンドポイントが設定されている必要があります。 例えば、vpc-2f09a348 です。

プロパティ	説明
サブネット ID	VPC 内のサブネットの ID。サブネットにはマッピングで使用するソースおよびターゲットにアクセスするためのエンドポイントが含まれている必要があります。 例えば、subnet-b46032ec です。
セキュリティグループ ID	サーバーレスランタイム環境が ENI にアタッチするセキュリティグループの ID。タスクで使用するソースおよびターゲットにアクセスできるセキュリティグループ。 例えば、sg-e1fb8c9a です。
ロール名	サーバーレスランタイム環境が AWS アカウントで想定できる IAM ロールの名前。 このロールには、ENI を作成、読み取り、削除、リスト、デタッチおよびアタッチする権限が必要です。補足ファイルの場所に対する読み取りおよび書き込み権限も必要です。 ロールのポリシーを作成するときに、Informatica アカウント番号および外部 ID を使用します。
AWS タグ	AWS アカウントで作成される ENI のラベルを付ける AWS タグ。 各タグは、Key=string,Value=string というフォーマットのキーと値のペアにする必要があります。Key と Value は大文字小文字の区別があります。複数のタグはスペースで区切ります。
補足ファイルの場所	特定のトランスフォーメーションおよびコネクタ用の JAR ファイルや外部ライブラリなど補足ファイルを格納するための Amazon S3 の場所。 例えば、Java トランスフォーメーションでサードパーティまたはカスタムの Java パッケージを使用する場合、JAR ファイルを S3 の場所に追加し、サーバーレスランタイム環境用の S3 の場所を指定します。 s3://<bucket name>/<folder name>の形式を使用します。

## サーバーレスランタイム環境の編集

環境のステータスに基づいて、サーバーレスランタイム環境のプロパティを編集できます。

- 稼働中。サーバーレスコンピューティングユニットの最大数またはタスクタイムアウトを更新できます。  
サーバーレスコンピューティングユニットの最大数またはタスクタイムアウトを編集すると、更新された値が後続のタスク実行で有効になります。
- 失敗。任意のプロパティを更新できます。プロパティを有効にするには、サーバーレスランタイム環境を再デプロイします。

サーバーレスランタイム環境が異なるステータスを持つ場合は、サーバーレスランタイム環境を削除し、新しい環境を作成してプロパティを編集する必要があります。

サーバーレスランタイム環境を削除する前に、次のタスクを完了します。

- Monitor を使用して、環境でジョブが実行されていないことを確認します。
- サーバーレスランタイム環境を使用している接続およびタスクから、そのサーバーレスランタイム環境を削除します。

## サーバーレスランタイム環境の再デプロイ

次の状況では、サーバーレスランタイム環境を再デプロイできます。

- ライセンスを変更する。

- 組織がサーバーレスコンピューティングユニットを使い果たしたため、サーバーレスランタイム環境がシャットダウンする。組織にコンピューティングユニットをさらに追加して、サーバーレスランタイム環境を再デプロイできます。
- クラウド環境で設定を更新する。例えば、補足ファイルの場所にある JAR ファイルを更新する場合や、IAM ロールにアタッチされたポリシーを更新する場合です。

サーバーレスランタイム環境を再デプロイする前に、Monitor を使用して、環境でジョブが実行されていないことを確認します。次に、Administrator で、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、【再デプロイ】をくりくします。

## サーバーレスランタイム環境のクローン作成

サーバーレスランタイム環境のクローンを作成して、同様の設定を持つ別の環境を作成できます。例えば、クラウド環境内の別のサブネットに接続したり、別のセキュリティグループを使用したりする、同様のサーバーレスランタイム環境を作成することができます。

サーバーレスランタイム環境のクローンを作成するには、サーバーレスランタイム環境の【アクション】メニューを展開して、【クローン】をクリックします。

## ルールおよびガイドライン

サーバーレスランタイム環境を作成する場合、次のルールおよびガイドラインを考慮してください。

- 組織には最大で 10 のサーバーレスランタイム環境を作成できます。トライアルライセンスでは、最大で 2 つの環境を作成できます。
- サーバーレスランタイム環境あたり最大で 10 のタスクを同時に実行できます。
- サーバーレスランタイム環境が使用可能になるには少なくとも 5 分かかります。【サーバーレス環境】ページを使用して、環境のステータスを追跡し、ステータスメッセージを確認します。

## ディザスタリカバリ

障害がサーバーレスランタイム環境をホストするリージョンまたは可用性ゾーンに影響を与える場合は、組織のディザスタリカバリ計画の一環として、安定したリージョンまたは可用性ゾーンの一時的なサーバーレスランタイム環境にジョブをリダイレクトします。

### ディザスタリカバリの手順

障害の発生中は、サーバーレスランタイム環境のすべての仮想マシンがシャットダウンし、その環境でジョブを実行できなくなります。

データの損失とダウンタイムを最小限に抑えるには、次のタスクを実行します。

1. 安定したリージョンまたは可用性ゾーンに一時的なサーバーレスランタイム環境を作成します。
2. ジョブで使用される接続が、安定したリージョンまたは可用性ゾーンで使用できることを確認します。
3. 不完全なジョブ実行に関連するデータをクリーンアップします。
4. ジョブを一時的な環境にリダイレクトします。

### プライマリ環境の復元

プライマリサーバーレスランタイム環境をホストするリージョンまたは可用性ゾーンが回復したら、プライマリ環境をリストアできます。

プライマリ環境をリストアするには、以下の操作を実行します。

1. プライマリ環境の AWS アカウントで作成された ENI をクリーンアップします。
2. プライマリ環境を再デプロイします。
3. ジョブをプライマリ環境にリダイレクトします。
4. 一時的な環境を削除します。

## サーバーレスランタイム環境でのコネクタ

サーバーレスランタイム環境で使えるコネクタは、環境で実行されるマッピングのタイプによって決まります。

次のいずれかのマッピングタイプに基づいてコネクタを使用します。

### エラスティックマッピング

サーバーレスランタイム環境は、次のコネクタを使用してソースおよびターゲットに接続できます。

- Amazon Redshift V2
- Amazon S3 V2
- JDBC V2
- Snowflake Cloud Data Warehouse V2

### マッピング

サーバーレスランタイム環境は、次のコネクタを使用してソースおよびターゲットに接続できます。

- Amazon Aurora コネクタ
- Amazon Redshift V2 コネクタ
- Amazon S3 V2 コネクタ
- Box コネクタ
- Box OAuth コネクタ
- CDM フォルダコネクタ
- Concur V2 コネクタ
- Coupa V2 コネクタ
- DB2 Warehouse on Cloud コネクタ
- Eloqua Bulk API コネクタ
- Google Analytics コネクタ
- Google BigQuery V2 コネクタ
- Google Cloud Spanner コネクタ
- Google Cloud Storage V2 コネクタ
- Marketo V3 コネクタ
- Microsoft Azure Blob Storage V3 コネクタ
- Microsoft Azure Cosmos DB SQL API コネクタ

- Microsoft Azure Data Lake Store Gen2 コネクタ
- Microsoft Azure Data Lake Store V3 コネクタ
- Microsoft Azure SQL Data Warehouse V3 コネクタ
- Microsoft Dynamics 365 for Sales コネクタ
- Microsoft Dynamics CRM コネクタ
- Microsoft SQL Server コネクタ
- MongoDB コネクタ
- MySQL コネクタ
- NetSuite V2 コネクタ
- Oracle コネクタ
- PostgreSQL コネクタ
- REST V2 コネクタ
- Salesforce コネクタ
- Salesforce Marketing Cloud コネクタ
- Salesforce OAuth コネクタ
- ServiceNow コネクタ
- Snowflake Cloud Data Warehouse V2 コネクタ
- SuccessFactors ODATA コネクタ
- SuccessFactors SOAP コネクタ
- Workday V2 コネクタ
- Zendesk V2 コネクタ

**注:** サーバーレスランタイム環境の使用方法は、コネクタ固有です。詳細については、関連するコネクタのヘルプを参照してください。



## 第 13 章

# Secure Agent サービス

Secure Agent サービスは、Secure Agent がデータ処理に使用するプラグブルマイクロサービスです。例えば、Secure Agent はデータ統合サーバーを使用してデータ統合ジョブを実行し、プロセスサーバーを使用してアプリケーション統合を実行してオーケストレーションジョブを処理します。各 Secure Agent サービスは、エージェントで実行されている他のサービスとは独立して実行されます。

独立したサービスアーキテクチャには、次の利点があります。

- コネクタまたはパッケージを追加したときに、Secure Agent が再起動しない。
- サービスは、別のサービスの再起動時に影響を受けない。例えば、データ統合サーバーを再起動しても、プロセスオーケストレーションジョブは引き続き実行されます。
- アップグレード中のダウンタイムは最小化されます。アップグレードプロセスは、Secure Agent の新しいバージョンをインストールし、コネクタパッケージを更新し、データ統合サーバーの構成の変更を適用します。ダウンタイムを最小化するために、古いエージェントは引き続き使用可能なままで、アップグレード中にデータ統合ジョブを実行し続けます。Secure Agent の新しいバージョンは、アップグレードプロセスの完了後に開始されるジョブを実行します。

Secure Agent で実行されるジョブは、ライセンスと組織で使用されている Informatica Intelligent Cloud Services によって異なります。

以下の表に、Secure Agent で実行できるサービスと、それらのサービスを使用する Informatica Intelligent Cloud Services を示します。

Secure Agent サービス	説明	次により使用
API マイクロゲートウェイサービス	Secure Agent で実行されるアプリケーションの統合プロセスを管理します。 <b>プレビューに関する注意:</b> Fall 2020 October リリースでは、API マイクロゲートウェイサービスがプレビューで使用可能になりました。	アプリケーションの統合、API マネージャ
B2B プロセッサ	B2B Gateway のインバウンドおよびアウトバウンドプロセスフローを実行します。 <b>注:</b> Informatica グローバルカスタマサポートから指示されない限り、このサービスは設定しないでください。	B2B Gateway
CIH プロセッサ	プライベートパブリケーションリポジトリを使用する組織のために、Cloud Integration Hub のパブリケーションおよびサブスクリプションを実行します。	Cloud Integration Hub
CMI ストリーミングエージェント	一括取り込みサービスでストリーミング取り込みジョブを実行します。	一括取り込みサービス

Secure Agent サービス	説明	次により使用
共通統合コンポーネント	シェルスクリプトまたはバッチコマンドをタスクフローのコマンドタスクステップで実行します。	データ統合
データベース取り込み	一括取り込みサービスでデータベース取り込みジョブを実行します。	一括取り込みサービス
データ統合サーバー	マッピング、タスク、およびタスクフローインスタンスなどのデータ統合ジョブを実行します。	B2B Gateway Cloud Integration Hub、 Azure のデータアクセラレータ、 データ統合 データプロファイリング
EDC 検索エージェント	Azure のデータアクセラレータのため、およびデータ統合でのデータカタログ検出のために、Enterprise Data Catalog データアセットを検出します。 <b>注:</b> Informatica グローバルカスタマサポートから指示されない限り、このサービスは設定しないでください。	Azure のデータアクセラレータ、 データ統合
エラスティックサーバー	エラスティッククラスターおよびそのクラスターで実行するエラスティックジョブを管理します。	データ統合
ファイル統合サービス	リモートサーバーとのファイルの送信または受信、あるいはその両方に、HTTPS、AS2 および SFTP などのファイル転送プロトコルを使用します。	B2B Gateway、データ統合
一括取り込み	ファイル取り込みタスクおよびファイルリスナジョブを実行します。 <b>注:</b> Informatica グローバルカスタマサポートから指示されない限り、このサービスは設定しないでください。	一括取り込みサービス
OI データコレクタ	データコレクタを実行し、オペレーションインサイトのための PowerCenter 統合サービスグリッド自動スケーリングを実行します。 <b>注:</b> Informatica グローバルカスタマサポートから指示されない限り、このサービスは設定しないでください。	オペレーションインサイト
プロセスサーバー	アプリケーション統合プロセス、コネクタ、および接続を実行します。	アプリケーションの統合、 アプリケーション統合 コンソール

各サービスは、Tomcat 設定や Tomcat JRE 設定など、一連の設定プロパティを独自に備えています。パフォーマンスを最適化するため、または Informatica グローバルカスタマサポートから指示された場合は、サービスを設定したり、サービスのプロパティを変更しなければならないことがあります。Secure Agent サービスは、エージェントで実行されている他のサービスとは独立して実行されます。

# API マイクロゲートウェイサービス

API マイクロゲートウェイサービスは、Secure Agent で実行されるアプリケーションの統合プロセスを管理します。

**プレビュー情報:** 2020 October リリースから、API マイクロゲートウェイサービスをプレビューに使用できるようになりました。

評価目的でのプレビュー機能はサポートされていますが、保証対象外で本番環境には対応していません。非本番環境でのみ使用することをお勧めします。Informatica では、本番環境用に次のリリースでプレビュー機能を導入するつもりですが、市場や技術的な状況の変化に応じて導入しない場合もあります。詳細については、Informatica グローバルカスタマサポートにお問い合わせください。機能を使用するには、組織が適切なライセンスを所有している必要があります。

API マイクロゲートウェイサービスは、次の API マネージャのアクセスポリシーをサポートしています。

- IP フィルタリングポリシー
- レート制限ポリシー
- 基本認証

API マイクロゲートウェイサービスは、API マイクロゲートウェイプロキシを作成およびデプロイするための REST API を提供します。アプリケーションの統合プロセスは、サービス URL および SOAP サービス URL のエンドポイントを公開します。

API マイクロゲートウェイサービスを使用して、管理が必要な API エンドポイントへの API マイクロゲートウェイプロキシを構築できます。API マイクロゲートウェイサービスは、組織の Secure Agent マシン上に不変の Docker イメージとしてパッケージ化された API マイクロゲートウェイを構築します。その後、API マイクロゲートウェイサービスを使用して、API アクセス用の Secure Agent Docker ランタイム環境で Docker イメージコンテナに Docker イメージをデプロイします。API マイクロゲートウェイでは、アプリケーションの統合エンドポイントに要求を転送する前に設定した API アクセスポリシーが適用されます。

Docker イメージはブルーグリーンデプロイメントストラテジを使用して Secure Agent Docker ランタイム環境でホストされるため、API マイクロゲートウェイコンポーネントの更新中のダウンタイムはありません。

詳細およびカスタムライセンスの要求については、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。

## API Microgateway Service のプロパティ

API Microgateway Service の動作を変更または最適化するには、Secure Agent を編集するときに、**【システム構成の詳細】** 領域で API Microgateway Service のプロパティを設定します。API Microgateway Service を使用して、アプリケーション統合 API エンドポイントを管理できます。

次の図に、API Microgateway Service のプロパティを示します。

▼ System Configuration Details		
Service:	API Microgateway Service ▼	
Type:	All Types ▼	
Type	Name	Value
AGENT_RUNTIME_SETTINGS	project-name	'project1'
AGENT_RUNTIME_SETTINGS	docker-registry-name	'info.agent.apimgw'
DOCKER_CONTAINER_SETTINGS	blue	<a href="#">http-port: '16090'</a> <a href="#">https-port: '16095'</a>
DOCKER_CONTAINER_SETTINGS	green	<a href="#">http-port: '17090'</a> <a href="#">https-port: '17095'</a>
DOCKER_CONTAINER_SETTINGS	haproxy	<a href="#">http-port: '6090'</a> <a href="#">https-port: '6095'</a>

以下の API Microgateway Service のプロパティを設定できます。

タイプ	名前	説明
AGENT_RUNTIME_SETTINGS	project-name	API 設定を保存するプロジェクトの名前。新しいプロジェクトを作成する場合など、必要に応じて名前を変更できます。
AGENT_RUNTIME_SETTINGS	docker-registry-name	Secure Agent マシン上の名前付きおよびタグ付きの API Microgateway Docker イメージをすべて含むローカルの Docker レジストリの名前。 <b>注:</b> Docker イメージまたはタグの名前に制限付きの文字が含まれる場合、イメージの構築は失敗します。Docker イメージおよび名前タグには、次の文字を含めることはできません: - , .
DOCKER_CONTAINER_SETTINGS	blue	Secure Agent マシンに最初にデプロイされる Docker イメージコンテナ (green と交互になります)。 blue コンテナの次のデフォルトポートを変更できます。 - http-port: '16090' - https-port: '16095'

タイプ	名前	説明
DOCKER_CONTAINER_SETTINGS	green	Secure Agent マシンに 2 番目にデプロイされる Docker イメージコンテナ (blue と交互になります)。 green コンテナの次のデフォルトポートを変更できます。 - http-port: '17090' - https-port: '17095'
DOCKER_CONTAINER_SETTINGS	haproxy	Secure Agent マシン上の Docker イメージコンテナのルーター。停止時間をゼロにするために、blue コンテナと green コンテナの間でトラフィックを切り替えます。 haproxy コンテナの次のデフォルトポートを変更できます。 - http-port: '6090' - https-port: '6095'

**注:** 3 つの Docker イメージコンテナをすべて停止することで、API Microgateway を停止することができます。

## CMI ストリーミングエージェント

CMI ストリーミングエージェントを使用して、ストリーミング統合タスクを定義し、展開します。ストリーミング統合タスクを一括取り込みサービスで設定します。

CMI ストリーミングエージェントは、オンプレミスシステムで実行され、一括取り込みストリーミングサービスと連携して動作します。オンプレミスシステムで、CMI ストリーミングエージェントは一括取り込みストリーミングで展開されたジョブを実行します。エージェントは各ジョブのステータスおよび統計情報を更新します。

**注:** Informatica Intelligent Cloud Services 一括取り込みサービスの 2020 年 4 月のリリースよりも前、CMI ストリーミングエージェントは、ストリーミング取り込みエージェントという名前でした。

## CMI ストリーミングエージェントのプロパティ

CMI ストリーミングエージェントの動作を変更または最適化するには、ランタイム環境でエージェントプロパティを設定します。CMI ストリーミングエージェントのプロパティは、Secure Agent の編集時に **【システム構成の詳細】** 領域で設定します。

CMI ストリーミングエージェントのエンジン、エージェント、およびスクリプトのプロパティを設定できます。

次の図は、CMI ストリーミングエージェントのプロパティの一部を示しています。

▼ System Configuration Details

Service: 

CMI Streaming Agent

Type: 

All Types

Type	Name	Value
Engine	MaxLogFileSize	'5MB'
Engine	LogLevel	'DEBUG'
Agent	DataflowPullInterval	60
Agent	JVM	'-Xms256M -Xmx256M'
Agent	LogLevel	'DEBUG'
Agent	MaxLogFileSize	'10MB'
Agent	MaxNumberOfBackups	5
Scripts	LogLevel	'DEBUG'
Scripts	MaxFileSize	'5MB'
Scripts	MaxBackupIndex	5

CMI ストリーミングエージェントの次のプロパティを設定できます。

タイプ	プロパティ名	説明
Engine	MaxLogFileSize	エンジンが作成可能なログファイルの最大サイズ。 デフォルトは 5 MB です。
エンジン	LogLevel	エンジンのログレベル。
エージェント	DataflowPullInterval	エージェントがタスクで更新を確認するまでの間隔。 デフォルトは 60 秒です。
エージェント	JVM	エージェントの JVM プロパティのリスト。例：[-Xms256M -Xmx256M]
エージェント	LogLevel	エージェントのログレベル。
エージェント	MaxLogFileSize	エージェントが作成可能なログファイルの最大サイズ。 デフォルトは 10MB です。

タイプ	プロパティ名	説明
エージェント	MaxNumberOfBackups	エージェントのバックアップログファイルの最大数。 デフォルトは 5 です。
スクリプト	LogLevel	スクリプトのログレベル。
スクリプト	MaxFileSize	最大ファイルサイズ。この最大ファイルサイズに達した後、ログは ロールオーバーされ、新しいファイルが作成されます。 デフォルトは 10MB です。
スクリプト	MaxBackupIndex	ロールオーバー後に保持するバックアップファイルの最大数。 デフォルトは 5 です。

## 共通統合コンポーネント

共通統合コンポーネントサービスは、タスクフローのコマンドタスクステップ内で指定されたコマンドを実行する Secure Agent サービスです。

共通統合コンポーネントサービスを表示または設定するには、共通統合コンポーネントサービスとコマンド実行者パッケージのライセンスを所有している必要があります。

いくつかのサービスプロパティを設定して、共通統合コンポーネントサービスのパフォーマンスを最適化できます。サービスプロパティは、Secure Agent の編集時に変更できます。

共通統合コンポーネントサービスが処理するすべての要求は、次のディレクトリに記録されます。

<Secure Agent インストールディレクトリ>\apps\Common\_Integration\_Components\logs\<バージョン>

各コマンドタスクのログファイルは、次のディレクトリ内で参照できます。

<Secure Agent インストールディレクトリ>\apps\Common\_Integration\_Components\logs\command\<コマンドジョブ ID>

## 共通統合コンポーネントプロパティ

共通統合コンポーネントサービスの動作を変更する、または最適化するには、Secure Agent の編集時にプロパティを **【システム構成の詳細】** セクションで設定します。

次の画像は、共通統合コンポーネントサービスのプロパティを示しています。

▼ System Configuration Details

Service:	Common Integration Components ▼	
Type:	All Types ▼	
Type	Name	Value
Tomcat	NetworkTimeoutPeriod	300
Tomcat	NetworkRetryInterval	5
Tomcat	JRE_OPTS	'-Xms32m -Xmx512m -XX:MaxPermSize=128m'
Platform	LCM_JRE_OPTS	'-Xms32m -Xmx256m'
SYSTEM_CFG	TunnelTimeoutPeriod	300
SYSTEM_CFG	HTTP_CONNECTION_TIMEOUT_SECONDS	60
SYSTEM_CFG	HTTP_SOCKET_TIMEOUT_SECONDS	60
COMMAND_CFG	MaximumConcurrentJobs	10

以下の共通統合コンポーネントサービスのプロパティを設定できます。

タイプ	名前	説明
Tomcat	JRE_OPTS	Apache Tomcat プロセスの JRE VM オプション。
プラットフォーム	LCM_JRE_OPTS	Apache Tomcat プロセスを開始する、停止する、またはステータスを取得するための JRE オプション。 <b>注:</b> Informatica グローバルカスタマサポートから指示されない限り、このプロパティ値は変更しないでください。
SYSTEM_CFG	HTTP_CONNECTION_TIMEOUT_SECONDS	Secure Agent が Informatica Intelligent Cloud Services と通信するための HTTP 接続を設定するために待機する秒単位での最大時間。 デフォルトは 60 です。 <b>注:</b> Informatica グローバルカスタマサポートから指示されない限り、このプロパティ値は変更しないでください。
SYSTEM_CFG	HTTP_SOCKET_TIMEOUT_SECONDS	Secure Agent と Informatica Intelligent Cloud Services との間の HTTP 接続でデータパケットの転送中の秒単位での最大アイドル時間。 デフォルトは 60 です。 <b>注:</b> Informatica グローバルカスタマサポートから指示されない限り、このプロパティ値は変更しないでください。



タイプ	名前	説明
COMMAND_CFG	MaximumConcurrentJobs	<p>単一の Secure Agent によって実行できる同時コマンドタスクの最大数。</p> <p>1 つの Secure Agent グループ内の各 Secure Agent のデフォルト値は 10 です。</p> <p>例えば、1 つの Secure Agent グループ内に 3 つの Secure Agent がある場合、このサービスが処理できる同時コマンドタスクの最大数は 30 です。</p> <p>最大制限を超えたすべてのコマンド実行要求はキュー入れられ、Secure Agent が使用可能になると実行されます。</p>
<p><b>注:</b> Informatica グローバルカスタマサポートから指示されない限り、共通統合コンポーネントサービスの他のプロパティ値は変更しないでください。</p>		

## データベース取り込みサービス

データベース取り込みサービス（DBMI エージェント）を使用すると、データベース統合タスクを定義および実行できます。データベース統合サービスで一括取り込みタスクを設定します。

Secure Agent をランタイム環境にダウンロードした後、一括取り込みデータベースと DBMI パッケージの両方のカスタムライセンスを所有している場合には、Secure Agent が実行されているオンプレミスシステムに DBMI パッケージがプッシュされます。その後、必要に応じて Secure Agent で実行されるデータベース取り込みサービスのプロパティを設定できます。

### データベース取り込みサービスのプロパティ

Secure Agent が使用するデータベース取り込みサービス（DBMI エージェント）の動作を変更または最適化するには、ランタイム環境のデータベース取り込みのプロパティを設定します。

プロパティを設定するには、ランタイム環境を開きます。[システム構成の詳細] の下で、[編集] をクリックします。次に、[データベース取り込み] サービスと [DBMI\_AGENT\_CONFIG] タイプを選択します。

以下の表に、これらのエージェントプロパティを示します。

プロパティ	説明
maxTaskUnits	Secure Agent が実行されているオンプレミスマシンで同時に実行できるデータベース統合タスクの最大数。デフォルト値は 10 です。
serviceLogRetentionPeriod	<p>最終更新がファイルに書き込まれた後に、各内部データベース取り込みサービスログファイルが保持される日数。この保持期間が経過すると、ログファイルは削除されます。デフォルト値は 7 日です。</p> <p><b>注:</b> サービスログは、それらが作成された Secure Agent ホスト (&lt;infaagent&gt;/apps/Database_Ingestion/logs) に保持されます。</p>
taskLogRetentionPeriod	最終更新がジョブログファイルに書き込まれた後、各ジョブログファイルを保存する日数。この保持期間が経過すると、ログファイルは削除されます。デフォルト値は 7 日です。

プロパティ	説明
ociPath	Oracle ソースおよびターゲットの場合、Oracle Call Interface (OCI) ファイル oci.dll または libcIntsh.so へのパス。実行中の DBMI エージェントの場合、この値は Windows の PATH 環境変数で指定されたパス、または Linux の LD_LIBRARY_PATH 環境変数で指定されたパスに付加されます。
serviceUrl	データベース取り込みサービスが Informatica Intelligent Cloud Services クラウドへの接続に使用する URL。
logLevel	データベース取り込みサービスが生成するログに含める詳細レベル。次のオプションがあります。 <ul style="list-style-type: none"> <li>- トレース</li> <li>- デバッグ</li> <li>- 情報</li> <li>- 警告</li> <li>- エラー</li> </ul> デフォルト値はトレースです。

## データベース取り込みエージェントの環境変数

データベース取り込み（DBMI）エージェントの動作を変更または最適化するには、次の環境変数を定義します。

環境変数	説明
DBMI_REPLACE_UNSUPPORTED_CHARS	Microsoft Azure SQL Data Warehouse のターゲットに対して、ターゲットが正しく処理できない文字データ内の文字をデータベース取り込みジョブで置き換えるかどうかを制御します。文字の置き換えを有効にするには、この環境変数を true に設定します。  DBMI_REPLACE_UNSUPPORTED_CHARS=true  設定後、一括取り込みデータベースは、DBMI_UNSUPPORTED_CHARS_REPLACEMENT 環境変数に指定されている文字を使用して、サポートされていない文字を置き換えます。
DBMI_UNSUPPORTED_CHARS_REPLACEMENT	DBMI_REPLACE_UNSUPPORTED_CHARS 環境変数が true に設定されている場合に、Microsoft Azure SQL Data Warehouse ターゲットが正しく処理できないソースデータ内の文字を置き換える文字を指定します。 デフォルト値: ? (疑問符)
DBMI_WRITER_CONN_POOL_SIZE	データベース統合ジョブが変更データをターゲットにプロパゲートするために使用する接続の数を示します。デフォルト値は 8 です。有効な値は 4～8 です。

環境変数	説明
DBMI_WRITER_RETRIES_MAX_COUNT	データベース統合ジョブがソースデータを Amazon S3 または Microsoft Azure Data Lake Storage Gen2 ターゲットにロードしている最中にネットワークの問題が発生した場合に、データベース統合ジョブで初期ロードまたは増分ロードを続行する要求を再試行する最大回数を指定します。再試行がすべて失敗した場合、ジョブは失敗となります。 デフォルト値は 5 です。
DBMI_WRITER_RETRIES_INTERVAL_IN_MILLIS	ネットワークで問題が発生した場合に、データベース統合ジョブが Amazon S3 または Microsoft Azure Data Lake Storage Gen2 ターゲットへの初期ロードまたは増分ロードを続行する要求を再試行する前に待機する間隔（ミリ秒単位）を指定します。 デフォルト値は 1000 です。

**注:** 環境変数を定義または変更したら、データベース取り込みエージェントを再起動して、変更を有効にします。

## データ統合サーバー

データ統合サーバーは、マッピング、タスク、およびタスクフローインスタンスなどのデータ統合ジョブを実行する Secure Agent サービスです。

データ統合サーバーでは、エラスティックマッピングおよび関連するマッピングタスクを実行しません。タスクフローにエラスティックマッピングに基づいたマッピングが含まれている場合、データ統合サーバーはエラスティックサーバーに対するマッピングタスクを保留にして、タスクフロー内の別のタスクを実行します。

いくつかのサービスプロパティを設定して、データ統合サーバーのパフォーマンスを最適化できます。例えば、ネットワークの回復機能設定または Secure Agent の接続タイムアウト期間を変更できます。サービスプロパティは、Secure Agent の編集時に変更できます。

## データ統合サーバーの回復機能

ネットワークの一時的な問題が発生している際、Secure Agent が接続の再確立を試みている間、データ統合タスクを続行できます。データ統合サーバーのネットワークの回復機能プロパティを設定できます。

Secure Agent が接続の再確立を試みる方法は、次のデータ統合サーバーのプロパティで決定されます。

### NetworkTimeoutPeriod

Secure Agent で Informatica Intelligent Cloud Services との通信の再確立を試行する時間の長さを決定します。期間の終わりに通信が確立されていない場合、実行されていた進行中のデータ統合タスクは停止します。デフォルト値は 300 秒です。

### NetworkRetryInterval

Secure Agent が指定されたタイムアウト期間内に Informatica Intelligent Cloud Services への接続を試行する頻度を決定します。デフォルト値は 5 秒です。

例えば、デフォルト設定の場合、ネットワークが停止すると、Secure Agent は Informatica Intelligent Cloud Services との通信の再確立を 300 秒間試行します。その 300 秒の期間中、Secure Agent は 5 秒ごとに Informatica Intelligent Cloud Services への接続を試行します。300 秒の期間内に Secure Agent が通信を再

確立すれば、進行中のデータ統合タスクは影響を受けません。Secure Agent は、300 秒の期間内に通信を再確立できない場合、進行中のデータ統合タスクを停止します。

## データ統合サーバーのプロパティ

データ統合サーバーの動作を変更または最適化するには、データ統合サーバーのプロパティを設定します。データ統合サーバーのプロパティは、Secure Agent の編集時に **【システム構成の詳細】** 領域で設定します。

次の画像は、データ統合サーバーのプロパティを示しています。

▼ System Configuration Details		
Service:	Data Integration Server ▼	
Type:	All Types ▼	
Type	Name	Value
Tomcat	NetworkTimeoutPeriod	300
Tomcat	NetworkRetryInterval	5
Tomcat JRE	INFA_SSL	
Tomcat JRE	INFA_MEMORY	'-Xms32m -Xmx512m -XX:MaxPermSize=128m'
Tomcat JRE	JRE_OPTS	'-Xrs'
Tomcat JRE	JAVA_LIBS	
Tomcat Log4j	log4j_rootLogger	'INFO, tomcatLog'
Tomcat Log4j	log4j_appender_tomcatLog	'org.apache.log4j.FileAppender'
Tomcat Log4j	log4j_appender_tomcatLog_layout	'org.apache.log4j.PatternLayout'
Tomcat Log4j	log4j_appender_tomcatLog_layout_ConversionPattern	'%d %d{z} %p [%c] - %m%n'

設定可能なデータ統合サーバーのプロパティを次に示します。

タイプ	名前	説明
Tomcat	NetworkTimeoutPeriod	Secure Agent が Informatica Intelligent Cloud Services との通信の再確立を試行するまでの時間（秒）。デフォルトは 300 です。
Tomcat	NetworkRetryInterval	Secure Agent が、指定したタイムアウト期間内に Informatica Intelligent Cloud Services への接続を試行する頻度（秒）。デフォルトは 5 です。
Tomcat JRE	JRE_OPTS	Apache Tomcat プロセスの JRE VM オプション。
Tomcat JRE	INFA_MEMORY	Apache Tomcat プロセスの仮想マシンメモリに対して設定される JRE VM オプション。
DTM	AgentConnectionTimeout	Secure Agent 通信で、タイムアウトするまでに待機を要求する秒数。デフォルトは 5 です。

タイプ	名前	説明
DTM	JVMOption1 - JVMOption5	<p>最大および最小の JVM ヒープサイズ、インテリジェント構造検出の最大レコードサイズ、特定のコネクタのプロキシ設定などの、データ統合サーバーの詳細プロパティを設定する JVM オプション。例えば、最大 JVM ヒープサイズをデフォルト値の 512 MB から 2048 MB に変更するには、JVMOption1 を '-Xmx2048m' に設定します。</p> <p>デフォルトでは、JVMOption1 - JVMOption5 を使用して、最大 5 つの詳細プロパティを設定できます。追加のプロパティを設定するには、JVMOption6 や JVMOption7 などの名前を付けた、データ統合サーバー用のカスタム DTM プロパティを追加します。オプション番号が連続していて、番号を飛ばしていないことを確認してください。</p> <p>設定できる JVM オプションの詳細については、データ統合のヘルプ、適切なコネクタのヘルプ、または Informatica Network の <a href="#">Knowledge Base</a> を参照してください。</p>
<p><b>注:</b> Informatica グローバルカスタマサポートから指示されない限り、データ統合サーバーの他のプロパティ値は変更しないでください。</p>		

## エラスティックサーバー

エラスティックサーバーは、エラスティッククラスタとクラスタで実行されるエラスティックジョブを管理する Secure Agent サービスです。

エラスティックサーバーがログファイルに書き込む詳細のレベルを指定するために、サービスプロパティを設定できます。kops ロールと Secure Agent ロールをセットアップするために設定する必要のあるサービスプロパティもあります。詳細については、Data Integration Elastic の管理に関する項目を参照してください。

### エラスティックサーバーのプロパティ

エラスティックサーバーの動作を変更するには、Secure Agent の編集時に **【システム構成の詳細】** 領域でエラスティックサーバーのプロパティを設定します。

次の図は、エラスティックサーバーのプロパティを示しています。

The screenshot shows the 'System Configuration Details' window. At the top, there are two dropdown menus: 'Service:' set to 'Elastic Server' and 'Type:' set to 'All Types'. Below these is a table with three columns: 'Type', 'Name', and 'Value'.

Type	Name	Value
LOG4J_CFG	log4j_app_log_level	'INFO'
AWS_CFG	agent_role_external_id_key	
AWS_CFG	privileged_role_arn_key	
AWS_CFG	role_session_duration_secs_key	

設定できるエラスティックサーバーのプロパティを次に示します。

タイプ	名前	説明
LOG4J_CFG	log4j_app_log_level	<p>エラスティックサーバーがログファイルに書き込む詳細のレベル。「INFO」などの文字列としてログレベルを入力します。</p> <p>ログレベルを大きくすると、エラスティックサーバーがログファイルに書き込むメッセージに、より優先度の高いログレベルのメッセージが含まれます。例えば、ログレベルが INFO の場合、ログには FATAL、ERROR、WARNING、および INFO コードのメッセージが記録されます。</p> <p>有効な値は次のとおりです。</p> <ol style="list-style-type: none"><li>1. FATAL。サービスがシャットダウンする、または利用不可能になる修復不能なシステム障害が含まれます。</li><li>2. ERROR。接続の失敗、メタデータの保存または取得の失敗、サービスのエラーが含まれます。</li><li>3. WARNING。修復可能なシステム障害または警告が含まれます。</li><li>4. INFO。システムおよびサービスの変更に関するメッセージが含まれます。</li><li>5. TRACE。ユーザー要求の失敗がログとして記録されます。</li><li>6. DEBUG。ユーザー要求がログとして記録されます。</li></ol>
AWS_CFG	agent_role_external_id_key	<p>Secure Agent が kops ロールを使用する場合に Secure Agent で指定する外部 ID。kops ロールの信頼関係で外部 ID を設定する場合に必要です。</p> <p>Azure 環境では、このプロパティは無視してください。</p>
AWS_CFG	privileged_role_arn_key	<p>kops ロールの ARN。</p> <p>AWS 環境で個別の kops ロールと Secure Agent ロールを設定する場合に必要です。Azure 環境では、このプロパティは無視してください。</p>
AWS_CFG	role_session_duration_secs_key	<p>AWS AssumeRole API のセッション時間（秒単位）。デフォルトのセッション時間は 1,800 秒（30 分）です。</p> <p>kops ロールに設定されている最大 CLI/API セッション期間をオーバーライドします。エラスティックサーバーに設定されているセッション期間が kops ロールのセッション期間よりも長い場合、Secure Agent が kops ロールを使用できない場合があります。</p> <p>Azure 環境では、このプロパティは無視してください。</p>

## ファイル統合サービス

ファイル統合サービスを使用して、組織とリモートファイルサーバーの間でファイルを転送します。

ファイル統合サービスは、エージェントが AS2 などの高度なファイル転送プロトコルの実行に使用する Secure Agent のサービスです。

組織でリモートパートナーからファイルを受信出来るようにする前に、ファイルサーバーを設定しておく必要があります。管理者の「ファイルサーバー」ページで、ファイル統合サービスに関連付けられる組織のファイ

ルサーバーを設定します。設定には、ファイルサーバーの詳細、暗号化の方法、および許可されるファイルタイプなどのプロパティが含まれます。

ファイル統合サービスを停止または開始するには、サービスを使用するファイルサーバーを停止または開始します。

ファイルサーバーの設定に関する詳細については、[「ファイルサーバーの設定プロセス」](#) (ページ 166)を参照して下さい。

ファイル統合サービスを使用するには、組織が適切なライセンスを持っている必要があります。ファイル統合サービスを設定するには、管理者ロールが割り当てられている必要があります。

## 一括取り込み（ファイル）

一括取り込みファイルの動作を変更または最適化するには、[一括取り込み] プロパティを設定します。プロパティは、Secure Agent の編集時に **【システム構成の詳細】** 領域で設定します。

以下のプロパティを設定する事ができます。

タイプ	名前	説明
AGENT_RUNTIME_SETTINGS	file-listener-snapshot-dir	新しいファイルリスナコンポーネントのスナップショットが追加されるディレクトリ。次のディレクトリパスを追加できます。 <ul style="list-style-type: none"><li>- MassIngestionRuntime ディレクトリに対する相対パス。例: ../data/monitor。</li><li>- 絶対パス。以下に例を示します。 &lt;Secure agent installation directory&gt;/apps/MassIngestionRuntime/data/monitor <i>Secure agent installation directory</i> には Secure Agent がインストールされているディレクトリの名前が入ります。</li></ul> <b>注:</b> グループに複数の Secure Agent が存在する場合は、すべてのエージェントで共有されるスナップショットディレクトリを使用します。
AGENT_RUNTIME_SETTINGS	mi-task-workspace-dir	エージェント内のカスタムの場所のディレクトリ。ファイル取り込みタスクがファイルをターゲットに転送するときに中間ステージング領域として使用するエージェント内のカスタムディレクトリです。このパスは、共有場所、マウントされた場所、およびエージェント内のデフォルトの場所とは異なる場所にすることができます。
AGENT_RUNTIME_SETTINGS	file-listener-max-pool-size	ファイルリスナを実行するスレッドの最大数。デフォルトは 20 です。
AGENT_RUNTIME_SETTINGS	file-listener-core-pool-size	スレッドの合計数。デフォルトは 20 です。
AGENT_RUNTIME_SETTINGS	ftp-receive-socket-buffer-size	FTP インバウンドパケットのバッファサイズ。デフォルトは 16 バイトです。
AGENT_RUNTIME_SETTINGS	ftp-send-socket-buffer-size	FTP アウトバウンドパケットのバッファサイズ。デフォルトは 16 バイトです。

タイプ	名前	説明
AGENT_RUNTIME_SETTINGS	http-client-timeout	Informatica Intelligent Cloud Services へのエージェントの要求のタイムアウト時間（秒単位）。デフォルトは 30 秒です。
PGP_SETTINGS	public-keyring-path	パブリックキーリングを保存するディレクトリ。次のディレクトリパスを追加できます。 <ul style="list-style-type: none"> <li>- 一括取り込みがインストールされるディレクトリに対する相対パス。以下に例を示します。  <code>../data/pubring.pkr</code>  <code>pubring.pkr</code> にはパブリックキーリングを保存するファイルの名前が入ります。</li> <li>- 絶対パス。以下に例を示します。  <code>&lt;Secure agent installation directory&gt;/apps/MassIngestionRuntime/data/pubring.pkr</code>  <code>pubring.pkr</code> にはパブリックキーリングを保存するファイルの名前が、<code>Secure agent installation directory</code> にはエージェントがインストールされているディレクトリの名前が入ります。</li> </ul>
PGP_SETTINGS	secret-keyring-path	シークレットキーリングを保存するディレクトリ。次のディレクトリパスを追加できます。 <ul style="list-style-type: none"> <li>- 一括取り込みがインストールされるディレクトリに対する相対パス。以下に例を示します。  <code>../data/secring.pkr</code>  <code>secring.pkr</code> にはシークレットキーリングを保存するファイルの名前が入ります。</li> <li>- 絶対パス。以下に例を示します。  <code>&lt;Secure agent installation directory&gt;/apps/MassIngestionRuntime/data/secring.pkr</code>  <code>secring.pkr</code> にはシークレットキーリングを保存するファイルの名前が、<code>Secure Agent installation directory</code> にはエージェントがインストールされているディレクトリの名前が入ります。</li> </ul>
JVM_SETTINGS	app-heap-size	一括取り込みファイルアプリケーションの最小および最大ヒープサイズ。 デフォルトは-Xms256m -Xmx2048m です。
JVM_SETTINGS	lcm-heap-size	ライフサイクル管理スクリプトの最小および最大ヒープサイズ。 デフォルトは-Xms32m -Xmx128m です。

## プロセスサーバー

プロセスサーバーとは、アプリケーションの統合のプロセス、コネクタ、および接続を実行する Secure Agent サービスです。

Secure Agent にアプリケーション統合のアセットをデプロイしたら、プロセスサーバーにもデプロイします。アセットを実行すると、プロセスサーバーによって実行されます。



PostgreSQL データベースには Secure Agent のプロセスサーバーサービスが付属しており、プロセスサーバーが収集および生成したメタデータが格納されます。

システムの次の場所にある PostgreSQL ディレクトリを検索します。

```
<Secure Agent installation directory>\apps\process-engine\data\PostGreSql
```

## プロセスサーバーのプロパティ

プロセスサーバーの動作を変更または最適化するには、プロセスサーバーのプロパティを設定します。サーバー、Secure Agent グループ、Java 仮想マシン、コネクタ、データベース、およびログプロパティを設定できます。

次の図に、一部のプロセスサーバーのプロパティを示しています。

Type	Name	Value
server	host-name	'ink17.informatica.com'
server	shutdown-port	7005
server	key-alias	'localhost'
server	key-store	'./conf/ae.keystore'
server	key-store-password	'password'
server	trust-store	'./conf/ae.cacerts'
server	trust-store-password	'changeit'
server	ldap-enabled-realm	false
server	ldap-properties	<div>- key: connectionURL value: ldap://\$(host.name):10389 - key: connectionName value: uid=admin,ou=system - key: connectionPassword value: \$(pe.ldap.password) - key: authentication value: simple - key: userBase value: ou=people,DC=\$(host.name),DC=informatica,DC=com - key: userSearch value: (uid=0) - key: roleBase value: ou=groups,DC=\$(host.name),DC=informatica,DC=com - key: roleName value: cn - key: roleSearch value: (uniqueMember=0)</div>
server	host-name	'localhost'
server	shutdown-port	7005
server	key-alias	'localhost'
server	key-store	'./conf/ae.keystore'
server	key-store-password	'password'
server	trust-store	'./conf/ae.cacerts'
server	trust-store-password	'changeit'
server	ldap-enabled-realm	false
server	ldap-properties	<div>- key: connectionURL value: ldap://\$(host.name):10389 - key: connectionName value: uid=admin,ou=system - key: connectionPassword value: \$(pe.ldap.password) - key: authentication value: simple - key: userBase value: ou=people,DC=\$(host.name),DC=informatica,DC=com - key: userSearch value: (uid=0) - key: roleBase value: ou=groups,DC=\$(host.name),DC=informatica,DC=com - key: roleName value: cn - key: roleSearch value: (uniqueMember=0)</div>
server	ssl-enabled-protocols	'TLSv1.2'
server	ephemeral-DH-key-size	2048
server	use-secure-ciphers-only	true

注: [システム構成の詳細] の [カスタム構成の詳細] を編集しないでください。変更内容は反映されません。

以下のサーバープロパティを設定できます。

名前	通信方式	説明
host-name	Secure Agent チャンネル	プロセスエンジンサーバーのホスト名。
shutdown-port	Secure Agent チャンネル	プロセスサーバー Tomcat のシャットダウンポート。
key-alias	HTTPS	HTTPS 通信のセキュリティキーが含まれるキーストアレコードの識別子。
key-store	HTTPS	アプリケーションの統合が HTTPS 通信に使用するキーストアファイルへのパス。Secure Agent をインストールした場合は、デフォルトの場所である <Secure Agent インストールディレクトリ>/apps/process-engine/conf/ae.keystore からキーストアを探します。ここで、ae.keystore はキーストアファイルです。 <b>重要:</b> キーストアファイルへのパスのみを入力します。
key-store-password	HTTPS	キーストアのパスワード。デフォルトパスワードは password です。
trust-store	HTTPS	アプリケーションの統合が HTTPS 通信に使用するトラストストアファイルへのパス。Secure Agent をダウンロードした場合は、デフォルトの場所である process-engine/conf/ae.cacerts からトラストストアを探します。ここで、ae.cacerts はトラストストアファイルです。 サービスエンドポイント認証の公開証明書をインポートする場合は、<Secure Agent インストールディレクトリ>\apps\process-engine\conf\certs に格納します。 <b>重要:</b> トラストストアファイルへのパスのみを入力します。
trust-store-password	HTTPS	トラストストアのパスワード。デフォルトのパスワードは changeit です。パスワードは変更できます。
ldap-enabled-realm	HTTP/HTTPS	認証に LDAP プロバイダを使用する場合は、このプロパティを [True] に設定します。クラスタ化された Secure Agent を使用する場合は、LDAP プロバイダを認証の一括管理用として使用します。
ldap-properties	HTTP/HTTPS	設定する必要がある LDAP プロパティ。LDAP プロバイダに合うように既存のプロパティを編集します。 <b>注:</b> LDAP パスワードは画面に表示されません。\$(pe.ldap.password)の値は環境変数 PE_LDAP_PASSWORD から取得されます。
ssl-enabled-protocols	HTTPS	使用する TLS プロトコル。デフォルトのプロトコルは最も安全なプロトコルである TLSv1.2 です。互換性の問題が発生した場合のみ、この値を TLSv1.0 または TLSv1.1 などの古いバージョンに変更します。
ephemeral-DH-key-size	HTTPS	安全なアルゴリズムのキーの長さ。デフォルト値は 2048 です。互換性の問題が発生した場合のみ、この値を変更します。
use-secure-ciphers-only	HTTPS	エンドポイントの呼び出し時に使用する暗号セットを安全な暗号のみに制限します。デフォルト値は [True] です。互換性の問題が発生した場合のみ、この値を [False] に変更します。

次の Secure Agent グループ（UI では「クラスタ」）のプロパティを設定できます。

名前	通信方式	説明
name	HTTP/ HTTPS	Secure Agent グループの名前。
primary-node	HTTP/ HTTPS	Secure Agent をマスタエージェントにする場合は、このプロパティを [True] に設定します。マスタエージェントを選択する場合は、Secure Agent クラスタを作成します。クラスタでは、すべての Secure Agent がマスタ Secure Agent の PostgreSQL データベースを共有します。
load-balance-url	HTTP/ HTTPS	Secure Agent にデプロイされたプロセスの呼び出しに使用できるロードバランサ URL。 ロードバランサを使用する場合に適用されます。

次の Java 仮想マシンのプロパティを設定できます。

名前	通信方式	説明
min-heap	Secure Agent チャネル	プロセスサーバーが Tomcat JVM に割り当てる最小ヒープメモリ。
max-heap	Secure Agent チャネル	プロセスサーバーが Tomcat JVM に割り当てる最大ヒープメモリ。
additional-properties	Secure Agent チャネル	Tomcat JVM セットに追加できるカスタムシステムプロパティ。例えば、カスタムプロパティ -Dsun.net.inetaddr.ttl=60 を設定できます。

以下のコネクタプロパティを設定できます。

名前	通信方式	説明
http-port	HTTP	Secure Agent がデータを送信する HTTP ポート。デフォルトのポートは 7080 です。 REST および SOAP エンドポイントの URL の構造について詳しくは、アプリケーションの統合ヘルプを参照してください。
http-maxThreads	HTTP	プロセスサーバーが HTTP を介してアプリケーションの統合で作成する接続の最大数。
http-connectionTimeout	HTTP	プロセスサーバーが HTTP 接続の応答を待機する最大時間（ミリ秒単位）。
https-port	HTTPS	Secure Agent がデータを送信する HTTPS ポート。デフォルトのポートは 7443 です。 REST および SOAP エンドポイントの URL の構造について詳しくは、アプリケーションの統合ヘルプを参照してください。
https-maxThreads	HTTPS	プロセスサーバーが HTTPS を介してアプリケーションの統合で作成する接続の最大数。
https-connectionTimeout	HTTPS	プロセスサーバーが HTTPS 接続の応答を待機する最大時間（ミリ秒単位）。

名前	通信方式	説明
secure-channel maxThreads	Secure Agent チャンネル	プロセスサーバーがアプリケーションの統合で作成する接続の最大数。
secure-channel-connectionTimeout	Secure Agent チャンネル	プロセスサーバーが接続の応答を待機する最大時間（ミリ秒単位）。

以下のデータベースプロパティを設定できます。

名前	通信方式	説明
type	Secure Agent チャンネル	プロセスサーバーが実行されるデータベースタイプ。 <b>重要:</b> この設定は変更しないでください。アプリケーションの統合 Secure Agent は他のデータベースをサポートしていません。
driver	Secure Agent チャンネル	プロセスサーバーが実行されるデータベースドライバ。 <b>重要:</b> この設定は変更しないでください。Informatica Cloud Secure Agent は他のデータベースをサポートしていません。
URL	Secure Agent チャンネル	プロセスサーバーがデータベースにアクセスするときの URL。 <b>重要:</b> この設定は変更しないでください。Informatica Cloud Secure Agent は他のデータベースをサポートしていません。
maxActive	Secure Agent チャンネル	プロセスサーバーデータベースに同時に割り当てられるアクティブな接続の最大数。
maxIdle	Secure Agent チャンネル	データベースで一度にアイドル状態のままにできる接続の最大数。アイドル状態の接続数がこの数を越えると、プロセスサーバーは接続を解放します。
maxWait	Secure Agent チャンネル	接続が存在しない場合にデータベースが待機する最大時間。
connection-properties	Secure Agent チャンネル	データベース接続プロパティのキーと値のペア。デフォルトでは、一部のキーが使用できます。 デフォルトのキーは削除しないでください。ただし、次のキーの値は変更できます。 他のキーと値のペアを追加できます。例えば、次のキーと値のペアを追加できます。 キー: autoReconnect 値: true

以下のログプロパティを設定できます。

名前	通信方式	説明
1catalina_org_apache_juli_FileHandler_level	Secure Agent チャンネル	ファイル内のログのレベル: <Secure Agent インストールディレクトリ>\apps\process-engine\logs\catalina.log. デフォルト: FINE
2localhost_org_apache_juli_FileHandler_level	Secure Agent チャンネル	ファイル内のログのレベル: <Secure Agent インストールディレクトリ>\apps\process-engine\logs\localhost.log. デフォルト: FINE
3manager_org_apache_juli_FileHandler_level	Secure Agent チャンネル	ファイル内のログのレベル: <Secure Agent インストールディレクトリ>\apps\process-engine\logs\manager.log. デフォルト: FINE
4host_manager_org_apache_juli_FileHandler_level	Secure Agent チャンネル	ファイル内のログのレベル: <Secure Agent インストールディレクトリ>\apps\process-engine\logs\host-manager.log. デフォルト: FINE
java_util_logging_ConsoleHandler_level	Secure Agent チャンネル	Tomcat の起動時に表示される CMD ウィンドウでのログのレベル。 デフォルト: FINE
org_apache_catalina_core_ContainerBase_Catalina_localhost_level	Secure Agent チャンネル	仮想マシンで Tomcat をホストするときの localhost.log ファイルでのログのレベル。 デフォルト: INFO

名前	通信方式	説明
org.apache.catalina.core.ContainerBase.Catalina_localhost.manager.level	Secure Agent チャンネル	仮想マシンで Tomcat をホストするときの manager.log ファイルでのログのレベル。 デフォルト: INFO
org.apache.catalina.core.ContainerBase.Catalina_localhost.host-manager.level	Secure Agent チャンネル	仮想マシンで Tomcat をホストするときの host-manager.log ファイルでのログのレベル。 デフォルト: INFO

## デフォルト接続データベースのプロパティ

次の表では、connection-properties データベースプロパティで利用可能なデフォルトキーについて説明します。

キー	説明
timeBetweenEvictionRuns	アイドル状態のオブジェクト evictor スレッドの実行と実行の間にプロセスサーバーが待機する時間（ミリ秒）。
testOnBorrow value	プロセスサーバーはプールからオブジェクトを借用する前にオブジェクトを検証します。プロセスサーバーがオブジェクトを検証できない場合、プールからこのオブジェクトは削除されます。次に、プロセスサーバーは別のオブジェクトを借用しようとします。
testWhileIdle	プロセスサーバーは、アイドル状態のオブジェクト evictor（存在する場合）によってオブジェクトを検証します。プロセスサーバーがオブジェクトを検証できない場合、プールからこのオブジェクトは削除されます。
validationQuery value	呼び出し元に返す前にこのプールの接続を検証する SQL クエリ。このプロパティを指定する場合は、クエリが 1 つ以上の行を返す SQL SELECT ステートメントである必要があります。

## ログレベル

次の表に、プロセスサーバーの【ログ】プロパティで設定できるレベルを示しています。

レベル	説明
SEVERE	エラーを記録します。
WARNING	潜在的に有害な状況を記録します。
INFO	アプリケーションの進行状況の概要を表す情報イベントを記録します。
CONFIG	INFO レベルよりも詳細な情報イベントを記録します。
FINE	アプリケーションのデバッグに使用できる詳細な情報イベントを記録します。

レベル	説明
FINER	FINE レベルよりも詳細な情報イベントを記録します。
FINEST	すべてのイベントを記録します。

## プロセスサーバーのサイズ決定に関する推奨事項

作業負荷に応じて Secure Agent のプロセスサーバーサービスを設定します。

リソースを最適化するには、次のサイズ決定に関する推奨事項を参照してください。

推奨事項	小	中	大
プロセス数	75	175	350
リソースキャッシュ (MB)	75	175	350
作業マネージャの最小スレッドプール	50	100	150
作業マネージャの最大スレッドプール	250	500	750
JVM 最小ヒープ (MB)	デフォルト	768	1024
JVM 最大ヒープ (MB)	デフォルト	デフォルト	4096

デフォルトの [JVM 最小ヒープ] は 512 MB で、デフォルトの [JVM 最大ヒープ] は 1536 MB です。

[プロセス数]、[リソースキャッシュ]、[作業マネージャの最小スレッドプール]、および [作業マネージャの最大スレッドプール] を設定するには、次の手順を実行します。

1. [Informatica Cloud] > [モニタ] > [サービスおよびプロセスコンソール] に移動します。
2. [コンソール] リストから、Secure Agent を選択します。
3. [管理] > [サーバーの設定] > [サーバープロパティ] に移動します。
4. [プロセス数]、[リソースキャッシュ]、[作業マネージャの最小スレッドプール]、および [作業マネージャの最大スレッドプール] プロパティの値を変更します。
5. [保存] をクリックします。

[JVM 最小ヒープ] および [JVM 最大ヒープ] を設定するには、次の手順を実行します。

1. [Informatica Cloud] > [設定] > [ランタイム環境] に移動します。
2. Secure Agent を選択し、ページ上部で [編集] をクリックします。
3. [システム構成の詳細] までスクロールします。
4. [JVM 最小ヒープ] および [JVM 最大ヒープ] の値を変更します。
5. ページ上部の [OK] をクリックします。

[プロセス数]、[リソースキャッシュ]、[作業マネージャの最小スレッドプール]、[作業マネージャの最大スレッドプール] を設定するには、アプリケーション統合コンソールサービスの [サーバー設定] セクションに移動します。

[JVM 最小ヒープ] および [JVM 最大ヒープ] を設定するには、管理者サービスの [ランタイム環境] セクションに移動します。

UNIX オペレーティングシステムでプロセスサーバーを起動すると、次のエラーが表示されることがあります。

Cannot write to temp location [/tmp]

このエラーが発生するのは、UNIX が 1 つのプロセスで作成できるファイルの数を制限しているためです。1 つのプロセスで作成できるファイルの最大数は 1024 です。

このエラーを回避するには、開くファイルの制限を少なくともデフォルト値である 1024 の 10 倍に増やすことをお勧めします。システム管理者に、最大ユーザープロセスなどのその他の関連パラメータの値を増やすように依頼します。

Secure Agent のためのプロセスサーバーのサイズ決定の詳細については、以下のドキュメントを参照してください。

<https://network.informatica.com/docs/DOC-17439>

## Secure Agent との通信

Informatica Intelligent Cloud Services は、Secure Agent チャンネルまたは HTTP や HTTPS 直接リンクを介して Secure Agent からプロセスサーバーにデータを送信します。

Secure Agent は、次の 2 つの方法でプロセスサーバーと通信します。

### Secure Agent チャンネル

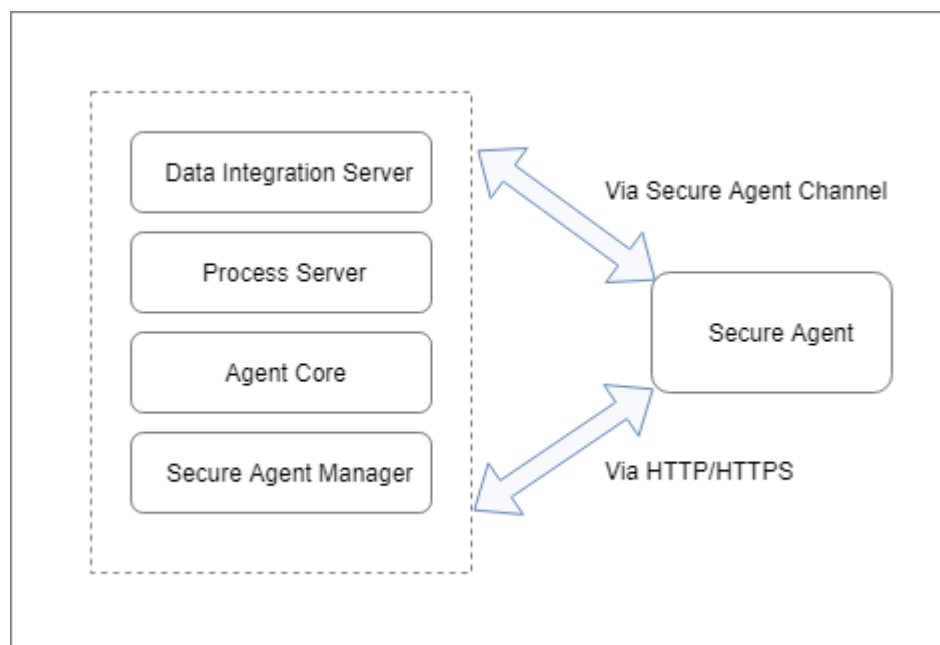
接続された各 Secure Agent とプロセスサーバー間にトンネルを作成するセキュアチャンネル。

### HTTP または HTTPS

Secure Agent がプロセスサーバーにデータを直接送信する場合のプロトコル。この通信方法を使用すると、Informatica Intelligent Cloud Services は認証プロバイダに対して資格情報を検証します。

各プロセスサーバープロパティが使用する通信方法の詳細については、[Process Server Properties \(ページ 129\)](#)を参照してください。

次の図に、Secure Agent とプロセスサーバー間の 2 つの通信方法を示します。





## プロセスサーバーのための Secure Agent の設定

ビジネスのニーズに応じて、アセットを単一の Secure Agent、Secure Agent グループ、Secure Agent クラスターにデプロイします。

アプリケーションの統合プロセス、接続、またはサービスコネクタを Secure Agent にデプロイする場合、これらのアセットを Secure Agent のプロセスサーバーサービスにデプロイします。そのプロセスサーバーサービスを使用するすべての Secure Agent は、同じ PostgreSQL データベースを使用します。

アセットを次の Secure Agent 構成に割り当てることができます。

### 単一の Secure Agent

単一の Secure Agent はグループ内の唯一のエージェントであったり、グループの複数のエージェントの 1 つであったりする可能性があります。

詳細については、[Deploy to a Single Secure Agent \(ページ 137\)](#)を参照してください。

### Secure Agent グループ

Secure Agent グループには複数のエージェントが含まれます。アセットを Secure Agent グループにデプロイすると、Informatica Intelligent Cloud Services によって負荷分散が実行されます。ステートレス要求を処理する場合や OData 要求専用の Secure Agent を使用する場合、要求を分散させるために Secure Agent グループ構成を使用します。

詳細については、[Deploy to a Secure Agent Group \(ページ 138\)](#)を参照してください。

### Secure Agent クラスター

Secure Agent クラスターは、1 つのマスタ Secure Agent を持つエージェントグループです。すべてのプロセスサーバーでプロセス実行アクティビティに関する情報を受信するようにする場合は、Secure Agent クラスター構成を使用します。

詳細については、[Deploy to a Secure Agent Cluster \(ページ 139\)](#)を参照してください。

以下の表は、さまざまなシナリオにおける Secure Agent のプロセス実行の概要を示しています。

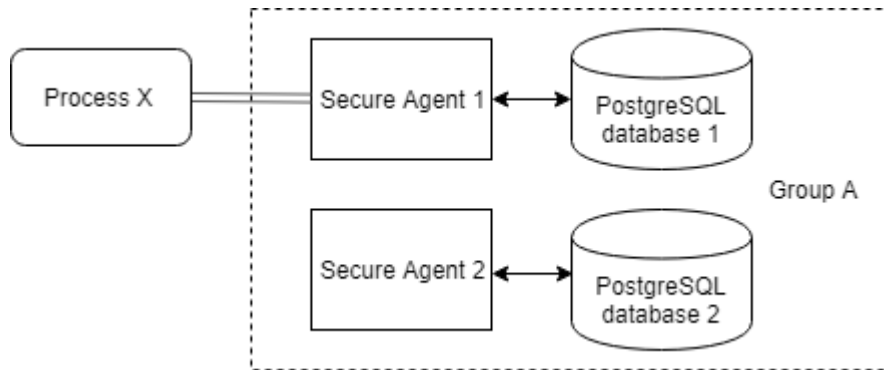
	単一の Secure Agent	Secure Agent グループ	Secure Agent クラスター
使用可能なエージェント	プロセスが実行される。	プロセスが実行される。	プロセスが実行される。
使用不可能なエージェント	プロセスは実行されない。	プロセスは使用可能な Secure Agent のいずれかで実行される。	プロセスは使用可能な Secure Agent のいずれかで実行される。
エージェントが実行中に停止	プロセスは実行されない。	Secure Agent が停止したときにプロセスが停止される。	別の Secure Agent でプロセスの実行が継続される。

## 単一の Secure Agent へのデプロイ

アセットをグループ内の単一のエージェントに直接デプロイできます。

アセットを単一の Secure Agent にデプロイする場合、Secure Agent グループ内の他のプロセスサーバーはいずれも、アセット定義を受信しません。

次の図は、プロセス X を Secure Agent 1 に直接デプロイした場合の構成例を示しています。



プロセス X を実行できるのは Secure Agent 1 だけです。Secure Agent 1 が使用不可能になると、プロセスは実行されません。

## Secure Agent グループへのデプロイ

Secure Agent グループには複数のエージェントが含まれます。アセットを Secure Agent グループにデプロイすることができます。

ステートレス要求を処理する場合や OData 要求専用の Secure Agent を使用する場合、要求を分散させるために Secure Agent グループ構成を使用します。

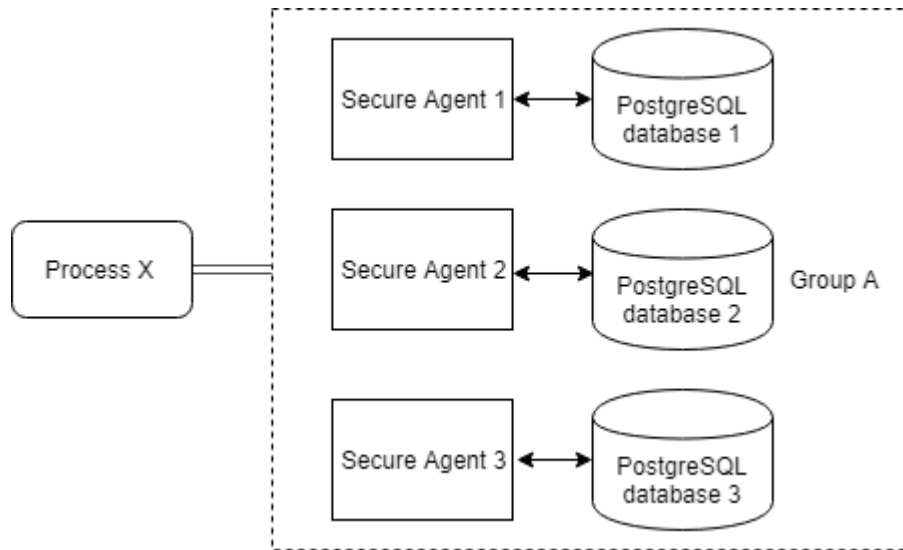
Secure Agent グループでは、受信された要求が Informatica Intelligent Cloud Services によって、使用可能な Secure Agent にラウンドロビン方式でディスパッチされます。

アセットを Secure Agent グループにデプロイすると、負荷分散された構成を使用することになります。Informatica Intelligent Cloud Services によって負荷分散が実行されます。また、load-balance-url プロセスサーバープロパティを設定して、カスタムロードバランサを使用することもできます。詳細については、[Process Server Properties \(ページ 129\)](#)を参照してください。

Secure Agent グループの詳細については、[Secure Agent Groups with Multiple Agents \(ページ 84\)](#)を参照してください。

グループ内のすべての Secure Agent は個別の PostgreSQL データベースを使用します。アセットを Secure Agent グループにデプロイすると、グループ内のすべてのプロセスサーバーが、新規のアセット定義または更新されたアセット定義に関する詳細を受信します。ただし、グループ内の他のプロセスサーバーはアセットの実行アクティビティに関する詳細を受信しません。例えば、プロセス実行中に Secure Agent で障害が発生しても、プロセスはグループ内の別の Secure Agent で継続して実行されません。

次の図は、プロセス X を Secure Agent グループ A にデプロイした場合の構成例を示しています。



プロセス X を変更して再パブリッシュすると、3 つすべての Secure Agent が更新された定義を受信します。すべての Secure Agent がプロセスを実行できます。

例えば、プロセスが開始され、Secure Agent 1 と Secure Agent 2 が使用不可能な場合、負荷分散された構成によって、Secure Agent 3 がプロセス X を実行することが保証されます。ただし、Secure Agent 1 と Secure Agent 2 は、プロセスが失敗したか正常に終了したかどうかについての情報を受信しません。プロセス X の実行中に Secure Agent 3 が停止した場合、プロセスはそれ以降実行されません。

## Secure Agent クラスタへのデプロイ

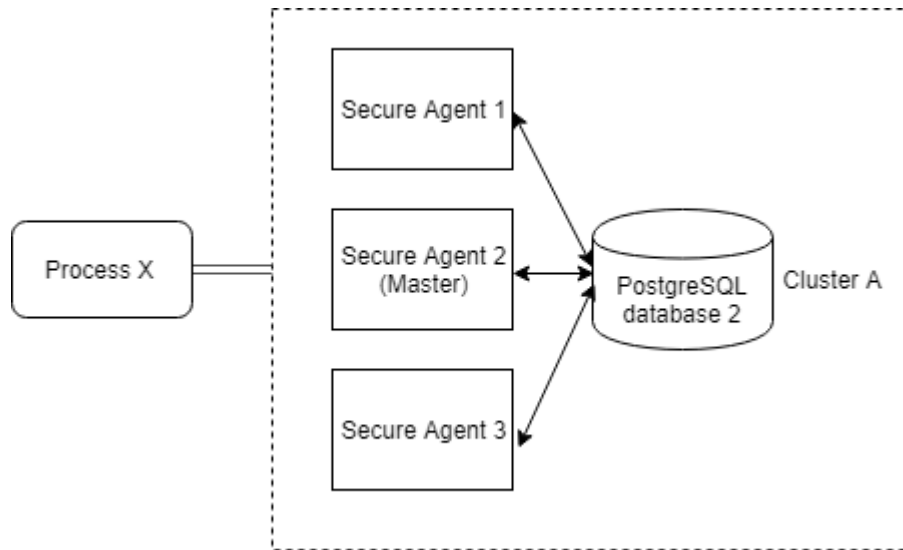
Secure Agent クラスタは、1 つのマスタ Secure Agent を持つエージェントグループです。アセットを Secure Agent クラスタにデプロイすることができます。

アセットを Secure Agent クラスタにデプロイすると、すべてのプロセスサーバーはプロセス実行アクティビティに関する情報を受信します。マスタ Secure Agent は情報を受信し、他のすべての Secure Agent に送信します。プロセス実行中に Secure Agent で障害が発生すると、プロセスはクラスタ内の別の Secure Agent で継続して実行されます。

クラスタ内のすべてのプロセスサーバーはマスタエージェントの PostgreSQL データベースを共有します。

マスタ Secure Agent を定義するには、`primary-node` プロセスサーバープロパティを使用してください。詳細については、[Process Server Properties \(ページ 129\)](#)を参照してください。

次の図は、プロセス X を Secure Agent クラスタ A にデプロイした場合の構成例を示しています。



Secure Agent 3 がプロセス X の実行を開始し、途中でこのエージェントが停止した場合、Secure Agent 1 または Secure Agent 2 がそのプロセスの実行を継続します。

## Windows での PostgreSQL データベースの管理

PostgreSQL データベースを管理するには、バイナリとユーティリティスクリプトを使用します。

**重要:** PostgreSQL データベースを管理するには、システム管理者権限を持たないユーザーとしてログインする必要があります。システム管理者は、PostgreSQL バイナリとユーティリティスクリプトを実行できません。

PostgreSQL バイナリに基づいていくつかのユーティリティスクリプトが作成されています。これらのユーティリティスクリプトを使用すると、PostgreSQL データベースを簡単に管理できます。

次のディレクトリには、PostgreSQL データベースのファイルが含まれます。

- PostgreSQL バイナリ: <Secure Agent installation directory>\apps\process-engine\data\db\postgresql-windows-x64-binaries\pgsql\bin
- PostgreSQL ユーティリティスクリプト: <Secure Agent installation directory>\apps\process-engine\data\db\util
- PostgreSQL ログ: <Secure Agent installation directory>\apps\process engine\logs\PostGreSql\postgresql.log
- PostgreSQL データ: <Secure Agent installation directory>\apps\process engine\data\PostGreSql\Data

PostgreSQL スクリプトの詳細については、<https://www.postgresql.org/docs/current/static/index.html> で PostgreSQL のヘルプを参照してください。

以降の一部のセクションには、次のデフォルト値を使用するサンプルコマンドが含まれています。

- デフォルトのデータベース名: activevos
- デフォルトのデータベースユーザー名: bpeluser
- デフォルトのデータベースパスワード: bpel

## Windows での PostgreSQL データベースのバックアップ

PostgreSQL データベースをバックアップするには、スクリプト db\_backup.bat を使用します。

PostgreSQL データベースをバックアップするには、次の手順を実行します。

1. <Secure Agent installation directory>\apps\process-engine\data\db\util に移動します。
2. 次のコマンドを実行します。  
db\_backup.bat <dbusername> <dbpassword> <path to backup file along with name of backup file with a ".dump" extension>

例えば、次のコマンドを実行すると、Secure Agent はバックアップファイル「BackupFile1.dump」を C:\postgre\backup に作成します。

```
db_backup.bat bpeluser bpel "C:\postgre\backup\BackupFile1.dump"
```

## Windows での PostgreSQL データベースのリストア

PostgreSQL データベースをバックアップファイルからリストアするには、コマンド db\_restore.bat を使用します。

PostgreSQL データベースファイルをバックアップファイルからリストアするには、次の手順を実行します。

1. <Secure Agent installation directory>\apps\process-engine\data\db\util に移動します。
2. 次のコマンドを実行します。  
db\_restore.bat <dbusername> <dbpassword> <path to dump file>

例えば、次のコマンドを実行すると、ファイル BackupFile1.dump を使用して PostgreSQL データベースがリストアされます。

```
db_restore.bat bpeluser bpel "C:\postgre\backup\BackupFile1.dump"
```

## Windows での PostgreSQL データベースのリセット

PostgreSQL データベースをシャットダウンしてから、db\_reset.bat コマンドを使用してリセットします。

PostgreSQL データベースを元の状態にリセットするには、次の手順を実行します。

1. <Secure Agent installation directory>\apps\process-engine\data\db\util に移動します。
2. サーバーをシャットダウンするには、次のコマンドを実行します。  
server\_stop.bat
3. PostgreSQL データベースをリセットするには、次のコマンドを実行します。  
db\_reset.bat

## Windows での PostgreSQL サーバーの起動

Windows でプロセスサーバーを起動するには、次の手順を実行します。

1. <Secure Agent installation directory>\apps\process-engine\data\db\util に移動します。
2. 次のスクリプトを実行します。  
server\_start.bat

## Windows での PostgreSQL サーバーの停止

Windows で PostgreSQL サーバーを停止するには、次の手順を実行します。

1. <Secure Agent installation directory>\apps\process-engine\data\db\util に移動します。

2. 次のスクリプトを実行します。  
server\_stop.bat

## Windows での PostgreSQL サーバーステータスの取得

Windows で PostgreSQL サーバーステータスを取得するには、次の手順を実行します。

1. <Secure Agent installation directory>\apps\process-engine\data\db\util に移動します。
2. 次のスクリプトを実行します。  
server\_status.bat

## Windows での PostgreSQL データベースのクリーンアップ

PostgreSQL データベースをクリーンアップし、古いタブルを削除して領域を確保します。スクリプト db\_maintenance.bat を使用して、PostgreSQL データベースをクリーンアップします。

デフォルトで、PostgreSQL データベースの自動クリーンアップが行われます。データベースを手動でクリーンアップする場合は、次の手順を実行します。

1. <Secure Agent installation directory>\apps\process-engine\data\db\util に移動します。
2. データベース全体をクリーンアップするには、次のコマンドを実行します。  
db\_maintenance.bat <dbusername> <dbpassword> vacuum
3. 単一テーブルをクリーンアップするには、次のコマンドを実行します。  
db\_maintenance.bat <dbusername> <dbpassword> vacuum <tablename>

例えば、次のコマンドを実行すると、「aeoprocesslogdata」テーブルがクリーンアップされます。

```
db_maintenance.bat bpeluser bpel vacuum aeoprocesslogdata
```

また、PostgreSQL データベースの期間クリーンアップをスケジュールすることもできます。詳細を確認するには、[管理者] の [メンテナンス] セクションの [PostgreSQL メンテナンスのスケジュール] トピックを参照してください。

## Windows での PostgreSQL データベースの再インデックス化

PostgreSQL でデータをクリーンアップした後、インデックスをクリーンアップして使用領域を解放するには、再インデックス化オプションを使用します。スクリプト db\_maintenance.bat を使用して、PostgreSQL データベースを再インデックス化します。

PostgreSQL データベースを再インデックス化するには、次の手順を実行します。

1. <Secure Agent インストールディレクトリ>\apps\process-engine\data\db\util に移動します。
2. データベース全体を再インデックス化するには、次のコマンドを実行します。  
db\_maintenance.bat <dbusername> <dbpassword> reindex
3. 単一テーブルを再インデックス化するには、次のコマンドを実行します。  
db\_maintenance.bat <dbusername> <dbpassword> reindex <tablename>

例えば、次のコマンドを実行すると、「aeoprocesslogdata」テーブルが再インデックス化されます。

```
db_maintenance.bat bpeluser bpel reindex aeoprocesslogdata
```

また、PostgreSQL データベースの期間インデックス化をスケジュールすることもできます。詳細を確認するには、[管理者] の [メンテナンス] セクションの [PostgreSQL メンテナンスのスケジュール] トピックを参照してください。

## Windows でのトランザクションログのリセット

制御情報の破損が原因で PostgreSQL サーバーが起動しない場合は、コマンド `pg_resetxlog.exe` を使用して制御情報をリセットします。

PostgreSQL データベースの制御情報をリセットするには、次の手順を実行します。

1. `<Secure Agent installation directory>\apps\process-engine\data\db\postgresql-windows-x64-binaries\pgsql\bin` に移動します。
2. 次のコマンドを実行します。  
`pg_resetxlog.exe -D <path to postgresql data directory>`

例えば、次のコマンドを実行すると、「Data」ディレクトリのトランザクションログがリセットされます。

```
pg_resetxlog.exe -D "C:\postgre\apps\process-engine\data\PostGreSql\Data"
```

## Linux での PostgreSQL データベースの管理

PostgreSQL データベースを管理するには、バイナリとユーティリティスクリプトを使用します。

**重要:** PostgreSQL データベースを管理するには、ルートアクセス権を持たないユーザーとしてログインする必要があります。ルートユーザーは、PostgreSQL バイナリとユーティリティスクリプトを実行できません。

PostgreSQL バイナリに基づいていくつかのユーティリティスクリプトが作成されています。これらのユーティリティスクリプトを使用すると、PostgreSQL データベースを簡単に管理できます。

次のディレクトリには、PostgreSQL データベースのファイルが含まれます。

- PostgreSQL バイナリ: `<Secure Agent installation directory>/apps/process-engine/data/db/postgresql-linux-x64-binaries/pgsql/bin`
- PostgreSQL ユーティリティスクリプト: `<Secure Agent installation directory>/apps/process-engine/data/db/util`
- PostgreSQL ログ: `<Secure Agent installation directory>/apps/process-engine/logs/PostGreSql/postgresql.log`
- PostgreSQL データ: `<Secure Agent installation directory>/apps/process-engine/data/PostGreSql/Data`

PostgreSQL スクリプトの詳細については、<https://www.postgresql.org/docs/current/static/index.html> で PostgreSQL のヘルプを参照してください。

一部のセクションには、次のデフォルト値を使用するサンプルコマンドが含まれています。

- デフォルトのデータベース名: `activevos`
- デフォルトのデータベースユーザー名: `bpeluser`
- デフォルトのデータベースパスワード: `bpel`

## Linux での PostgreSQL データベースのバックアップ

PostgreSQL データベースをバックアップするには、スクリプト `db_backup` を使用します。

PostgreSQL データベースをバックアップするには、次の手順を実行します。

1. `<Secure Agent installation directory>/apps/process-engine/data/db/util` に移動します。
2. 次のコマンドを実行します。  
`db_backup.sh <dbusername> <dbpassword> <path to backup file along with name of backup file>.dump。`

例えば、次のコマンドを実行すると、Secure Agent はバックアップファイル「`backupfile1.dump`」を `/home/data/myfolder/` に作成します。

```
db_backup.sh bpeluser bpel "/home/data/myfolder/backupfile1.dump"
```

## Linux での PostgreSQL データベースのリストア

PostgreSQL データベースをバックアップファイルからリストアするには、スクリプト `db_restore.sh` を使用します。

PostgreSQL データベースファイルをバックアップファイルからリストアするには、次の手順を実行します。

1. `<Secure Agent installation directory>/apps/process-engine/data/db/util` に移動します。
2. 次のコマンドを実行します。  
`db_restore.sh <dbusername> <dbpassword> <path to dump file>`

例えば、次のコマンドを実行すると、ファイル `backupfile1.dump` を使用して PostgreSQL データベースがリストアされます。

```
db_restore.sh bpeluser bpel "/home/data/myfolder/backupfile1.dump",
```

## Linux での PostgreSQL データベースのリセット

最初に PostgreSQL データベースをシャットダウンしてから、スクリプト `db_reset.sh` を使用してリセットします。

PostgreSQL データベースを元の状態にリセットするには、次の手順を実行します。

1. `<Secure Agent installation directory>/apps/process-engine/data/db/util` に移動します。
2. サーバーをシャットダウンするには、次のスクリプトを実行します。  
`server_stop.sh`
3. PostgreSQL データベースをリセットするには、次のスクリプトを実行します。  
`db_reset.sh`

## Linux での PostgreSQL サーバーの起動

PostgreSQL サーバーを起動するには、次の手順を実行します。

1. `<Secure Agent installation directory>/apps/process-engine/data/db/util` に移動します。
2. 次のスクリプトを実行します。  
`server_start.sh`

## Linux での PostgreSQL サーバーの停止

PostgreSQL サーバーを停止するには、次の手順を実行します。

1. `<Secure Agent installation directory>/apps/process-engine/data/db/util` に移動します。
2. 次のスクリプトを実行します。  
`server_stop.sh`

## Linux での PostgreSQL サーバースtatusの取得

Linux で PostgreSQL サーバーのステータスを取得するには、次の手順を実行します。

1. `<Secure Agent installation directory>/apps/process-engine/data/db/util` に移動します。
2. 次のスクリプトを実行します。  
`server_status.sh`



## Linux での PostgreSQL データベースのクリーンアップ

PostgreSQL データベースをクリーンアップし、古いタブルを削除して領域を確保します。スクリプト `db_maintenance.sh` を使用して、PostgreSQL データベースをクリーンアップします。

デフォルトで、PostgreSQL データベースの自動クリーンアップが行われます。データベースを手動でクリーンアップする場合は、次の手順を実行します。

1. `<Secure Agent installation directory>/apps/process-engine/data/db/util` に移動します。
2. データベース全体をクリーンアップするには、次のコマンドを実行します。  
`db_maintenance <dbusername> <dbpassword> vacuum`
3. 単一テーブルをクリーンアップするには、次のコマンドを実行します。  
`db_maintenance.sh <dbusername> <dbpassword> vacuum <tablename>`

例えば、次のコマンドを実行すると、「`aeprocesslogdata`」テーブルがクリーンアップされます。

```
db_maintenance.sh bpeluser bpel vacuum aeprocesslogdata
```

また、PostgreSQL データベースの期間クリーンアップをスケジュールすることもできます。詳細を確認するには、*[管理者]* の *[メンテナンス]* セクションの *[PostgreSQL メンテナンスのスケジュール]* トピックを参照してください。

## Linux での PostgreSQL データベースの再インデックス化

PostgreSQL でデータをクリーンアップした後、インデックスをクリーンアップして使用領域を解放するには、再インデックス化オプションを使用します。スクリプト `db_maintenance.sh` を使用して、PostgreSQL データベースを再インデックス化します。

PostgreSQL データベースを再インデックス化するには、次の手順を実行します。

1. `<Secure Agent installation directory>/apps/process-engine/data/db/util` に移動します。
2. データベース全体を再インデックス化するには、次のコマンドを実行します。  
`db_maintenance <dbusername> <dbpassword> reindex`
3. 単一テーブルを再インデックス化するには、次のコマンドを実行します。  
`db_maintenance.sh <dbusername> <dbpassword> reindex <tablename>`

例えば、次のコマンドを実行すると、「`aeprocesslogdata`」テーブルが再インデックス化されます。

```
db_maintenance.sh bpeluser bpel reindex aeprocesslogdata
```

また、PostgreSQL データベースの期間インデックス化をスケジュールすることもできます。詳細を確認するには、*[管理者]* の *[メンテナンス]* セクションの *[PostgreSQL メンテナンスのスケジュール]* トピックを参照してください。

## Linux でのトランザクションログのリセット

制御情報の破損が原因で PostgreSQL サーバーが起動しない場合は、コマンド `pg_resetxlog` を使用して制御情報をリセットします。

PostgreSQL データベースの制御情報をリセットするには、次の手順を実行します。

1. `<Secure Agent installation directory>/apps/process-engine/data/db/postgresql-linux-x64-binaries/pgsql/bin` に移動します。
2. 次のコマンドを実行します。  
`pg_resetxlog -D <path to postgresql data directory>`

例えば、次のコマンドを実行すると、「Data」ディレクトリのトランザクションログがリセットされます。

```
pg_resetxlog -D "home/apps/process engine/data/PostGreSql/Data"
```

# Secure Agent サービスプロパティの設定

Secure Agent サービスプロパティを設定するには、**【ランタイム環境】** ページを開いて Secure Agent を編集します。サービスプロパティの値を変更またはリセットして、サービスのカスタムプロパティを追加および削除できます。また、Secure Agent 名を変更することもできます。

**注:** カスタムプロパティはコネクタ固有です。カスタムプロパティの詳細については、該当するコネクタのヘルプを参照してください。

1. **【ランタイム環境】** ページで、Secure Agent の名前をクリックします。  
**注:** Secure Agent グループ内の Secure Agent を一覧表示するには、Secure Agent グループの展開が必要になる場合があります。
2. **【詳細】** タブをクリックします。
3. 右上隅の **【編集】** をクリックします。
4. Secure Agent の名前を変更するには、**【エージェント名】** フィールドに新しい名前を入力します。
5. サービスプロパティを編集するには、次の手順を実行します。
  - a. **【システム構成の詳細】** 領域で、サービスを選択します。
  - b. 設定プロパティの種類を選択します。
  - c. 変更するプロパティを含む行で **【エージェント設定の編集】** アイコンをクリックして、新しいプロパティ値を入力します。
  - d. プロパティをシステムデフォルト値にリセットするには、**【エージェント設定をシステムデフォルトにリセット】** アイコンをクリックします。
6. サービスのカスタムプロパティを追加するには、次の手順を実行します。
  - a. **【カスタム構成の詳細】** 領域までスクロールダウンします。  
次の画像は、**【カスタム構成の詳細】** 領域を示しています。

Custom Configuration Details

Service	Type	Sub-type	Name	Value
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

- b. 設定するサービスを選択します。
  - c. 設定プロパティの種類を選択します。
  - d. 設定プロパティタイプにサブタイプがある場合は、適切なサブタイプを選択します。  
例えば、ログレベルを決定するには、サブタイプとして **【情報】** または **【デバッグ】** を選択します。
  - e. プロパティの名前と値を入力します。
  - f. **【追加】** アイコンをクリックします。
7. カスタムプロパティを削除するには、カスタムプロパティの隣にある **【削除】** アイコンをクリックします。
  8. すべての設定プロパティをデフォルト設定にリセットするには、**【すべてリセット】** をクリックします。
  9. **【保存】** をクリックします。

## 第 14 章

# Secure Agent のインストール

Secure Agent は Windows または Linux にインストールできます。また、マシンで Secure Agent を実行する必要がなくなった場合、または Secure Agent を再インストールする場合には、Secure Agent をアンインストールすることができます。

インストールとアンインストールの手順は、オペレーティングシステムによって異なります。

Secure Agent を使用して、エラスティックマッピングに基づくマッピングタスクを実行する場合、Secure Agent はクラウドプラットフォームの Linux 仮想マシンにインストールされている必要があります。

## Windows での Secure Agent のインストール

Windows 上では、Secure Agent が Windows サービスとして実行されます。Secure Agent をインストールするときには、Informatica Cloud Secure Agent Manager もインストールします。

デフォルトでは、Windows を起動すると Secure Agent も起動されます。Secure Agent Manager を使用して、Secure Agent を停止および再起動します。また、Secure Agent Manager を使用して、Secure Agent のステータスをチェックし、プロキシ情報を設定することもできます。

Secure Agent Manager は、[スタート] メニューまたはデスクトップアイコンから起動できます。Secure Agent Manager を閉じると、最小化されて Windows タスクバーの通知領域に表示され、すぐにアクセスできるようにされます。

Secure Agent をインストールするときには、次のタスクを実行します。

1. Secure Agent をインストールするマシンが最小要件を満たしていることを確認します。
2. Secure Agent インストーラのファイルをダウンロードします。
3. Secure Agent をインストールして登録します。

## Windows での Secure Agent の要件

Secure Agent は、インターネット接続が可能であり、Informatica Intelligent Cloud Services にアクセス可能な任意のマシンにインストールすることができます。

Windows で Secure Agent をインストールする前に、次の要件を確認してください。

- Secure Agent をインストールするコンピュータがサポート対象のオペレーティングシステムを使用していることを確認します。Secure Agent でサポート対象のオペレーティングシステムの一覧については、Informatica Network 上の [Product Availability Matrices page](#) にある Informatica Intelligent Cloud Services の製品可用性マトリックス (PAM) を参照してください。
- Secure Agent をインストールするマシンに 5 GB 以上の空きディスク容量があることを確認します。

- Secure Agent のインストールに使用するアカウントに、フラットのソースまたはターゲットファイルが格納されているすべてのリモートディレクトリに対するアクセス権が付与されていることを確認します。
- マシンに他の Secure Agent がインストールされていないことを確認します。マシンに別の Secure Agent がインストールされている場合は、まずそのエージェントをアンインストールする必要があります。

Secure Agent の要件の詳細については、Informatica グローバルカスタマサポートにお問い合わせください。

## ファイアウォールの設定

組織で保護ファイアウォールを使用している場合は、Informatica Intelligent Cloud Services のドメイン名または IP アドレス範囲を承認済みのドメイン名または IP アドレスの一覧に含めます。Secure Agent が使用するポートを有効にする必要があります。これにより、Secure Agent で、ファイアウォールを介してすべての必要なタスクを実行できるようにします。

Secure Agent はインターネットに接続するためにポート 443 (HTTPS) を使用します。トラフィックがポート 443 を通過することを許可するようにファイアウォールを設定してください。

ドメインと IP アドレスのホワイトリストはデータセンターに応じて異なります。これは POD (Point of Deployment) と呼ばれます。POD は、Informatica Intelligent Cloud Services で任意のサービスを開いたときに表示される URL から特定できます。URL 文字列の最初の数文字が POD を表します。例えば、URL が `usw3.dm-us.informaticacloud.com` で始まる場合、POD は USW3 です。

Informatica Network の [this Knowledge Base article](#)、または管理者の **【ランタイム環境】** ページの上部にあるリンクをクリックすると、さまざまな POD の Informatica Intelligent Cloud Services ドメインと IP アドレスのホワイトリストを確認することができます。

## Windows での Secure Agent の権限

Secure Agent には、ソースとターゲットの間でデータを転送するために特定の権限が必要です。

Windows に Secure Agent をインストールする場合、その Secure Agent はローカル管理者グループの一部になっている必要があります。

## Windows 設定の構成

Windows で Secure Agent を使用する前に、プロキシ設定と Windows Secure Agent サービスログインを設定します。

プロキシ設定は、Secure Agent Manager で設定できます。Windows で Windows Secure Agent サービスのログインを設定します。

**注:** Informatica Cloud Data ウィザードで Secure Agent を使用する場合、Secure Agent に対してプロキシ設定または Windows サービスログインを設定する必要はありません。

## Windows での Secure Agent のダウンロードおよびインストール

Windows マシンに Secure Agent をインストールするには、Secure Agent インストールプログラムをダウンロードして実行してから、エージェントを登録する必要があります。

Secure Agent の登録にはインストールトークンが必要です。インストールトークンを取得するには、エージェントのダウンロード時にトークンをコピーするか、または管理者で **【インストールトークンの生成】** オプションを使用します。トークンは 24 時間後に有効期限が切れます。

Secure Agent をダウンロードしてインストールする前に、そのマシンに他の Secure Agent がインストールされていないことを確認します。他のエージェントが存在する場合は、アンインストールする必要があります。

1. 管理者を開いて **【ランタイム環境】** を選択します。

2. **【ランタイム環境】** ページで、**【Secure Agent のダウンロード】** をクリックします。
3. Windows 64 ビットオペレーティングシステムプラットフォームを選択し、インストールトークンをコピーしてから **【ダウンロード】** をクリックします。  
インストールプログラムがご使用のマシンにダウンロードされます。インストールプログラムの名前は agent64\_install\_ng\_ext.exe です。
4. インストールプログラムの実行:
  - a. Secure Agent インストールディレクトリを指定し、**【次へ】** をクリックします。
  - b. **【インストール】** をクリックしてエージェントをインストールします。

Secure Agent Manager が開き、次の図に示すようにエージェントを登録するように求めるプロンプトが表示されます。

5. エージェントのダウンロード時にインストールトークンをコピーしなかった場合は、管理者の **【ランタイム環境】** ページで **【インストールトークンの生成】** をクリックし、トークンをコピーします。
6. Secure Agent Manager で、次の情報を入力し、**【登録】** をクリックします。

オプション	説明
ユーザー名	Informatica Intelligent Cloud Services へのアクセスに使用するユーザー名。
インストールトークン	コピーしたトークン。

Secure Agent Manager が Secure Agent のステータスを表示します。すべてのサービスが起動するまで 1 分かかります。

- お客様の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は、プロキシサーバー情報を入力します。
- Secure Agent Manager を閉じます。  
Secure Agent Manager は、最小化されてタスクバーに表示され、停止されるまでサービスとして実行し続けます。

## Windows でのプロキシ設定

組織で送信プロキシサーバーを使用してインターネットに接続する場合、Secure Agent は、そのプロキシサーバー経由で Informatica Intelligent Cloud Services に接続します。Secure Agent のインストーラにより、ブラウザで設定されている設定項目に基づいて Secure Agent のプロキシサーバー設定が設定されます。プロキシサーバーの設定は、Secure Agent Manager から変更できます。

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。

- Secure Agent Manager で、**【プロキシ】** をクリックします。
- プロキシサーバーの設定値を入力するには、**【プロキシサーバーを使用】** をクリックします。
- 次の情報を入力します。

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

- 【OK】** をクリックします。  
Secure Agent Manager によって Secure Agent が再起動され、設定が適用されます。

## Windows Secure Agent サービスへのログインの設定

Windows では、Secure Agent サービスのネットワークログインを設定します。Secure Agent は、ログインに関連付けられている特権と権限によってネットワークにアクセスできます。

Secure Agent がディレクトリにアクセスしてタスクを設定および実行できるように、Secure Agent がインストールされているマシンのログインを設定します。接続を設定する、タスクを設定する、およびフラットファイルまたは FTP/SFTP 接続タイプを使用するタスクを実行する場合、Secure Agent には、関連するディレクトリでの読み取りおよび書き込み権限が必要です。

例えば、ディレクトリを参照してフラットファイルまたは FTP/SFTP 接続を設定するには、Secure Agent のログインでそのディレクトリへのアクセス権限を必要とする場合があります。Secure Agent のログインに適切な権限が付与されていないと、Informatica Intelligent Cloud Services では、**【ディレクトリの参照】** ダイアログボックスにディレクトリを表示できません。

- Windows の **【管理ツール】** から、**【サービス】** ウィンドウに移動します。
- 【サービス】** ウィンドウで、Informatica Cloud Secure Agent サービスを右クリックし、**【プロパティ】** を選択します。
- 【プロパティ】** ダイアログボックスで、**【ログオン】** タブをクリックします。
- ログインを設定するには、**【このアカウント】** を選択します。

5. アカウントとパスワードを入力します。  
ドメインで定義されているネットワークセキュリティに応じて、必須の特権と権限が付与されているアカウントを使用します。デフォルトのアカウント形式は、<ドメイン名>\<ユーザー名>です。
6. **【OK】** をクリックします。
7. **【サービス】** ウィンドウで、Secure Agent サービスを再起動して変更を有効にします。

## Windows での Secure Agent のアンインストール

Secure Agent をアンインストールできます。マシンで Secure Agent を実行する必要がなくなった場合、または Secure Agent を再インストールする場合には、Secure Agent をアンインストールすることができます。

Secure Agent をアンインストールする前に、接続またはタスクがそれを使用するように構成されていないことを確認します。

1. **【スタート】 > 【すべてのプログラム】 > [Informatica Cloud Secure Agent] > [Informatica Cloud Secure Agent のアンインストール]** をクリックします。

Secure Agent のアンインストーラが起動します。

2. **【アンインストール】** をクリックします。
3. アンインストールが完了したら、**【完了】** をクリックします。
4. インストールディレクトリに残されているすべてのファイルを削除します。

Secure Agent をアンインストールした後は、Secure Agent のインストールに関連付けられているすべてのファイルとディレクトリを削除します。

## Linux での Secure Agent のインストール

Linux の場合、Secure Agent はプロセスとして実行されます。シェルコマンドラインを使用して、Secure Agent をインストール、登録、起動、停止、およびアンインストールすることができます。

また、シェルコマンドラインを使用して Secure Agent のステータスをチェックすることもできます。

Secure Agent をインストールするときには、次のタスクを実行します。

1. Secure Agent をインストールするマシンが最小要件を満たしていることを確認します。
2. Secure Agent インストーラのファイルをダウンロードします。
3. Secure Agent をインストールして登録します。



## Linux での Secure Agent の要件

Secure Agent は、インターネット接続が可能であり、Informatica Intelligent Cloud Services にアクセス可能な任意のマシンにインストールすることができます。Linux で Secure Agent をインストールする前に、システム要件を確認してください。

Linux で Secure Agent をインストールする前に、次の要件を確認してください。

- Secure Agent をインストールするコンピュータがサポート対象のオペレーティングシステムを使用していることを確認します。Secure Agent でサポート対象のオペレーティングシステムの一覧については、Informatica Network 上の [Product Availability Matrices page](#) にある Informatica Intelligent Cloud Services の製品可用性マトリックス（PAM）を参照してください。
- Secure Agent をインストールするマシンに 5 GB 以上の空きディスク容量があることを確認します。
- Secure Agent のインストールに使用するアカウントに、フラットのソースまたはターゲットファイルが格納されているすべてのリモートディレクトリに対するアクセス権が付与されている必要があります。
- PowerCenter を使用する場合は、PowerCenter のインストールに使用したアカウントとは別のユーザーアカウントを使用して、Secure Agent をインストールします。

Informatica Intelligent Cloud Services と PowerCenter は、いくつかの共通の環境変数を使用します。Informatica Intelligent Cloud Services に対して環境変数が正しく設定されていない場合、ジョブは実行時に失敗する可能性があります。

Secure Agent の要件の詳細については、Informatica グローバルカスタマサポートにお問い合わせください。

## ファイアウォールの設定

組織で保護ファイアウォールを使用している場合は、Informatica Intelligent Cloud Services のドメイン名または IP アドレス範囲を承認済みのドメイン名または IP アドレスの一覧に含めます。Secure Agent が使用するポートを有効にする必要があります。これにより、Secure Agent で、ファイアウォールを介してすべての必要なタスクを実行できるようにします。

Secure Agent はインターネットに接続するためにポート 443（HTTPS）を使用します。トラフィックがポート 443 を通過することを許可するようにファイアウォールを設定してください。

ドメインと IP アドレスのホワイトリストはデータセンターに応じて異なります。これは POD（Point of Deployment）とも呼ばれます。POD は、Informatica Intelligent Cloud Services で任意のサービスを開いたときに表示される URL から特定できます。URL 文字列の最初の数文字が POD を表します。例えば、URL が `usw3.dm-us.informaticacloud.com` で始まる場合、POD は USW3 です。

Informatica Network の [this Knowledge Base article](#)、または管理者の **【ランタイム環境】** ページの上部にあるリンクをクリックすると、さまざまな POD の Informatica Intelligent Cloud Services ドメインと IP アドレスのホワイトリストを確認することができます。

## Linux での Secure Agent の権限

Secure Agent には、ソースとターゲットの間でデータを転送するために特定の権限が必要です。

Linux に Secure Agent をインストールする場合、その Secure Agent には、インストールディレクトリに対する読み取り/書き込み/実行権限が必要です。



## Linux での Secure Agent のダウンロードおよびインストール

Linux マシンに Secure Agent をインストールするには、Secure Agent インストールプログラムをダウンロードして実行してから、エージェントを登録する必要があります。

Secure Agent の登録にはインストールトークンが必要です。インストールトークンを取得するには、エージェントのダウンロード時にトークンをコピーするか、または管理者で **【インストールトークンの生成】** オプションを使用します。トークンは 24 時間後に有効期限が切れます。

Secure Agent をダウンロードしてインストールする前に、同じ Linux ユーザーアカウントを使用してそのマシンに他の Secure Agent がインストールされていないことを確認します。他のエージェントが存在する場合は、アンインストールする必要があります。

1. 管理者を開いて **【ランタイム環境】** を選択します。
2. **【ランタイム環境】** ページで、**【Secure Agent のダウンロード】** をクリックします。
3. Linux 64 ビットオペレーティングシステムプラットフォームを選択し、インストールトークンをコピーしてから **【ダウンロード】** をクリックします。

インストールプログラムがご使用のマシンにダウンロードされます。インストールプログラムの名前は agent64\_install\_ng\_ext.bin です。

4. Secure Agent を実行するマシン上のディレクトリにインストールプログラムを保存します。

**注:** ファイルパスにスペースが含まれていると、インストールに失敗します。

5. シェルコマンドラインから、インストールプログラムをダウンロードしたディレクトリに移動し、次のコマンドを入力します。

```
。 /agent64_install_ng_ext.bin -i console
```

6. インストーラが終了したら、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
```

7. Secure Agent を起動するには、次のコマンドを入力します。

```
。 /infaagent startup
```

Secure Agent Manager が起動します。Informatica Intelligent Cloud Services へのアクセスに使用するユーザー名を使用してエージェントを登録する必要があります。また、インストールトークンを指定する必要もあります。

8. エージェントのダウンロード時にインストールトークンをコピーしなかった場合は、管理者の **【ランタイム環境】** ページで **【インストールトークンの生成】** をクリックし、トークンをコピーします。

9. <Secure Agent インストールディレクトリ>/apps/agentcore ディレクトリで、Informatica Intelligent Cloud Services のユーザー名とコピーしたトークンを使用して次のコマンドを入力します。

```
。 /consoleAgentManager.sh configureToken <user name> <install token>
```

Secure Agent の登録ステータスは、次のコマンドを使用して確認できます。

```
。 /consoleAgentManager.sh isConfigured
```

## Linux でのプロキシ設定

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

Secure Agent のインストーラにより、ブラウザで設定されている設定項目に基づいて Secure Agent のプロキシサーバー設定が設定されます。Secure Agent に定義されているプロキシサーバーの設定は、コマンドラインから更新できます。

Linux マシンで Secure Agent のプロキシサーバーを設定するには、proxy.ini ファイルを更新するシェルコマンドを使用します。ネットワーク管理者に問い合わせ、プロキシの設定項目を決めてください。

1. 次のディレクトリに移動します。  
`<Secure Agent installation directory>/apps/agentcore`
2. proxy.ini ファイルを更新するには、次のコマンドを入力します。  
`./consoleAgentManager.sh configureProxy <proxy host> <proxy port> <proxy user name> <proxy password>`
3. Secure Agent を再起動します。

## Linux での Secure Agent のアンインストール

Secure Agent をアンインストールできます。マシンで Secure Agent を実行する必要がなくなった場合、または Secure Agent を再インストールする場合には、Secure Agent をアンインストールすることができます。

Secure Agent をアンインストールする前に、接続またはタスクがそれを使用するように構成されていないことを確認します。

1. コマンドラインから次のディレクトリに移動します。  
`<Secure Agent installation directory>/apps/agentcore`
2. 次のコマンドを入力して、Secure Agent Linux プロセスを停止します。  
`./infaagent shutdown`
3. Secure Agent をアンインストールするには、Secure Agent をインストールしたディレクトリで `rm -rf` を実行して Secure Agent のファイルを削除します。

## 第 15 章

# スケジュール

タスクまたはタスクフローを、指定した時間または一定の間隔で実行するようにスケジュールを作成できます。また、スケジュールされたタスクまたはジョブが実行されないブラックアウト期間を定義することもできます。

スケジュールを作成し、**Administrator** の管理者ページでブラックアウト期間を設定します。スケジュールを作成した後で、データ統合などの別のサービスのタスクおよびタスクフローに関連付けることができます。

スケジュールを作成するときは、日付と時刻を指定します。関連付けられたアセットを午前 12:00 から午後 11:55 の間の一日中実行するようにスケジュールすることができます。Informatica Intelligent Cloud Services によって、開始時刻、終了時刻などのすべての時間設定に短いスケジュールオフセットが追加される場合があります。その結果、スケジュールされたタスクとタスクフローは、予想よりも後で開始される場合があります。たとえば、正午まで 1 時間ごとに実行するようにスケジュールを設定し、組織のスケジュールオフセットが 10 秒であるとします。Informatica Intelligent Cloud Services では、スケジュールの終了時刻が午後 12:00:10 に延長されます。1 時間ごとの最後のタスクまたはタスクフローは午後 12:00:10 に開始されます。組織のスケジュールオフセットを確認するには、データ統合サービスの **【スケジュールオフセット】** 組織プロパティを確認してください。

スケジュールでは次のタスクを実行できます。

### スケジュールとタスクまたはタスクフローの関連付け

タスクまたはタスクフローにスケジュールを関連付けるには、タスクまたはタスクフローを編集します。例えば、スケジュールをマッピングタスクに関連付けるには、データ統合でマッピングタスクを編集し、**【スケジュール】** ページでスケジュールを選択します。

スケジュールを含むタスクまたはタスクフローをコピーすると、そのスケジュールは新しいアセットに関連付けられません。スケジュールを新しいアセットに関連付けるには、アセットを編集します。

### スケジュール済みタスクの監視

モニタの **【すべてのジョブ】** ページからスケジュールされたタスクを監視することができます。スケジュールされたタスクは、**【マイジョブ】** ページには表示されません。

### スケジュールのエクスポート

組織からスケジュールをエクスポートして、別の組織にインポートできます。**【スケジュール】** ページでスケジュールをエクスポートします。スケジュールがタスクまたはタスクフローに関連付けられている場合、タスクまたはタスクフローはエクスポートファイルに含まれません。

### スケジュールの削除

**【スケジュール】** ページでスケジュールを削除します。

**注:** タスクまたはタスクフローで使用されているスケジュールを削除することはできません。スケジュールを削除する前に、すべてのタスクとタスクフローからスケジュールを削除します。

# ブラックアウト期間の設定

ブラックアウト期間を設定すると、指定した期間中は組織内のすべてのスケジュールされたタスクおよびタスクフローが実行できなくなります。組織には1つのブラックアウト期間を設定できます。

ブラックアウト期間を設定するには、管理者で【スケジュール】を選択し、【ブラックアウト期間】をクリックします。ブラックアウト期間が【スケジュール】ページに表示されます。

## 繰り返し頻度

繰り返し頻度では、タスクを実行する頻度を決定します。以下の表に、繰り返し頻度のオプションを示します。

オプション	説明
繰り返ししない	タスクをスケジュールどおりに実行しますが、繰り返ししません。
N分ごと	指定した時間（分単位）に基づく間隔でタスクを実行します。以下のオプションを設定することができます。 <ul style="list-style-type: none"><li>- 繰り返し頻度。頻度を分単位で選択します。オプションは、5、10、15、20、30、45 です。</li><li>- 日。タスクを実行する曜日。1つ以上の曜日を選択できます。</li><li>- 時間範囲。タスクを開始する時間。[終日]を選択するか、時間範囲を設定します。時間範囲は00時00分から23時55分で設定できます。</li><li>- 繰り返しオプション。タスクを実行する日の範囲。[無期限に繰り返す]を選択するか、終了日時を設定できます。</li></ul>
n時間ごと	スケジュールの開始時刻に基づき、タスクを1時間間隔で実行します。 以下のオプションを設定することができます。 <ul style="list-style-type: none"><li>- 繰り返し頻度。頻度を時間単位で選択します。オプションは、1、2、3、4、6、8、12 です。</li><li>- 日。タスクを実行する曜日。1つ以上の曜日を選択できます。</li><li>- 時間範囲。タスクを開始する時間。[終日]を選択するか、時間範囲を設定します。時間範囲は00時00分から23時55分で設定できます。</li><li>- 繰り返しオプション。タスクを実行する日の範囲。[無期限に繰り返す]を選択するか、終了日時を設定できます。</li></ul>
日次	毎日スケジュールで設定した開始時刻にタスクを実行します。 以下のオプションを設定することができます。 <ul style="list-style-type: none"><li>- 繰り返し頻度。タスクを実行する頻度。[毎日]または[すべての平日]を選択します。</li><li>- 繰り返しオプション。タスクを実行する日の範囲。[無期限に繰り返す]を選択するか、終了日時を設定できます。</li></ul>
週次	スケジュールの開始時刻に基づき、1週間間隔でタスクを実行します。 以下のオプションを設定することができます。 <ul style="list-style-type: none"><li>- 日。タスクを実行する曜日。1つ以上の曜日を選択できます。</li><li>- 繰り返しオプション。タスクを実行する日の範囲。[無期限に繰り返す]を選択するか、終了日時を設定できます。</li></ul> <p>曜日を指定しない場合、タスクは開始日と同じ曜日に定期的に実行されます。</p>

オプション	説明
隔週	<p>スケジュールの開始時刻に基づき、タスクを 2 週間隔で実行します。</p> <p>以下のオプションを設定することができます。</p> <ul style="list-style-type: none"> <li>- 日。タスクを実行する曜日。1 つ以上の曜日を選択できます。少なくとも 1 つの日を選択する必要があります。</li> <li>- 繰り返しオプション。タスクを実行する日の範囲。[無期限に繰り返す] を選択するか、終了日時を設定できます。</li> </ul> <p>午後 5:00 に開始する隔週スケジュールを火曜日に設定し、タスクを 2 週間隔で月曜日に実行する場合、このスケジュールのタスク実行は次の月曜日に開始します。</p>
月次	<p>スケジュールの開始時刻に基づき、1 カ月間隔でタスクを実行します。</p> <p>以下のオプションを設定することができます。</p> <ul style="list-style-type: none"> <li>- 日付。タスクを実行する日付。次のいずれかのオプションを設定できます。 <ul style="list-style-type: none"> <li>- 1～28 の間で正確な日付を選択します。月の後半のある曜日にタスクを実行する場合は、&lt;n&gt; &lt;day of the week&gt; オプションを使用します。</li> <li>- &lt;n&gt; &lt;day of the week&gt; を選択します。&lt;n&gt; のオプションは、[第 1]、[第 2]、[第 3]、[第 4]、[最終] です。&lt;day of the week&gt; のオプションは、[日]、[日曜日] - [土曜日] です。</li> </ul> <p>ヒント: [日付] オプションでは、月の初日または最終日にタスクを実行するように設定できます。</p> </li> <li>- 繰り返しオプション。タスクを実行する日の範囲。[無期限に繰り返す] を選択するか、終了日時を設定できます。</li> </ul>

## タイムゾーンとスケジュール

Informatica Intelligent Cloud Services は、時間を世界協定時刻 (UTC) で保存します。ログインすると、Informatica Intelligent Cloud Services で時間が変換され、ユーザープロファイルに関連付けられたタイムゾーンで表示されます。

スケジュールを作成するときに、使用するスケジューラのタイムゾーンを選択します。自分のタイムゾーンまたは組織のタイムゾーンとは異なるタイムゾーンを選択できます。

## 夏時間への移行とスケジュール

Informatica Intelligent Cloud Services は、隔週のタスクを除くすべてのタスクに夏時間の変更を適用します。

夏時間を有効にすると、午前 2 時 00 分 - 午前 2 時 59 分に実行するようにスケジュールされたタスクは、時刻が午前 2 時 00 分から午前 3 時 00 分に変更される日は実行されません。タスクが隔週で午前 2 時に実行するようにスケジュールされている場合は、時刻が変更される日の午前 3 時にそのタスクが実行され、次回は午前 2 時に実行されます。

夏時間により、標準時が開始されるときに午前 1 時 00 分 - 午前 1 時 59 分に実行するようにスケジュールされたタスクが再実行されることはありません。例えば、毎日午前 1 時半に実行するようにスケジュールされたタスクがあるとします。時刻が午前 2 時から午前 1 時に変更されても、このタスクが午前 1 時半に再実行されることはありません。

**ヒント:** Informatica Intelligent Cloud Services で午前 2 時前後の時刻変更時にスケジュールされた実行がスキップされないようにするため、午前 12:59 から午前 3:01 の間はジョブの実行をスケジュールしないでください。

# スケジュールの設定

**【スケジュール】** ページでスケジュールを設定します。マッピングタスクおよび同期タスクの場合は、タスクを構成するときに新しいスケジュールを作成することもできます。スケジュールは、1 回だけ実行するように設定したり、指定した間隔で無期限に、または指定した終了時刻まで実行するように設定したりすることができます。

- 1. 管理者で **【スケジュール】** を選択します。
- 2. スケジュールを作成するには、**【新しいスケジュール】** をクリックします。  
スケジュールを編集するには、スケジュールを含む行の編集アイコンをクリックします。
- 3. 以下のプロパティを設定します。

プロパティ	説明
スケジュール名	スケジュールの名前。 各スケジュール名は組織内で一意である必要があります。スケジュール名には、英数字、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。名前の大文字と小文字は区別されません。
説明	スケジュールの説明。 最大長は 255 文字です。
開始	スケジュールを開始する日付と時刻。 日付の形式は MM/DD/YYYY です。時刻は 24 時間形式です。 [カレンダー] ボタンをクリックし、開始日付を選択します。開始日時は、一定間隔で繰り返すタスクおよびタスクフロージョブの繰り返し頻度に影響することがあります。 例えば、開始日が 11 月 10 日で、繰り返し頻度が毎月の場合、スケジュールは毎月 10 日に関連付けられたアセットを実行します。開始時刻を 3 時 10 分、繰り返し頻度を 1 時間にした場合、アセットは毎時 10 分 to 実行されます。 デフォルトは、スケジュールを作成するユーザーの現在の日付、現在の時刻、およびタイムゾーンです。

プロパティ	説明
タイムゾーン	使用するスケジュールのタイムゾーンを選択します。タイムゾーンは、組織のタイムゾーンやユーザーのタイムゾーンとは異なるものにすることができます。
繰り返す	<p>スケジュールの繰り返し頻度。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"> <li>- 繰り返さない</li> <li>- N 分ごと</li> <li>- n 時間ごと</li> <li>- 日次</li> <li>- 週次</li> <li>- 隔週</li> <li>- 月次</li> </ul> <p>デフォルトは「繰り返さない」です。</p>

4. **【保存】** をクリックします。

## スケジュールのエクスポート

組織からスケジュールをエクスポートし、それらのスケジュールを他の組織にインポートできます。スケジュールに関連付けられているアセットは、エクスポートファイルには含まれません。**【スケジュール】** ページでスケジュールをエクスポートします。

1. 管理者で **【スケジュール】** を選択します。
2. **【エクスポート】** をクリックします。
3. **【スケジュールのエクスポート】** ダイアログボックスで、エクスポートするスケジュールを選択します。
4. オプションとして、エクスポートジョブ名を更新します。  
デフォルトでは、ジョブ名は SchedulesExport\_<日付> です。
5. **【エクスポート】** をクリックします。  
管理者によって、スケジュールをエクスポートするためのエクスポートジョブが作成されます。
6. エクスポートジョブのステータスを確認し、エクスポートファイルをダウンロードするには、モニタで **【インポート/エクスポートログ】** ページを開き、**【エクスポート】** タブをクリックします。  
エクスポートジョブを含む行で、またはジョブの詳細ページでエクスポートファイルをダウンロードできます。

データ統合など、別のサービスの **【エクスプローラ】** ページでスケジュールをインポートできます。アセットのインポートについて詳しくは、そのサービスのヘルプを参照してください。

スケジュールをインポートした後、それらをターゲット組織のアセットに関連付けることができます。

## 第 16 章

# バンドル管理

バンドルは関連するマッピング、マッピングタスク、マップレット、および Visio テンプレートのセットであり、データ統合ユーザーがデータ統合プロジェクトで使用できます。データ統合ユーザーはバンドルを設計、作成、およびパブリッシュします。管理者はバンドルを管理します。

組織の管理者である場合は、次の操作を実行してバンドルを管理できます。

### バンドルをインストールする。

バンドル設計者が参照として使用するように構成した公開、非公開、または非表示バンドルをインストールできます。バンドルはデータ統合のアドオンバンドルプロジェクトにインストールされます。組織のユーザーはバンドル内のアセットを使用できますが、編集することはできません。

### バンドルをコピーする。

バンドル設計者がコピー用に構成した公開、非公開、または非表示バンドルをコピーできます。バンドルをコピーするときに、バンドルの内容をコピーするデータ統合フォルダを選択します。バンドルを複数回コピーし、その内容を毎回別のプロジェクトまたはフォルダに保存することができます。バンドルをコピーすると、組織内のユーザーはアセットを編集できます。

### バンドルをアップグレードする。

バンドルをインストールし、新しいバージョンのバンドルが使用できるようになると、バンドルをアップグレードして最新バージョンを入手できます。

### バンドルをアンインストールする。

インストール済みのバンドルが組織で不要になった場合は、アンインストールすることができます。

インストール済み、または組織で使用可能なバンドルを表示するには、管理者で【アドオンバンドル】を選択します。【アドオンバンドル】ページには、インストール済みバンドル、コピーされたバンドル、インストールまたはコピーに使用可能なバンドルに関する情報が表示されます。

バンドルタイプの詳細、バンドルの作成、またはバンドルのパブリッシュについては、データ統合サービスのヘルプの「マッピング」を参照してください。

## バンドルのインストール

バンドル設計者が参照として使用するように構成した公開、非公開、または非表示バンドルをインストールできます。【アドオンバンドル】ページの「使用可能なバンドル」タブでバンドルをインストールします。

非表示バンドルをインストールする前に、バンドルのアクセスコードを取得します。組織内で作成されたバンドルのアクセスコードを取得するには、データ統合で【バンドル】ページを開き、バンドル名をクリックして



**【アクセスコードのコピー】** をクリックします。組織の外部で作成されたバンドルのアクセスコードを取得するには、バンドルパブリッシャに問い合わせてください。

1. 管理者で、**【アドオンバンドル】** を選択します。
2. **【使用可能なバンドル】** をクリックします。  
[使用可能なバンドル] タブには、インストールまたはコピーに使用できる公開および非公開バンドルが一覧表示されます。
3. インストールするバンドルが非表示バンドルの場合は、**【検索】** フィールドにバンドルのアクセスコードを入力します。
4. バンドル名をクリックして、**【バンドルの詳細】** ページを開きます。
5. **【許可】** フィールドが **【参照】** または **【参照とコピー】** に設定されていることを確認します。  
コピー専用で構成されたバンドルをインストールすることはできません。
6. **【インストール】** をクリックします。

データ統合でバンドルがアドオンバンドルプロジェクトに追加され、アセットが使用できる状態になります。また、バンドルは管理者の **【アドオンバンドル】** ページにある **【インストール済みバンドル】** タブに一覧表示されます。

## バンドルのコピー

バンドル設計者がコピー用に構成した公開、非公開、または非表示バンドルをコピーできます。**【アドオンバンドル】** ページの **【使用可能なバンドル】** タブでバンドルをコピーします。バンドルをコピーするたびに、**【コピーされたバンドル】** タブにイベントが記録されます。

非表示バンドルをコピーする前に、バンドルのアクセスコードを取得してください。組織内で作成されたバンドルのアクセスコードを取得するには、データ統合で **【バンドル】** ページを開き、バンドル名をクリックして **【アクセスコードのコピー】** をクリックします。組織の外部で作成されたバンドルのアクセスコードを取得するには、バンドルパブリッシャに問い合わせてください。

1. 管理者で、**【アドオンバンドル】** を選択します。
2. **【使用可能なバンドル】** をクリックします。  
[使用可能なバンドル] タブには、インストールまたはコピーに使用できる公開および非公開バンドルが一覧表示されます。
3. コピーするバンドルが非表示バンドルの場合は、**【検索】** フィールドにバンドルのアクセスコードを入力します。
4. バンドル名をクリックして、**【バンドルの詳細】** ページを開きます。
5. **【許可】** フィールドが **【コピー】** または **【参照とコピー】** に設定されていることを確認します。  
参照のみとして使用するように構成されているバンドルをコピーすることはできません。
6. **【バンドルの内容を次の場所にコピー...】** をクリックします。
7. **【参照】** ダイアログボックスで、バンドルの内容をコピーするデータ統合プロジェクトまたはフォルダを選択します。
8. **【選択】** をクリックします。  
バンドル内のアセットが、選択したプロジェクトまたはフォルダにコピーされます。

## バンドルのアップグレード

更新バージョンが入手可能になった時点で、インストール済みバンドルをアップグレードできます。バンドルステータスは、[アドオンバンドル] ページの [インストール済みバンドル] タブで確認できます。

1. 管理者で、[アドオンバンドル] を選択します。
2. [インストール済みバンドル] をクリックします。  
[バンドルステータス] 列は、バンドルが最新かどうか、またはアップグレードが利用可能かどうかを示します。
3. バンドル名をクリックして、[バンドルの詳細] ページを開きます。
4. [アップグレード] をクリックします。

## バンドルのアンインストール

組織内のユーザーがバンドルを必要としなくなった場合は、アンインストールします。[アドオンバンドル] ページの [インストール済みバンドル] タブでバンドルをアンインストールします。

**注:** バンドルをアンインストールすると、組織のすべてのバンドルアセットが削除されます。バンドル内のアセットを使用するタスクを保持する場合は、タスクでそのアセットを削除してからバンドルをアンインストールします。

1. 管理者で、[アドオンバンドル] を選択します。
2. [インストール済みバンドル] をクリックします。
3. バンドル名をクリックして、[バンドルの詳細] ページを開きます。
4. [Uninstall (アンインストール)] をクリックします。

バンドルをアンインストールすると、[使用可能なバンドル] タブに一覧表示されます。

## 第 17 章

# イベント監視

アセットおよびセキュリティログを使用して、組織内のアセット、ライセンス、ユーザー、および Secure Agent のイベントを監視できます。ログを表示するには、「監査ログ-表示」特権を持つロールを割り当てる必要があります。

次のログを使用してイベントを監視できます。

### アセットログ

次の情報が表示されます。

- 各アセットが作成、更新、コピー、または削除されたときや、アセットを変更したユーザー名など、アセットのイベント。
- 組織内のユーザーが Informatica Intelligent Cloud Services にログインしたときなど、ユーザーの認証イベント。
- ライセンスが追加、削除、または変更されたときなど、ライセンスに関連するイベント。

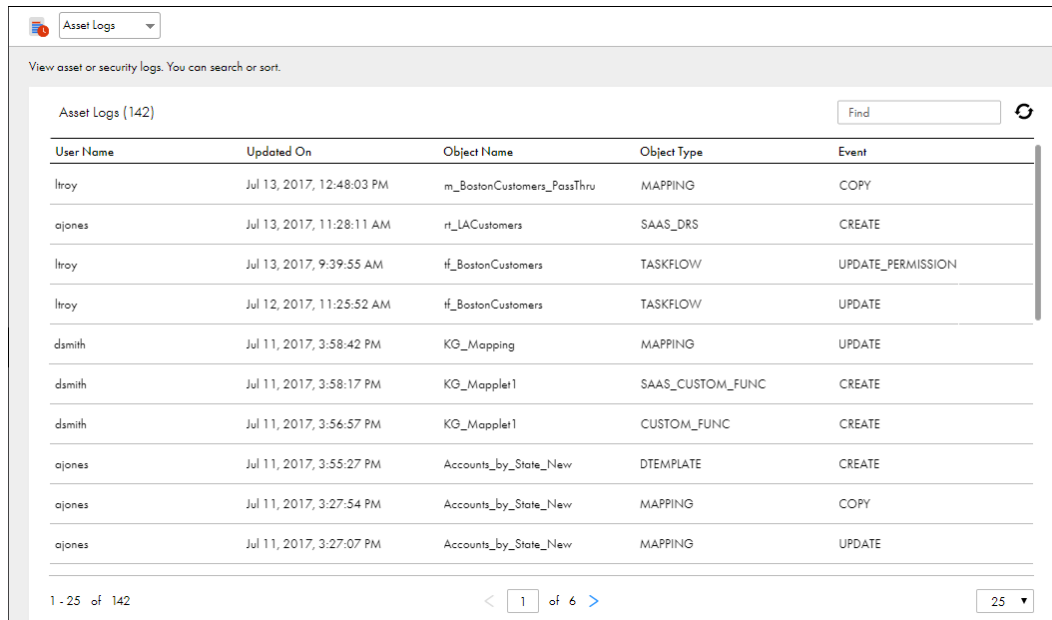
アセットログを開くには、管理者を開いて **【ログ】** を選択し、ページ上部の **【アセットログ】** を選択します。

### セキュリティログ

各エージェントが作成または更新されたとき、組織情報が更新されたとき、エージェントまたは組織を変更したユーザーの名前など、Secure Agent および組織のイベントが表示されます。

セキュリティログを開くには、管理者を開いて **【ログ】** を選択し、ページ上部の **【セキュリティログ】** を選択します。

次の図は、アセットログを示しています。



Asset Logs (142)

Find

User Name	Updated On	Object Name	Object Type	Event
ltray	Jul 13, 2017, 12:48:03 PM	m_BostonCustomers_PassThru	MAPPING	COPY
ajones	Jul 13, 2017, 11:28:11 AM	rt_LACustomers	SAAS_DRS	CREATE
ltray	Jul 13, 2017, 9:39:55 AM	tf_BostonCustomers	TASKFLOW	UPDATE_PERMISSION
ltray	Jul 12, 2017, 11:25:52 AM	tf_BostonCustomers	TASKFLOW	UPDATE
dsmith	Jul 11, 2017, 3:58:42 PM	KG_Mapping	MAPPING	UPDATE
dsmith	Jul 11, 2017, 3:58:17 PM	KG_Mapplet1	SAAS_CUSTOM_FUNC	CREATE
dsmith	Jul 11, 2017, 3:56:57 PM	KG_Mapplet1	CUSTOM_FUNC	CREATE
ajones	Jul 11, 2017, 3:55:27 PM	Accounts_by_State_New	DTEMPLATE	CREATE
ajones	Jul 11, 2017, 3:27:54 PM	Accounts_by_State_New	MAPPING	COPY
ajones	Jul 11, 2017, 3:27:07 PM	Accounts_by_State_New	MAPPING	UPDATE

1 - 25 of 142

< 1 of 6 >

25

デフォルトでは、ログには過去 90 日間のイベントが表示されます。イベントが監査ログに表示される期間を変更するには、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。

ログに表示されるプロパティは、次の方法でカスタマイズできます。

- 列を非表示にするには、列見出し領域を右クリックし、非表示にする列をオフにします。
- ログイベントをソートするには、ソート基準にするプロパティの列見出しをクリックします。ソート順序を逆転させるには、列見出しをもう一度クリックします。
- 特定のイベントのログを検索するには、検索文字列を **【検索】** フィールドに入力します。オブジェクト名またはイベントタイプを検索できます。

## 第 18 章

# ファイル転送

HTTPS、AS2、SFTP などのファイル転送プロトコルを使用して、リモートパートナーとファイルを交換できます。

ファイルを交換するために、B2B Gateway を使用すること、またはデータ統合 REST API sendfiles リソースを使用することができます。

リモートパートナーとファイルを交換するには、ファイル統合サービスに関連付けられた組織のファイルサーバーを設定してパートナーのサーバーと安全に通信できるようにします。ファイル統合サービスは、高度なファイル転送プロトコルを実行する Secure Agent のサービスです。

次のタイプのファイルサーバーを設定できます。

### AS2 サーバー

AS2 ファイル転送でパートナーからファイルを受信するには、AS2 サーバーを設定してリモート AS2 サーバーからファイルを受信できます。

AS2 ファイルをパートナーのサーバーに送信するには、接続を設定してから Informatica Intelligent Cloud Services の REST API を使用してパートナーにファイルを送信します。詳細については、データ統合のヘルプの AS2 コネクタのヘルプを参照してください。

例えば、パートナーの AS2 サーバーと EDI メッセージを交換するとします。パートナーからファイルを受信するには、ファイルサーバーを設定してパートナーのサーバーからのファイルを承認します。パートナーのサーバーにファイルを送信するには、パートナーに AS2 接続を設定します。次に、sendfiles REST API リソースを使用して POST 要求を送信する事で、パートナーのサーバーに EDI メッセージを転送します。

### HTTPS サーバー

HTTPS ファイル転送でパートナーとファイルを交換するには、HTTPS サーバーを設定し、パートナーがそのサーバーに接続してサーバーとの間でファイルをアップロードおよびダウンロードできるようにします。

### SFTP サーバー

SFTP ファイル転送でパートナーとファイルを交換するには、SFTP サーバーを設定し、パートナーがそのサーバーに接続してサーバーとの間でファイルをアップロードおよびダウンロードできるようにします。

### プロキシサーバー

1 つまたは複数のファイル統合プロキシサーバーを demilitarized zone（非武装ゾーン）（DMZ）内にインストールして設定できます。パートナーのサーバーは、組織のファイルサーバーと直接通信する代わりに、プロキシサーバーと通信できます。複数のファイルサーバーが同じファイル統合プロキシサーバーを使用できます。

プロキシサーバーは Windows オペレーティングシステムと Linux オペレーティングシステムにインストールできます。

組織とファイルを交換するリモートパートナーごとに、ファイルサーバーユーザーアカウントを作成します。ファイルサーバーユーザーのプロトコルアクセシビリティを定義します（つまり、AS2、HTTPS、SFTP、またはこれらのサーバーの組み合わせ）。各ファイルサーバーユーザーに、ホームディレクトリが作成されるか割り当てられます。ネットワーク共有場所をユーザーのホームディレクトリに定義でき、そのユーザーに対してフォルダレベルおよびファイルレベルの権限を定義できます。

モニタの【ファイル転送ログ】 ページでファイル転送ジョブを監視できます。ファイル転送ジョブの監視の詳細については、モニタのヘルプを参照してください。

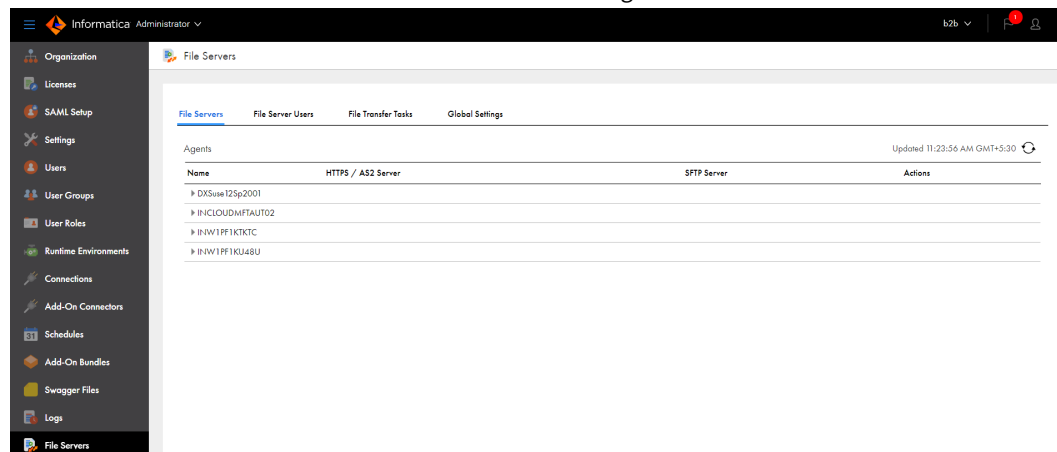
ファイルを交換するには、次のライセンスが必要です。

- ファイル統合サービス
- HTTPS ファイルを交換する場合は HTTPS サーバー
- AS2 ファイルを交換する場合は AS2 サーバーと AS2 コネクタ
- SFTP ファイルを交換する場合は SFTP サーバー

## ファイルサーバーの設定プロセス

リモートパートナーと Informatica Intelligent Cloud Services 組織との間でファイルを交換するようにファイルサーバー、ファイルサーバーユーザー、グローバル設定を設定します。

ファイル統合サービスを使用する Secure Agent ごとにファイルサーバーを設定できます。管理者の【ファイルサーバー】 ページでファイルサーバーを設定します。【ファイルサーバー】 ページに、ファイル統合サービスを使用できる組織内のすべてのランタイム環境と Secure Agent が一覧表示されます。



外部パートナーがお客様の組織とファイルを交換できるようになる事には、以下のタスクが含まれます。

- ファイルサーバープロパティを設定します。AS2、HTTPS、および SFTP サーバーを設定できます。
- オプションで、1 つ以上のプロキシサーバーをパートナーのファイルサーバーと組織のファイルサーバーとの間の仲介としてインストールおよび設定します。
- リモートパートナーのサーバーユーザーがお客様のサーバーとファイルを交換できるように設定します。
- ファイルを交換するデフォルトフォルダを指定します。

## 始める前に

ファイルサーバーを設定する前に、適切なライセンスがある事、およびパートナーとパブリックキーを交換している事を確認します。

組織がリモートサーバーとファイルを交換できるようにするには、次のタスクを完了します。

1. パートナーにパブリックキーを送信します。
2. パートナーのパブリックキーを受信します。
3. パートナーのパブリックキーを自分のトラストストアにインポートします。
4. ファイルサーバーを設定します。

Secure Agent でファイル統合サービスが実行中である事を確認します。Secure Agent サービスのステータスの確認方法については、[第 13 章, 「Secure Agent サービス」 \(ページ 113\)](#)を参照してください。

## ファイルサーバー

ファイルサーバーを設定し、リモートパートナーとファイルを交換します。

以下のサーバーを設定する事ができます。

- AS2 サーバー。パートナーから AS2 ファイル転送でファイルを受信します。
- HTTPS サーバー。パートナーはサーバーに接続し、ファイルをアップロードおよびダウンロードします。
- SFTP サーバー。パートナーはサーバーに接続し、ファイルをアップロードおよびダウンロードします。
- プロキシサーバー。パートナーのファイルサーバーと組織のファイルサーバーとの間を仲介します。

## ファイルサーバーの設定

ファイルサーバーのプロパティを設定し、サーバーとリモートパートナーとの間でファイルを交換します。

1. Administrator で、**[ファイルサーバー]** を選択します。
2. **[ファイルサーバー]** タブで、リモートサーバーとのファイルの交換に使用するファイル統合サービスを実行する Secure Agent を選択します。
3. **[エージェント用のファイルサーバー]** ページで、設定するサーバーのタイプ (HTTPS サーバー、AS2 サーバー、SFTP サーバー、またはプロキシサーバー) のタブを選択します。
4. ファイルサーバーのプロパティを設定し、**[保存]** をクリックします。
  - AS2 サーバーのプロパティの詳細については、[「AS2 サーバーの設定プロパティ」 \(ページ 168\)](#)を参照してください。
  - HTTPS サーバーのプロパティの詳細については、[「HTTPS サーバー設定プロパティ」 \(ページ 172\)](#)を参照してください。
  - SFTP サーバーのプロパティの詳細については、[「SFTP サーバー設定プロパティ」 \(ページ 174\)](#)を参照してください。
  - プロキシサーバーのプロパティの詳細については、[「プロキシサーバー設定プロパティ」 \(ページ 177\)](#)を参照してください。

## AS2 サーバーの設定プロパティ

ファイル統合サービスを使用する各ランタイム環境では、AS2 サーバーを設定してリモート AS2 サーバーからファイルを受信できます。

AS2 サーバープロパティを [エージェント用のファイルサーバー] ページの [AS2 サーバー] タブで設定します。

以下のタイプのプロパティを設定します。

- 全般的なプロパティ
- SSL プロパティ
- メッセージのセキュリティプロパティ
- MDN プロパティ
- アップロード制限のプロパティ

### 全般プロパティ

以下の表に、全般的な AS2 サーバーのプロパティを示します。

プロパティ	説明
AS2 の有効化サーバー	AS2 サーバーを有効にするかどうか。 有効にしない場合、AS2 サーバーでファイルを受信出来ません。 デフォルトでは無効になっています。
AS2 サーバー ID	送信者が使用する名前または ID。ID に関する次のルールに注意してください。 <ul style="list-style-type: none"><li>- 値は大文字と小文字が区別されます。</li><li>- ID には最大 128 文字の ASCII 文字、特殊文字、スペースを含めることができます。</li></ul>
ポート	AS2 サーバーのポート番号。 デフォルトは 15400 です。
ローカルアドレス	AS2 サーバーのローカルアドレス。
SSL の有効化	リモート AS2 サーバーとの通信で SSL 暗号化を使用するかどうか。 デフォルトでは無効になっています。



## SSL プロパティ

以下の表に、SSL のプロパティを示します。

プロパティ	説明
SSL プロトコル	SSL と TLS のどちらのプロトコルを使用するか。 次のいずれかの値を選択します。 <ul style="list-style-type: none"><li>- TLS 送信を保護するために、SSL の新しいバージョンである Transport Layer Security が使用されます。</li><li>- SSL。送信を保護するために、従来の Secure Socket Layer プロトコルが使用されます。</li></ul> デフォルトは SSL です。
SSL プロトコル 有効	許容する TLS と SSL のバージョンをカンマで区切って指定します。 サポートされているバージョンは次のとおりです。 <ul style="list-style-type: none"><li>- TLS: TLSv1.2 および TLSv1.3</li><li>- SSL: SSLv2Hello および SSLv3</li></ul> 値が未指定の場合、選択したプロトコルのすべてのバージョンが有効になります。
クライアント認証	クライアントにサーバーとの認証に使用する証明書が必要かどうか。 次のいずれかの値を選択します。 <ul style="list-style-type: none"><li>- なし。SSL 接続が証明書を確認せずに実行され、ユーザーはパスワードを使用して認証されます。送信された情報のいずれかで証明書が必要となる場合、接続に失敗します。</li><li>- 必須。有効な証明書が使用可能にならないと、SSL 接続ではユーザーを接続または認証しません。</li><li>- オプション。SSL 接続で有効な証明書を検索しますが、証明書がない場合は引き続きパスワード認証を行います。</li></ul>
キーストアの場合	クライアントがファイル統合サービスとの通信の認証に使用する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合。 パスとファイル名が含まれます。
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。
キーストアタイプ	プライベートキーストアのタイプ。 以下の値を使用します。 <ul style="list-style-type: none"><li>- JKS</li><li>- PKCS12</li></ul>
キーエイリアス	MDN の署名に使用するプライベートキーのキーエイリアスまたは証明書。
トラストストアの場合	ファイル統合サービスが HTTPS 通信に使用するトラストストアファイルへのパス。
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。
トラストストアのタイプ	トラストストアのタイプ。 以下の値を使用します。 <ul style="list-style-type: none"><li>- JKS</li><li>- PKCS12</li></ul>

## メッセージのセキュリティプロパティ

以下の表に、基本的なメッセージのセキュリティプロパティを示します。

プロパティ	説明
暗号化が必要	ファイル統合サービスが受信するファイルを暗号化する必要があるかどうか。 デフォルトでは有効になっています。
署名が必要	リモート AS2 サーバーのファイルにデジタル署名を含める必要があるかどうか。署名が必要な場合、ファイル統合サービスは署名がないメッセージを却下します。 デフォルトでは有効になっています。
認証	ユーザーが認証を受ける必要があるかどうか。 デフォルトでは無効になっています。
暗号化証明書のエイリアス	受信メッセージの復号化に使用するキーエイリアスまたは証明書。エイリアスは、キーストアの証明書を参照します。 AS2 メッセージを送信するすべてのパートナーは、この証明書のパブリックパートを持っている必要があります。

## MDN プロパティ

以下の表に、受信メッセージのプロパティを示します。

プロパティ	説明
MDN 署名証明書のエイリアス	AS2 サーバーが受信メッセージに署名するために使用するプライベートキーを指すエイリアス。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。
非同期 MDN の自動承認	受信確認を自動または手動で送信するかどうか。
非同期 MDN のプロキシを有効化	プロキシサーバーが非同期 MDN に対して有効かどうかを決定します。 デフォルトでは無効になっています。
プロキシタイプ	この接続に使用するプロキシサーバーのタイプ。 次のいずれかのタイプを選択します。 <ul style="list-style-type: none"><li>- SOCKS。SOCKS バージョン 4 または 5 を使用できます。</li><li>- HTTPS。</li><li>- Informatica ファイルサーバープロキシ。</li></ul> 使用するプロキシサーバーのタイプをネットワーク管理者に確認してください。
ホスト	ネットワークのプロキシサーバーのホスト名または IP アドレス。
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。

## アップロード制限のプロパティ

AS2 ファイルのアップロード時に許可または拒否するファイルのタイプを指定できます。以下の表に、アップロード制限を制御するプロパティを示します。

プロパティ	説明
ファイル拡張子のフィルタタイプ	ファイル拡張子リストの拡張子を承認または拒否するかどうか。 以下の値を使用します。 <ul style="list-style-type: none"><li>- フィルタしない。すべてのファイルタイプを承認します。</li><li>- 承認。ファイル拡張子プロパティでリストされた拡張子を持つファイルを承認します。</li><li>- 拒否。ファイル拡張子プロパティでリストされた拡張子を持つファイルを許可しません。</li></ul>
ファイル拡張子	ファイル拡張子のリスト。ファイル拡張子のフィルタタイプに対応するファイル拡張子を追加します。例えば、ファイル拡張子のフィルタタイププロパティで .csv ファイルおよび .txt ファイルを承認するには、 <b>【承認】</b> を選択してからファイル拡張子のリストに csv および txt を追加します。 拡張子をリストに追加するには、テキストボックスに拡張子を入力してから <b>【追加】</b> をクリックします。 リストから拡張子を削除するには、拡張子を強調表示してから <b>【削除】</b> をクリックします。
大文字と小文字が区別されるファイル拡張子	ファイル拡張子リストを使用してフィルタする場合に、大文字と小文字を考慮に入れるかどうか。有効にすると、ファイル拡張子リストで使用される大文字と小文字が一致しない拡張子を使用したファイルはアップロード出来ません。 例えば、ファイル拡張子リストに csv があるが CSV はない場合、拡張子 csv を使用したファイルはアップロードできますが、拡張子 CSV を使用したファイルはアップロード出来ません。
拡張子付きのファイルを許可	ファイル拡張子フィルタを有効にするかどうか。有効にすると、このページで設定されたファイル拡張子のプロパティによってアップロードできるファイルのタイプが決まります。 デフォルトでは有効になっています。
拡張子なしのファイルを許可	ファイル名に拡張子が含まれていないファイルを許可するかどうか。 デフォルトでは有効になっています。
名前なしのファイルを許可	名前のないファイルを許可するかどうか。Secure Agent は、次の形式を使用して名前なしでファイルを保存します: as2data_<datetime> datetime は、ミリ秒を含む現在のタイムスタンプです。 デフォルトでは有効になっています。
ファイル名サフィックスのタイムスタンプ (オプション)	ファイル名にタイムスタンプを付加するかどうか。有効にすると、ファイル名の末尾にタイムスタンプが付加されます。

プロパティ	説明
最大アップロードサイズ	AS2 サーバーがアップロードできる最大ファイルサイズ（メガバイト単位）。デフォルトは 5 MB です。
ファイルが存在する場合	<p>フォルダ内にすでに存在するファイルを再び受け取ったときに実行するアクションを選択します。</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"> <li>- 名前の変更: 新しく受け取ったファイルの名前を変更します。</li> <li>- 追加: 既存のファイルに変更を追加します。</li> <li>- 上書き: 新しく受け取ったファイルで既存のファイルを上書きします。</li> <li>- エラー: ファイルがすでに存在する場合、エラーを表示します。</li> </ul>

## HTTPS サーバー設定プロパティ

ファイル統合サービスを使用する各ランタイム環境では、リモート HTTPS サーバーとファイルを交換するように HTTPS サーバーを設定できます。

【エージェント用のファイルサーバー】 ページの **【HTTPS サーバー】** タブで HTTPS サーバーのプロパティを設定します。HTTPS サーバーを介してファイルを交換するには、HTTPS ライセンスが必要です。

以下のタイプのプロパティを設定します。

- 全般
- SSL
- アップロード制限

### 全般プロパティ

次の表に、HTTPS サーバーの一般的なプロパティを示します。

プロパティ	説明
HTTPS サーバーの有効化	HTTPS サーバーを有効にするかどうか。 有効にしない場合、HTTPS サーバーはファイルを受信できません。 デフォルトでは無効になっています。
ポート	HTTPS サーバーのポート番号。 デフォルトは 15400 です。
ローカルアドレス	HTTPS サーバーのローカルアドレス。
SSL の有効化	リモート HTTPS サーバーとの通信で SSL 暗号化を使用するかどうか。 デフォルトでは無効になっています。

## SSL プロパティ

以下の表に、SSL のプロパティを示します。

プロパティ	説明
SSL プロトコル	SSL と TLS のどちらのプロトコルを使用するか。 次のいずれかの値を選択します。 <ul style="list-style-type: none"><li>- TLS 送信を保護するために、SSL の新しいバージョンである Transport Layer Security が使用されます。</li><li>- SSL。送信を保護するために、従来の Secure Socket Layer プロトコルが使用されます (デフォルト)。</li></ul>
SSL プロトコル 有効	許容する TLS と SSL のバージョンをカンマで区切って指定します。 サポートされているバージョンは次のとおりです。 <ul style="list-style-type: none"><li>- TLS: TLSv1.1、TLSv1.2、および TLSv1.3</li><li>- SSL: SSLv2Hello および SSLv3</li></ul> 値が未指定の場合、選択したプロトコルのすべてのバージョンが有効になります。
クライアント認証	クライアントにサーバーとの認証に使用する証明書が必要かどうか。 次のいずれかの値を選択します。 <ul style="list-style-type: none"><li>- なし。SSL 接続が証明書を確認せずに実行され、ユーザーはパスワードを使用して認証されます。送信される情報に証明書が必要な場合、接続は失敗します。</li><li>- 必須。有効な証明書が使用可能にならないと、SSL 接続ではユーザーを接続または認証しません。</li><li>- オプション。SSL 接続で有効な証明書を検索しますが、証明書がない場合は引き続きパスワード認証を行います。</li></ul>
キーストアの場所	プライベートキーと関連する証明書を保存するキーストアの場所。クライアントは、キーストアファイルを使用して、ファイル統合サービスとの通信を認証します。 パスとファイル名が含まれます。
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。
キーストアタイプ	プライベートキーストアのタイプ。 以下の値を使用します。 <ul style="list-style-type: none"><li>- JKS</li><li>- PKCS12</li></ul>
キーエイリアス	MDN の署名に使用するプライベートキーのキーエイリアスまたは証明書。
トラストストアの場所	ファイル統合サービスが HTTPS 通信に使用するトラストストアファイルへのパス。
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。
トラストストアのタイプ	トラストストアのタイプ。 以下の値を使用します。 <ul style="list-style-type: none"><li>- JKS</li><li>- PKCS12</li></ul>

## アップロード制限のプロパティ

HTTPS ファイルのアップロード時に許可または拒否するファイルのタイプを指定できます。

以下の表に、アップロード制限を制御するプロパティを示します。

プロパティ	説明
ファイル拡張子のフィルタタイプ	ファイル拡張子リストの拡張子を承認または拒否するかどうか。 以下の値を使用します。 <ul style="list-style-type: none"><li>- フィルタしない。すべてのファイルタイプを承認します。</li><li>- 承認。ファイル拡張子プロパティでリストされた拡張子を持つファイルを承認します。</li><li>- 拒否。ファイル拡張子プロパティでリストされた拡張子を持つファイルを許可しません。</li></ul>
ファイル拡張子	ファイル拡張子のリスト。ファイル拡張子のフィルタタイプに対応するファイル拡張子を追加します。例えば、ファイル拡張子のフィルタタイププロパティで、CSV ファイルおよび.txt ファイルを承認するには、 <b>【承認】</b> を選択してからファイル拡張子のリストに CSV および txt を追加します。 拡張子をリストに追加するには、テキストボックスに拡張子を入力してから <b>【追加】</b> をクリックします。 リストから拡張子を削除するには、拡張子を強調表示してから <b>【削除】</b> をクリックします。
大文字と小文字が区別されるファイル拡張子	ファイル拡張子リストを使用してフィルタする場合に、大文字と小文字を考慮に入れるかどうか。有効にすると、ファイル拡張子リストで使用される大文字と小文字が一致しない拡張子を使用したファイルはアップロード出来ません。 例えば、ファイル拡張子リストに CSV があるが CSV はない場合、拡張子 CSV を使用したファイルはアップロードできますが、拡張子 CSV を使用したファイルはアップロード出来ません。
拡張子付きのファイルを許可	ファイル拡張子フィルタを有効にするかどうか。有効にすると、このページで設定されたファイル拡張子のプロパティによってアップロードできるファイルのタイプが決まります。 デフォルトでは有効になっています。
拡張子なしのファイルを許可	ファイル名に拡張子が含まれていないファイルを許可するかどうか。 デフォルトでは有効になっています。
名前なしのファイルを許可	名前なしのファイルを許可するかどうか。Secure Agent は、次の形式を使用して名前なしでファイルを保存します: as2data_<datetime>datetime は、ミリ秒を含む現在のタイムスタンプです。 デフォルトでは無効になっています。
最大アップロードサイズ (MB)	HTTPS サーバーアップロードのファイルサイズの制限 (MB)。 デフォルトは 5MB です。

## SFTP サーバー設定プロパティ

ファイル統合サービスを使用する各ランタイム環境では、SFTP サーバーを設定してファイルを交換できます。

SFTP サーバープロパティを **【エージェント用のファイルサーバー】** ページの **【SFTP サーバー】** タブで設定します。以下のタイプのプロパティを設定します。

- 全般的なプロパティ
- アルゴリズムのプロパティ
- ホストキーのプロパティ

- アップロード制限のプロパティ

## 全般プロパティ

以下の表に、一般的な SFTP サーバーのプロパティを示します。

プロパティ	説明
有効な SFTP サーバー	SFTP サーバーを有効にするかどうか。 有効にしない場合、SFTP サーバーでファイルを送受信出来ません。 デフォルトでは無効になっています。
ポート	SFTP サーバーのポート番号。 デフォルトは 15002 です。
ローカルアドレス	SFTP サーバーのローカル IP アドレス。
SCP の有効化	session control protocol (セッション管理プロトコル) (SCP) を使用して接続を作成するかどうか。 デフォルトでは無効になっています。
アイドルタイムアウト	接続を閉じるまでの接続がアイドルな秒数。 デフォルトは 300 です。
最大ログイン	サーバーに同時にログインできる最大ユーザー数。 デフォルトは 500 です。
ログイン失敗遅延	失敗したログイン試行の間の遅延秒数。 デフォルトは 0 です。
最大ログイン失敗	1 人のユーザーに許可される失敗したログイン試行回数。 デフォルトは 5 です。
ウェルカムメッセージ	サーバーへの接続の確立時に表示するメッセージ。

## アルゴリズムのプロパティ

次のアルゴリズムタイプを **【SFTP サーバー】** タブの **【アルゴリズム】** セクションで有効にします。

- 暗号アルゴリズム
- Message Authentication Code (メッセージ認証コード) (MAC) アルゴリズム
- 圧縮アルゴリズム
- キー交換アルゴリズム

SFTP ファイル交換のためのアルゴリズムの使用を設定するときは、次のルールとガイドラインを考慮します。

- アルゴリズムを **【使用可能】** と **【選択済み】** リストの間で移動できます。ファイル統合サービスは **【選択済み】** リスト内に列挙されたアルゴリズムを適用します。
- アルゴリズムタイプに選択済みアルゴリズムがない場合、ファイル統合サービスは **【使用可能】** リスト内に列挙されたすべてのアルゴリズムを適用します。
- ファイル統合サービスは、リストに列挙された順序で上から下にアルゴリズムを適用します。リスト内のアルゴリズムは、上矢印および下矢印を使用して、順序を変更できます。

## ホストキーのプロパティ

以下の表に、ホストキーのプロパティを示します。

プロパティ	説明
RSA キーファイルの場所	RSA ホストキーファイルの場所。
RSA キーパスフレーズ	RSA キーのパスフレーズ。
DSA キーファイルの場所	DSA ホストキーファイルの場所。
DSA キーパスフレーズ	DSA キーのパスフレーズ。

## アップロード制限のプロパティ

SFTP ファイルの交換時に許可または拒否するファイルのタイプを指定できます。以下の表に、アップロード制限を制御するプロパティを示します。

プロパティ	説明
ファイル拡張子のフィルタタイプ	ファイル拡張子リストの拡張子を承認または拒否するかどうか。 以下の値を使用します。 <ul style="list-style-type: none"><li>- フィルタしない。すべてのファイルタイプを承認します。</li><li>- 承認。ファイル拡張子プロパティでリストされた拡張子を持つファイルを承認します。</li><li>- 拒否。ファイル拡張子プロパティでリストされた拡張子を持つファイルを許可しません。</li></ul> デフォルトは <b>【フィルタしない】</b> です。
ファイル拡張子	ファイル拡張子のリスト。ファイル拡張子のフィルタタイプに対応するファイル拡張子を追加します。例えば、ファイル拡張子のフィルタタイププロパティで <code>.csv</code> ファイルおよび <code>.txt</code> ファイルを承認するには、 <b>【承認】</b> を選択してからファイル拡張子のリストに <code>csv</code> および <code>txt</code> を追加します。 拡張子をリストに追加するには、テキストボックスに拡張子を入力してから <b>【追加】</b> をクリックします。 リストから拡張子を削除するには、拡張子を強調表示してから <b>【削除】</b> をクリックします。
大文字と小文字が区別されるファイル拡張子	ファイル拡張子リストを使用してフィルタする場合に、大文字と小文字を考慮に入れるかどうか。有効にすると、ファイル拡張子リストで使用される大文字と小文字が一致しない拡張子を使用したファイルはアップロード出来ません。 例えば、ファイル拡張子リストに <code>csv</code> があるが <code>CSV</code> はない場合、拡張子 <code>csv</code> を使用したファイルはアップロードできますが、拡張子 <code>CSV</code> を使用したファイルはアップロード出来ません。 デフォルトでは無効になっています。
拡張子なしのファイルを許可	ファイル名に拡張子が含まれていないファイルを許可するかどうか。 デフォルトでは無効になっています。
拡張子付きのファイルを許可	ファイル拡張子フィルタを有効にするかどうか。有効にすると、このページで設定されたファイル拡張子のプロパティによってアップロードできるファイルのタイプが決まります。 デフォルトでは有効になっています。



## プロキシサーバー設定プロパティ

ファイル統合サービスを使用する各ランタイム環境では、1 つまたは複数のプロキシサーバーを設定できます。

プロキシサーバープロパティを [エージェント用のファイルサーバー] ページの [プロキシサーバー] タブで設定します。

プロキシサーバーを追加するには、[Add Proxy Configuration (プロキシ設定の追加)] をクリックし、[保存] をクリックします。

**注:** プロキシサーバーを DMZ にもインストールします。詳細については、[「ファイル統合プロキシサーバーのインストール」 \(ページ 178\)](#) を参照してください。

以下のタイプのプロパティを設定します。

- 全般的なプロパティ
- 内部ファイルサーバーとプロキシサーバーを関連付けるサービスマッピングプロパティ

### 全般プロパティ

以下の表に、全般的なプロキシサーバーのプロパティを示します。

プロパティ	説明
有効	プロキシサーバーが有効かどうか。 デフォルトは [はい] です。
コントローラのアドレス	プロキシサーバーが組織のファイルサーバーからの管理接続をリスンする DMZ 内のサーバーの外部 IP アドレス。
コントローラのポート	プロキシサーバーが組織のファイルサーバーからの管理接続をリスンする DMZ 内のサーバーのポート番号。 デフォルトは 9100 です。
スレッドの最小数	プロキシサーバーのインストール場所への接続のために予約されたスレッドの最小数。 デフォルトは 10 です。
スレッドの最大数	プロキシサーバーが処理できる同時要求の最大数。 デフォルトは 2000 です。
スレッドキープアライブ時間	終了までのアイドルスレッド待機秒数。 デフォルトは 60 です。

### サービスマッピングプロパティ

プロキシサーバーのサービスマッピングを設定するには、[Proxy Server Configuration (プロキシサーバーの設定)] ページで、[Service Mappings (サービスマッピング)] の隣の [追加] をクリックし、マッピングパラメータを設定し、[OK] をクリックします。必要に応じていくつでもサービスマッピングを追加し、内部ファイルサーバーとプロキシサーバーを関連付けられます。

以下の表に、サービスマッピングプロパティを示します。

プロパティ	説明
ラベル	マッピングのラベル。
送信元アドレス	プロキシサーバーの IP アドレス。
送信元ポート	プロキシサーバーのポート番号。
送信先アドレス	内部ファイルサーバーの IP アドレス。
送信先ポート	内部ファイルサーバーのポート番号。
ロードバランサールール	マッピングと一緒に使用するロード分散ルールの名前。ルールの名前は、プロキシサーバーのインストール内にある proxy.xml ファイルにある名前と同一である必要があります。詳細については、「 <a href="#">ファイル統合プロキシサーバーのインストール</a> 」(ページ 178)を参照してください。

## ファイル統合プロキシサーバーのインストール

ファイル統合プロキシサーバーを DMZ にインストールし、サーバーパラメータを設定します。サーバーは Windows オペレーティングシステムと Linux オペレーティングシステムにインストールできます。

**注:** 管理者の Informatica Intelligent Cloud Services で、プロキシサーバーを有効にし、サーバープロパティを設定します。詳細については、「[プロキシサーバー設定プロパティ](#)」(ページ 177)を参照してください。

1. fis-proxy-server.zip ファイルを DMZ 内のサーバーにコピーします。
2. Java 1.8 (OpenJDK または Oracle) をダウンロードし、DMZ 内のサーバーにインストールします。
3. fis-proxy-server/bin フォルダから、次のファイルのいずれかを編集します。
  - Windows オペレーティングシステムでは、setenv.bat を編集します。
  - Linux オペレーティングシステムでは、setenv.sh を編集します。
  - a. JAVA\_HOME を Java 1.8 の JDK Home または JRE ホームに設定します。
  - b. fis-proxy-server のフォルダパスを FIS\_PROXY\_HOME に設定します。
4. fis-proxy-server/config フォルダから、proxy.xml ファイルを編集し、次の変数の値を設定します。

変数	説明
controllerAddress	プロキシサーバーが組織のファイルサーバーからの管理接続をリスンする DMZ 内のサーバーの外部 IP アドレス。
dataAddress	プロキシサーバーが組織のファイルサーバーからのデータ接続をリスンする DMZ 内のサーバーの内部 IP アドレス。
proxyAddress	プロキシサーバーが受信接続をリスンする DMZ 内のサーバーの IP アドレス。
forwardProxyLocalAddress	プロキシサーバーがリモートサーバーへの送信接続を転送プロキシとして確立する DMZ 内のサーバーの IP アドレス。

必要に応じて、ポート番号を変更します。

5. プロキシサーバーを開始するには、次のコマンドのいずれかを実行します。
    - Windows オペレーティングシステムでは、`fis-proxy.bat start` を実行します。
    - Linux オペレーティングシステムでは、`fis-proxy.sh start` を実行します。
  6. プロキシサーバーを停止するには、次のコマンドのいずれかを実行します。
    - Windows オペレーティングシステムでは、`fis-proxy.bat stop` を実行します。
    - Linux オペレーティングシステムでは、`fis-proxy.sh stop` を実行します。
- プロキシサーバーはログを `fis-proxy-server/logs` フォルダに保存します。

## ファイルサーバー

**【ファイルサーバー】** ページでファイル統合サービスファイルサーバーを停止または開始することができます。設定変更の後、ファイルサーバーを停止および開始します。

### HTTPS、AS2 および SFTP サーバーの停止と開始

HTTPS、AS2 または SFTP サーバーを停止または開始するには、次のアクションを実行します。

1. Administrator で、**【ファイルサーバー】** を選択します。
2. **【ファイルサーバー】** タブで、サーバーを実行する Secure Agent の名前の横の矢印をクリックします。
3. **【アクション】** メニューから、以下のいずれかのオプションを選択します。
  - AS2 サーバーを起動
  - AS2 サーバーを停止
  - HTTPS サーバーを起動
  - HTTPS サーバーを停止
  - SFTP サーバーを起動
  - SFTP サーバーを停止

Informatica Intelligent Cloud Services はアクションを示すエントリを監査ログに追加します。

### プロキシサーバーの停止と開始

プロキシサーバーを停止または開始するには、次のアクションを実行します。

1. Administrator で、**【ファイルサーバー】** を選択します。
2. **【ファイルサーバー】** タブで、プロキシサーバーを停止または開始するファイル統合サービスを実行する Secure Agent を選択します。
3. **【エージェント用のファイルサーバー】** ページで、**【プロキシサーバー】** タブを選択します。
4. 停止または開始するサーバーの **【アクション】** メニューから、**【停止】** または **【開始】** を選択します。

Informatica Intelligent Cloud Services はアクションを示すエントリを監査ログに追加します。

# ファイルサーバーのユーザー

ファイルを組織と交換する各リモートパートナーに、ユーザーアカウントを作成します。このユーザーアカウントによって、パートナーとお客様のサーバーでファイルを交換できるようになります。

リモートパートナーごとに、以下のタイプのプロパティを設定します。

- ユーザー名、電子メールアドレス、パスワードなどの全般的なプロパティ。
- HTTPS、AS2、および SFTP サーバーのサーバー固有プロパティ。
- フォルダ権限。

**注:** ファイルサーバーユーザーのアカウントは、Informatica Intelligent Cloud Services のユーザーアカウントとは異なります。ファイルサーバーユーザーのアカウントによって、リモートパートナーユーザーがファイルをお客様の組織のファイルサーバーと交換できるようになります。Informatica Intelligent Cloud Services のユーザーアカウントによって、ユーザーは Informatica Intelligent Cloud Services 組織にアクセスできるようになります。

## ファイルサーバーユーザーの設定

パートナーユーザーを設定して、パートナーが組織とファイルを交換できるようにします。

ファイルサーバーユーザーを作成すると、そのユーザーは Informatica Intelligent Cloud Services から電子メールを受信します。ユーザーの設定時にシステムで生成されたパスワードを追加するように選択していた場合は、生成されたパスワードがこの電子メールに記載されています。

1. Administrator で、**[ファイルサーバー]** > **[ファイルサーバーのユーザー]** をクリックします。
2. **[ユーザーの追加]** をクリックします。
3. 次のアクションを実行し、**[保存]** をクリックします。
  - ユーザーの全般情報を入力します。
  - ユーザーがファイルを組織内の AS2 サーバーに送信できるようにするには、AS2 プロトコルを有効にし、AS2 設定を設定します。
  - ユーザーがファイルを組織内の SFTP サーバーと交換できるようにするには、SFTP プロトコルを有効にし、SFTP 設定を設定します。
  - ユーザーがファイルを組織内の HTTPS サーバーと交換できるようにするには、HTTPS プロトコルを有効にし、HTTPS 設定を設定します。
  - そのユーザーにフォルダとファイルの権限を追加します。デフォルトでは、ユーザーはデフォルトのホームディレクトリ上のすべて権限を持っています。

## ファイルサーバーユーザーのプロパティ

ファイルサーバーユーザーのプロパティを設定します。

### 全般プロパティ

以下の表に、ユーザーの全般プロパティを示します。

プロパティ	説明
ユーザー名	ファイルサーバーユーザーのユーザー名。
説明	ユーザーの説明。

プロパティ	説明
会社名	会社の名前。
電子メール	ユーザーの電子メールアドレス。
パスワードの生成	<p>ユーザーのパスワードを作成するかどうか、またはシステムでシステム生成のパスワードを作成できるようにするか。</p> <p>パスワードには以下の特性を含める必要があります。</p> <ul style="list-style-type: none"> <li>- 8 文字以上で指定する。</li> <li>- 大文字を 1 文字以上含める。</li> <li>- 数字を 1 つ以上含める。</li> <li>- 次の特殊文字を 1 つ以上含める: @ \$ ! &amp; * ~ - _</li> </ul>

## AS2 サーバーのプロパティ

以下の表に、ファイルサーバーユーザーの AS2 サーバーのプロパティを示します。

プロパティ	説明
AS2 プロトコルの有効化	<p>AS2 プロトコルが有効かどうか。</p> <p>AS2 サーバーでファイルを受信しないようにするには、これを無効にします。</p> <p>デフォルトでは有効になっています。</p>
認証タイプ	<p>【パスワード】、【証明書】、【両方】、または【いずれか】が必要かどうか。</p> <p>認証に【パスワード】を使用する場合、【全般】タブで定義したパスワード生成が使用されます。</p> <p>認証に【証明書】を使用する場合、AS2 サーバーの【クライアント認証】設定を【オプション】または【必須】に設定する必要があります。</p>
SHA1 のフィンガープリント	<p>認証に【証明書】、【両方】、または【いずれか】を使用する場合、パートナーの証明書の SHA1 フィンガープリントを入力します。証明書の SHA1 フィンガープリントは、トラストストアからコピーできます。</p>
AS2 ID	パートナーユーザーの AS2 ID。
署名証明書エイリアス	<p>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。</p>
デフォルトのアップロードフォルダ	<p>AS2 ファイルが受信時に保存される場所。デフォルトの場所は、ユーザーのデフォルトのホームディレクトリです。</p> <p>空欄の場合、ファイルはホームディレクトリに保存されます。詳細については、<a href="#">「グローバル設定」</a> (ページ 184) を参照してください。</p>

## SFTP サーバプロパティ

以下の表に、ファイルサーバユーザーの SFTP サーバのプロパティを示します。

プロパティ	説明
有効な SFTP プロトコル	SFTP プロトコルが有効かどうか。 SFTP サーバでファイルを送受信しないようにするには、これを無効にします。 デフォルトでは有効になっています。
認証タイプ	<b>[パスワード]</b> 、 <b>[パブリックキー]</b> 、 <b>[両方]</b> 、または <b>[いずれか]</b> が必要かどうか。 パスワードが認証に使用される場合、 <b>[全般]</b> タブで定義したパスワード生成が使用されます。 認証に <b>[パブリックキー]</b> を使用する場合、Secure Agent にキーを配置する必要があります。
パブリックキーの場所	Secure Agent 上のパブリックキーの場所への絶対パス。 認証に <b>[パブリックキー]</b> 、 <b>[両方]</b> 、または <b>[いずれか]</b> を使用する場合に適用されます。

## HTTPS サーバプロパティ

以下の表に、ファイルサーバユーザーの HTTPS サーバのプロパティを示します。

プロパティ	説明
HTTPS プロトコルの有効化	HTTPS プロトコルが有効かどうか。 HTTPS サーバでファイルを受信しないようにするには、これを無効にします。 デフォルトでは有効になっています。
認証タイプ	<b>[パスワード]</b> 、 <b>[証明書]</b> 、または <b>[いずれか]</b> が必要かどうか。 パスワードが認証に使用される場合、 <b>[全般]</b> タブで定義したパスワード生成が使用されます。 認証に <b>[証明書]</b> を使用する場合は、HTTPS サーバの <b>[クライアント認証]</b> 設定を <b>[オプション]</b> または <b>[必須]</b> に設定する必要があります。
SHA1 のフィンガープリント	認証に <b>[証明書]</b> または <b>[いずれか]</b> を使用する場合、パートナーの証明書の SHA1 フィンガープリントを入力します。証明書の SHA1 フィンガープリントは、トラストストアからコピーできます。

## フォルダ権限プロパティ

デフォルトでは、ユーザーのホームディレクトリおよびユーザー名が、ファイルサーバの **[グローバル設定]** タブに定義されたデフォルトのホームディレクトリの下に作成され、そのユーザーは自分のホームディレクトリに対するすべての権限を持ちます。ユーザーのホームディレクトリが別の場所になるように編集できます。

別のフォルダおよびファイルへの権限を追加するには、**[追加]** をクリックし、権限を定義します。

以下の表に、ユーザーのフォルダ権限プロパティを示します。

プロパティ	説明
エイリアス	権限を付与するフォルダまたはファイルのエイリアス。エイリアスは【ファイルサーバーのユーザー】ページの【名前】カラムの下に表示されます。
パス	ユーザー権限を付与するフォルダまたはファイルのパス。
タイプ	権限がフォルダまたはファイルのどちらに対するものであるかを決定します。
フォルダ権限	フォルダに対するユーザーの権限。
ファイル権限	ファイルに対するユーザーの権限。
ディスクスペース制限	ユーザーがフォルダ上で使用できるディスクスペースを制限するかどうかと、制限する場合、許可されるディスク上のスペース。 フォルダ権限に適用されます。

## ファイルサーバーユーザーの削除

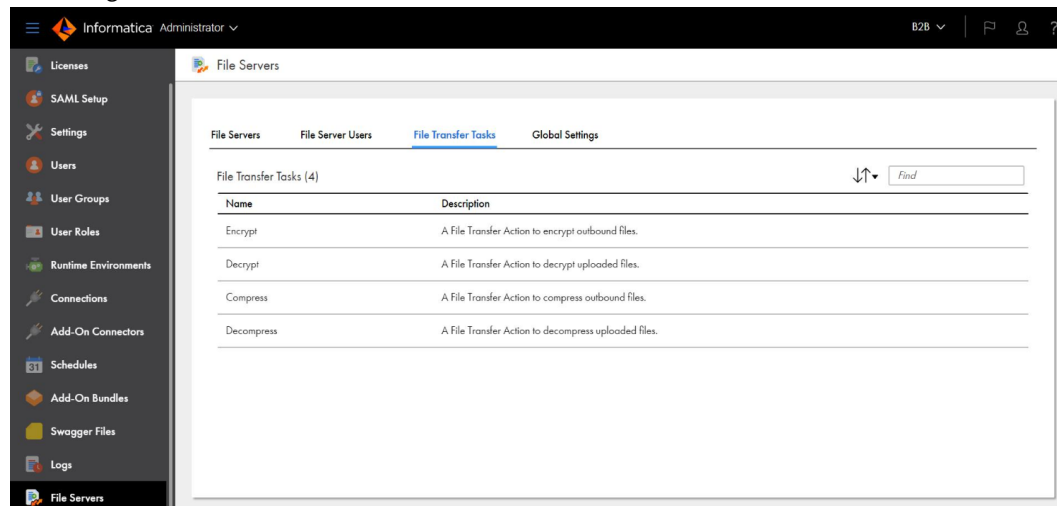
ユーザーが組織で作業をしなくなった場合に、ファイルサーバーユーザーを削除する必要がある場合があります。

1. Administrator で、【ファイルサーバー】 > 【ファイルサーバーのユーザー】を選択します。
2. ユーザー名を含む行で【アクション】をクリックし、【ユーザーの削除】を選択します。

## ファイル転送タスク

ファイル転送タスクは、パートナーのインバウンドおよびアウトバウンドプロセスに関連します。

【ファイルサーバー】ページには、ファイル統合サービスを使用できる組織内のすべてのランタイム環境と Secure Agent が一覧表示されます。



【ファイル転送タスク】 タブには、定義済みのファイル転送タスクが一覧表示されます。これらのタスクを使用すると、ファイルサーバーからファイルを受信するとき、またはファイルサーバーにファイルを送信ときにアクションを実行できます。このタブには、読み取り専用モードでプロジェクトが一覧表示されます。

【ファイル転送タスク】 タブには、次の定義済みファイル転送タスクが含まれます。

名前	説明
暗号化	アウトバウンドファイルをソースの場所からファイルサーバーユーザーのホームディレクトリに転送するときに、PGP を使用してそれらのファイルを暗号化するファイル転送タスク。
復号化	アップロード済みのファイルをファイルサーバーユーザーのホームディレクトリからターゲットの場所に転送するときに、PGP を使用してそれらのファイルを復号化するファイル転送タスク。
圧縮	アウトバウンドファイルをソースの場所からファイルサーバーユーザーのホームディレクトリに転送するときに、それらのファイルを圧縮するファイル転送タスク。Zip、Tar、Gzip のうちのいずれかの圧縮方式を選択できます。
圧縮解除	アップロード済みのファイルをファイルサーバーユーザーのホームディレクトリからターゲットの場所に転送するときに、それらのファイルを圧縮解除するファイル転送タスク。Unzip、Untar、Gunzip のうちのいずれかの圧縮解除方式を選択できます。

定義済みタスクを実行するために、REST API も使用できます。B2B Gateway を使用してタスクを実行することもできます。

詳細については、*REST API リファレンス*を参照してください。

## グローバル設定

ファイル転送用に設定されたすべてのファイルサーバーに適用するプロパティを設定します。

### フォルダ設定

【デフォルトのホームディレクトリ】 プロパティを設定して、リモートサーバーから受信したすべてのファイルが保存されるデフォルトのディレクトリを指定します。ユーザー固有のホームディレクトリが、グローバルホームディレクトリの下に作成されます。

**注:** デフォルトのホームディレクトリの値を変更するときは、常にファイルサーバーを停止してから開始する必要があります。

### SMTP サーバーの設定

以下の表に、すべてのリモートファイルサーバーに適用する SMTP サーバーの設定を一覧表示します。

プロパティ	説明
ホスト	電子メールタイプの MDN に使用する SMTP 設定のホスト名。
ポート	SMTP が実行されているポート。
ユーザー名	SMTP サーバーに接続するユーザー名。
パスワード	SMTP ユーザーのパスワード。



プロパティ	説明
接続タイプ	SMTP 接続のタイプ。 次のいずれかの値を選択します。 - ノーマル - implicitSSL - explicitSSL デフォルトは [ノーマル] です。
電子メールから	電子メール MDN の送信元の電子メールアドレス。
名前から	電子メールに表示される名前。

## PGP 設定

パブリックキーおよび秘密鍵を保存するディレクトリを指定するために、**【パブリックキーリング】** および **【秘密鍵リング】** を設定します。パスが指定されていない場合、PGP キーリングのデフォルトのパスが使用されます。

**注:** 複数の Secure Agent がある場合、構成プロパティファイルを編集するのに PGP コマンドラインインタフェース (PGP-CLI) が役立ちます。pgp-configuration.properties ファイルでの PGP 設定の変更を反映するために、FIS アプリケーションを再起動する必要があります。構成ファイルは、FIS パッケージにバンドルされている PGP クライアントの conf フォルダ内にあります。

## 第 19 章

# トラブルシューティング

次のセクションを使用して、管理者のエラーをトラブルシューティングします。

代表的なエラーメッセージとソリューションの一覧については、Informatica Cloud コミュニティの記事 ["Troubleshooting: Common Error Messages"](#) を参照してください。

## Secure Agent のトラブルシューティング

Secure Agent をインストールしましたが、別のマシンにも Secure Agent をインストールしたいと考えています。どのようにすればよいでしょうか？

新しいマシンで、自分のログイン情報を使用してデータ統合に接続します。次に、Secure Agent をダウンロードしてインストールします。

### Secure Agent のエラー

Secure Agent を開始しましたが、そのステータスが非アクティブになっています。

Secure Agent の開始には数分かかることがあります。ステータスは 5 秒ごとに更新されます。Secure Agent がアクティブにならない場合は、次のタスクを実行します。

- 組織がプロキシサーバーを使用してインターネットにアクセスする場合は、プロキシ設定が正しく設定されていることを確認します。
- Secure Agent をインストールしたディレクトリにある infaagent.log の詳細情報を表示します。

Secure Agent が正常にインストールされない、または開始されません。

Secure Agent が正常にインストールされないか開始されない場合は、次のタスクを実行します。

1. Secure Agent をインストールしたディレクトリにある infaagent.log で、インストールの詳細情報を確認します。
2. Windows で実行されている Secure Agent のイベントビューアで、アプリケーションログを表示します。

サービスの 1 つを正常に再起動した後に、エラーステータスが表示されます。

サービスがエラーステータスで失敗すると、サービスが正常に起動された後でも、サービスのエラーステータスが引き続き [エージェントサービスの詳細] に表示されることがあります。古いメッセージをクリーンアップする内部ジョブが実行されるまで、エラーはページに表示されます。このエラーは無視してかまいません。

Secure Agent をアンインストールしようとしています、Secure Agent のステータスは「稼動中」のままです。

最初に Secure Agent を停止せずに Secure Agent をアンインストールすると、Agent Core と他のサービスの実行が数分間継続することがあります。この問題を回避するには、Secure Agent を停止してからアンインストールします。

## AWS 上のエラスティッククラスタのトラブルシューティング

### エラスティッククラスタが起動しない理由

エラスティッククラスタが起動に失敗した理由を見つけるには、Secure Agent マシンの次のディレクトリにある ccs-operation.log ファイルを使用します。

<Secure Agent installation directory>/apps/At\_Scale\_Server/<version>/ccs\_home/

次のテーブルに、クラスタが起動しないいくつかの理由を示します。

理由	考えられる原因
kops がクラスタの更新に失敗した。	AWS アカウントで VPC 制限に到達した。
マスターノードの起動に失敗した。	マスターインスタンスタイプは、指定されたリージョンまたは可用性ゾーン、または AWS アカウントではサポートされていません。
すべてのワーカーノードを起動できなかった。	ワーカーインスタンスタイプは、指定されたリージョンまたは可用性ゾーン、または AWS アカウントではサポートされていません。
Kubernetes API サーバーが起動できなかった。	ユーザー定義のマスターロールでエラーが発生しました。

これらの理由の少なくとも 1 つが原因でクラスタが起動に失敗すると、ccs-operation.log ファイルに BadClusterConfigException が表示されます。

例えば、次のようなエラーが発生する可能性があります。

```
2019-06-27 00:50:02.012 [T:000060] SEVERE : [CCS_10500] [Operation of <cluster instance ID>: start_cluster-
<cluster instance ID>]: com.informatica.cloud.service.ccs.exception.BadClusterConfigException: [[CCS_10207]
The cluster configuration for cluster [<cluster instance ID>] is incorrect due to the following error: [No
[Master] node has been created on the cluster. Verify that the instance type is supported.]. The Cluster
Computing System will stop the cluster soon.]
```

クラスタで BadClusterConfigException が発生した場合、エージェントはすぐにクラスタを停止して、追加のリソースコストの発生を防ぎ、潜在的なリソースリークを回避します。エージェントは、設定エラーが解決されるまで、クラスタの回復を試みません。

ccs-operation.log ファイルを調べてエラスティッククラスタのトラブルシューティングを行ったが、情報が不十分であった。他にどこを調べればよいか。

エラスティッククラスタのインスタンス専用の cluster-operation ログを確認できます。外部コマンドセットの実行が開始されると、ccs-operation ログに cluster-operation ログへのパスが表示されます。

以下に例を示します。

```
2020-06-15 21:22:36.094 [reqid:] [T:000057] INFO : c.i.c.s.c.ClusterComputingService [CCS_10400]
Starting to run command set [<command set>] which contains the following commands: [
 <commands> ;
]. The execution log can be found in the following location: [/data2/home/cldagnt/SystemAgent/apps/
At_Scale_Server/35.0.1.1/ccs_home/3xukm9iqp5zeahyrb7rqoz.k8s.local/infa/cluster-operation.log].
```

指定されたフォルダには、クラスタのインスタンスに属するすべての cluster-operation ログが含まれます。ログを使用して、コマンドセットの完全な stdout および stderr 出力ストリームを表示できます。

ログ名の数字はログの生成を示し、各 cluster-operation ログは最大 10 MB です。例えば、外部コマンドの実行中にクラスタインスタンスが 38 MB のログメッセージを生成した場合、フォルダには 4 つの cluster-operation ログが含まれます。最新のログのファイル名では 0 で、最も古いログのファイル名では 3 です。cluster-operation0.log ファイルのメッセージを表示して、最新のエラーを表示できます。

エラスティックサーバーのログレベルを DEBUG に設定すると、ccs-operation ログに cluster-operation ログと同じ詳細レベルが表示されます。

## エラスティッククラスタを開始するジョブを実行したが、VPC 制限に到達した。

クラスタのエラスティック構成で VPC を指定していない場合は、Secure Agent が AWS アカウントで新しい VPC を作成します。AWS アカウントの VPC の数が各リージョンで制限されているため、VPC 制限に到達した可能性があります。

VPC 制限に到達した場合は、エラスティック構成を編集し、次のいずれかのタスクを実行します。

- それぞれのリージョンを指定します。
- 可用性ゾーンを削除します。次に、既存の VPC および使用するクラスタの VPC 内の特定のサブネットを指定します。

クラスタでプロビジョニングされたクラウドリソースは、クラスタが新しいリージョンまたは既存の VPC で起動する場合に再利用されます。例えば、Secure Agent が VPC 制限のエラーを受信する前に Amazon EBS ボリュームをプロビジョニングしたとします。EBS ボリュームは削除されず、次の起動時に再利用されます。

## エラスティッククラスタを起動するジョブを実行したが、次のエラーが発生し、クラスタの作成に失敗した。

```
Failed to create cluster [<cluster instance ID>] due to the following error: [[CCS_10302] Failed to invoke AWS
SDK API due to the following error: [Access Denied (Service: Amazon S3; Status Code: 403; Error Code:
AccessDenied; Request ID: <request ID>; S3 Extended Request ID: <S3 extended request ID>)].]
```

Secure Agent は、Amazon S3 がエージェントの要求を拒否したためにエラスティッククラスタの作成に失敗しました。

S3 バケットポリシーが、クライアントによる暗号化ヘッダーを含む要求の送信を求めていることを確認してください。

## 起動に失敗した Kubernetes API サーバーをトラブルシューティングする方法

Kubernetes API サーバーの起動に失敗すると、エラスティッククラスタの起動に失敗します。この失敗をトラブルシューティングするには、代わりに Kubernetes API サーバーログを使用します。

Kubernetes API サーバーログを見つけるには、次のタスクを実行します。

1. Secure Agent マシンからマスターノードに接続します。
2. マスターノードで、ディレクトリ /var/log/ にある Kubernetes API Server ログファイルを見つけます。

## エラスティッククラスタのステージング場所を更新したら、エラスティックマッピングに次のエラーが発生し、失敗するようになった。

Error while executing mapping. ExecutionId '<execution ID>'. Cause: [Failed to start cluster for [01000D250000000000005]. Error reported while starting cluster [Cannot apply cluster operation START because the cluster is in an error state.]].

エラスティック構成で S3 ステージングの場所を変更する前にステージングの場所に対する権限を変更すると、このエラーが発生してマッピングが失敗します。

ステージングの場所を更新する場合は、最初にエラスティック構成で S3 ステージングの場所を変更してから、AWS のステージングの場所に対する権限を変更します。ロールベースのセキュリティを使用した場合は、Secure Agent マシンでステージングの場所に対する権限を変更する必要もあります。

エラーを修正するには、次のタスクを実行します。

1. ステージングの場所の権限に対する変更を元に戻します。
2. S3 ステージングの場所を元に戻すようにエラスティック構成を編集します。
3. 構成を保存すると、クラスタが停止します。
4. 構成の S3 ステージングの場所を更新してから、AWS でステージングの場所に対する権限を変更します。

## エラスティッククラスタのステージング場所を更新したら、エージェントジョブログに次のエラーメッセージが表示されるようになった。

Could not find or load main class com.informatica.compiler.InfaSparkMain

このエラーメッセージは、クラスタノードがアクセス権限のためにステージングの場所から Spark バイナリをダウンロードできない場合に表示されます。

ジョブが使用するコネクタのタイプに基づいて、ステージングの場所のアクセス権限を確認します。

### Amazon データソースへの直接アクセスを持つコネクタ

エラスティックジョブで資格情報ベースのセキュリティを使用する場合は、Amazon S3 V2 および Amazon Redshift V2 接続の資格情報がステージングの場所へのアクセスに使用できることを確認します。

エラスティックジョブでロールベースのセキュリティを使用する場合は、エラスティッククラスタおよびステージングの場所が同じ AWS アカウント内に存在することを確認します。

### Amazon データソースへの直接アクセスがないコネクタ

ユーザー定義のワーカーロールを使用する場合は、ワーカーロールがエラスティックジョブのステージングの場所とデータソースの両方にアクセスできることを確認します。

デフォルトのワーカーロールを使用する場合は、Secure Agent ロールがエラスティックジョブのステージングの場所とデータソースの両方にアクセスできることを確認します。

## エラスティッククラスタのステータスが不明の場合に実行すべきこと。

クラスタのステータスが不明の場合は、最初に Secure Agent が稼働している事を確認します。エージェントが稼働していない場合は、エージェントを有効にして、クラスタの稼働開始を確認します。

クラスタが始動しない場合は、管理者がクラスタをリストするコマンドを実行できます。コマンド出力が一部または使用中のクラスタ状態を返す場合、管理者はクラスタを削除するコマンドを実行する事ができます。

コマンドの詳細については、Administrator ヘルプで *Data Integration Elastic* 管理に関するヘルプを参照してください。

## Secure Agent マシンを再起動したら、エラスティッククラスタのステータスがエラーになった。

Secure Agent マシンおよび Secure Agent が稼働していることを確認します。次に、Monitor でエラスティッククラスタを停止します。AWS 環境では、クラスタの停止に 3~4 分かかる場合があります。クラスタが停止したら、エラスティックジョブを実行してクラスタを再起動できます。

## init スクリプトが失敗したノードの初期化スクリプトログを見つける方法

init スクリプトログを見つけるには、次のタスクを実行します。

1. Secure Agent マシンの次のディレクトリに、ccs-operation.log ファイルがあります。  
<Secure Agent installation directory>/apps/At\_Scale\_Server/<version>/ccs\_home/
2. ccs-operation.log ファイルで、次のようなメッセージを見つけます。  
Failed to run the init script for cluster [<cluster instance ID>] on the following nodes: [<cluster node IDs>]. Review the log in the following S3 file path: [<cloud platform location>].
3. メッセージで示されているクラウドプラットフォームの場所に移動します。
4. クラスタノード ID を、init スクリプトが失敗したノードの init スクリプトログファイル名と一致させます。

## 次のエラーメッセージでのエラスティッククラスタのリソース要件の計算方法

```
2019-04-26T19:04:11.762+00:00 <Thread-16> SEVERE: java.lang.RuntimeException: [java.lang.RuntimeException: The Cluster Computing System rejected the Spark task [Infaspark0] due to the following error: [[CCS_10252] Cluster [6bjwune8v4bkt3vneoki9.k8s.local] doesn't have enough resources to run the application [spark--infaspark0e6674748-b038-4e39-a2a9-3fd49e63f289infaspark0-driver] which requires a minimum resource of [(KB memory, mCPU)]. The cluster must have enough nodes, and each node must have at least [(KB memory, mCPU)] to run this job.].]
```

最初のリソース要件は、Spark ドライバと Spark エグゼキュータが必要とするリソースの総数です。

2 番目のリソース要件は、最低 1 つの Spark プロセスを実行するための各ワーカーノードの最小リソース要件に基づいて計算されます。

リソースは次の式を使用して計算されます。

```
Memory: MAX(driver_memory, executor_memory)
CPU: MAX(driver_CPU, executor_CPU)
```

Spark プロセスは、Spark ドライバプロセスまたは Spark 実行者プロセスのいずれかです。クラスタでは、各ノードがドライバまたは実行者のいずれかを実行するための最小要件を満たすノードを 2 つ使用するか、ドライバと実行者の両方を実行するために十分なリソースを持つ 1 つのノードを使用する必要があります。

**注:** ドライバおよびエグゼキュータのリソース要件は、マッピングタスクの次の詳細セッションプロパティを設定する方法に応じて異なります。

```
spark.driver.memory
spark.executor.memory
spark.executor.cores
```

最小リソース要件の詳細については、Administrator ヘルプで *Data Integration Elastic 管理* に関するヘルプを参照してください。

## カスタム AMI を使用してクラスタノードを作成する前に行う必要があること

カスタム AMI (Amazon マシンイメージ) を使用してクラスタノードを作成する場合は、AMI に AWS CLI のインストールが含まれていることを確認します。

Secure Agent は AWS CLI を使用して、タグを Amazon リソースにプロパゲートし、ログを集計します。また、クラスタノードは AWS CLI を使用して初期化スクリプトを実行します。

カスタム AMI の使用方法については、Informatica グローバルカスタマーサポートにお問い合わせください。

VPC にインターネットトラフィックを制限する要件がある。エラスティッククラスタがこれらの要件に準拠するように設定したい。

デフォルトでは、エラスティッククラスタはインターネット接続ロードバランサを使用して、インターネット上のトラフィックをルーティングします。

インターネットトラフィックを制限するには、エラスティッククラスタが内部ロードバランサを使用するように設定できます。

内部ロードバランサを使用するには、次のタスクを実行します。

1. 内部ロードバランサを有効にするには、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。
2. VPC とサブネットをエラスティック構成で指定します。
3. サブネットが NAT ゲートウェイを使用しており、クラスタ依存関係がインターネットからダウンロードできることを確認します。

インターネット接続ロードバランサと内部ロードバランサの詳細については、AWS のマニュアルを参照してください。

## Microsoft Azure 上のエラスティッククラスタのトラブルシューティング

Blob Storage にステージングとログの場所を設定した後、エラスティックマッピングが失敗し、セッションログに次のエラーメッセージが表示される。

```
20-02-11T00:52:43.273+00:00 <WorkflowExecutorThread20> INFO: [LDTM_0075] Total time to perform the LDTM operation: 84,962 ms
2020-02-11T00:52:43.305+00:00 <InfaDisnextHadoopMappingExecutor-3-64> SEVERE: java.lang.RuntimeException: java.lang.RuntimeException: java.lang.RuntimeException: Failed to upload the local file in the path [/mnt/resource/informatica/secureagent/apps/At_Scale_Server/33.0.1.1/metadata/0100edc7-f043-43f7-a5e1-a39f0774c2c7InfaSpark0/submit_InfaSpark0_staticCode.jar] to the following shared storage location: [<Blob Storage location>] due to the following error: [java.lang.RuntimeException: [org.apache.hadoop.fs.azure.AzureException: com.microsoft.azure.storage.StorageException: The account being accessed does not support http.]].
2020-02-11T00:52:43.306+00:00 <InfaDisnextHadoopMappingExecutor-3-64> INFO: Spark Mapping Ended with state: Failed
```

Blob Storage では HTTPS 経由でリクエストを行う必要があるため、エラーが表示されます。エラーを解決するには、Azure ポータルを使用して、ステージングとログの場所を保持するストレージアカウントの [Secure transfer required (セキュア転送が必要)] オプションを無効にします。

エラスティッククラスタのステータスが不明の場合に実行すべきこと。

クラスタのステータスが不明の場合は、最初に Secure Agent が稼働していることを確認します。エージェントが稼働していない場合は、エージェントを有効にして、クラスタの稼働開始を確認します。

クラスタが始動しない場合は、管理者がクラスタをリストするコマンドを実行できます。コマンド出力が一部または使用中のクラスタ状態を返す場合、管理者はクラスタを削除するコマンドを実行する事ができます。

コマンドの詳細については、Administrator ヘルプで *Data Integration Elastic* 管理に関するヘルプを参照してください。



## Secure Agent マシンを再起動したら、エラスティッククラスタのステータスがエラーになった。

Secure Agent マシンおよび Secure Agent が稼働していることを確認します。次に、Monitor でエラスティッククラスタを停止します。Azure 環境では、クラスタの停止に 10 分かかる場合があります。クラスタが停止したら、エラスティックジョブを実行してクラスタを再起動できます。

## init スクリプトが失敗したノードの初期化スクリプトログを見つける方法

init スクリプトログを見つけるには、次のタスクを実行します。

1. Secure Agent マシンの次のディレクトリに、ccs-operation.log ファイルがあります。  
<Secure Agent installation directory>/apps/At\_Scale\_Server/<version>/ccs\_home/
2. ccs-operation.log ファイルで、次のようなメッセージを見つけます。  
Failed to run the init script for cluster [<cluster instance ID>] on the following nodes: [<cluster node IDs>]. Review the log in the following S3 file path: [<cloud platform location>].
3. メッセージで示されているクラウドプラットフォームの場所に移動します。
4. クラスタノード ID を、init スクリプトが失敗したノードの init スクリプトログファイル名と一致させます。

## エラスティッククラスタの一部のノードで、次の標準エラーが発生して init スクリプトが失敗した。

```
Created symlink from /etc/systemd/system/apt-daily.service to /dev/null.
Created symlink from /etc/systemd/system/apt-daily-upgrade.service to /dev/null.
Removed symlink /etc/systemd/system/timers.target.wants/apt-daily.timer.
Removed symlink /etc/systemd/system/timers.target.wants/apt-daily-upgrade.timer.
E: Could not get lock /var/lib/dpkg/lock-frontent - open (11: Resource temporarily unavailable)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontent), is another process using it?
```

ノードが init スクリプトと同時に内部プロセスを実行していたため、init スクリプトが失敗しました。エラーが引き続き表示される場合は、init スクリプトに必要な期間だけスリープコマンドを配置して、内部プロセスが完了するまで待ちます。

例えば、次のようにスリープコマンドを使用できます。

```
#!/bin/sh

while(sudo lsof /var/lib/dpkg/lock-frontent)
do
 echo "Sleeping 10s"
 sleep 10
done

sudo apt-get -y update
sudo apt-get install -y expect
```

## ccs-operation.log ファイルを調べてエラスティッククラスタのトラブルシューティングを行ったが、情報が不十分であった。他にどこを調べればよいか。

エラスティッククラスタのインスタンス専用の cluster-operation ログを確認できます。外部コマンドセットの実行が開始されると、ccs-operation ログに cluster-operation ログへのパスが表示されます。

以下に例を示します。

```
2020-06-15 21:22:36.094 [reqid:] [T:000057] INFO : c.i.c.s.c.ClusterComputingService [CCS_10400]
Starting to run command set [<command set>] which contains the following commands: [
 <commands> ;
]. The execution log can be found in the following location: [/data2/home/cldagnt/SystemAgent/apps/
At_Scale_Server/35.0.1.1/ccs_home/3xukm9iqp5zeahyrb7rqoz.k8s.local/infa/cluster-operation.log].
```



指定されたフォルダには、クラスタのインスタンスに属するすべての cluster-operation ログが含まれます。ログを使用して、コマンドセットの完全な stdout および stderr 出力ストリームを表示できます。

ログ名の数字はログの生成を示し、各 cluster-operation ログは最大 10 MB です。例えば、外部コマンドの実行中にクラスタインスタンスが 38 MB のログメッセージを生成した場合、フォルダには 4 つの cluster-operation ログが含まれます。最新のログのファイル名では 0 で、最も古いログのファイル名では 3 です。cluster-operation0.log ファイルのメッセージを表示して、最新のエラーを表示できます。

エラスティックサーバーのログレベルを DEBUG に設定すると、ccs-operation ログに cluster-operation ログと同じ詳細レベルが表示されます。

## 次のエラーメッセージでのエラスティッククラスタのリソース要件の計算方法

```
2019-04-26T19:04:11.762+00:00 <Thread-16> SEVERE: java.lang.RuntimeException: [java.lang.RuntimeException: The Cluster Computing System rejected the Spark task [InfoSpark0] due to the following error: [[CCS_10252] Cluster [6bjwune8v4bkt3vneokii9.k8s.local] doesn't have enough resources to run the application [spark--infaspark0e6674748-b038-4e39-a2a9-3fd49e63f289infaspark0-driver] which requires a minimum resource of [(KB memory, mCPU)]. The cluster must have enough nodes, and each node must have at least [(KB memory, mCPU)] to run this job.].]
```

最初のリソース要件は、Spark ドライバと Spark エグゼキュータが必要とするリソースの総数です。

2 番目のリソース要件は、最低 1 つの Spark プロセスを実行するための各ワーカーノードの最小リソース要件に基づいて計算されます。

リソースは次の式を使用して計算されます。

```
Memory: MAX(driver_memory, executor_memory)
CPU: MAX(driver_CPU, executor_CPU)
```

Spark プロセスは、Spark ドライバプロセスまたは Spark 実行者プロセスのいずれかです。クラスタでは、各ノードがドライバまたは実行者のいずれかを実行するための最小要件を満たすノードを 2 つ使用するか、ドライバと実行者の両方を実行するために十分なリソースを持つ 1 つのノードを使用する必要があります。

**注:** ドライバおよびエグゼキュータのリソース要件は、マッピングタスクの次の詳細セッションプロパティを設定する方法に応じて異なります。

```
spark.driver.memory
spark.executor.memory
spark.executor.cores
```

最小リソース要件の詳細については、Administrator ヘルプで *Data Integration Elastic* 管理に関するヘルプを参照してください。

# スケジュール済みタスクのトラブルシューティング

タスクがスケジュールされた時間に実行されません。

スケジュールがタスクを開始しようとしたときに、タスクの別のインスタンスがすでに実行されている場合、タスクはタスクがスケジュールされた時間に実行されません。例えば、5 分ごとに実行するようにタスクをスケジュールしたとします。最初のタスクは 12 pm に開始しますが、12:06 pm まで完了しません。最初のインスタンスが完了しないため、タスクの 2 番目のインスタンスは 12:05 pm に実行されません。データ統合は、次のタスクを午後 12:10 に開始します。

この問題を解決するには、次のタスクの実行が開始される前にタスクが完了するように、スケジュールを変更します。

# セキュリティのトラブルシューティング

次のセキュリティ違反エラーを受信しました。

There may have been a security violation while accessing the site. Verify that there are no malicious scripts running in your browser. This error also appears when you submit the form multiple times through a browser reload.

このエラーは、ページのオプションをクリックしたときに、そのページが前回のクリックによるロードを実行中であるときに発生します。データ統合に戻るには、[\[ここ\]](#) のリンクをクリックしてください。

[接続、レプリケーションタスクなどのオブジェクトに関する詳細を表示しようとする](#)と、[\[オブジェクトが見つかりません\]](#) ページが表示されます。

オブジェクトは最近削除されました。オブジェクトが存在しないと、[\[オブジェクトが見つかりません\]](#) ページが表示されます。ページを更新して、現在のオブジェクトを表示します。

[タスクを実行しようとする](#)と、[\[アクセスが拒否されました\]](#) ページが表示されます。

使用しているユーザーアカウントでの実行許可がないタスクを実行しようとする、[\[アクセスが拒否されました\]](#) ページが表示されます。タスクを実行するための適切なロールまたはアセットの権限がない可能性があります。タスクを実行する必要がある場合は、組織の管理者にユーザーアカウントの確認を依頼してください。

# 索引

## A

Administrator サービス  
概要 [11](#)  
AS2 サーバーの設定 [166](#)  
AS2 ファイルサーバーのプロパティ [168](#)  
AS2 ファイルの交換 [166](#)  
Azure DevOps ユーザー資格情報 [44](#)  
Azure のデータアクセラレータ  
Enterprise Data Catalog との統合 [19](#)

## C

Cloud Application Integration コミュニティ  
URL [9](#)  
Cloud 開発者コミュニティ  
URL [9](#)

## E

Enterprise Data Catalog  
Informatica Intelligent Cloud Services との統合 [19](#)

## G

GitHub ユーザー資格情報 [44](#)

## H

Hosted Agent  
説明 [81](#)

## I

Informatica Intelligent Cloud Services  
Web サイト [9](#)  
Informatica グローバルカスタマサポート  
連絡先情報 [10](#)  
IP アドレスフィルタリング  
設定 [16](#)

## L

Linux  
Secure Agent のアンインストール [154](#)  
Secure Agent の起動および停止 [101](#)  
プロキシの設定 [153](#)

## M

Microsoft Azure  
シングルサインオン設定プロパティ [27](#)

## N

NetworkRetryInterval  
データ統合サーバーのプロパティ [123](#)  
NetworkTimeoutPeriod  
データ統合サーバーのプロパティ [123](#)

## P

POD  
特定方法 [148](#), [152](#)

## S

SAML のシングルサインオン  
ID プロバイダのプロパティ [32](#)  
SAML ロールマッピングのプロパティ [35](#)  
Secure Agent の登録 [30](#)  
サービスプロバイダのプロパティ [33](#), [34](#)  
サービスプロバイダメタデータ [35](#)  
ユーザーの作成 [30](#)  
ユーザーの削除 [30](#)  
ユーザー資格情報のストレージ [30](#)  
概要 [29](#)  
信頼済み IP 範囲 [30](#)  
制限 [30](#)  
設定の概要 [31](#)  
設定手順 [31](#)  
要求条件 [30](#)  
Secure Agent  
IP アドレスホワイトリスト [148](#), [152](#)  
Linux でのアンインストール [154](#)  
Linux での起動および停止 [101](#)  
Linux での権限 [152](#)  
Linux での登録 [153](#)  
Linux での要件 [152](#)  
Linux へのインストール [153](#)  
Secure Agent Manager [100](#)  
Secure Agent グループ [83](#)  
Secure Agent グループからの削除 [90](#)  
Secure Agent グループへの追加 [89](#)  
Windows サービスログインの設定 [150](#)  
Windows でのアンインストール [151](#)  
Windows での権限 [148](#)  
Windows での停止および再起動 [101](#)  
Windows での登録 [148](#)  
Windows での要件 [147](#)  
Windows へのインストール [148](#)

## Secure Agent (続く)

- アップグレード [100](#)
  - インストール [147](#)
  - エラスティックサーバーサービスの概要 [125](#)
  - エラスティックサーバーの構成プロパティ [125](#)
  - カスタム構成のプロパティ [146](#)
  - サービスの開始 [96](#)
  - サービスの開始および停止 [94](#)
  - サービスの概要 [113](#)
  - サービスの停止 [96](#)
  - サービスを開始および停止する際のガイドライン [96](#)
  - データ統合サーバーサービスの概要 [123](#)
  - データ統合サーバーの設定プロパティ [124](#)
  - ドメインホワイトリスト [148](#), [152](#)
  - トラブルシューティング [186](#)
  - ネットワーク中断設定 [123](#)
  - ファイル取り込みの設定プロパティ [127](#)
  - ブラックアウトファイルの構造 [98](#)
  - ブラックアウトファイルの上書き [98](#)
  - ブラックアウト期間の設定 [97](#)
  - 概要 [91](#)
  - 拡張性 [84](#)
  - 共通統合コンポーネントプロパティ [119](#)
  - 削除 [99](#)
  - 詳細の表示、更新ステータス [92](#)
  - 接続プロパティの保存 [17](#)
  - 通信ポート [148](#), [152](#)
  - 負荷分散 [84](#)
  - 名前の変更 [99](#)
- ## Secure Agent Manager
- Secure Agent の停止および再起動 [101](#)
  - 使用 [100](#)
- ## Secure Agent グループ
- Secure Agent の削除 [90](#)
  - Secure Agent の追加 [89](#)
  - Secure Agent の追加および削除 [87](#)
  - グループの共有 [87](#)
  - サービスの有効化および無効化 [85](#), [87](#)
  - サービス割り当てのガイドライン [86](#)
  - 依存性の表示 [91](#)
  - 概要 [83](#)
  - 既存のグループへの新規エージェントの追加 [90](#)
  - 共有グループでのファイル接続 [87](#)
  - 権限の変更 [87](#)
  - 作成 [87](#)
  - 削除 [87](#)
  - 名前の変更 [87](#)
- ## Secure Agent サービス
- CMI ストリーミングエージェント [117](#)
  - DBMI エージェントプロパティ [121](#)
  - アップグレード設定 [41](#)
  - データベース取り込みエージェントの環境変数 [122](#)
  - データベース取り込みサービスのプロパティ [121](#)
  - ローリングアップグレード [47](#)
  - ローリングアップグレードエラーの処理 [48](#)
  - 再開スケジュールの設定 [48](#)
  - 有効化および無効化 [85](#)
- ## SFTP サーバー設定 [166](#)
- SFTP ファイルサーバープロパティ [174](#)
  - SFTP ファイルの交換 [166](#)

## W

Web サイト [9](#)

## Windows

- プロキシの設定 [100](#), [150](#)

## Windows サービス

- Secure Agent ログインの設定 [150](#)

## あ

- アセット
  - 特権の割り当て [64](#)
- アセットログ
  - 最大ログエントリ [18](#)
  - 表示 [163](#)
- アップグレード通知 [10](#)
- アドオンバンドル
  - バンドルを参照してください。 [160](#)

## い

- イベント
  - 監視 [163](#)

## え

- エコシステムのシングルサインオン
  - 構成プロパティ [27](#)
- エラスティッククラスタ
  - AWS [187](#)
  - Microsoft Azure [191](#)
  - トラブルシューティング [187](#), [191](#)
  - メータリングの使用状況レポート [39](#)
- エラスティックサーバー
  - 概要 [125](#)

## お

- オブジェクトの依存関係
  - Secure Agent グループの表示 [91](#)

## か

- カスタム構成のプロパティ
  - Secure Agent [146](#)

## さ

- サーバーレスランタイム環境
  - IAM ロール [105](#)
  - ガイドライン [110](#)
  - クローン作成 [110](#)
  - コネクタ [111](#)
  - サーバーレスコンピューティングユニット [103](#)
  - ディザスタリカバリ [110](#)
  - プロパティ [107](#)
  - メータリングの使用状況レポート [39](#)
  - 概要 [103](#)
  - 再デプロイ [109](#)
  - 編集集中 [109](#)
  - 要求条件 [104](#), [106](#)
- サブ組織
  - ライセンスの同期 [26](#)
  - Enterprise Data Catalog 統合プロパティ [19](#)
  - アセットのエクスポートとインポート [23](#)
  - アドオンコネクタ [23](#)
  - スケジュールオフセット [18](#)

## サブ組織 (続く)

- ソース管理の無効化 [44](#)
- ソース管理の有効化 [43](#)
- ソース管理リポジトリの変更 [43](#)
- ソース管理設定 [41](#), [42](#)
- データ統合サービスのプロパティ [18](#)
- プロパティ [15](#)
- メータリング [36](#)
- ライセンス [25](#)
- ライセンスの編集 [26](#)
- ライセンスの有効期限 [26](#)
- 既存サブ組織の削除 [22](#)
- 既存組織のリンク [21](#)
- 作成 [21](#)
- 作成する理由 [20](#)
- 親組織からのリンク解除 [22](#)
- 親組織のアクセスを拒否 [23](#)
- 接続プロパティの保存 [17](#)
- 全般プロパティ [15](#)
- 追加と削除 [21](#)
- 認証プロパティ [16](#)
- 別の組織への切り替え [23](#)
- 無効化および有効化 [22](#)
- 例 [20](#)

## し

- システムステータス [10](#)
- ジョブの使用状況
  - 監視 [36](#)
- ジョブの制限数
  - 監視 [36](#)

## す

- スケジュール
  - Secure Agent サービスの再開 [48](#)
  - インポート [159](#)
  - エクスポート [159](#)
  - スケジュールオフセット [18](#)
  - スケジュール済みタスクの監視 [155](#)
  - タイムゾーン [157](#)
  - タスクまたはタスクフローとの関連付け [155](#)
  - ブラックアウト期間の設定 [156](#)
  - ユーザーのスケジュール済みジョブの再割り当て [57](#)
  - 夏時間 [157](#)
  - 繰り返し頻度 [156](#)
  - 削除 [155](#)
  - 設定 [158](#)
  - 説明 [155](#)
- ステータス
  - Informatica Intelligent Cloud Services [10](#)
- ストーリーミング取り込み
  - Secure Agent [117](#)

## せ

- セキュリティ
  - トラブルシューティング [194](#)
- セキュリティの質問
  - 編集 [13](#)
- セキュリティログ
  - 最大ログエントリ [18](#)
  - 表示 [163](#)

## そ

- ソース管理
  - OAuth を使用したアクセスの設定 [42](#)
  - サブ組織の設定 [42](#)
  - チェックアウトの取り消し [47](#)
  - ベストプラクティス [45](#)
  - リポジトリ URL の変更 [43](#)
  - リポジトリへのアクセスの設定 [44](#)
  - リポジトリへの読み取り/書き込みアクセスの設定 [41](#)
  - リポジトリへの読み取り専用アクセスの設定 [41](#)
  - 開発ガイドライン [45](#)
  - 設定 [41](#)
  - 設定のガイドライン [45](#)
  - 組織の設定 [41](#)
  - 組織の無効化 [44](#)
  - 組織の有効化 [43](#)

## た

- タイムゾーン
  - ユーザープロファイルの変更 [13](#)
  - 説明 [157](#)

## て

- ディレクトリ
  - アクセスする Secure Agent ログインの設定 [150](#)
- データ統合サーバー
  - 概要 [123](#)
- データ統合のデータカタログページ
  - 表示と非表示 [19](#)

## と

- トラブルシューティング
  - Administrator サービス [186](#)
  - Secure Agent [186](#)
  - エラスティッククラスタ [187](#), [191](#)
  - セキュリティ [194](#)

## は

- パートナーファイルサーバー [166](#)
- パスワード
  - 再利用 [16](#)
  - 最小混合文字数 [16](#)
  - 最小長 [16](#)
  - 変更 [13](#)
  - 有効期限 [16](#)
- バンドル
  - アップグレード [162](#)
  - アンインストール [162](#)
  - インストール [160](#)
  - コピー [161](#)
  - 管理 [160](#)
  - 表示 [160](#)

## ふ

- ファイアウォール
  - 設定 [148](#), [152](#)

ファイルサーバー  
AS2 プロパティ [168](#)  
SFTP のプロパティ [174](#)  
プロキシのプロパティ [177](#)  
設定 [167](#)  
停止および開始 [179](#)  
ファイルサーバーの設定  
グローバル設定 [184](#)  
ユーザー [180](#)  
ファイル統合サービス  
ファイルサーバー [166](#), [167](#)  
ファイルサーバーのユーザー [180](#)  
ファイルサーバーの停止および開始 [179](#)  
ブラックアウト期間  
Secure Agent に対する設定 [97](#)  
Secure Agent のブラックアウトファイル構造 [98](#)  
Secure Agent ブラックアウトファイルの上書き [98](#)  
組織用の設定 [156](#)  
プロキシサーバー設定 [166](#)  
プロキシファイルサーバープロパティ [177](#)  
プロキシ設定  
Linux での設定 [153](#)  
Windows 上での設定 [100](#), [150](#)  
プロファイル  
編集 [13](#)

## ほ

ホワइटリスト  
Secure Agent の IP アドレス [148](#), [152](#)  
Secure Agent のドメイン [148](#), [152](#)

## め

メータリング  
すべてのメーターの表示 [36](#)  
メーター定義 [37](#)  
ライセンスメトリックの表示 [36](#)  
使用状況のグラフの表示 [40](#)  
使用状況の詳細の表示 [40](#)  
使用状況レポート [39](#)  
組織とサブ組織 [36](#)  
メータリングの使用状況レポート  
ダウンロード [39](#)  
情報 [39](#)  
メンテナンスの停止 [10](#)

## ゆ

ユーザー  
アプリケーション統合の匿名ユーザー [51](#)  
グループの割り当て [52](#)  
サービスの割り当ておよび割り当て解除 [55](#)  
スケジュール済みジョブの再割り当て [57](#)  
ユーザーグループへの割り当て [59](#)  
ユーザー統計 [51](#)  
リセット [56](#)  
ロールの割り当て [52](#)  
ログイン日時のダウンロード [51](#)  
ロック解除 [56](#)  
概要 [49](#)  
構成例 [60](#)  
作成 [55](#)  
削除 [57](#)  
詳細 [52](#)

ユーザー (続く)  
定義 [49](#)  
認証方法 [50](#)  
編集 [52](#)  
無効化 [56](#)  
ユーザーグループ  
メンバの追加と削除 [59](#)  
ユーザーへの割り当て [52](#)  
ロールの割り当て [59](#)  
概要 [58](#)  
構成例 [60](#)  
作成 [59](#)  
削除 [60](#)  
詳細 [59](#)  
定義 [49](#)  
編集 [59](#)  
名前の変更 [59](#), [60](#)  
ユーザープロファイル  
編集 [13](#)

## ら

ライセンス  
サブ組織 [25](#)  
サブ組織のライセンスの編集 [26](#)  
タイプ [24](#)  
管理 [24](#)  
組織階層ライセンス [20](#), [25](#)  
有効期限 [26](#)  
ライセンスメトリック  
表示 [36](#)  
ランタイム環境  
Hosted Agent [81](#)  
Secure Agent グループ [83](#)  
Secure Agent グループの共有 [87](#)  
Secure Agent のインストール [147](#)  
サービスの有効化および無効化 [85](#)  
サービス割り当てのガイドライン [86](#)  
概要 [81](#)  
共有グループでのファイル接続 [87](#)

## り

リモートファイルサーバー [166](#)

## ろ

ロール  
カスタム [63](#), [75](#)  
クロスサービス [68](#)  
クロスサービスロールの特権 [69](#)  
サービス固有 [73](#)  
サービス固有のロールの特権 [73-75](#)  
システム定義 [63](#), [68](#)  
ユーザーグループへの割り当て [59](#)  
ユーザーへの割り当て [52](#)  
ユーザー設定の例 [60](#)  
概要 [63](#)  
作成 [75](#)  
削除 [76](#)  
詳細 [64](#)  
定義 [49](#)  
特権の割り当て [64](#)  
有効および無効 [63](#)

ログインの拒否  
トラブルシューティング [194](#)