



Informatica® Operational Insights
September 2022

オペレーションインサイト

© 著作権 Informatica LLC 2017, 2022

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: 2022-11-22

目次

序文.....	7
第 I 部 : オペレーションインサイトの紹介	8
第 1 章 : オペレーションインサイトの概要.....	9
アラートの設定	10
コレクタについて	11
オペレーションインサイトを使用したサービスとアプリケーションの監視.....	13
Informatica のリソース.....	13
Informatica マニュアル.....	13
Informatica Intelligent Cloud Services Web サイト.....	13
Informatica Intelligent Cloud Services コミュニティ.....	13
Informatica Intelligent Cloud Services マーケットプレイス.....	14
データ統合コネクタのドキュメント.....	14
Informatica ナレッジベース.....	14
Informatica Intelligent Cloud Services Trust Center.....	14
Informatica グローバルカスタマサポート.....	14
第 II 部 : Informatica Intelligent Cloud Services の監視.....	16
第 2 章 : Secure Agent のインストールと設定.....	17
Secure Agent 前提条件.....	17
Windows での Secure Agent のインストール.....	18
Windows での Secure Agent の要件.....	18
Windows での Secure Agent のダウンロードおよびインストール.....	19
Configuring the firewall.....	20
Windows でのプロキシ設定.....	21
Windows Secure Agent サービスへのログインの設定.....	22
Windows での Secure Agent のアンインストール.....	23
Linux での Secure Agent のインストール.....	23
Linux での Secure Agent の要件.....	23
Linux での Secure Agent のダウンロードおよびインストール.....	24
Configuring the firewall.....	25
Linux でのプロキシ設定.....	26
Linux での Secure Agent のアンインストール.....	27
第 3 章 : Informatica Intelligent Cloud Services インフラストラクチャ の監視.....	28
マップの場所への Secure Agent またはドメインの追加.....	29
インフラストラクチャの健全性の監視.....	29
Secure Agent の監視.....	30

OI データコレクタサービスの監視.	31
グラフの詳細の拡大.	32
インフラストラクチャのアラート.	33
インフラストラクチャのアラートの設定.	34
アラートスクリプトの使用.	34
Secure Agent サービスのアラートの設定.	36
第 4 章 : Informatica Intelligent Cloud Services データ統合の監視.	37
データ統合の分析の表示.	38
データ統合ジョブの表示.	40
[ジョブ] ページの設定.	42
ジョブデータのエクスポート.	43
特定のジョブの詳細の表示.	44
特定のアセットのジョブ履歴の表示.	45
データ統合接続の表示.	47
データ統合の接続イベントの表示.	47
スケジュール済みのジョブの表示.	48
データ統合アラート.	49
データ統合ジョブのアラートの設定.	49
第 5 章 : Informatica Intelligent Cloud Services アプリケーション統合 の監視.	51
アプリケーション統合アセットの全体的な使用状況と健全性の表示.	51
アプリケーション統合プロセスレポートの表示.	58
アプリケーション統合アセットの使用状況の監視.	59
受信 API 呼び出しの表示.	59
アプリケーション統合プロセスの実行の表示.	61
アプリケーション統合の接続呼び出しの表示.	64
ライセンス制限に対する API トランザクションの表示.	68
第 6 章 : Informatica Intelligent Cloud Services データプロファイリン グの監視.	70
データプロファイリングサービスジョブの表示.	71
データプロファイリングの特定のジョブの詳細の表示.	72
第 7 章 : Informatica Intelligent Cloud Services 一括取り込みの監視.	74
取り込みジョブの監視.	74
すべての取り込みジョブの監視.	75
ジョブのプロパティ.	78
取り込みジョブの詳細の表示.	78
アプリケーション取り込みジョブの詳細.	79
データベース統合ジョブの詳細.	85
ファイル取り込みジョブの詳細.	91

ストーリーミング統合ジョブの詳細.	93
一括取り込みアラート.	97
一括取り込みジョブのアラートの設定.	98
第 III 部 : オンプレミスアプリケーションの監視.	99
第 8 章 : ドメインの登録と管理.	100
監視モデルリポジトリサービスの有効化.	100
ドメイン接続の設定.	101
ドメインの詳細の入力.	103
ドメインの設定設定コレクタ.	103
コレクタスケジュールの設定.	103
ドメインの設定健全性統計コレクタ.	104
コレクタスケジュールの設定.	104
ドメインの設定リソース使用率統計コレクタ.	104
履歴データの収集.	105
監視統計モデルリポジトリへの接続.	105
コレクタスケジュールの設定.	106
PowerCenter リポジトリコレクタの設定.	106
履歴データの収集.	107
PowerCenter リポジトリの追加.	107
コレクタスケジュールの設定.	108
Data Engineering Integration コレクタの設定.	108
履歴データの収集.	109
クラスタ設定の選択.	109
コレクタスケジュールの設定.	109
Kerberos 認証を使用した、保護されたクラスタへの接続.	110
Data Quality コレクタの設定.	111
コレクタスケジュールの設定.	111
オンボーディング設定の最終処理.	111
ドメインの検索.	111
ドメインの編集または登録解除.	112
タイムゾーンの設定.	112
第 9 章 : Data Engineering Integration ドメインの監視.	114
Data Engineering Integration ジョブの分析の表示.	115
ジョブ実行データの表示.	115
Data Engineering Integration プロジェクトの作成.	116
第 10 章 : Data Quality ドメインの監視.	118
Data Quality ジョブ分析の表示.	119
ジョブ実行サマリデータの表示.	119
Data Quality プロジェクトの作成.	120

第 11 章 : PowerCenter ドメインの監視	122
PowerCenter ワークフロー分析の表示.	123
PowerCenter ワークフロー実行データの表示.	123
異常なワークフロー実行動作の表示.	124
推奨事項の表示.	125
リソース使用率のヒートマップの表示.	126
ドメインリソース使用率の表示.	127
PowerCenter プロジェクトの作成.	128
PowerCenter リポジトリフィルタの使用.	129
PowerCenter アラート.	129
索引	131

序文

Informatica Intelligent Cloud Services オペレーションインサイトを使用して、Informatica インフラストラクチャのパフォーマンスと運用効率を可視化し、分析を表示して、ジョブ、アセット、および接続を監視する方法について説明します。ワークフローとジョブ実行メトリックを使用して障害のトラブルシューティングを行う方法と、リソース消費分析を確認して、容量の増加やリソースを再割り当てを行う必要がある時期を予測する方法について説明します。ドメイン内または Secure Agent の問題について警告するように電子メール通知を設定する方法、および潜在的な問題に対処するために推奨事項と異常なワークフロー検出という形でインサイトを使用する方法について解説します。

パート I: オペレーションインサイトの紹介

- [オペレーションインサイトの概要, 9 ページ](#)

第 1 章

オペレーションインサイトの概要

オペレーションインサイトは Informatica Intelligent Cloud Services のサービスであり、Informatica インフラストラクチャのパフォーマンスと運用効率を可視化します。オペレーションインサイトを使用して、Informatica Cloud サービスと Informatica オンプレミス製品を監視します。

オペレーションインサイトは、インフラストラクチャ内のランタイム環境、Informatica Cloud Secure Agents、Secure Agent サービス、Informatica Intelligent Cloud Services、およびドメインを認識します。ランタイム統計とアセット設定メタデータは、設定可能なスケジュールでアセットからサービスにアップロードされ、Informatica デプロイメントの正確かつ最新の概要を提供します。

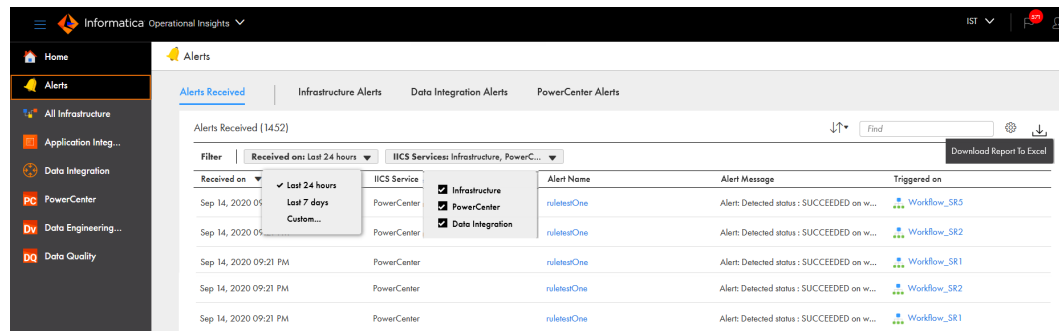
オペレーションインサイトの分析駆動型の機能は、次のような機能を提供します。

- 包括的な監視統計により、Informatica アセットの健全性を迅速に評価できます。
- ジョブ実行とデータ処理の統計に基づくデータ処理分析により、Informatica への投資の使用状況を評価できます。
- ランタイムジョブの実行、ワークフロー、およびタスクのメトリックを使用することで、パフォーマンスの低下と実行の失敗をトラブルシューティングできます。
- リソース消費分析は、容量の増加やリソースの再割り当てを行う必要がある時期を予測する場合に役立ちます。
- 電子メール通知は、Data Engineering Integration、Data Quality、または PowerCenter ドメイン内の問題、または Secure Agent の問題に関する警告を送信します。
- 推奨事項と異常なワークフロー検出という形でのインサイトは、ドメイン内のエラーおよび異常な動作を特定する場合に役立ちます。

アラートの設定

組織内のサービスで問題が発生したときにアラートを送信するようにオペレーションインサイトを設定できます。[アラート] ページを使用して、Informatica アセットのアラートを設定および管理します。

次の図は、[アラート] ページを示しています。



[アラート] ページには、次のタブが表示されます。

アラートを受信

組織内のサービスについて、ユーザーが受信したすべてのアラート通知に関する情報を表示します。過去 24 時間、過去 1 週間、またはカスタムの日付範囲からアラートを表示するように選択できます。デフォルトは 24 時間です。サービスに基づいて通知をフィルタリングすることもできます。アラート名をドリルダウンして、アラートの詳細を表示できます。

インフラストラクチャのアラート

ドメイン、Secure Agent、および Secure Agent サービスのアラートを設定します。親組織とサブ組織のアラートを設定できます。組織内外の受信者にアラート通知メールを送信するように Secure Agent を設定できます。

注: 組織を新しい POD に移行してから最初の 30 日間は、Secure Agent がダウンしていることを知らせる電子メール通知を受け取る場合があります。この通知は組織が移行前に使用していた Secure Agent に関するものであるため、無視してかまいません。

データ統合アラート

データ統合ジョブのアラートを設定および管理します。特定のステータスにあるジョブ、またはしきい値の制限に達したジョブにアラートを設定できます。特定のしきい値の制限に達したジョブを再開または停止するようにオペレーションインサイトを設定することもできます。

一括取り込みアラート

アプリケーション取り込みおよびデータベース取り込みジョブのアラートを設定および管理します。特定のジョブ状態を取得するジョブにアラートを設定し、選択した組織全体または特定のタスクアセットにアラートを適用できます。

PowerCenter のアラート

PowerCenter ワークフローインスタンスの異常または異常な動作に関する PowerCenter ワークフローアラートおよび CLAIRE アラートを設定および管理します。PowerCenter ドメインのワークフローまたはオペレーションインサイトで作成されたプロジェクトで発生する問題に対するアラートを設定できます。

コレクタについて

コレクタは、Informatica ドメインと通信する Secure Agent 内で実行されるコンポーネントです。特定のアセットからデータを収集するためにコレクタを設定する必要はありません。Secure Agent はドメイン内のすべてのアセットを認識しており、有効化された各コレクタは関連するアセットから運用データとメタデータを収集します。

コレクタは、すべての Informatica リリース 10.x ドメインからデータを収集できます。必要に応じて、ドメイン設定コレクタ以外のコレクタを無効にすることができます。各コレクタのデフォルトの収集スケジュールを変更することもできます。

ドメイン登録プロセスの最終ステップとして【保存】をクリックすると、コレクタはデータの収集と Informatica Intelligent Cloud Services へのアップロードを開始します。データは収集時にオペレーションインサイトにアップロードされます。

以下のコレクタは、Secure Agent とともにデプロイされます。

コレクタ	説明	デフォルトの収集頻度	収集されたメタデータ
ドメイン設定コレクタ	ノードとサービスを含む、ドメインとすべてのドメインアセットの設定メタデータを収集してアップロードします。*	24 時間ごと	<ul style="list-style-type: none">- ドメインの詳細: ドメイン名、ドメイン内のノードのリスト、ドメイン内のグリッドの詳細。- ノードの詳細: 名前、HTTP ポート、ログディレクトリ、最大プロセス、実行中のサービスのリスト。- 各ノードのシステム設定: オペレーティングシステムの詳細、CPU コアの数、CPU 速度、物理メモリの詳細。
ドメイン健全性統計コレクタ	ノードやアプリケーションサービスなど、ドメインアセットの可用性の統計を収集してアップロードします。*	5 分ごと	<ul style="list-style-type: none">- 可用性の統計: ドメイン、ノード、サービス、およびグリッド。
ドメインリソース使用率統計コレクタ	ドメイン内のすべてのノードの CPU とメモリの消費の統計を収集してアップロードします。 コレクタは、ドメインの監視設定で指定された監視モデルリポジトリサービスによって管理されるモデルリポジトリから統計を収集します。	毎時	<ul style="list-style-type: none">- CPU 使用率: 各ノードで実行されている Informatica プロセスとすべてのプロセス。- メモリ使用率: 各ノードで実行されている Informatica プロセスとすべてのプロセス。

コレクタ	説明	デフォルトの収集頻度	収集されたメタデータ
Data Engineering Integration コレクタ	<p>Hadoop で実行されている Data Engineering Integration ジョブの統計を収集してアップロードします。</p> <p>統計を収集する各 Hadoop クラスタの設定情報を含むクラスタ設定を指定する必要があります。</p>	毎時	<ul style="list-style-type: none"> - Hadoop クラスタ設定: Hadoop ディストリビューション別のクラスタとノードの数。 - Hadoop クラスタリソースの使用率: Informatica プロセスと各クラスタノードで実行されているすべてのプロセスの CPU とメモリの使用率。 - ジョブ実行の統計: ジョブのタイプ、挿入/却下された行数、失敗/成功したマッピングの数、処理済みのデータの量、開始時間と終了時間、ジョブを送信したデータ統合サービス。 - 実行時メトリック: 各クラスタまたはすべてのクラスタで実行された一意のマッピングとワークフローの数と種類。
データ品質コレクタ	<p>Hadoop で実行される Data Quality ジョブの統計を収集してアップロードします。</p>	毎時	<ul style="list-style-type: none"> - ジョブ実行の統計: ジョブのタイプ、挿入/却下された行数、失敗/成功したマッピングの数、処理済みのデータの量、開始時間と終了時間、ジョブを送信したデータ統合サービス。 - 実行時メトリック: 各クラスタまたはすべてのクラスタで実行された一意のマッピングとワークフローの数と種類。
PowerCenter リポジトリコレクタ	<p>ドメイン内の PowerCenter リポジトリからランタイムワークフローとセッションメトリックを収集してアップロードします。</p> <p>統計を収集する PowerCenter リポジトリごとに、リポジトリデータベースの JDBC 接続の詳細を指定する必要があります。</p>	毎時	<ul style="list-style-type: none"> - ワークフローの詳細: ワークフロー名、開始時刻と終了時刻、ステータス（成功、失敗など）、ワークフローを送信した PowerCenter 統合サービス。 - セッションタスク: タスク ID とタイプ、開始時刻と終了時刻、読み取られた行、書き込まれた行、タスクが実行されたノード。 - リポジトリフォルダの詳細: フォルダ ID と名前。

* オペレーションインサイトを使用して監視するために登録した Informatica ドメインに複数のゲートウェイノードがあり、ドメインがマスターゲートウェイノードから別のゲートウェイノードにフェイルオーバーした場合、ドメイン設定コレクタとドメイン健全性統計コレクタは、コレクションをドメイン内の他のゲートウェイノードに内部的に切り替え、シームレスに作業を続けます。

オペレーションインサイトを使用したサービスとアプリケーションの監視

Informatica Intelligent Cloud Services オペレーションインサイトを使用して、次の Informatica Cloud サービスを監視します。

- Informatica 環境
- Informatica Intelligent Cloud Services アプリケーション統合
- Informatica Intelligent Cloud Services データ統合
- Informatica Intelligent Cloud Services Data Quality
- Informatica Intelligent Cloud Services データプロファイリング
- Informatica Intelligent Cloud Services 一括取り込み

Informatica Intelligent Cloud Services オペレーションインサイトを使用して、次の Informatica オンプレミスアプリケーションを監視します。

- Data Engineering Integration ドメイン
- Data Quality ドメイン
- PowerCenter ドメイン

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。

パート II: Informatica Intelligent Cloud Services の監視

この部には、以下の章があります。

- [Secure Agent のインストールと設定, 17 ページ](#)
- [Informatica Intelligent Cloud Services インフラストラクチャの監視, 28 ページ](#)
- [Informatica Intelligent Cloud Services データ統合の監視, 37 ページ](#)
- [Informatica Intelligent Cloud Services アプリケーション統合の監視, 51 ページ](#)
- [Informatica Intelligent Cloud Services データプロファイリングの監視, 70 ページ](#)
- [Informatica Intelligent Cloud Services 一括取り込みの監視, 74 ページ](#)

第 2 章

Secure Agent のインストールと設定

Secure Agent と通信するには、オペレーションインサイトが監視するすべてのドメインを設定する必要があります。Secure Agent のインストールは、オンプレミス製品にのみ行う必要があります。Informatica Intelligent Cloud Services には Secure Agent をインストールしません。

ドメインが既存の Secure Agent にアクセスできる場合は、オペレーションインサイトへのドメインの登録時に、Secure Agent を使用するようにドメインを設定できます。組織内の複数のドメインを設定して、同じ Secure Agent を使用できます。

ドメインが Secure Agent にアクセスできない場合は、ドメイン内のノードに Secure Agent をダウンロードしてインストールする必要があります。Secure Agent は、インターネットにアクセスできるマシンにインストールする必要があります。

オペレーションインサイトサービスが 12 時間以上シャットダウンした場合、サービスへの Secure Agent 接続がタイムアウトすることに注意してください。ノードで Secure Agent を手動で再起動して、接続を再確立します。

注: オペレーションインサイトを使用して Informatica Intelligent Cloud Services の他のサービスを監視する場合は、Administrator のヘルプで Secure Agent の設定に関する情報を参照してください。

Secure Agent 前提条件

Secure Agent をダウンロードしてインストールする前に、次のタスクを実行します。

- Windows の場合は、管理者以外のユーザーとしてログインする必要があります。Linux の場合は、ルート以外のユーザーとしてログインする必要があります。管理権限またはルートアクセス権限を持つユーザーとして Secure Agent をインストールすると、基盤となる Secure Agent データベースが起動しなくなります。
- (任意) JDBC および SAP コネクタのサードパーティライブラリをプロセスサーバーで使用する場合は、そのライブラリを次の場所にコピーします:
 <Secure Agent のインストールディレクトリ>\apps\process-engine\ext

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。

Secure Agent Manager または Windows サービスを使用して Secure Agent を停止および再起動できます。インストールプログラムの実行に使用するボリュームとは異なるボリュームに Secure Agent をインストールする場合は、Windows サービスから Secure Agent を起動および停止する必要があります。

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 でサポートされているオペレーティングシステムのリストについては、ナレッジベースの [Product Availability Matrix \(PAM\) for Informatica Intelligent Cloud Services](#) 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。

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 の設定の実行

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。

ヒント: Secure Agent インストールプログラムのチェックサムを確認するには、エージェントの REST API バージョン 2 リソースを使用します。エージェントリソースの詳細は、『*REST API リファレンス*』を参照してください。

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。このインストールプログラムの名前は agent64_install_ng_ext.<Agent Core バージョン>.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。

7. 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。
8. 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。

Configuring the firewall

If your organization uses a protective firewall, include the Informatica Intelligent Cloud Services and Operational Insights domain name or IP address ranges for your region in the list of approved domain

names or IP addresses. You must also configure Secure Agents used by the domains Operational Insights monitors to use the approved IP address ranges.

You should also enable the port that the Secure Agent uses. The Secure Agent uses port 443 (HTTPS) to connect to the internet. Configure your firewall to allow traffic to pass over port 443.

You must add the domain name or IP address ranges required by both Informatica Intelligent Cloud Services and Operational Insights to your list of approved domain names or IP addresses.

The allowlists of domains and IP addresses can vary according to your data center, which is also called a POD (Point of Deployment). You can identify your POD through the URL that appears when you open any service in Informatica Intelligent Cloud Services. The first few characters of the URL string identify the POD. For example, if the URL starts with `usw3.dm-us.informaticacloud.com`, your POD is USW3.

You can find the domains and IP addresses to allowlist for Informatica Intelligent Cloud Services in the following KB article on Informatica Network:

<https://kb.informatica.com/faq/7/Pages/20/524982.aspx>

You can find the domains and IP addresses to allowlist for Operational Insights in the following KB article on Informatica Network:

<https://kb.informatica.com/faq/7/Pages/21/532624.aspx>

To configure a Secure Agent to use the approved IP address ranges, complete the steps below:

1. Add either the domain names or the IP address ranges for your region to your list of approved addresses.
2. Log in to Operational Insights.
3. Select a domain, and then click the **Details** tab.
4. Locate the name of the Secure Agent the domain uses in the Secure Agent Group property.
5. Click **Secure Agents** in the left hand navigation bar.
6. Select a Secure Agent, then click **Manage**.

The Details page for the Secure Agent opens in the Administrator application.

7. Click **Edit**.
8. Click the + symbol next to a property in the Custom Configuration section of the page to add a new custom property.
9. Select **OpsInsights Data Collector** from the Service menu, and then select **OpsInsights** from the Type menu.
10. Enter `useStaticIP` in the Name field, and then enter `true` in the Value field.
11. Click **Save**.

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。

1. Secure Agent Manager で、**[プロキシ]** をクリックします。
2. 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。

3. 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。

4. **[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。

1. Windows の **[管理ツール]** から、**[サービス]** ウィンドウに移動します。
2. **[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。
3. **[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。
4. 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。

注: Secure Agent をアンインストールしても、Secure Agent ディレクトリからログファイルは削除されません。マシンに Secure Agent を再インストールする場合は、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する必要があります。そうしないと、再インストールは失敗します。ログファイルを保存する場合は、別のディレクトリにコピーしてから、Secure Agent のインストールディレクトリを削除してください。

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 でサポートされているオペレーティングシステムのリストについては、ナレッジベースの [Product Availability Matrix \(PAM\) for Informatica Intelligent Cloud Services](#) 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。

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。

エージェントを登録すると、デフォルトで独自の Secure Agent グループに追加されます。エージェントは別の Secure Agent グループに追加することもできます。

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。

ヒント: Secure Agent インストールプログラムのチェックサムを確認するには、エージェントの REST API バージョン 2 リソースを使用します。エージェントリソースの詳細は、『*REST API リファレンス*』を参照してください。

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。このインストールプログラムの名前は `agent64_install_ng_ext.<Agent Core バージョン>.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. エージェントを登録するには、<Secure Agent の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、次のいずれかのコマンドを入力します。

- エージェントを独自の Secure Agent グループに追加するには、次のコマンドを使用します。
`./consoleAgentManager.sh configureToken <user name> <install token>`
- エージェントを既存の Secure Agent グループに追加するには、次のコマンドを使用します。
`./consoleAgentManager.sh configureTokenWithRuntime <user name> <install token> <Secure Agent group name>`

注: 存在しない Secure Agent グループ名がコマンドに含まれている場合、Secure Agent はグループに割り当てられません。有効な Secure Agent グループ名を使用するようにしてください。

以下の表にコマンドのオプションの一覧を示します。

オプション	説明
ユーザー名	必須。Secure Agent をインストールするユーザーの Informatica Intelligent Cloud Services ユーザー名。
インストールトークン	必須。コピーしたインストールトークン。
Secure Agent グループ名	オプション。既存の Secure Agent グループにエージェントを追加する場合、代わりに含めます。このオプションがコマンドに含まれていない場合、エージェントは独自の Secure Agent グループに追加されます。

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`

Configuring the firewall

If your organization uses a protective firewall, include the Informatica Intelligent Cloud Services and Operational Insights domain name or IP address ranges for your region in the list of approved domain names or IP addresses. You must also configure Secure Agents used by the domains Operational Insights monitors to use the approved IP address ranges.

You should also enable the port that the Secure Agent uses. The Secure Agent uses port 443 (HTTPS) to connect to the internet. Configure your firewall to allow traffic to pass over port 443.

You must add the domain name or IP address ranges required by both Informatica Intelligent Cloud Services and Operational Insights to your list of approved domain names or IP addresses.

The allowlists of domains and IP addresses can vary according to your data center, which is also called a POD (Point of Deployment). You can identify your POD through the URL that appears when you open any service in Informatica Intelligent Cloud Services. The first few characters of the URL string identify the POD. For example, if the URL starts with `usw3.dm-us.informaticacloud.com`, your POD is USW3.

You can find the domains and IP addresses to allowlist for Informatica Intelligent Cloud Services in the following KB article on Informatica Network:

<https://kb.informatica.com/faq/7/Pages/20/524982.aspx>

You can find the domains and IP addresses to allowlist for Operational Insights in the following KB article on Informatica Network:

<https://kb.informatica.com/faq/7/Pages/21/532624.aspx>

To configure a Secure Agent to use the approved IP address ranges, complete the steps below:

1. Add either the domain names or the IP address ranges for your region to your list of approved addresses.
2. Log in to Operational Insights.
3. Select a domain, and then click the **Details** tab.
4. Locate the name of the Secure Agent the domain uses in the Secure Agent Group property.
5. Click **Secure Agents** in the left hand navigation bar.
6. Select a Secure Agent, then click **Manage**.

The Details page for the Secure Agent opens in the Administrator application.

7. Click **Edit**.
8. Click the + symbol next to a property in the Custom Configuration section of the page to add a new custom property.
9. Select **OpsInsights Data Collector** from the Service menu, and then select **OpsInsights** from the Type menu.
10. Enter useStaticIP in the Name field, and then enter true in the Value field.
11. Click **Save**.

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て、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。

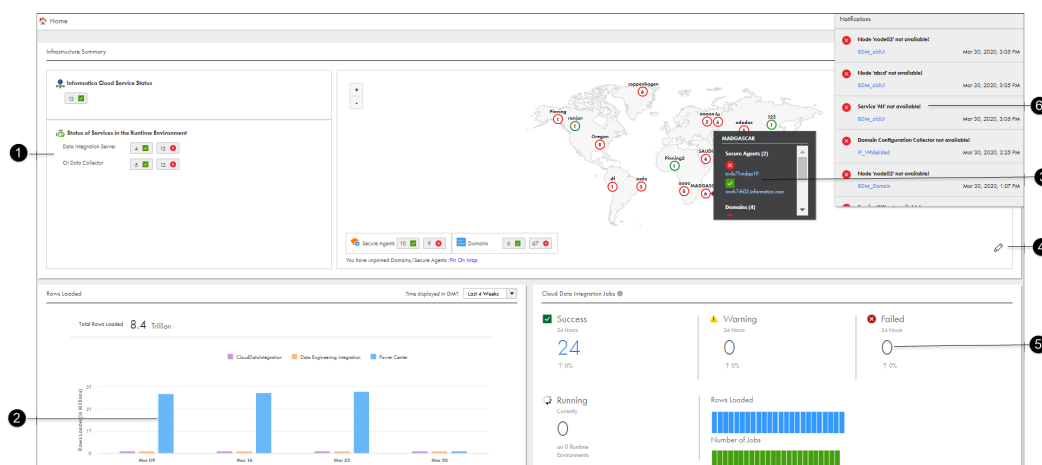
Secure Agent をアンインストールする前に、接続またはタスクがそれを使用するように構成されていないことを確認します。

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 3 章

Informatica Intelligent Cloud Services インフラストラクチャの監視

オペレーションインサイトを使用して、Informatica Intelligent Cloud Services インフラストラクチャを監視できます。ホームページを使用して、Informatica アセットの全体的な使用状況と健全性を評価します。親組織のユーザーは、サブ組織に切り替えてサブ組織のホームページを使用して、切り替え先のサブ組織のアセットの使用状況と健全性を表示できます。



このページからは次のようなタスクを実行できます。

タスク	説明
1	インフラストラクチャで実行されている Secure Agent サービスのステータスのサマリを表示します。サービスをクリックして、サービスが実行されるランタイム環境の分析を表示します。ランタイム環境の監視に関する詳細については、「 Secure Agent の監視 」(ページ 30)を参照してください。
2	インフラストラクチャ内のすべてのサービスとドメインについて、過去 4 週間または過去 6 か月間のデータ処理の統計のサマリを表示します。棒グラフのセグメントをクリックして、サービスまたはドメインタイプの分析を表示します。

タスク	説明
3	場所をクリックして、その場所内の Secure Agent またはドメインのステータスを表示します。ポップアップパネルにロケーション内のアセットが表示されます。詳細を表示するには、アセット名をクリックします。
4	このアイコンをクリックして、新しい場所をマップに追加するか、既存の場所を編集します。詳細については、「 マップの場所への Secure Agent またはドメインの追加 」(ページ 29)を参照してください。
5	組織が Informatica Intelligent Cloud Services の他のサービスを使用している場合は、このページに、各サービスに対する収集された分析の概要が表示されます。パネル内の値をクリックして、詳細な分析を表示します。 Informatica Intelligent Cloud Services の監視の詳細については、 第 4 章, 「Informatica Intelligent Cloud Services データ統合の監視」 (ページ 37)を参照してください。
6	通知アイコンをクリックして、オペレーションインサイトリソースで発生した問題に関するアラートを表示します。

マップの場所への Secure Agent またはドメインの追加

オペレーションインサイトの【ホーム】ページに表示されるインタラクティブなマップで、地理的な場所ごとに Secure Agent とドメインを整理できます。Secure Agent とドメインを場所に割り当てると、パフォーマンスを分析し、企業全体の容量と処理能力を判断するために役立ちます。親組織のユーザーは、サブ組織に切り替えて、サブ組織の地理的な場所ごとに Secure Agent を編成できます。

Secure Agent またはドメインをマップに追加するには、次の手順を実行します。

1. マップ上の編集（鉛筆）アイコンをクリックします。
2. リストから Secure Agent またはドメインを選択し、【固定】をクリックします。
3. マップ上の場所を追加する場所にピンを配置します。
Secure Agent またはドメインを既存の場所に追加するには、場所内にピンを配置します。
4. 新しい場所を追加する場合は、場所の名前を入力します。

インフラストラクチャの健全性の監視

【Secure Agent &グループ】パネルを使用して、Informatica インフラストラクチャ内のアセットのステータスを表示します。親組織のユーザーは、サブ組織に切り替えて【Secure Agent &グループ】パネルを使用して、サブ組織のアセットを表示できます。

【Secure Agent &グループ】パネルには、次のようなアセットのステータスが表示されます。

- それぞれのランタイム環境で実行されている各 Secure Agent。
- 各 Secure Agent で実行されているサービス。

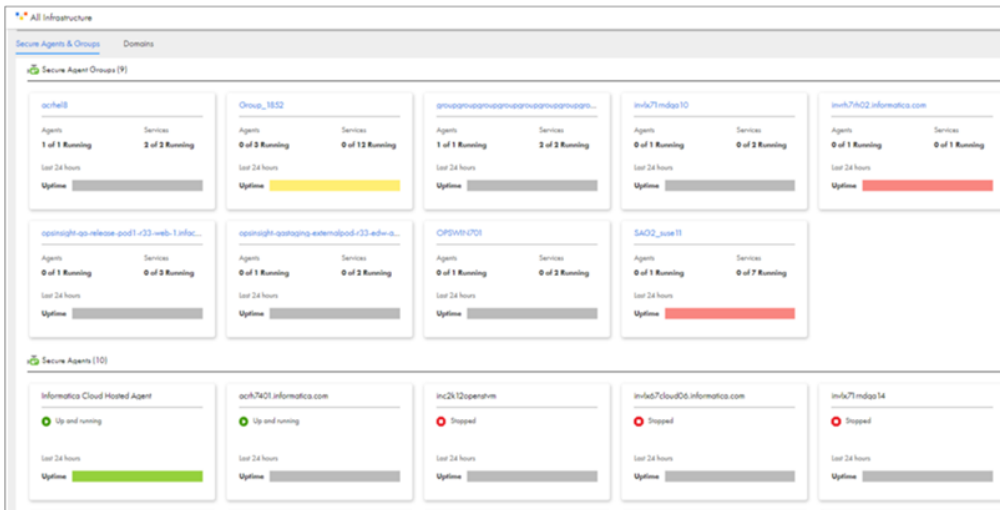
- Informatica インフラストラクチャ内のアセットのステータスを表示するには、次の手順を実行します。

- [Secure Agent &グループ]** パネルに、Informatica アセットのステータスが表示されます。

【すべてのインフラストラクチャ】 ページの **【Secure Agent &グループ】** パネルを使用して、Secure Agent のステータスと、Secure Agent が実行する Secure Agent サービスを表示します。Secure Agent サービスは、Secure Agent がデータ処理に使用するマイクロサービスです。サブ組織にログインするか、親組織からサブ組織に切り替えて、サブ組織の **【Secure Agent &グループ】** パネルを使用できます。

- [すべてのインフラストラクチャ] ページが表示されます。

次の図は、[すべてのインフラストラクチャ] ページの [Secure Agent &グループ] パネルを示しています。



Secure Agent グループにカーソルを合わせると、すべてのエージェントとサービスのリストと、各ランタイム環境での対応するステータスが表示されます。[アップタイム] バーにカーソルを合わせると、各ランタイム環境の過去 24 時間の時間範囲に従って、すべての Secure Agent のステータスが表示されます。Secure Agent のステータスは、次の色で表示されます。

- 緑: すべてのエージェントが実行中です。
- 黄: 少なくとも 1 つのエージェントが実行されています。
- 赤: すべてのエージェントがダウンしています。

- 灰色: データが取得されませんでした。
2. Secure Agent グループ内のランタイム環境、エージェント、またはサービスの名前をクリックします。
[ランタイム環境] ページが表示されます。このページには、環境内で実行されている Secure Agent、Secure Agent サービス、およびジョブのステータスが表示されます。
[リソース使用率] グラフには、選択した期間にランタイム環境で実行されているサービスによる全体的なリソース使用率が表示されます。リソース使用率: [ディスク使用率] グラフには、先月の日次の使用済みディスク容量と空きディスク容量が表示されます。
[リソース使用率] グラフを使用してドメインを表示する方法については、[「ドメインリソース使用率の表示」 \(ページ 127\)](#)を参照してください。
[リソース使用率] グラフを使用してドメインを表示する方法については、「オンプレミスアプリケーションの監視」を参照してください。

OI データコレクタサービスの監視

Secure Agent で実行される OI データコレクタサービスを監視できます。

OI データコレクタサービスは、オペレーションインサイトで使用される運用データとドメイン関連のメタデータを収集するデータコレクタを実行します。Secure Agent は、収集された運用データとドメイン関連のメタデータを Informatica Intelligent Cloud Services にアップロードします。

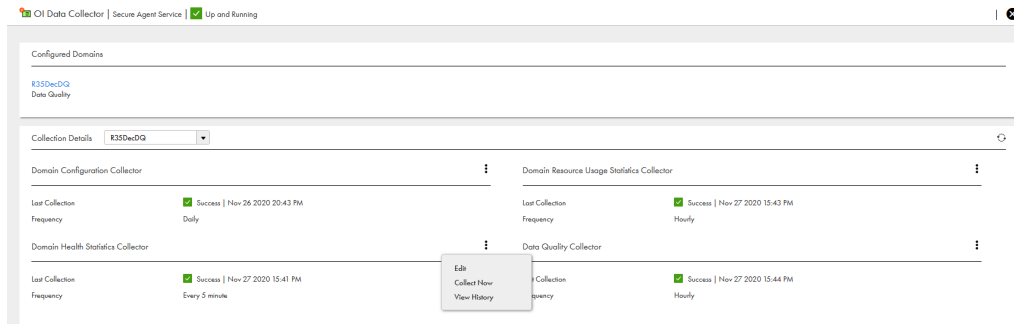
このページには、Secure Agent で実行されている OI データコレクタサービスに対する次のようなデータが表示されます。

- サービスのステータス。
- OI データコレクタサービスが実行しているデータコレクタがデータを収集するドメインのリスト。
- 各ドメインで有効になっているデータコレクタのリストと、最新の収集ステータス。

OI データコレクタサービスのステータスを表示するには、次の手順を実行します。

1. ページの左側にあるナビゲーションバーで **[すべてのインフラストラクチャ]** をクリックします。
[すべてのインフラストラクチャ] ページに、各ランタイム環境で実行されている Secure Agent および Secure Agent サービスのステータスが表示されます。
2. OI データコレクタサービスを実行している Secure Agent をクリックします。
3. **[OI データコレクタ]** リンクをクリックします。
4. コレクタのメニューから、次のオプションを選択できます。
 - コレクタの設定を変更するには、**[編集]** を選択します。
 - オンデマンドデータ収集をトリガするには、**[今すぐ収集]** を選択します。

- オンデマンドデータ収集の履歴を表示するには、**【履歴の表示】** を選択します。



注: 更新することで、最新の収集の詳細を取得できます。

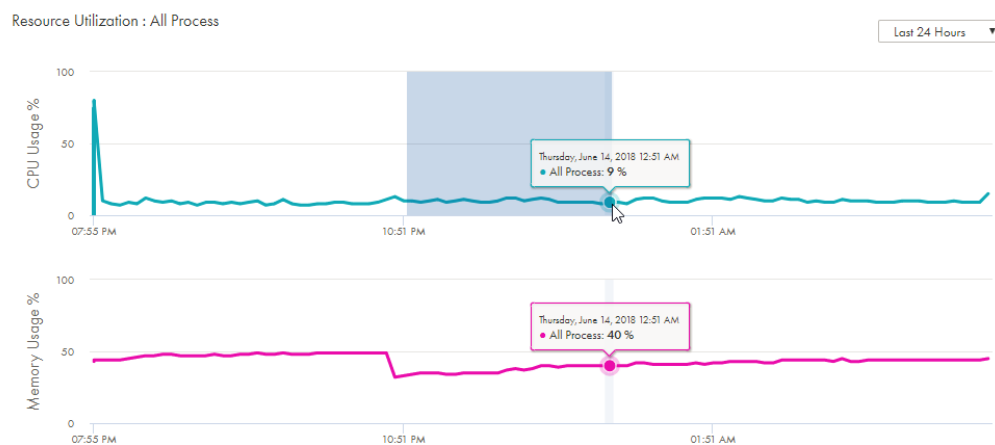
グラフの詳細の拡大

グラフを拡大して、特定のタイムフレームの Secure Agent リソース使用率の詳細を表示できます。開始時刻と終了時刻を選択して、グラフを拡大します。

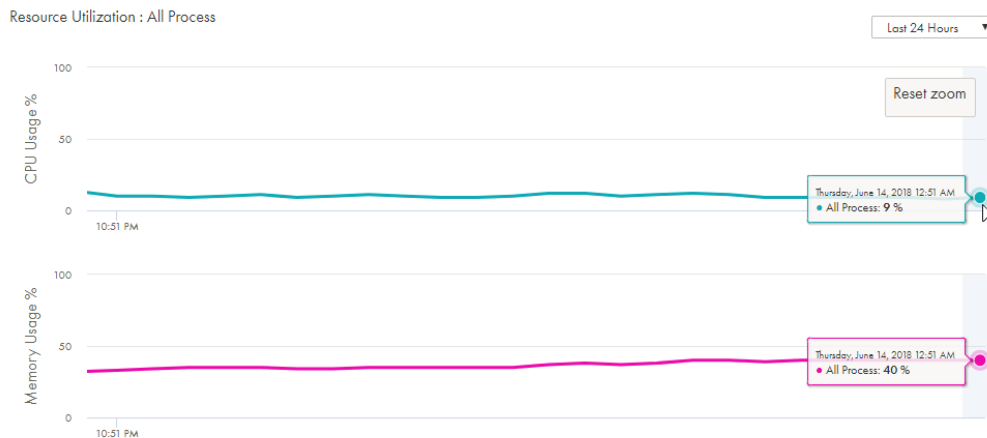
グラフの詳細を拡大するには、次の手順を実行します。

1. グラフのタイムフレームの開始点にカーソルを移動します。
2. マウスを左クリックします。
3. カーソルをグラフのタイムフレームの終点までドラッグします。

次の図は、午後 10 時 51 分から午後 12 時 51 分までのタイムフレームが選択されていることを示しています。



次の図に示すように、リソース使用率グラフが更新され、指定したタイムフレームのデータのみが表示されます。



4. グラフを元の状態に戻すには、**【ズームのリセット】** をクリックします。

インフラストラクチャのアラート

ドメイン内または Secure Agent で問題が発生したときに電子メール通知を送信するようにオペレーションインサイトを設定できます。

次のようなイベントに対するアラートを設定できます。

- ドメインまたは Secure Agent が使用できない場合。
- ドメイン内で実行されているコレクタ、サービス、またはノードが使用できない場合。
- ドメインノード、ドメインサービス、または Secure Agent ホストによる CPU またはメモリの消費量が設定可能なしきい値を超えた場合。
- Secure Agent によるディスク使用量が設定可能なしきい値を超えた場合。

注: アラート通知は**ホームページ**で表示できます。

組織の Informatica アセットは、**【アラート】** ページの **【インフラストラクチャのアラート】** パネルで表示できます。サブ組織のアクセス特権を持つ親組織のユーザーは、サブ組織に切り替えてそれらのアセットを表示できます。

オペレーションインサイトが監視するドメインまたは Secure Agent ごとに、個々のアラートまたはすべてのアラートを有効化または無効化することができます。また、Informatica Intelligent Cloud Services ユーザー、ユーザーグループ名、またはアラート通知を受信する組織外の電子メール受信者を指定します。

アラートがトリガされたときに、オペレーションインサイトが実行するアラートスクリプトを作成して、追加のアクションを実行できます。アラートスクリプトの作成と使用の詳細については、[「アラートスクリプトの使用」 \(ページ 34\)](#)を参照してください。

インフラストラクチャのアラートの設定

インフラストラクチャのアラートの設定時に、アラートのソース（ドメイン、Secure Agent、または Secure Agent サービス）を設定できます。アラートの受信者を含めることや、必要に応じて追加のアクションのスク립トを含めることもできます。

1. 左側のナビゲーションバーにある **【アラート】** をクリックします。
2. **【インフラストラクチャのアラート】** タブをクリックします。
3. ドメイン、Secure Agent、または Secure Agent サービスを選択します。
4. 有効にする各アラートを設定します。
5. Informatica Intelligent Cloud Services ユーザー名またはユーザーグループ名を選択するか、問題が発生したときに電子メール通知を受信する組織外の電子メール受信者を手動で入力します。

注: 親組織からサブ組織に切り替えてアラートを設定した場合、オペレーションインサイトにはサブ組織に登録されているすべての親組織ユーザーが表示されないことがあります。電子メール受信者リストにユーザーが表示されない場合は、電子メールアドレスを手動で入力します。

6. アラートがトリガされたときにオペレーションインサイトが実行するアラートスク립トを使用して追加のアクションを実行する場合は、**【カスタムスク립トの実行】** チェックボックスをオンにして、Secure Agent ホスト上のスク립トファイルへのパスを入力します。

アラートスク립トの使用法の詳細については、[「アラートスク립トを使用するための Secure Agent の設定」 \(ページ 35\)](#)を参照してください。

7. 必要に応じて、Secure Agent サービスのアラートを設定します。

サービスのアラートの設定については、[「Secure Agent サービスのアラートの設定」 \(ページ 36\)](#)を参照してください。

アラートスク립トの使用

サポートチケットの作成や CPU の統計のスナップショットの取得など、アラートがトリガされたときに追加のタスクを実行するためにオペレーションインサイトが実行するスク립トを作成できます。

オペレーションインサイトには、有効化した Secure Agent アラートに対応するルールが含まれています。スク립トで実行する各ルールの名前を指定します。ルールごとに、オペレーションインサイトがスク립トに渡すパラメータを指定します。

アラートスク립トによって、バッチファイル、シェルスクリプト、または EXE ファイルを呼び出すことができます。実行可能ファイルまたはプログラムは自己完結型である必要があります。

スク립トを Secure Agent ホストのディレクトリにコピーします。スク립トが実行されるたびに、オペレーションインサイトは、スク립トが実行される Secure Agent ホスト上の同じディレクトリにあるログファイルにスク립トの出力とエラーを書き込みます。

スク립ト出力ディレクトリが Secure Agent インストールディレクトリの下にある場合、Windows でログファイルを開くとエラーが表示されることがあります。この問題を解決するには、次のいずれかの手順を実行します。

- 管理者特権でログファイルを開きます。
- スクリプト出力ディレクトリと其中的のファイルに対する読み取り、書き込み、および実行の権限を付与します。

または、Secure Agent インストールディレクトリの外にスク립ト出力ディレクトリを作成し、以前のログファイルを新しいスク립ト出力ディレクトリに手動で移動することもできます。Administrator で、**【ランタイム環境】** ページを開きます。Secure Agent を編集し、**【OI データコレクタ】** サービスを選択します。OpsInsights の **scriptLogDir** プロパティ値を編集し、Secure Agent インストールディレクトリの外部にあるスク립ト出力ディレクトリを指定します。

[Click here](#) をクリックして、アラートスクリプトの例を表示します。

アラートスクリプトのルールとパラメータ

スクリプトファイルで指定するルールにルール名とルールパラメータを追加します。パラメータをキーと値のペアとして指定します。

スクリプトでは複数のルールを設定できます。

次の表に、Secure Agent アラートに関連付けられたルール名とパラメータを示します。

Secure Agent のアラート	ルール名	ルールのパラメータ
Secure Agent は 15 分間使用できません。	secure-agent-unavailable-rule	"ruleName": "secure-agent-unavailable-rule", "timestamp": "\${timestamp}", "agentName": "\${agentName}"
Secure Agent による CPU 使用率が、30 分にわたって xx%を超えています。	secure-agent-cpu-overused-rule	"ruleName": "secure-agent-cpu-overused-rule", "timestamp": "\${timestamp}", "agentName": "\${agentName}", "actualUsage": "\${actualUsage}", "thresholdValue": "\${thresholdValue}"
Secure Agent によるメモリ使用率が、30 分にわたって xx%を超えています。	secure-agent-memory-overused-rule	"ruleName": "secure-agent-memory-overused-rule", "timestamp": "\${timestamp}", "agentName": "\${agentName}", "actualUsage": "\${actualUsage}", "thresholdValue": "\${thresholdValue}"

アラートスクリプトを使用するための Secure Agent の設定

アラートスクリプトを使用するように Secure Agent を設定するには、次の手順を実行します。

1. スクリプトファイルを Secure Agent ホストにコピーします。
2. 左側のナビゲーションバーにある **【アラート】** をクリックします。
3. **【インフラストラクチャのアラート】** をクリックします。
4. アラートスクリプトを使用する Secure Agent を選択します。
5. **【カスタムスクリプトの実行】** チェックボックスを選択します。
6. **【編集】** リンクをクリックし、Secure Agent ホスト上のスクリプトファイルへのパスを入力します。
7. **【保存】** リンクをクリックします。

Secure Agent スクリプトログのページ

スクリプトが実行されるディレクトリに保持する Secure Agent スクリプトログファイルの数を指定できます。アプリケーションは、指定した値までの最新のログファイルを保持し、古いログファイルをすべて削除します。

デフォルトでは、アプリケーションは最新の 50 個のスクリプトログファイルを保持します。

1. **[Secure Agent]** をクリックします。
2. Ops Insights コレクタが実行されている Secure Agent を選択します。
3. scriptLogRetentionCount プロパティの値として保持するログファイルの数を入力します。

Secure Agent サービスのアラートの設定

Secure Agent の個々のサービスで問題が発生したときにアラートを送信するようにオペレーションインサイトを設定できます。

Secure Agent サービスの次のようなイベントに対するアラートを設定できます。

- サービスが使用できない場合
- サービスによる CPU 使用率が設定可能なしきい値を超えた場合
- サービスによるメモリ使用率が設定可能なしきい値を超えた場合

Secure Agent サービスにアラートを設定するには、次の手順を実行します。

1. **[アラート]** ページの **[インフラストラクチャのアラート]** タブで、Secure Agent を選択します。
2. Secure Agent のアラートが無効になっている場合は、アラートを有効にします。
 - a. **[すべて有効化]** をクリックします。
 - b. 個々の Secure Agent アラートを有効または無効にします。
3. **[サービス固有アラートの追加]** をクリックします。
4. アラートを設定する Secure Agent サービスを選択します。
5. 有効にする各アラートを設定します。
6. 問題が発生したときに電子メール通知を受信する Informatica Intelligent Cloud Services ユーザー、ユーザーグループ名、または組織外の電子メール受信者を入力します。
7. アラートがトリガされたときにオペレーションインサイトで追加のアクションを実行する場合は、**[カスタムスクリプトの実行]** を有効にしてから、Secure Agent マシン上のスクリプトファイルへのパスを入力します。
8. 追加の Secure Agent サービスに対して、手順 [3](#) から [7](#) を繰り返します。

第 4 章

Informatica Intelligent Cloud Services データ統合の監視

組織が Informatica Intelligent Cloud Services データ統合を使用している場合は、オペレーションインサイトを使用して、データ統合アセット、データ統合ジョブ、特定のジョブの詳細、特定のアセットのジョブ履歴、スケジュール済みのジョブ、およびデータ統合接続の分析を表示できます。**データ統合**ページでデータ統合の分析を表示します。

次のようなタイプのデータ統合アセットを監視できます。

- コマンドタスク
- データ転送タスク
- 動的マッピングタスク
- マッピングとマッピングタスク
- マスキングタスク
- 一括取り込みタスク
- PowerCenter タスク
- レプリケーションタスク
- 同期タスク
- タスクフローとリニアタスクフロー

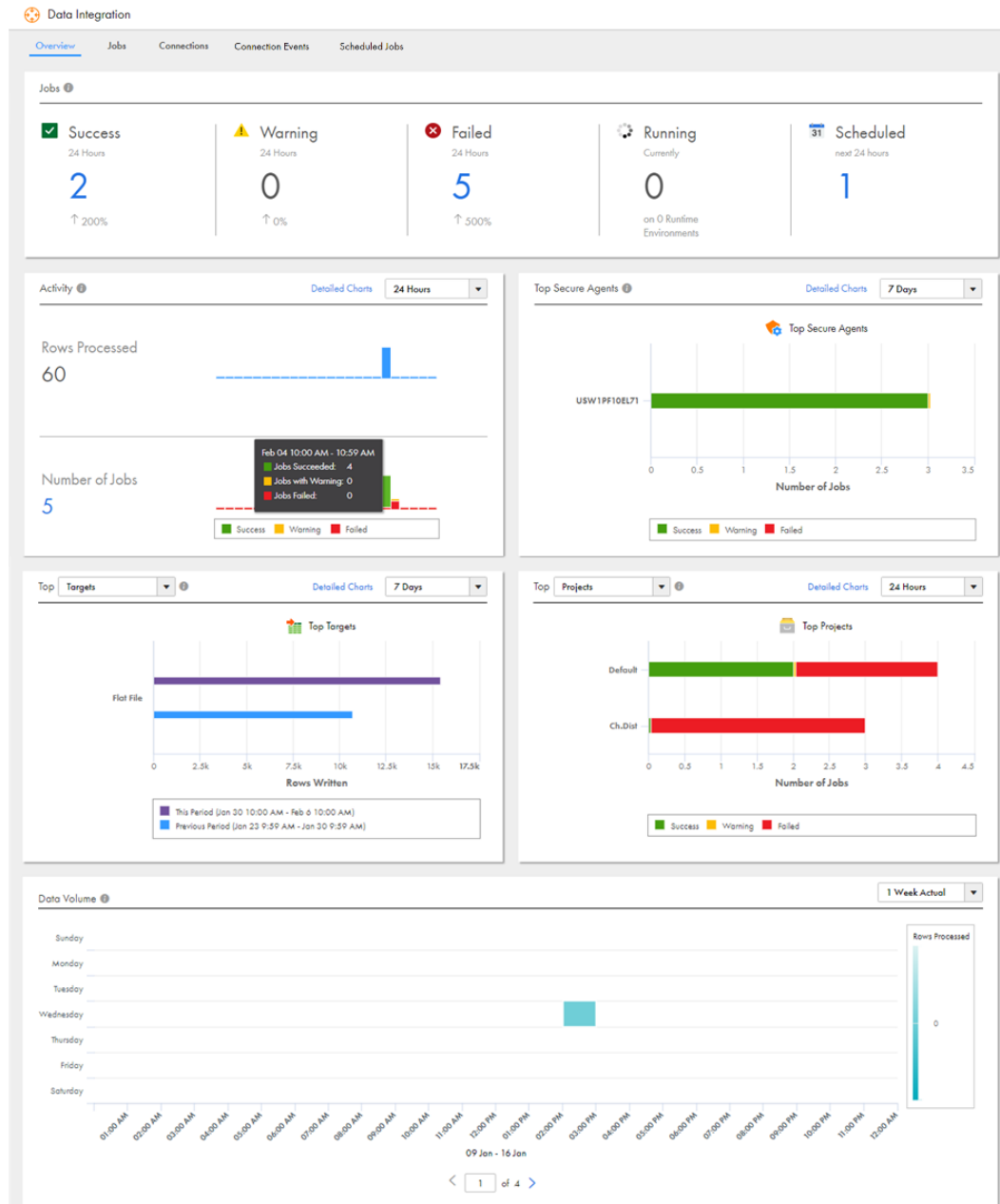
データ統合の使用に関する詳細については、データ統合のヘルプを参照してください。

オペレーションインサイトを使用してデータ統合アセットを監視するには、適切なライセンスが必要です。詳細について、またはこの機能をリクエストする場合は、Informatica グローバルカスタマサポートにお問い合わせください。

データ統合の分析の表示

【データ統合】ページの【概要】タブを使用して、過去 24 時間に組織で実行されたジョブの分析を表示します。【概要】タブのパネルでは、データ処理とジョブ実行の分析の特定の領域に関するインサイトを確認できます。

次の図は、【概要】タブを示しています。



【概要】タブの任意のグラフのバーにカーソルを合わせると、サマリの詳細が表示されます。選択した期間に完了したジョブに関する詳細情報を表示するには、グラフのバーをクリックします。

ジョブに関する情報は、最新のデータ更新時のものが表示されます。データは、毎正時に約 1 時間ごとに更新されます。

【概要】タブには、次のようなパネルがあります。

ジョブ

過去 24 時間に組織で実行中または実行されたジョブの分析の概要が表示されます。【履歴】パネルには、完了したジョブが表示されます。【最新】パネルをクリックすると、現在実行中のジョブと最近完了したジョブが表示されます。【最近】パネルは手動で更新できます。

番号をクリックすると、関連するジョブがいずれかのパネルに表示されます。表示されている数値は、最新のデータ更新の 24 時間前のものです。

アクティビティ

選択した期間に処理された行数と実行されたジョブ数が表示されます。過去 24 時間または過去 7 日間のデータを表示するように選択することができます。

【詳しいグラフ】をクリックして、選択した期間中に処理されたデータの合計行数と実行されたジョブの数に関する分析を表示します。

上位 Secure Agent

組織内で最も頻繁に使用されている Secure Agent に対して実行されたジョブの数を示します。グラフにカーソルを合わせると、ステータスに応じてジョブが表示されます。過去 24 時間または過去 7 日間のデータを表示するように選択することができます。

【詳しいグラフ】をクリックして、選択した期間中に、選択した Secure Agent によって処理されたデータの行数と実行されたジョブの数を表示します。

上位ターゲットと上位ソース

【上位ターゲット】パネルには、組織内で最も頻繁に使用されている 5 つの接続によって書き込まれたデータ行のサマリが表示されます。【トップソース】パネルを表示するには、メニューから【ソース】を選択します。【トップソース】パネルには、組織内で最も頻繁に使用されている 5 つの接続によって読み取られたデータ行のサマリが表示されます。過去 24 時間または過去 7 日間のデータを表示するように選択することができます。

【上位ターゲット】または【上位ソース】パネルで【詳しいグラフ】をクリックして、書き込みまたは読み取りされたデータの合計行数に関する分析と、選択した期間中に、選択したコネクタに対して実行されたジョブの数を表示します。

上位プロジェクトと上位フォルダ

【上位プロジェクト】パネルには、組織内の上位 5 つのプロジェクトで実行されたジョブのサマリが表示されます。グラフにカーソルを合わせると、ステータスに応じてジョブが表示されます。【上位フォルダ】パネルを表示するには、メニューから【フォルダ】を選択します。過去 24 時間または過去 7 日間のデータを表示するように選択することができます。

【上位プロジェクト】パネルまたは【上位フォルダ】パネルで【詳しいグラフ】をクリックして、選択した期間中に、選択したオブジェクトに対して読み取られた合計行数と実行されたジョブに関する分析を表示します。

データボリューム

1 時間ごとに処理される行の週ごとのサマリを表示します。次のような期間のデータを表示できます。

- 1 週間（実際）
- 2 週間（平均）
- 1 か月（平均）

グラフにカーソルを合わせると、その日時に関するジョブ情報が表示されます。1 週間の実際のデータを表示した場合は、その期間に完了したジョブの詳細を表示できます。矩形をクリックして、ジョブの詳細を表示します。

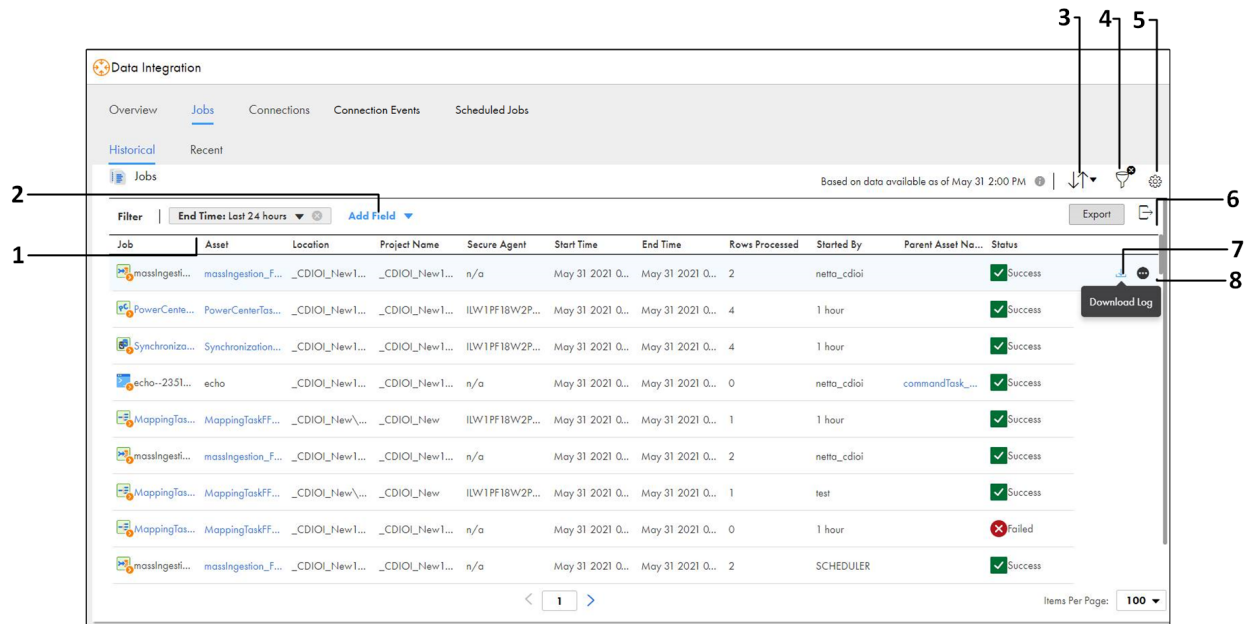
1 週間の実際のデータを表示した場合は、過去 1 か月の実際のデータを表示するように切り替えることができます。デフォルトは月の最初の週です。

データ統合ジョブの表示

【データ統合】ページの【ジョブ】タブをクリックして、組織で実行されたジョブの詳細を表示します。【ジョブ】タブは、完了したジョブを表示する【履歴】パネルと、現在実行中のジョブと最近完了したジョブを表示する【最新】パネルに分かれています。【ログのダウンロード】をクリックすると、ジョブのセッションログがダウンロードされます。

【履歴】パネル

次の図は、【履歴】パネルを示しています。



1. 期間を変更します。本日、過去 24 時間、または先週実行されたジョブを表示するか、カスタム範囲を入力できます。
2. 新しいフィルタを追加します。
3. ページ上のジョブをソートします。開始時刻または終了時刻でソートすることができます。
4. フィルタを追加または削除します。
5. 【設定】ウィンドウを開きます。
6. 【エクスポート】パネルを開きます。最大 10,000 行のジョブデータをエクスポートできます。
7. セッションログのダウンロード。
8. アラートの作成。

タスクに子ジョブが含まれている場合、オペレーションインサイトでは、親ジョブと子ジョブが別々のジョブとして一覧で表示されます。例えば、動的マッピングタスクに 3 つのジョブが含まれているとします。オペレーションインサイトでは、動的マッピングタスクと 3 つのジョブが【ジョブ】タブに一覧で表示されます。子ジョブに関する情報を表示するには、【ジョブ】タブでジョブ名をクリックします。【履歴】パネルから親ジョブの詳細を表示した場合、親ジョブの詳細には子ジョブに関する情報は表示されません。

【履歴】パネルには、タスクフローとリニアタスクフローの子ジョブが表示されますが、親ジョブは表示されません。

デフォルトでは、【履歴】パネルには、過去 24 時間以内に完了したジョブが表示されます。【終了時刻】フィルタを編集して、過去 1 時間から過去 30 日間までに完了したジョブを表示できます。以下のようなフィルタを適用できます。

- アセット

- アセットタイプ
- 終了時刻
- 場所
- 親アセット名
- プロジェクト名
- ランタイム環境
- 開始したユーザー名
- ステータス
- Secure Agent

デフォルトでは、ジョブごとに次のプロパティが表示されます。

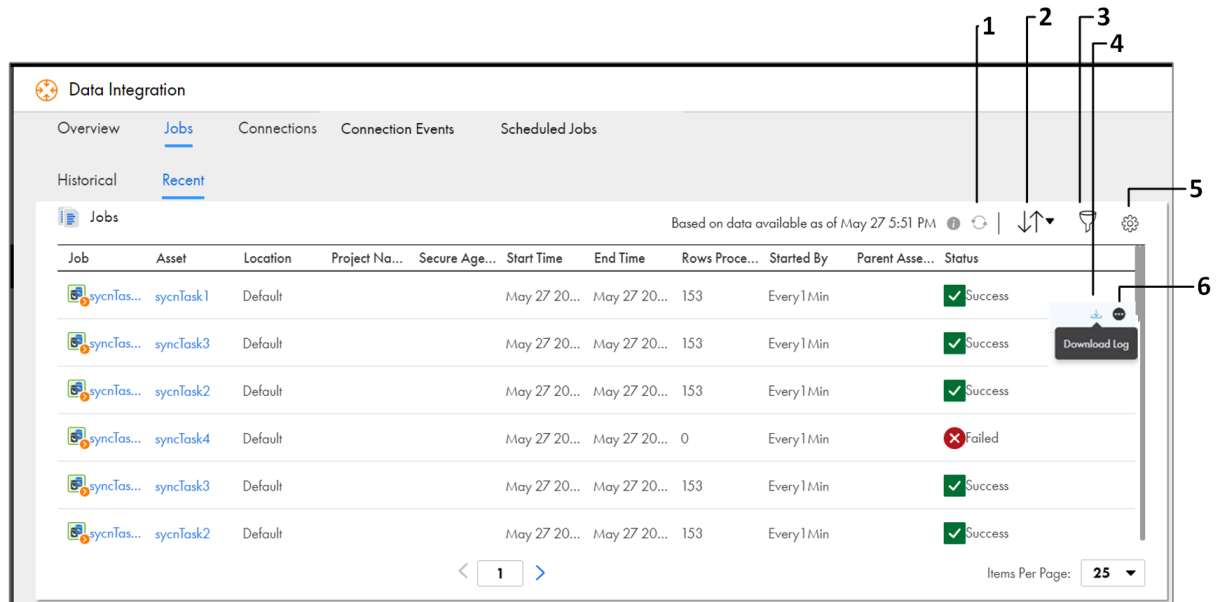
- ジョブ
- アセット
- 場所
- プロジェクト名
- Secure Agent
- 開始時刻
- 終了時刻
- 処理済みの行数
- 開始したユーザー名
- 親アセット名
- ステータス

カラムの見出し領域を右クリックして次のフィルタのいずれかを選択すると、追加のプロパティを表示できます。

- アセットタイプ
- サブタスク
- ランタイム環境
- 継続時間
- 成功した行
- 失敗した行
- 開始するユーザー名
- エラーメッセージ

[最新] パネル

以下の図は、[最新] パネルを示しています。



1. ジョブを現在のステータスに更新します。
2. ページ上のジョブをソートします。開始時刻または終了時刻でソートすることができます。
3. フィルタを追加または削除します。
4. セッションログのダウンロード。
5. [設定] ウィンドウを開きます。
6. アラートの作成。

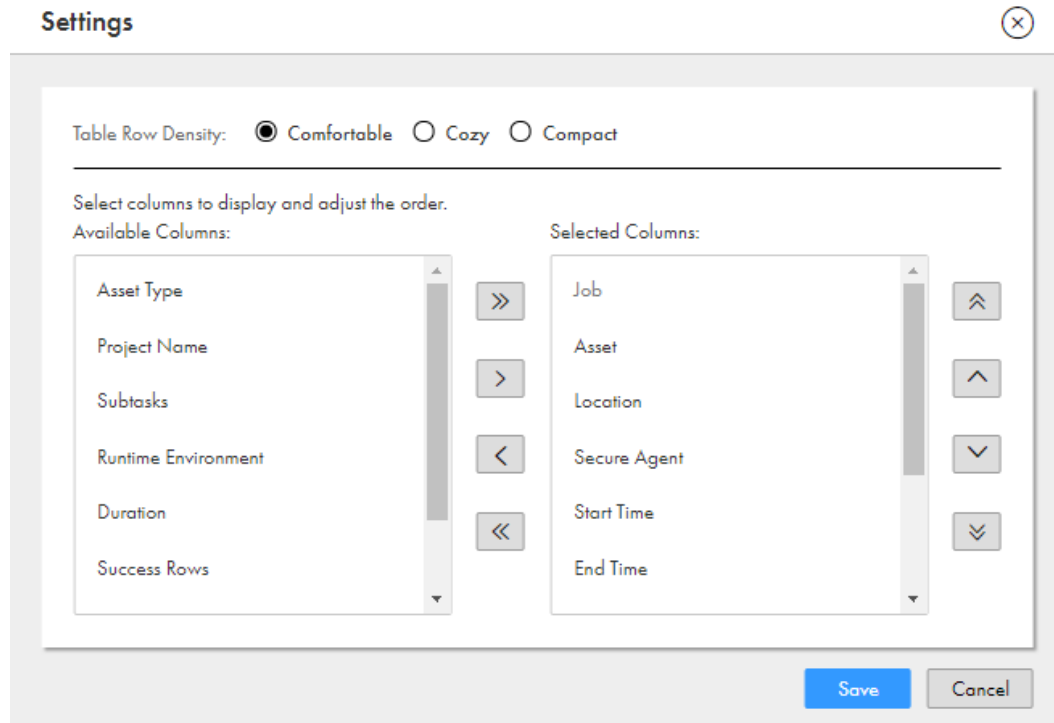
タスクまたはタスクフローに子ジョブが含まれている場合、オペレーションインサイトでは、親ジョブと子ジョブが別々のジョブとして一覧で表示されます。例えば、動的マッピングタスクに3つのジョブが含まれているとします。オペレーションインサイトでは、動的マッピングタスクと3つのジョブが[ジョブ]タブに一覧で表示されます。子ジョブに関する情報を表示するには、[ジョブ]タブまたは親ジョブの詳細ページでジョブ名をクリックします。

[ジョブ] ページの設定

[設定] ウィンドウで、[ジョブ] ページのプロパティとレイアウトを設定します。次のログイン時にこの設定がそのまま使用されます。

[設定] ウィンドウを開くには、[ジョブ] ページの **[設定]** をクリックします。

次の画像は【設定】ウィンドウを示しています。



次の表に、調整が可能な設定を示します。

設定	説明
[ジョブ] テーブル行密度	各行の高さとエントリ間のスペースを調整します。 以下の密度を選択することができます。 - 十分。最大の行の高さ。 - 適度。中程度の行の高さ。 - コンパクト。最小の行の高さ。
使用可能なカラム	【ジョブ】 ページに表示するカラムを決定します。 カラム名を選択し、左右の矢印を使用して【選択したカラム】 領域内または領域外に移動します。
カラム順序	選択したカラムを、【ジョブ】 ページに表示する順序に並べ替えます。 カラム名を選択し、上下の矢印を使用してカラムの位置を調整します。

ページ設定が完了したら、【保存】 をクリックします。

ジョブデータのエクスポート

【ジョブ】 ページの【履歴】 パネルからジョブデータを CSV ファイルにエクスポートします。ジョブデータをエクスポートすると、オペレーションインサイトは、現在のページフィルタが適用されたデータをエクスポートします。データをエクスポートした後に、ファイルをダウンロードするか、添付ファイルとして電子メールで送信できます。

1. 【エクスポート】 をクリックします。
2. 【ジョブデータのエクスポート】 ウィンドウで、ファイル名を入力します。

3. **【エクスポート】** をクリックします。
4. エクスポートジョブの詳細を表示するには、**【エクスポート】** パネルでファイル名をクリックします。
【エクスポートジョブの詳細】 ページには、エクスポートジョブのプロパティとフィルタ条件に関する情報が表示されます。
5. ファイルをダウンロードするには、次のいずれかのアクションを実行します。
 - **【エクスポート】** パネルで、**【ダウンロード】** をクリックします。
 - **【エクスポートジョブの詳細】** ページで、**【ダウンロード】** をクリックします。
6. ファイルを電子メールで送信するには、**【エクスポート】** パネルで **【電子メール】** をクリックします。
オペレーションインサイトは、Informatica Intelligent Cloud Services アカウントに関連付けられた電子メールアドレスにファイルを送信します。
メールが受信ボックスに表示されない場合は、スパムフォルダを確認してください。

特定のジョブの詳細の表示

特定のジョブをドリルダウンして、ジョブに関する詳細を表示し、セッションログをダウンロードできます。

ジョブの詳細を表示するには、**【ジョブ】** カラムでジョブ名をクリックします。

次の図は、マッピングタスクのジョブの詳細を示しています。

Job Properties

Asset:	MappingTaskFF_FF
Instance ID:	1159
Asset Type:	Mapping Task
Started By:	test
Start Time:	May 31, 2021, 12:30:21 PM
End Time:	May 31, 2021, 12:30:36 PM
Duration:	15 seconds
Runtime Environment:	ILW1PF18W2PM-11
Secure Agent:	ILW1PF18W2PM_changed

Results

Status:	Success
Success Rows:	1
Error Rows:	0
Error Message:	
Session Log:	Download Session Log

Individual Source/Target Results

Name	Success Rows	Error Rows	Error Message
Source	1	0	
tgt_cdioi_test_txt	1	0	

Navigation: < 1 > Items Per Page: 25

【結果】 領域の **【セッションログのダウンロード】** をクリックして、ジョブのセッションログをダウンロードします。

ジョブがタスクフロー、動的マッピングタスク、またはレプリケーションタスクによって開始されたものである場合は、タスクフローまたはタスクに関する詳細を表示できます。**【ジョブのプロパティ】** 領域でタスクフローまたはタスク名をクリックします。

次の図は、レプリケーションタスクの詳細を示しています。

Job Properties		Results	
Asset:	Account	Status:	✓ Success
Instance ID:	8	Success Rows:	734
Asset Type:	Replication Task	Error Rows:	0
Stop on Error:	Cancel processing the remaining objects	Error Message:	No errors encountered.
Started By:	ReplicationTask_salesforceWithEmailNotification-8	Session Log:	Download Session Log
Start Time:	May 31, 2021, 02:10:46 PM		
End Time:	May 31, 2021, 02:11:13 PM		
Duration:	27 seconds		
Runtime Environment:	ILW1PF18W2PM-i1		
Secure Agent:	ILW1PF18W2PM_changed		
Individual Source/Target Results			
Name	Success Rows	Error Rows	Error Message
SQL_Account	734	0	
SF52_ACCOUNT_csv	734	0	

ジョブが失敗した場合、[インサイト] 領域には、エラーの解決に役立つドキュメントへのリンクが表示されません。

次の図は、[インサイト] 領域を示しています。

▼ Insights(5)

ERROR: "FR_3000 Error opening file [C:\Twitter Connection\Src_Twitter.csv]. Operating system error message [The system cannot find the path specified.], every 2nd run"

... fails with the error FR_3000 Error opening file [C:\Twitter Connection\Src_Twitter, ... Operating system error message [The system cannot find the path specified.], every second run and the ...

[View Article on Informatica Network](#)

ERROR: "FR_3000 Error opening file [.\dummy_data.csv]. Operating system error message [The system cannot find the file specified.]" when running a task which has saved Query as source in Informatica Cloud

... dummy_data_csv' and can be noticed in the session log instead of the actual query Secure agent is unable to access SQ_dummy_data_csv file or the file is not available in the desired location.

[View Article on Informatica Network](#)

"FR_3000 Error opening file [<path of lookup file>]. Operating system error message [The system cannot find the path specified.]" for an DSS task with mapplet having Lookup transformation in Informatica Cloud

Operating system error message [The system cannot find the path specified.] This errors occurs when the mapplet used by the DSS task contains a Lookup transformation, and the lookup file does ...

[View Article on Informatica Network](#)

"FR_3000 Error opening file [filepath]. Operating system error message [The system cannot find the path specified.]" while using a Flat File connection for a DSS task in Informatica Cloud

... Service (DSS) task, the following error message is displayed: FR_3000 Error opening file [filepath]. ... Operating system error message [The system cannot find the path specified.]

[View Article on Informatica Network](#)

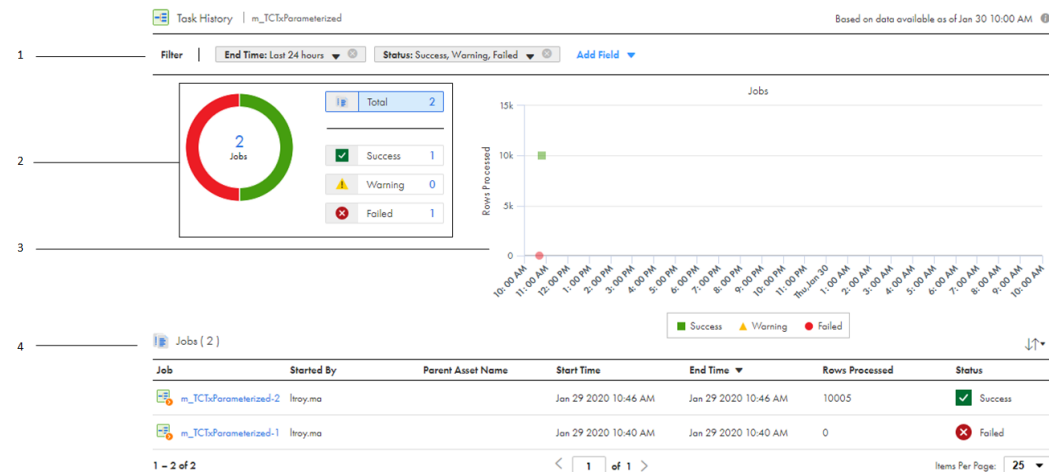
エラー修復の推奨事項を表示するには、適切なライセンスが必要です。

特定のアセットのジョブ履歴の表示

特定のマッピングまたはタスクのジョブ履歴を表示できます。[ジョブ履歴] ページを使用して、実行時間や完了ステータスなどのジョブ実行の分析を表示します。

アセットのジョブ履歴を表示するには、[ジョブ] タブでアセット名をクリックします。[ジョブ履歴] ページには、マッピングまたはタスクの各インスタンスに関する詳細が表示されます。

次の図に、【履歴】 ページを示します。



1. 終了時刻またはステータスでページをフィルタリングします。過去 24 時間または過去 7 日間のデータを表示できます。
次のような追加のフィルタを適用できます。

- ランタイム環境
- 開始したユーザー名

2. 特定のステータスのジョブを表示するには、ステータスをクリックします。
3. ジョブの行情報を表示するには、グラフ上のポイントにカーソルを合わせます。
4. ジョブインスタンス。ジョブリストは、開始時刻または終了時刻でソートすることができます。
デフォルトでは、【ジョブ】 領域には、各ジョブに対する次のようなプロパティが表示されます。

- ジョブ
- 開始したユーザー名
- 親アセット名
- 開始時刻
- 終了時刻
- 処理済みの行数
- ステータス

カラムの見出し領域を右クリックして、次のような追加のプロパティを表示することができます。

- プロジェクト
- サブタスク
- ランタイム環境
- 継続時間
- 成功した行
- 失敗した行
- エラーメッセージ

5. ジョブの【ジョブの詳細】 ページを表示するには、【ジョブ】 領域でジョブ名をクリックします。

データ統合接続の表示

【接続】タブをクリックして、組織内の接続の分析を表示します。

接続にアクセスするたびに、オペレーションインサイトでは、接続の詳細が【接続】タブに記録されます。タブの情報は1時間ごとに更新されます。

オペレーションインサイトは、コネクタの種類に基づいて組織内の接続をグループ化します。オペレーションインサイトの【コネクタタイプ】領域には、各タイプのアクティブな接続の数と非アクティブな接続の数が表示されます。過去33日間に、少なくとも1つのジョブを実行するためにアクティブな接続が使用されました。過去33日間に、ジョブの実行に非アクティブな接続は使用されませんでした。

デフォルトでは、オペレーションインサイトには、組織で最も頻繁に使用されるコネクタタイプの詳細が表示されます。特定のタイプの接続に関する詳細を表示するには、【コネクタタイプ】領域でコネクタタイプをクリックします。コネクタタイプをもう一度クリックすると選択が解除され、過去24時間にアクセスがあったすべての接続の詳細を確認できます。

一度に最大16個のコネクタタイプを表示できます。表示するコネクタタイプを選択するには、【さらに表示】をクリックします。

フィルタを適用して、特定のランタイム環境での接続、または特定のSecure Agentを使用する接続を表示できます。

次の図は、フラットファイル接続を表示するようにフィルタリングされた【接続】タブを示しています。

Connection	Connector	Runtime Environment	Secure Agent	Last Accessed	Rows Read	Rows Written
FF_test	Flat File	envh7cdasag23.informatica.com	envh7cdasag23.informatica.com	Jun 15 2022 06:31 AM	12	16
FF_test	Flat File	envh7cdasag23.informatica.com	envh7cdasag23.informatica.com	Jun 15 2022 05:31 AM	12	16
FF_test	Flat File	envh7cdasag23.informatica.com	envh7cdasag23.informatica.com	Jun 15 2022 04:31 AM	24	762
FF_test	Flat File	envh7cdasag23.informatica.com	envh7cdasag23.informatica.com	Jun 15 2022 03:31 AM	12	16
FF_test	Flat File	envh7cdasag23.informatica.com	envh7cdasag23.informatica.com	Jun 15 2022 02:31 AM	12	16
FF_test	Flat File	envh7cdasag23.informatica.com	envh7cdasag23.informatica.com	Jun 15 2022 01:31 AM	12	16
FF_test	Flat File	envh7cdasag23.informatica.com	envh7cdasag23.informatica.com	Jun 15 2022 12:31 AM	24	762
FF_test	Flat File	envh7cdasag23.informatica.com	envh7cdasag23.informatica.com	Jun 14 2022 11:31 PM	12	16
FF_test	Flat File	envh7cdasag23.informatica.com	envh7cdasag23.informatica.com	Jun 14 2022 10:31 PM	12	16
FF_test	Flat File	envh7cdasag23.informatica.com	envh7cdasag23.informatica.com	Jun 14 2022 09:31 PM	12	16
FF_test	Flat File	envh7cdasag23.informatica.com	envh7cdasag23.informatica.com	Jun 14 2022 08:31 PM	24	762
FF_test	Flat File	envh7cdasag23.informatica.com	envh7cdasag23.informatica.com	Jun 14 2022 07:31 PM	12	16

データ統合の接続イベントの表示

【接続イベント】タブをクリックして、組織内の接続イベントのレポートをダウンロードおよび表示します。

オペレーションインサイトが接続イベントをトリガするたびに、オペレーションインサイトでは、【接続イベント】タブにイベントの詳細が記録されます。

デフォルトでは、【接続イベント】タブには、アクセスがあった時間に応じて、接続の作成、更新、および削除が一覧で表示されます。ビューをフィルタリングして、選択したイベントタイプ、接続名、またはユーザー名のイベントを表示することができます。

適用するフィルタに従って、接続イベントのレポートをエクスポートできます。最大10,000件のイベントをエクスポートできます。

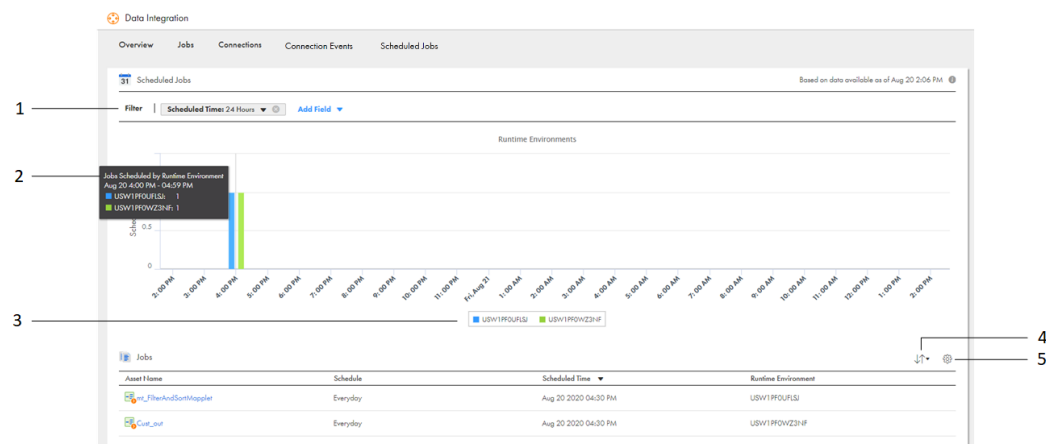
次の図は、更新イベントを表示するようにフィルタリングされた【接続イベント】タブを示しています。

Connection Name	Event Type	Event Time	User Name
Amazon RedShift test	Update	Feb 24 2022 02:48 PM	cdioi_qa-rel
Amazon RedShift test	Update	Feb 24 2022 02:48 PM	cdioi_qa-rel
Amazon RedShift test	Update	Feb 24 2022 02:48 PM	cdioi_qa-rel
Amazon RedShift test	Update	Feb 24 2022 02:48 PM	cdioi_qa-rel
Amazon RedShift test	Update	Feb 24 2022 02:48 PM	cdioi_qa-rel
Amazon RedShift test	Update	Feb 24 2022 02:48 PM	cdioi_qa-rel
Amazon RedShift test	Update	Feb 24 2022 02:48 PM	cdioi_qa-rel

スケジュール済みのジョブの表示

【データ統合】ページの【スケジュール済みのジョブ】タブをクリックして、組織内のスケジュール済みのジョブを表示します。【スケジュール済みのジョブ】タブには、選択したタイムフレームにおける各ランタイム環境の1時間あたりのスケジュール済みのジョブ数のグラフが表示されます。また、選択したタイムフレーム内の各ジョブの詳細も表示されます。

次の図は、【スケジュール済みのジョブ】タブを示しています。



1. ページをフィルタリングします。タイムフレーム、ランタイム環境、またはスケジュールごとにフィルタリングできます。
2. グラフにカーソルを合わせると、スケジュールされたジョブに関する詳細情報が表示されます。
3. ランタイム環境をクリックして、グラフ上で表示または非表示にします。
4. スケジュールされた時間でジョブテーブルをソートします。
5. テーブルの行密度を調整します。

ジョブの詳細を表示するには、ジョブ名をクリックします。

データ統合アラート

データ統合ジョブのアラート通知を送信するようにオペレーションインサイトを設定できます。組織内の特定のジョブのアラートを設定します。

例えば、プロジェクト内のマッピングタスクが 5 分以上実行されている場合に通知するようにアラートを設定することができます。または、順序データをターゲットにロードするタスクが失敗したときにアラートを受信するようにすることもできます。

アラートを設定するには、管理者またはオペレータユーザーロール、またはオペレーションインサイトのデータ統合ジョブアラート特権を持つカスタムユーザーロールが必要です。

以下のデータ統合アセットのアラートを設定できます。

- マッピングタスク
- 同期タスク
- 動的マッピングタスク
- データ転送タスク
- レプリケーションタスク
- PowerCenter タスク
- リニアタスクフロー

次のようなイベントに対するアラートを設定できます。

- ジョブが指定された状態にある場合。
- ジョブの期間が設定可能なしきい値を超えた場合。
- 処理された行数が設定可能なしきい値を超えた場合。
- エラー行数が設定可能なしきい値を超えた場合。

アラートの送信時に次のアクションを実行するようにオペレーションインサイトを設定することもできます。

- 指定したユーザーまたはユーザーグループに電子メールを送信する。
- 失敗したジョブを再開する。
- 実行中のジョブを停止する。

オペレーションインサイトは、組織内での最初の 1 時間あたり 550 件、1 日あたり 4000 件、および 1 週間あたり 28000 件のアラートに対して電子メールアラートを送信します。オペレーションインサイトが送信するアラートの最大数を変更するには、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。

データ統合ジョブのアラートの設定

【データ統合アラート】タブで、データ統合ジョブのアラートを設定します。

1. 【アラートの作成】をクリックします。
2. アラートの詳細を設定します。
 - a. アラートをすぐに有効化しない場合は、アラートを無効にします。
 - b. アラートの名前を入力します。必要に応じて、アラートの説明を入力します。

- c. アラートの範囲を設定します。次のいずれかのアクションを実行します。
 - アラートをタスクに適用するには、**【タスクアセット】**を選択してから**【選択...】**をクリックします。アセットを選択して**【選択】**をクリックします。
 - プロジェクトまたはフォルダにアラートを適用するには、**【プロジェクトまたはフォルダ】**を選択してから**【選択...】**をクリックします。プロジェクトまたはフォルダを選択し、**【選択】**をクリックします。
3. アラート条件を設定します。
4. アラートの電子メール通知を受信する Informatica Intelligent Cloud Services ユーザーまたはユーザーグループの名前を入力します。

サブスクライブしているサブ組織からアラートメールを受信するには、サブ組織にユーザーを作成します。サブ組織のユーザーにアラートメールを送信するようにオペレーションインサイト設定します。
5. アラート条件に基づいて、他のアラートアクションを設定します。
6. **【保存】**をクリックします。

第 5 章

Informatica Intelligent Cloud Services アプリケーション統合の監視

組織がアプリケーション統合を使用している場合は、オペレーションインサイトを使用してアプリケーション統合アセットの分析を表示できます。アプリケーション統合アセットをオペレーションインサイトで監視するには、組織にアプリケーション統合ライセンスがあり、アプリケーション統合メトリックの表示ができる環境である必要があります。

オペレーションインサイトは、アプリケーション統合アセットのステータスと使用状況をすばやく視覚的に評価し、必要に応じて適切な対処方法を実行するために役立つ複数のグラフを提供します。API 呼び出し、プロセス、接続、およびライセンスに関連する分析を表示できます。グラフのデータは 10 分ごとに更新されます。アプリケーション統合の使用に関する詳細については、アプリケーション統合のヘルプを参照してください。

アプリケーション統合の分析を表示するには、オペレーションインサイトサービスを開き、オペレーションインサイトのナビゲーションバーにある **【アプリケーション統合】** をクリックします。

注: Informatica は、アプリケーション統合用のオペレーションインサイトのサポートを段階的に導入しています。オペレーションインサイトは、まず地域ごとに導入し、次にご要望に応じて特定の顧客に対して順次有効化します。そして最終的に、すべてのアプリケーション統合の顧客に対して広く使用可能となります。広範なリリースの前にオペレーションインサイトとアプリケーション統合の併用を希望される場合は、カスタマサクセスマネージャにお問い合わせください。

アプリケーション統合アセットの全体的な使用状況と健全性の表示

【アプリケーション統合】 ページの **【概要】** タブをクリックして、全体的な分析を表示し、アプリケーション統合アセットの使用状況と健全性を評価します。

次のようなメトリックについてのインサイトを確認できます。

- 完了済みおよびフォールトプロセスの数
- 受信 API 呼び出しの数
- 全体の API 応答時間
- API 応答時間が平均 API 応答時間を超えるプロセス
- 組織で実行中の上位 10 のプロセス

注:【概要】タブは、複数のメトリックグラフを表示するプロセスパネルに分かれています。グラフでは、ライフサイクルの任意の時点で中断されたプロセスが除外されます。

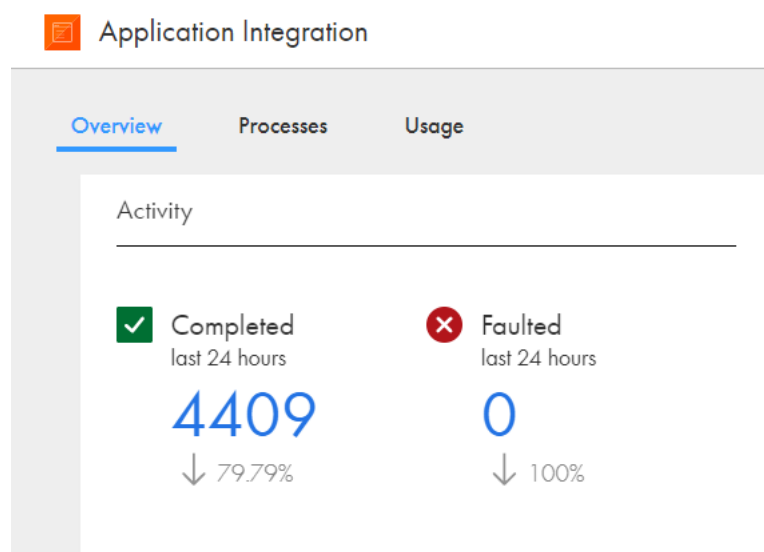
次のパネルを使用して、アプリケーション統合アセットの全体的な使用状況と健全性を表示できます。

アクティビティ

【アクティビティ】パネルには、過去 24 時間に組織内で完了済みおよびフォールトプロセスの合計数が表示されます。このパネルには、最後の期間以降の完了済みおよびフォールトプロセスの数の増減率も表示されます。

【アクティビティ】パネルを使用して、フォルトトレンドが増加傾向か減少傾向かを評価できます。

以下の図は、【アクティビティ】パネルを示しています。

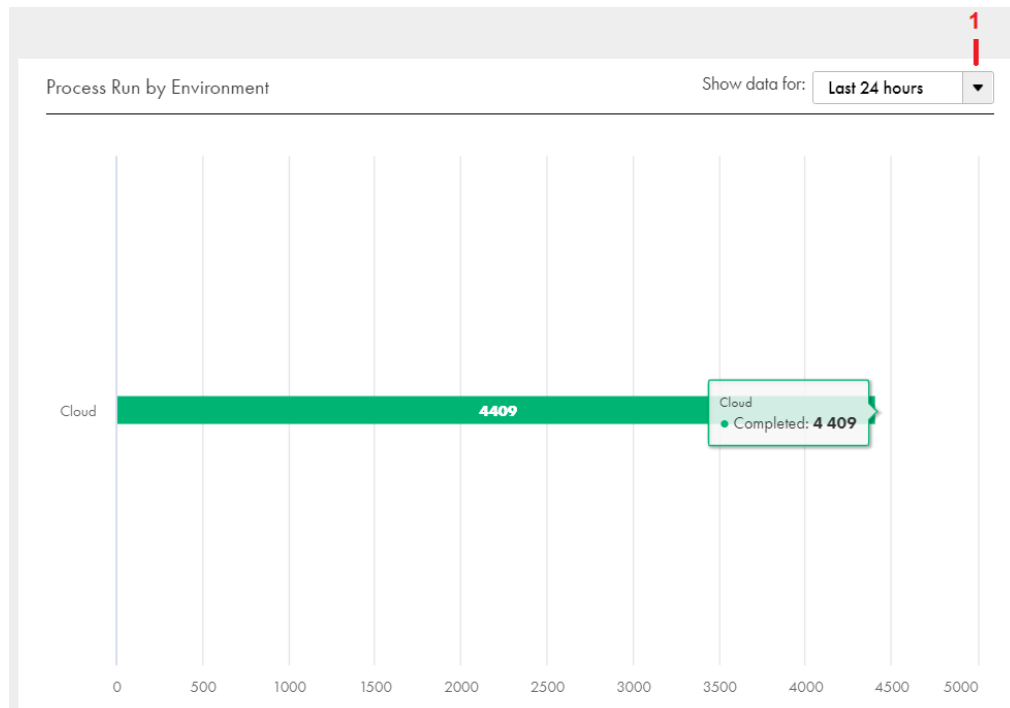


環境ごとのプロセス実行

【環境ごとのプロセス実行】パネルには、すべてのランタイム環境について、組織内で完了済みおよびフォールトプロセス実行の合計数が表示されます。デフォルトでは、パネルには過去 24 時間の情報が表示されます。

【環境ごとのプロセス実行】パネルを使用して、ランタイム環境間でロードバランシングを実行する必要があるかどうかを評価できます。

次の図は、【環境ごとのプロセス実行】パネルを示しています。



1. リストから、プロセス実行の数を表示する期間を選択します。次の値から選択することができます。

- 過去 24 時間
- 最近 7 日
- 最近 30 日

グラフのバーにカーソルを合わせると、選択した期間におけるすべてのランタイム環境のプロセス実行の数が表示されます。完了済みプロセス実行は緑色で表示され、フォールトプロセス実行は赤色で表示されます。

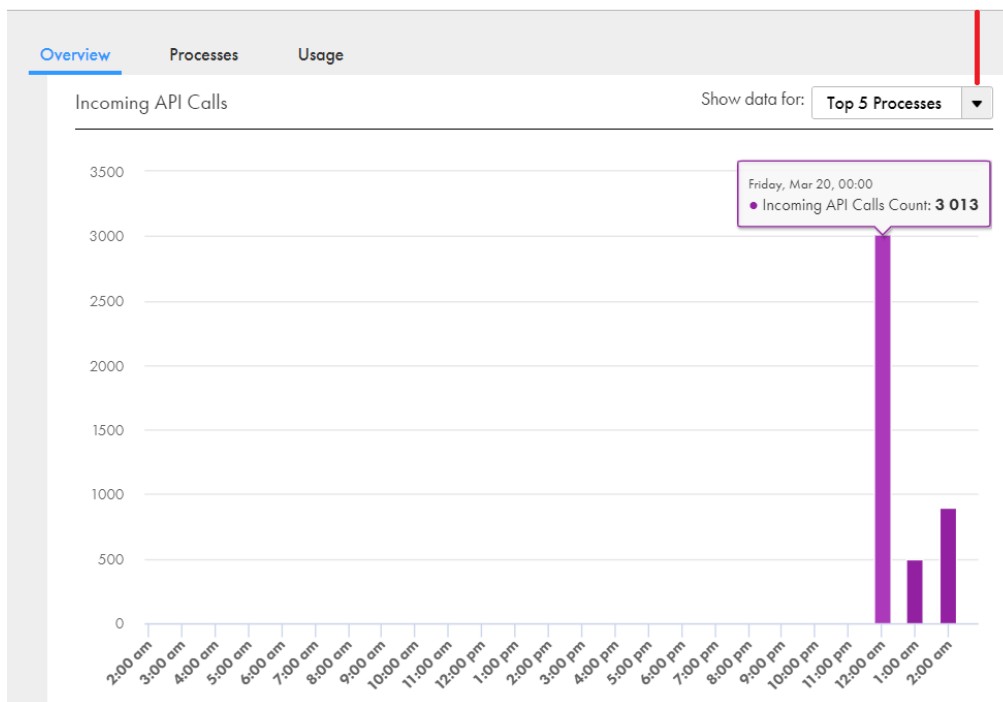
受信 API 呼び出し

【受信 API 呼び出し】 パネルには、過去 24 時間の 1 時間ごとの受信 API 呼び出しの数が表示されます。この数には、スケジュールされたプロセスおよびイベントベースのプロセスからの受信 API 呼び出しも含まれます。デフォルトでは、このパネルには受信 API 呼び出しが最も多い上位 5 つのプロセスが表示されます。

【受信 API 呼び出し】 パネルは、次のようなタスクに使用できます。

- 受信トラフィックを測定し、ピーク時とオフピーク時間を特定する。
- システムメンテナンスを実行する最適な時期を特定する。

次の図は、**【受信 API 呼び出し】** パネルを示しています。



1. リストから、受信 API 呼び出しの時間別の数を表示するプロセスまたはプロセスカテゴリを選択します。次の値から選択することができます。

- すべてのプロセス
- 上位 5 件のプロセス
- 下位 5 件のプロセス
- 特定のプロセス

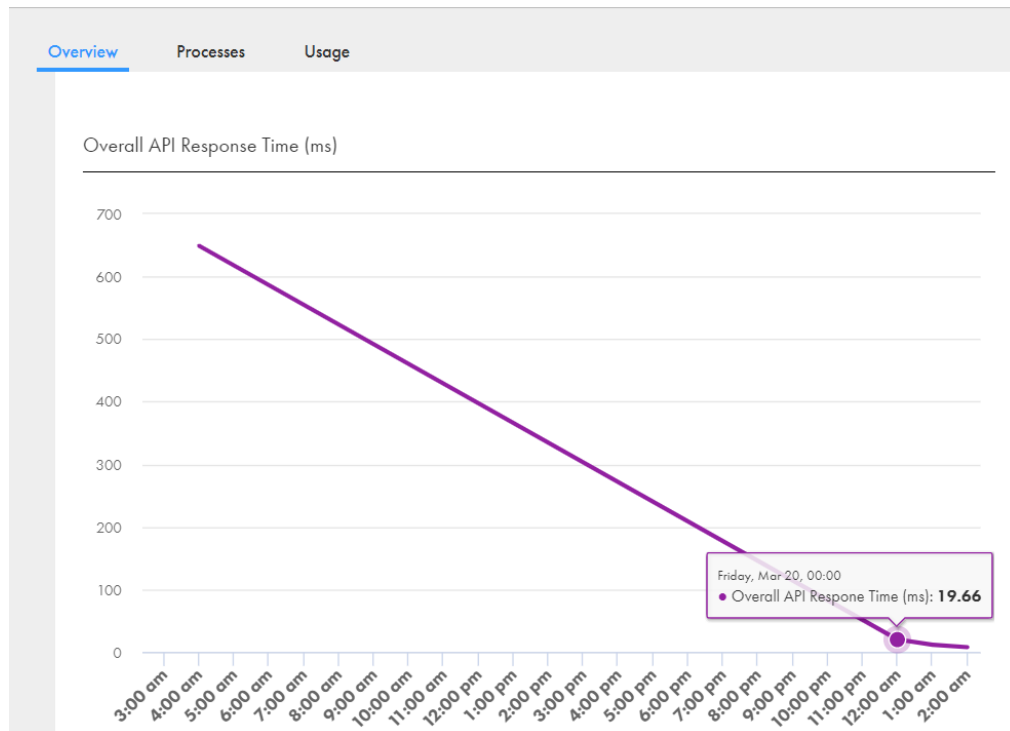
グラフのバーにカーソルを合わせると、受信 API 呼び出しの数が時間別に表示されます。

全体の API 応答時間

【**全体の API 応答時間**】パネルには、すべての完了済みおよびフォールトプロセス、および組織内のすべてのランタイム環境の全体の API 応答時間がミリ秒単位で表示されます。

全体の API 応答時間の増加は、これらの API で使用されている複雑な統合またはサードパーティの接続性の低下によって、パフォーマンスが低下していることを示しています。

次の図は、【**全体の API 応答時間**】パネルを示しています。



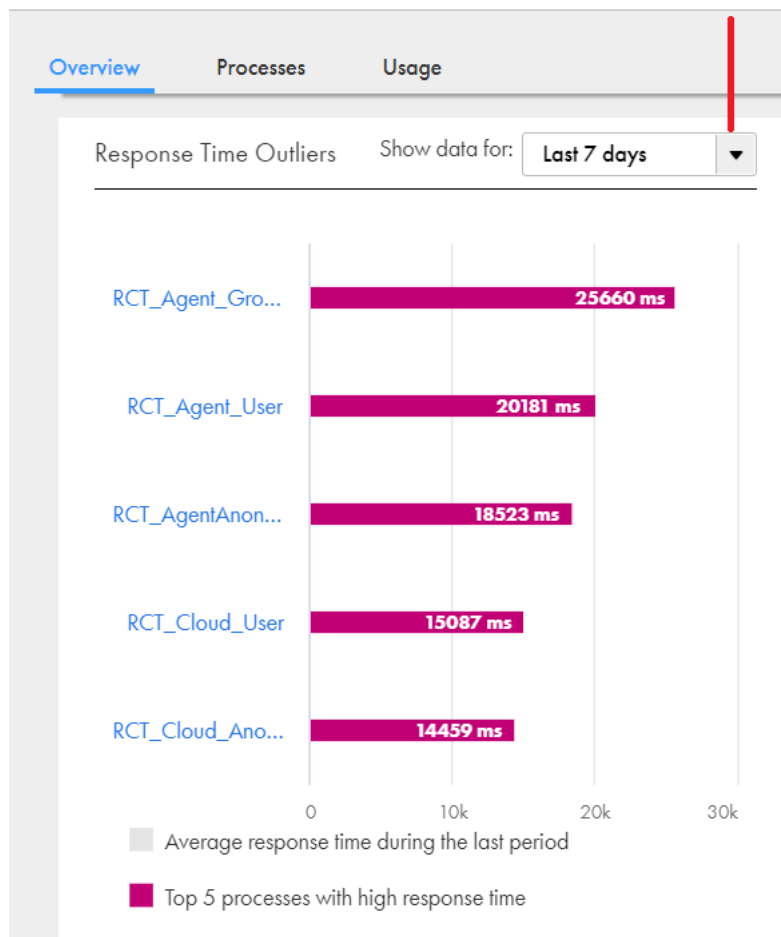
グラフのトレンド線の点にカーソルを合わせると、全体の API 応答時間がミリ秒単位で表示されます。

応答時間の異常値

【応答時間の異常値】 パネルには、選択した期間の API 応答時間が平均 API 応答時間よりも長い、組織内の上位 5 つの完了済みプロセスとフォールトプロセスが表示されます。デフォルトでは、このパネルには過去 7 日間の情報が表示されます。

API 応答時間が平均 API 応答時間よりも長いプロセスは、統合が複雑である可能性があります。最後の期間の平均 API 応答時間に対する値の比較は、最後の期間以降のプロセスの実行状況を評価する場合に役立ちます。

次の図は、**【応答時間の異常値】** パネルを示しています。



1. リストから、応答の異常値を表示する期間を選択します。次の値から選択することができます。

- 過去 24 時間
- 最近 7 日
- 最近 30 日

グラフのバーにカーソルを合わせると、プロセスの API 応答時間と、選択した期間の平均 API 応答時間が表示されます。

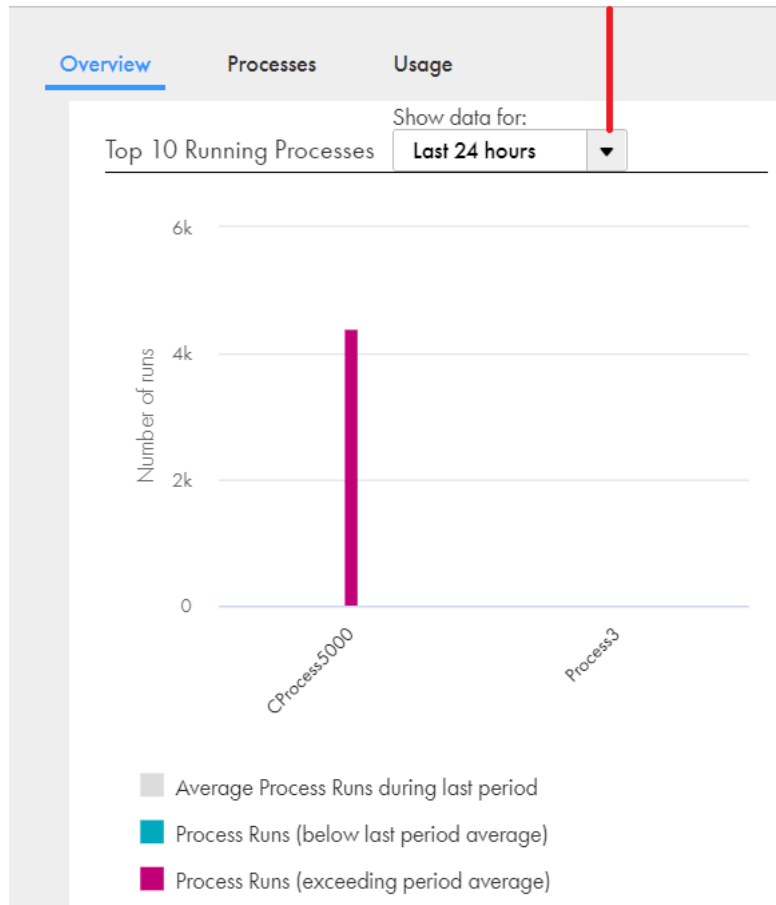
上位 10 件の実行中プロセス

【上位 10 件の実行中プロセス】 パネルには、実行数が最も多い、組織内の上位 10 件の完了済みプロセスとフォールトプロセスが表示されます。デフォルトでは、パネルには過去 24 時間の情報が表示されます。

【上位 10 件の実行中プロセス】 パネルを使用して、他のプロセスよりも適切な最適化が必要な組織内の重要なプロセスを特定できます。また、このパネルには、現在の期間と比較した最後の期間のプロセス実行の平均数が表示され、トレンドが示されます。

次の図は、【上位 10 件の実行中プロセス】 パネルを示しています。

Application Integration



1. リストから、上位 10 件の実行中のプロセスを表示する期間を選択します。次の値から選択することができます。

- 過去 24 時間
- 最近 7 日
- 最近 30 日

グラフのバーにカーソルを合わせると、現在の期間のプロセス実行の数と最後の期間の平均プロセス実行の数が表示されます。棒グラフの色分けを理解するには、次のガイドラインを使用してください。

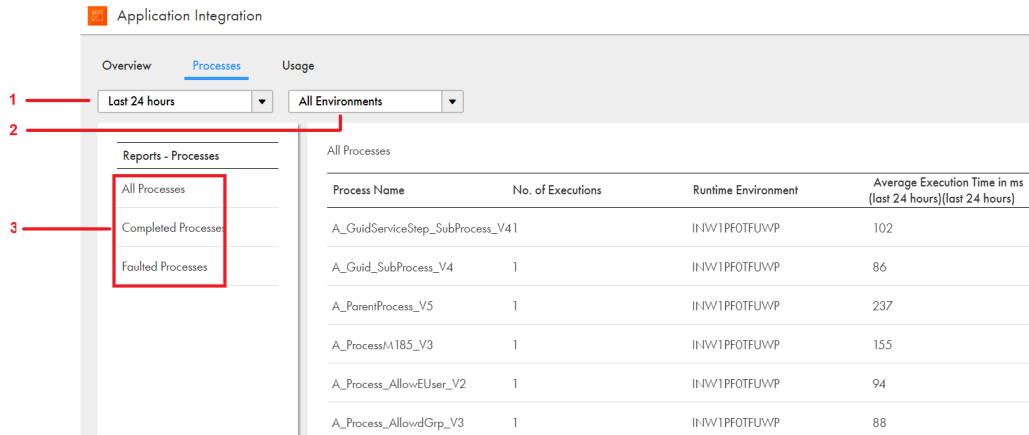
- 灰色のバーは、最後の期間のプロセス実行の平均数を示します。
- ピンク色のバーは、現在のプロセス実行の数が前の期間の平均を上回っていることを示します。
- 青いバーは、現在のプロセス実行の数が最後の期間の平均を下回っていることを示します。

注: 選択した期間に組織で実行されたプロセスが 10 件未満である場合、グラフに表示されるバーは 10 未満になります。

アプリケーション統合プロセスレポートの表示

【アプリケーション統合】ページの【プロセス】タブをクリックして、組織で実行されたプロセスのステータスと詳細に関するレポートを表示します。

次の図は、【プロセス】ページを示しています。



デフォルトでは、【プロセス】ページには、過去 24 時間のすべてのランタイム環境において、組織内で実行されたすべてのプロセスが表示されます。

1. リストから、プロセスレポートを表示する期間を選択します。次の値から選択することができます。

- 過去 24 時間
- 最近 7 日
- 最近 30 日
- 3 か月以内

2. リストから、プロセスレポートを表示するランタイム環境を選択します。次の値から選択することができます。

- すべての環境
- 特定のランタイム環境
- Cloud のみ
- すべてのエージェント

3. 左ペインで、プロセスレポートを表示するカテゴリを選択します。すべてのプロセス、完了済みプロセス、またはフォールトプロセスを表示できます。

プロセスごとに次のような詳細が表示されます。

- プロセス名
- 実行回数
- プロセスが実行されたランタイム環境
- プロセスの平均実行時間（ミリ秒）

アプリケーション統合アセットの使用状況の監視

【アプリケーション統合】ページの【使用状況】タブをクリックして、アプリケーション統合アセットの使用状況を監視します。API 呼び出し、プロセス、接続、およびライセンスに関連する分析を表示できます。

受信 API 呼び出しの表示

【使用状況】タブの下にある【API】タブをクリックして、API 呼び出しに関連する分析を表示します。日次および累積受信 API 呼び出しの数を表示し、プロセスおよびランタイム環境に基づく受信 API 呼び出しの数を分析することもできます。この数には、スケジュールされたプロセスおよびイベントベースのプロセスからの受信 API 呼び出しも含まれます。

【API】タブのパネルには、親プロセスからの API 呼び出しのみが表示され、サブプロセスからの API 呼び出しは表示されません。このパネルでは、ライフサイクルの任意の時点で中断されたプロセスが除外されます。

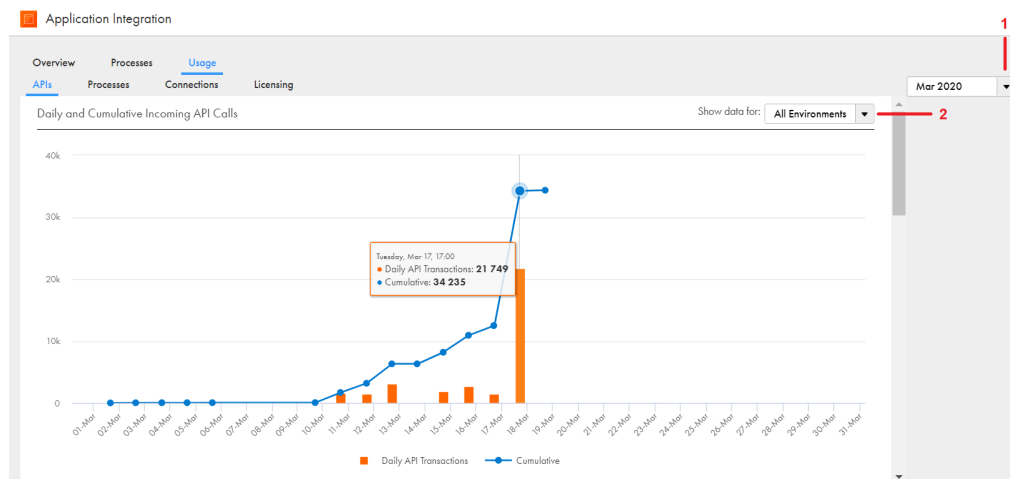
次のパネルを使用して、受信 API 呼び出しの分析を表示できます。

日次および累積受信 API 呼び出し

【日次および累積受信 API 呼び出し】パネルには、日次および累積受信 API 呼び出しの数が表示されます。デフォルトでは、このパネルには当月の情報と、すべてのランタイム環境の情報が表示されます。

【日次および累積受信 API 呼び出し】パネルを使用して、受信 API 呼び出しの急増または減少があるかどうかを評価し、それに応じてピークトラフィックの計画を行うことができます。

次の図は、【日次および累積受信 API 呼び出し】パネルを示しています。



1. リストから、日次および累積受信 API 呼び出しを表示する月を選択します。現在の月または過去 2 か月のいずれかを選択できます。

2. リストから、日次および累積受信 API 呼び出しを表示するランタイム環境またはランタイム環境のカテゴリを選択します。次の値から選択することができます。

- すべての環境
- 特定のランタイム環境
- Cloud のみ

- すべてのエージェント

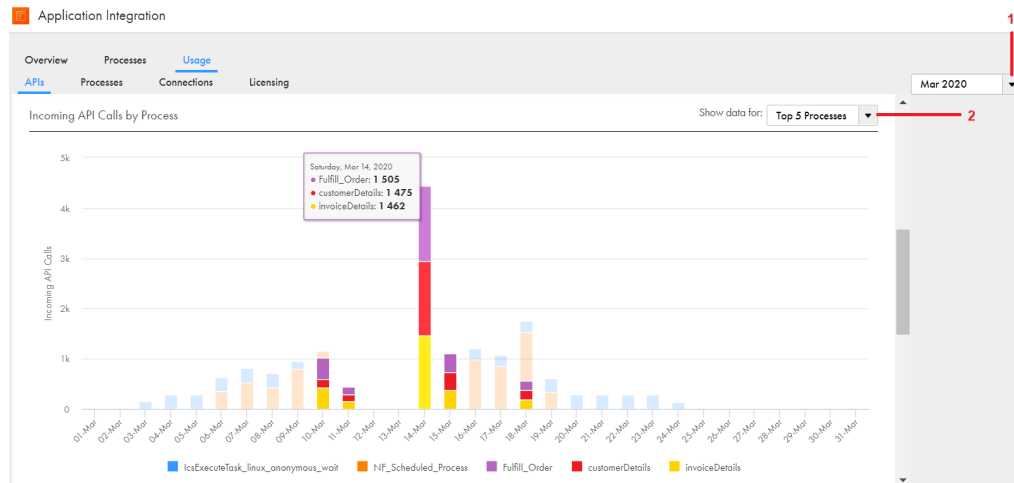
グラフのトレンド線のバーまたは点にカーソルを合わせると、日次および累積受信 API 呼び出しの数が表示されます。

プロセスごとの受信 API 呼び出し

【プロセスごとの受信 API 呼び出し】パネルには、選択したプロセスまたはプロセスカテゴリの日次受信 API 呼び出しの数が表示されます。デフォルトでは、このパネルには当月の情報と、受信 API 呼び出しが最も多い上位 5 つのプロセスが表示されます。

【プロセスごとの受信 API 呼び出し】パネルを使用して、他のプロセスよりも適切な最適化が必要な重要なプロセスを見つけることができます。

次の図は、【プロセスごとの受信 API 呼び出し】パネルを示しています。



1. リストから、日次受信 API 呼び出しを表示する月を選択します。現在の月または過去 2 か月のいずれかを選択できます。

2. リストから、日次受信 API 呼び出しの数を表示するプロセスまたはプロセスカテゴリを選択します。次の値から選択することができます。

- すべてのプロセス
- 上位 5 件のプロセス
- 下位 5 件のプロセス
- 特定のプロセス

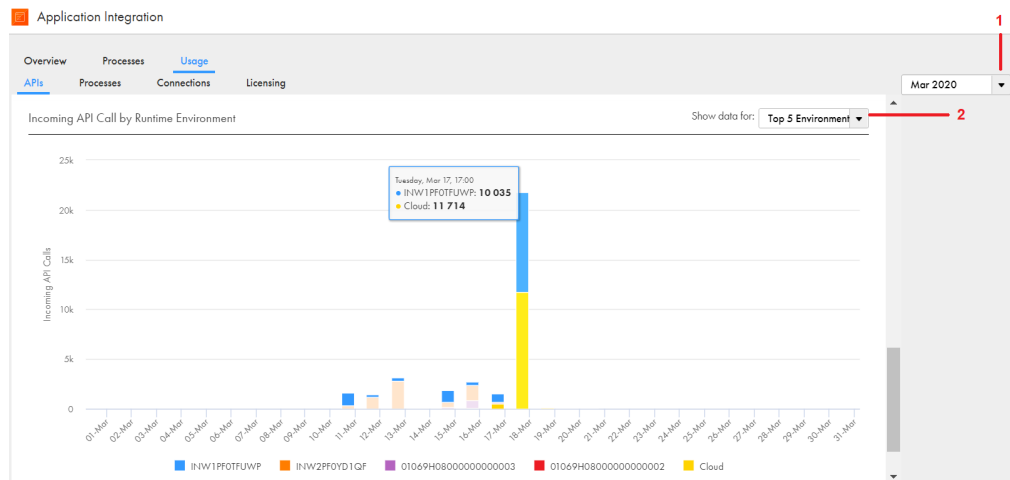
グラフのバーにカーソルを合わせると、指定したプロセスまたはプロセスカテゴリの日次受信 API 呼び出しの数が表示されます。

ランタイム環境ごとの受信 API 呼び出し

【ランタイム環境ごとの受信 API 呼び出し】パネルには、選択したランタイム環境またはランタイム環境カテゴリの日次受信 API 呼び出しの数が表示されます。デフォルトでは、このパネルには当月の情報と、受信 API 呼び出しが最も多い上位 5 つのランタイム環境が表示されます。

【ランタイム環境ごとの受信 API 呼び出し】パネルを使用して、さまざまなランタイム環境の負荷を評価し、負荷分散を実行したり、Secure Agent の容量を増やしたりすることができます。

次の図は、【ランタイム環境ごとの受信 API 呼び出し】パネルを示しています。



1. リストから、日次受信 API 呼び出しを表示する月を選択します。現在の月または過去 2 か月のいずれかを選択できます。

2. リストから、日次受信 API 呼び出しを表示するランタイム環境またはランタイム環境のカテゴリを選択します。次の値から選択することができます。

- すべての環境
- 上位 5 件の環境
- 下位 5 件の環境
- 特定のランタイム環境
- Cloud のみ
- すべてのエージェント

グラフのバーにカーソルを合わせると、日次受信 API 呼び出しの数がランタイム環境別に表示されます。

アプリケーション統合プロセスの実行の表示

【使用状況】 タブの下にある **【プロセス】** タブをクリックして、プロセスの実行に関連する分析を表示します。日次および累積プロセス実行、特定のプロセスの実行の数、および特定のランタイム環境で実行されたプロセスの数を表示できます。

【プロセス】 タブのパネルには、親プロセスおよびサブプロセスのメトリックが表示されます。このパネルでは、ライフサイクルの任意の時点で中断されたプロセスが除外されます。

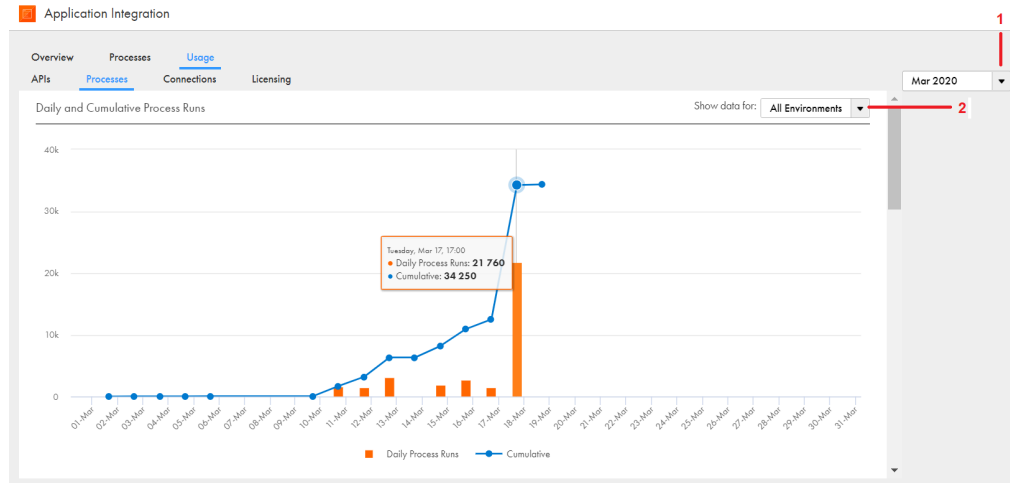
次のパネルを使用して、プロセス実行の分析を表示できます。

日次および累積プロセス実行

【日次および累積プロセス実行】 パネルには、日次および累積プロセスおよびサブプロセス実行の数が表示されます。デフォルトでは、このパネルには当月の情報と、すべてのランタイム環境の情報が表示されます。

【日次および累積プロセス実行】 パネルを使用して、プロセスおよびサブプロセスの実行の数に急増または減少があるかどうかを評価し、それに応じてピークトラフィックの計画を行うことができます。

次の図は、【日次および累積プロセス実行】パネルを示しています。



1. リストから、プロセス実行を表示する月を選択します。現在の月または過去 2 か月のいずれかを選択できます。

2. リストから、プロセス実行を表示するランタイム環境またはランタイム環境カテゴリを選択します。次の値から選択することができます。

- すべての環境
- 特定のランタイム環境
- Cloud のみ
- すべてのエージェント

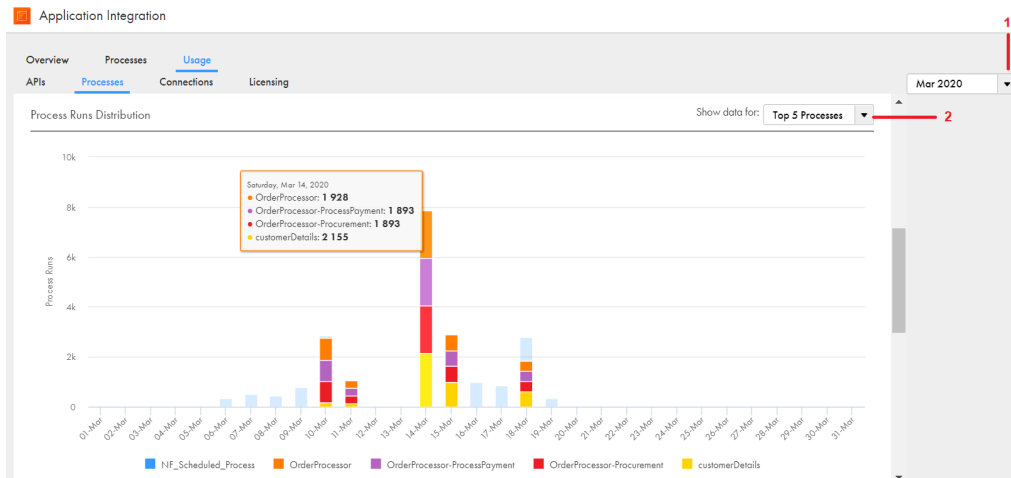
グラフのトレンド線のバーまたはポイントにカーソルを合わせると、日次および累積プロセス実行の数が表示されます。

プロセス実行分散

【プロセス実行分散】 パネルには、選択したプロセスまたはプロセスカテゴリの日次プロセスおよびサブプロセスの実行の数が表示されます。デフォルトでは、このパネルには当月の情報と、実行回数が最も多い上位 5 つのプロセスが表示されます。

【プロセス実行分散】 パネルを使用して、他のプロセスよりも適切な最適化が必要な重要なプロセスを見つけることができます。

次の図は、【プロセス実行分散】 パネルを示しています。



1. リストから、日次プロセス実行の数を表示する月を選択します。現在の月または過去 2 か月のいずれかを選択できます。

2. リストから、日次プロセス実行の数を表示するプロセスまたはプロセスカテゴリを選択します。次の値から選択することができます。

- すべてのプロセス
- 上位 5 件のプロセス
- 下位 5 件のプロセス
- 特定のプロセス

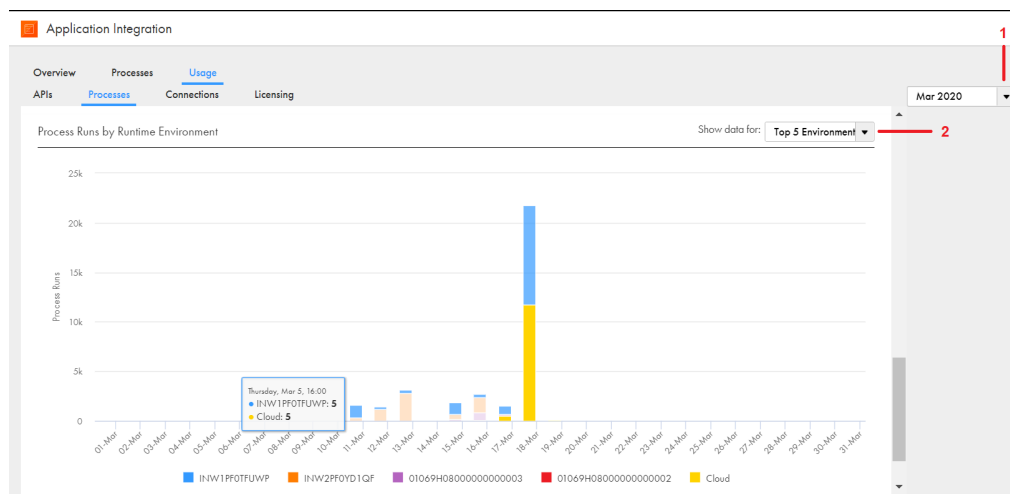
グラフのバーにカーソルを合わせると、指定したプロセスまたはプロセスカテゴリの日次プロセス実行の数が表示されます。

ランタイム環境ごとのプロセス実行

【ランタイム環境ごとのプロセス実行】 パネルには、選択したランタイム環境またはランタイム環境カテゴリの日次プロセスおよびサブプロセスの実行の数が表示されます。デフォルトでは、このパネルには当月の情報と、プロセス実行が最も多い上位 5 つのランタイム環境が表示されます。

【ランタイム環境ごとのプロセス実行】 パネルを使用して、さまざまなランタイム環境の負荷を評価し、負荷分散を実行したり、Secure Agent の容量を増やしたりすることができます。

次の図は、**【ランタイム環境ごとのプロセス実行】** パネルを示しています。



1. リストから、日次プロセス実行の数を表示する月を選択します。現在の月または過去 2 か月のいずれかを選択できます。

2. リストから、日次プロセス実行の数を表示するランタイム環境またはランタイム環境カテゴリを選択します。次の値から選択することができます。

- すべての環境
- 上位 5 件の環境
- 下位 5 件の環境
- 特定のランタイム環境
- Cloud のみ
- すべてのエージェント

グラフのバーにカーソルを合わせると、日次プロセス実行の数がランタイム環境別に表示されます。

アプリケーション統合の接続呼び出しの表示

【使用状況】 タブの下にある【接続】 タブをクリックして、接続に関連する分析を表示します。実行された日次および累積接続呼び出しの数を表示して、さまざまなエンドポイント、接続タイプ、およびランタイム環境に対して実行された接続呼び出しの数を分析することもできます。

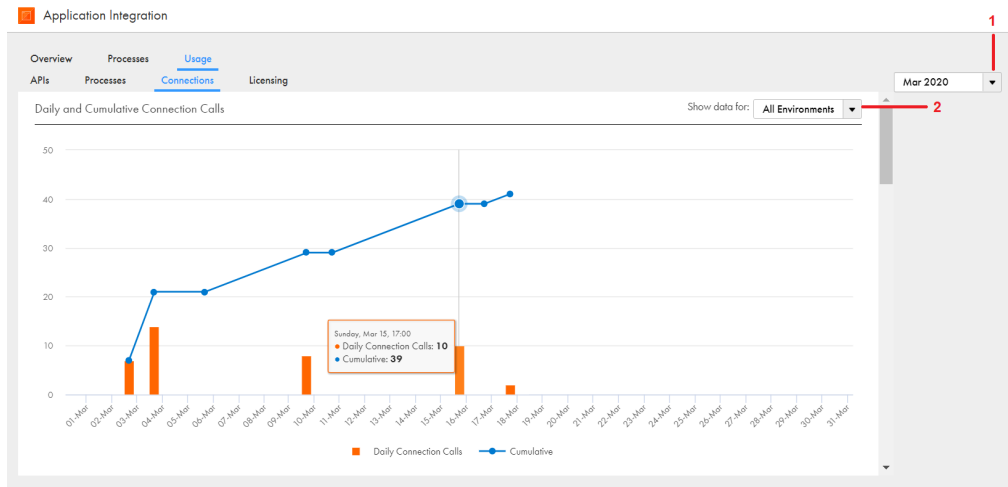
次のパネルを使用して、接続呼び出しの分析を表示できます。

日次および累積接続呼び出し

【日次および累積接続呼び出し】 パネルには、日次および累積接続呼び出しの数が表示されます。デフォルトでは、このパネルには当月の情報と、すべてのランタイム環境の情報が表示されます。

【日次および累積接続呼び出し】 パネルを使用して、接続の使用状況を把握できます。

次の図は、【日次および累積接続呼び出し】 パネルを示しています。



1. リストから、日次および累積接続呼び出しの数を表示する月を選択します。現在の月または過去 2 か月のいずれかを選択できます。

2. リストから、日次および累積接続呼び出しの数を表示するランタイム環境またはランタイム環境のカテゴリを選択します。次の値から選択することができます。

- すべての環境
- 特定のランタイム環境
- Cloud のみ
- すべてのエージェント

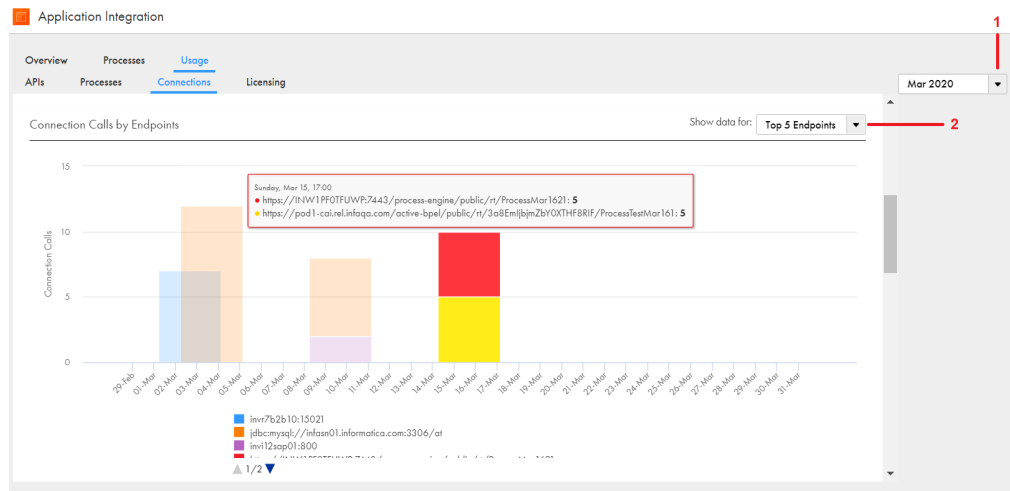
グラフのトレンド線のバーまたは点にカーソルを合わせると、日次および累積接続呼び出しの数が表示されます。

エンドポイントごとの接続呼び出し

【エンドポイントごとの接続呼び出し】 パネルには、選択したエンドポイントまたはエンドポイントカテゴリの日次接続呼び出しの数が表示されます。デフォルトでは、このパネルには当月の情報と、組織内の上位 5 つのエンドポイントが表示されます。

【エンドポイントごとの接続呼び出し】 パネルを使用して、最も頻繁に使用される接続エンドポイントを見つけることができます。

次の図は、【エンドポイントごとの接続呼び出し】 パネルを示しています。



1. リストから、日次接続呼び出しの数を表示する月を選択します。現在の月または過去 2 か月のいずれかを選択できます。

2. リストから、日次接続呼び出しの数を表示するエンドポイントまたはエンドポイントカテゴリを選択します。次の値から選択することができます。

- すべてのエンドポイント
- 上位 5 件のエンドポイント
- 下位 5 件のエンドポイント
- 特定のエンドポイント

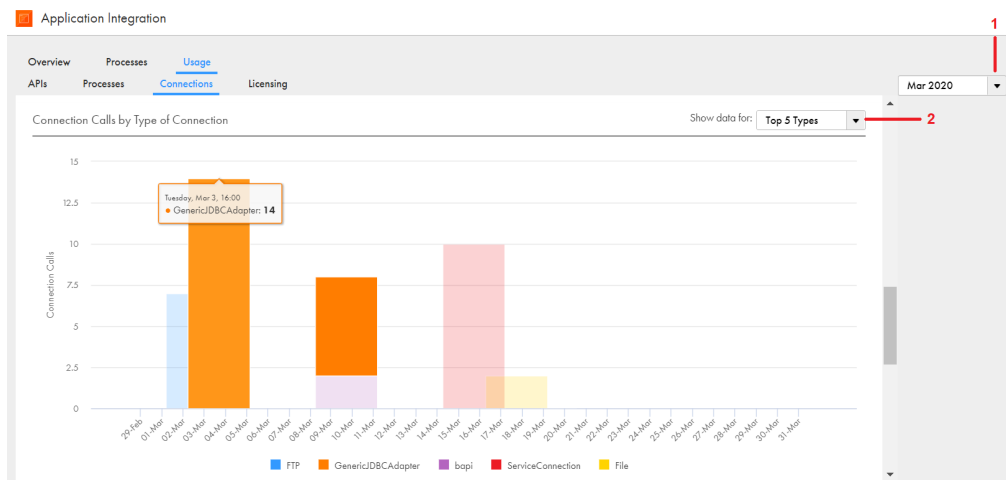
グラフのバーにカーソルを合わせると、指定したエンドポイントまたはエンドポイントカテゴリの日次プロセス実行の数が表示されます。

接続タイプごとの接続呼び出し

【接続タイプごとの接続呼び出し】 パネルには、選択した接続の日次接続呼び出しの数が表示されます。デフォルトでは、このパネルには当月の情報と、接続呼び出しが最も多い上位 5 つの接続タイプが表示されます。

【接続タイプごとの接続呼び出し】 パネルを使用して、最も頻繁に使用される接続タイプを見つけることができます。これは、オンプレミスシステムまたはクラウドベースのシステムに対して行われた接続呼び出しが多いかどうかを評価する場合に役立ちます。

次の図は、【接続タイプごとの接続呼び出し】 パネルを示しています。



1. リストから、日次接続呼び出しの数を表示する月を選択します。現在の月または過去 2 か月のいずれかを選択できます。

2. リストから、日次接続呼び出しの数を表示する接続タイプを選択します。次の値から選択することができます。

- すべてのタイプ
- 上位 5 件のタイプ
- 下位 5 件のタイプ
- 特定の接続タイプ

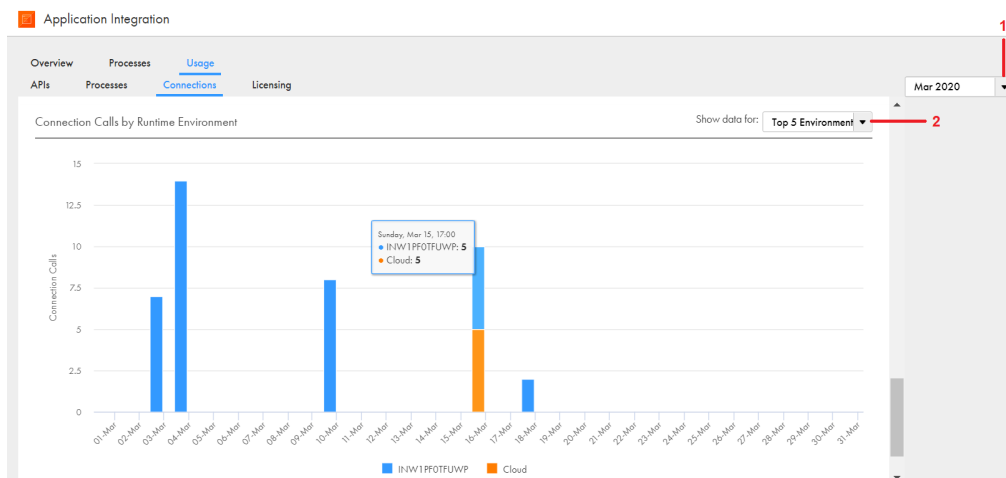
グラフのバーにカーソルを合わせると、日次接続呼び出しの数が接続タイプ別に表示されます。

ランタイム環境ごとの接続呼び出し

【ランタイム環境ごとの接続呼び出し】パネルには、選択したランタイム環境またはランタイム環境カテゴリの日次接続呼び出しの数が表示されます。デフォルトでは、このパネルには当月の情報と、接続呼び出しが最も多い上位 5 つのランタイム環境が表示されます。

【ランタイム環境ごとの接続呼び出し】パネルを使用して、さまざまなランタイム環境の負荷を評価し、負荷分散が必要かどうかを判断できます。

次の図は、【ランタイム環境ごとの接続呼び出し】パネルを示しています。



1. リストから、日次接続呼び出しの数を表示する月を選択します。現在の月または過去 2 か月のいずれかを選択できます。

2. リストから、日次接続呼び出しの数を表示するランタイム環境またはランタイム環境カテゴリを選択します。次の値から選択することができます。

- すべての環境
- 上位 5 件の環境
- 下位 5 件の環境
- 特定のランタイム環境
- Cloud のみ
- すべてのエージェント

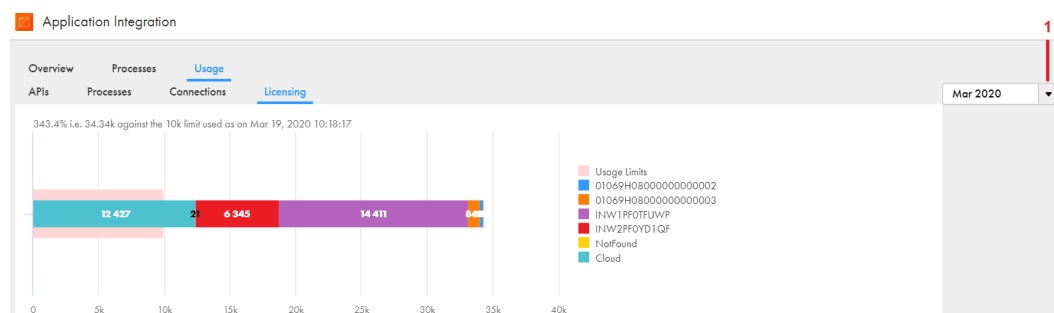
グラフのバーにカーソルを合わせると、日次接続呼び出しの数がランタイム環境別に表示されます。

ライセンス制限に対する API トランザクションの表示

【使用状況】 タブの下にある【ライセンス】 タブをクリックして、組織内のすべてのランタイム環境の API トランザクションの合計数が、アプリケーション統合ライセンスの Administrator で定義された最大 API トランザクション数に収まっているか、または超えているかどうかを評価します。

API トランザクションの合計数が、定義された最大 API トランザクション数を超えている場合は、その差がグラフにパーセンテージ値で表示されます。許可された最大制限を超えている場合、コストに影響する可能性があります。

次の図のグラフは、各ランタイム環境の API トランザクションの総数を示しており、2020 年 3 月 19 日の時点で API トランザクションの総数がライセンス制限を 343.4% 超えていることを示しています。



1. リストから、API トランザクションの数を表示する月を選択します。現在の月または過去 2 か月のいずれかを選択できます。

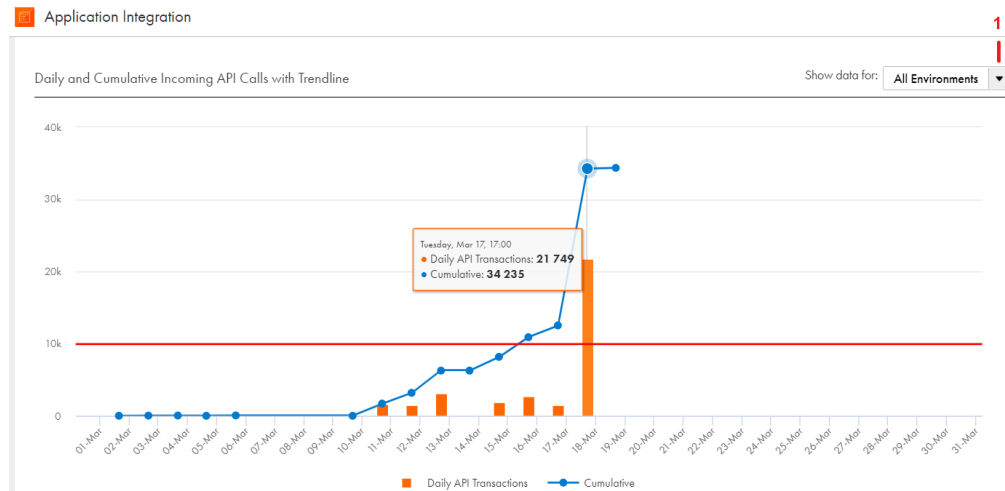
次のパネルを使用して、API トランザクション制限に対する日次および累積受信 API 呼び出しを表示できます。

日次および累積受信 API 呼び出しとトレンド線

【日次および累積受信 API 呼び出しとトレンド線】 パネルには、選択したランタイム環境またはランタイム環境カテゴリの日次および累積受信 API 呼び出しの数が表示されます。この数には、スケジュールされたプロセスおよびイベントベースのプロセスからの受信 API 呼び出しも含まれます。【日次および累積受信 API 呼び出しとトレンド線】 パネルは、API 呼び出しの合計数を、Administrator でアプリケーション

統合ライセンスに定義された最大 API トランザクション数と比較する場合に役立ちます。デフォルトでは、このパネルには当月の情報と、すべてのランタイム環境の情報が表示されます。

次の図は、[日次および累積受信 API 呼び出しとトレンド線] パネルを示しています。



1. リストから、日次および累積受信 API 呼び出しの数を表示するランタイム環境またはランタイム環境のカテゴリを選択します。次の値から選択することができます。

- すべての環境
- 特定のランタイム環境
- Cloud のみ
- すべてのエージェント

特定の月の日次および累積受信 API 呼び出しの数を表示するには、上にスクロールして、ページの右上部分に表示されるリストから月を選択します。現在の月または過去 2 か月のいずれかを選択できます。

グラフのトレンド先のバーまたはポイントにカーソルを合わせると、日次および累積受信 API 呼び出しの数が表示され、API トランザクションの制限と比較されます。グラフの赤い線は、アプリケーション統合ライセンスの Administrator で定義された最大 API トランザクション数を示しています。赤い線より上に伸びているポイントとバーは異常値です。

第 6 章

Informatica Intelligent Cloud Services データプロファイリングの監視

組織でデータプロファイリングを使用している場合は、オペレーションインサイトを使用して、データプロファイリングタスクのジョブステータスを表示できます。

データプロファイリングの使用に関する詳細については、データプロファイリングのヘルプを参照してください。

オペレーションインサイトでデータプロファイリングジョブを監視するには、データプロファイリングおよびオペレーションインサイトにアクセスする必要があります。また、オペレーションインサイト - 表示特権が必要です。

詳細について、またはこの機能をリクエストする場合は、Informatica グローバルカスタマサポートにお問い合わせください。

データプロファイリングサービスジョブの表示

組織で実行されたジョブの詳細を表示するには、左側のナビゲーションバーにある【データプロファイリング】をクリックします。

次の図は、【データプロファイリング】ページを示しています。

Instance Name	Location	Subtask	Start Time	End Time	Rows Processed	Status
x1 - run - 2-4	Default	2	Feb 24, 2020, 10:50:33 PM	Feb 24, 2020, 10:50:43 PM		Failed
q1-3	Default	1	Feb 24, 2020, 10:47:58 PM	Feb 24, 2020, 10:48:04 PM	0	Success
Profile_varifier - run - 2-3	Default	2	Feb 24, 2020, 10:35:25 PM	Feb 24, 2020, 10:35:35 PM		Failed
Outlier - Profile_varifier - ru...	Default	1	Feb 24, 2020, 10:34:41 PM	Feb 24, 2020, 10:34:44 PM	0	Success
Profile_varifier - run - 1-1	Default	4	Feb 24, 2020, 10:33:08 PM	Feb 24, 2020, 10:34:40 PM	1	Success
Outlier - x1 - run - 1-2	Default	1	Feb 24, 2020, 10:05:37 AM	Feb 24, 2020, 10:05:48 AM	0	Success
x1 - run - 1-1	Default	4	Feb 24, 2020, 10:04:00 AM	Feb 24, 2020, 10:05:34 AM	84020	Success

1. 期間を変更します。過去 24 時間、先週、先月、昨年に実行されたジョブを表示するか、カスタム範囲を入力できます。
2. 新しいフィルタを追加します。
3. ページ上のジョブをソートします。
4. フィルタを追加または削除します。
5. ジョブを検索します。

デフォルトでは、【ジョブ】ページには、過去 24 時間以内に完了したジョブが表示されます。フィルタを適用して、過去 30 日間に完了したジョブを表示することができます。以下のようなフィルタを適用できます。

- インスタンス名
- アセット名
- プロジェクト
- サブタスク
- ランタイム環境
- 開始時刻
- 終了時刻
- 継続時間
- 処理済みの行数
- 開始したユーザー名
- ステータス

デフォルトでは、各ジョブに対して次のプロパティが表示されます。

- インスタンス名
- プロジェクト

- サブタスク
- 開始時刻
- 終了時刻
- 処理済みの行数
- ステータス

カラムの見出し領域を右クリックして、次のような追加のプロパティを表示することもできます。

- アセット名
- ランタイム環境
- Secure Agent
- 更新時刻
- 継続時間
- 開始するユーザー名
- エラーメッセージ

データプロファイリングの特定のジョブの詳細の表示

特定のジョブをドリルダウンして、ジョブの詳細とサブタスクを表示できます。

[インスタンス名] カラムのインスタンス名をクリックして、**[ジョブの詳細]** ページを開きます。

次の図は、データプロファイリングタスクの **[ジョブの詳細]** ページを示しています。

The screenshot shows the 'Job Properties' page for a Data Profiling task. The top section displays job details:

- Instance Name: x1 - run - 6-13
- Asset Name: x1
- Asset Type: Data Profiling Task
- Started By: thor through UI
- Start Time: Feb 25, 2020, 01:06:49 AM
- End Time: Feb 25, 2020, 01:08:13 AM
- Duration: 00:01:24
- Runtime Environment: invc75dag004.informatica.com

The 'Results' section shows:

- Status: Success
- Error Message: No errors encountered.
- Profiled Rows: 84020

The 'Subtasks (4)' table lists the following subtasks:

Instance Name	Location	Start Time	End Time	Status
Loading data from staging area to met...	Default	Feb 25, 2020, 01:08:03 AM	Feb 25, 2020, 01:08:10 AM	Success
s_profiling_1_6_1-13	Default	Feb 25, 2020, 01:07:09 AM	Feb 25, 2020, 01:08:01 AM	Success
Generating data profiling mappings - 13	Default	Feb 25, 2020, 01:06:56 AM	Feb 25, 2020, 01:07:07 AM	Success
Fetching the source row count-13	Default	Feb 25, 2020, 01:06:53 AM	Feb 25, 2020, 01:06:55 AM	Success

[サブタスク] 領域で、インスタンスのサブタスクを表示できます。サブタスクをクリックして、サブタスクの詳細を表示します。

データプロファイリング、モニタ、オペレーションインサイトで次のサブタスクのランタイム環境と Secure Agent を表示できます。

- ソース行数のフェッチ
- s_profiling
- ドリルダウン
- クエリ

注: [ランタイム環境] フィールドに、Secure Agent グループの名前が表示されます。

[セッションログのダウンロード] をクリックすると、セッションログファイルがダウンロードされます。プロファイルマッピングジョブのセッションログファイルで、Secure Agent の次の詳細を表示できます。

- タスク名。プロファイリングタスクの名前。
- エージェントグループ ID。Secure Agent グループの ID。
- エージェントグループ名。Secure Agent グループの名前。
- エージェント ID。Secure Agent の ID。
- エージェント名。Secure Agent の名前。

第 7 章

Informatica Intelligent Cloud Services 一括取り込みの監視

一括取り込みサービスおよびオペレーションインサイトサービスから、取り込みジョブの進行状況、パフォーマンス、およびステータスを監視できます。

使用するサービスおよび取り込みジョブのタイプにより、次の監視情報を表示できます。

- 一括取り込みサービスの【**マイジョブ**】ページで、デプロイした取り込みタスクの取り込みジョブを監視します。タスクタイプ、ランタイム環境、開始時刻、継続時間、現在のジョブの状態などの、ジョブの全般プロパティを含む、ジョブのリストを表示できます。
- オペレーションインサイトサービスの【**一括取り込み**】ページで、組織のメンバがデプロイした取り込みジョブのすべてのタイプを監視します。次のタイプの情報を表示できます。
 - タスクタイプおよびジョブの状態ごとの、取り込みジョブの概数。
 - 失敗したジョブ、またはエラーあるいは警告ありの状態で行われているために注意が必要な最近のジョブ。
 - ジョブの全般プロパティを含む、タイプごとのすべての取り込みジョブのリスト。
- 自分のジョブのリストまたはすべてのジョブのリストから、ジョブ名をクリックして、特定のジョブの詳細をドリルダウンできます。概要ジョブ情報、ソースオブジェクト処理の詳細、および警告を表示できます。

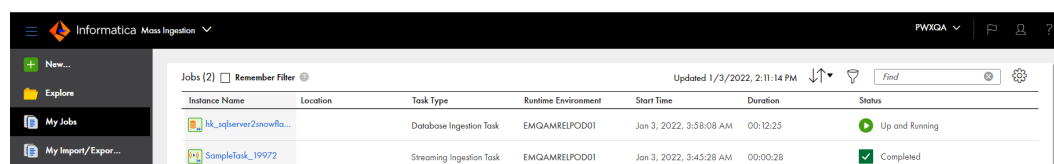
注: 通常、ジョブ名は取り込みタスク名に対応します。アプリケーション取り込みジョブとデータベース統合ジョブの場合、ジョブ名は *taskname-job_instance_number* の形式になります。数字はジョブがデプロイされるたびに増加します。

取り込みジョブの監視

一括取り込みの【**マイジョブ**】ページでは、デプロイしたタスクの取り込みジョブを監視できます。

【**マイジョブ**】ページには、ステータスなど、各ジョブインスタンスに関する情報が表示されます。

例えば、次の画像はデータベース統合ジョブとストリーミング統合ジョブが表示されている【**マイジョブ**】ページを示しています。



Instance Name	Location	Task Type	Runtime Environment	Start Time	Duration	Status
ik_sqlserver2snowfla...		Database Ingestion Task	EMGAMREPOD01	Jan 3, 2022, 3:58:08 AM	00:12:25	Up and Running
SampleTask_19972		Streaming Ingestion Task	EMGAMREPOD01	Jan 3, 2022, 3:45:28 AM	00:00:28	Completed

カラムの説明については、「[ジョブのプロパティ](#)」(ページ 78)を参照してください。これらのカラムは、オペレーションインサイトの「**一括取り込み**」ページにある「**すべてのジョブ**」タブのすべての取り込みジョブに対して表示されたものと同じです。

長いリストでジョブを検索するには、次のいずれかの方法を使用します。

- 一覧表示されたジョブをソートするには、カラムの見出しをクリックするか、[ソート] アイコンをクリックして、ソートするフィールドを選択します。アプリケーション取り込みジョブ、データベース取り込みジョブ、ストリーミング取り込みジョブのデフォルトのソート順は、タスクがデプロイされた時刻の順です（最新のものから表示）。ファイル取り込みジョブのデフォルトのソート順は、ジョブの開始時刻（最新から表示）です。
- ジョブインスタンス名に基づいてジョブを検索するには、*[検索]* テキストボックスにジョブ名または名前の一部を入力します。名前的一部分を入力すると、検索操作はインスタンス名の任意の場所にその文字列があるかどうかを検索します。一括取り込みでは、インスタンス名の検索文字列にパーセント記号 (%) ワイルドカードを含めて、「ing2%798」などの 1 つ以上の文字を表すようにすることができます。次の記号は含めないでください: 疑問符 (?)、番号記号 (#)、またはアンパサンド (&)。これらの記号のいずれかを含めると、検索操作は結果を返しません。
- ジョブのリストをフィルタするには、*[フィルタ]* アイコンをクリックします。**[フィルタの追加]** をクリックし、リストされた 1 つ以上のフィールドのフィルタ条件を入力します。**[インスタンス名]** フィールドに、完全なインスタンス名または名前的一部分を入力できます。一括取り込みでは、インスタンス名の値にパーセント記号 (%) ワイルドカードを含めて、「vp%test3」など名前の中の 1 つ以上の文字を表すようにすることができます。フィルタは、変更されるまで、現在のセッションの自分のユーザー名に対してのみ保存されます。一括取り込みでは、**[フィルタを記憶]** チェックボックスを選択することで、今後のセッション用にフィルタを保存できます。既存のフィルタ条件をクリアするには、フィルタアイコンをもう一度クリックします。

各ジョブ行の右端にあるアクション (...) メニューから、ジョブのステータスとタスクタイプに応じて、ジョブに対していくつかのアクションを実行できます。

すべての取り込みジョブの監視

オペレーションインサイトサービスの「**一括取り込み**」ページでは、アプリケーション取り込みジョブ、データベース統合ジョブ、ファイル取り込みジョブ、およびストリーミング統合を含む、一括取り込みサービスからデプロイされたすべての取り込みジョブを監視できます。

「**一括取り込み**」ページには、以下のタブがあります。

- [概要]** タブには、取り込みジョブのリストにジョブタイプと状態でフィルタを適用するために使用するボタンが表示されます。
- [すべてのジョブ]** タブには、組織内のメンバが作成およびデプロイしたすべてのタイプの取り込みジョブが表示されます。これには一括取り込みサービスの「**マイジョブ**」ページと同じカラムのプロパティが含まれます。

【概要】 タブ

【概要】 タブは、最初にすべてのステータスのすべてのタイプの取り込みジョブを一覧表示します。各ボタンには、そのジョブタイプまたはそのステータスのジョブの数が表示されます。以下に例を示します。

Instance Name	Location	Task Type	Runtime Environment	Start Time	Duration	Status
ms23_2T_m_30401	Shredding/Ref_IntelUsed	Database Ingestion Task	mlm74p01.informatica.com	May 2, 2022, 8:23:41 AM	00:02:56	Undeployed
18461-8452_20399	Krakra/Crakra_Target	Database Ingestion Task	EMGAAREP0001	May 2, 2022, 8:21:59 AM	00:28:50	Undeployed
ms23_2T_m_30404	Shredding/Ref_IntelUsed	Database Ingestion Task	mlm74p01.informatica.com	May 2, 2022, 8:21:22 AM	00:02:12	Completed

上部のボタンを使用してジョブタイプとステータスでジョブをフィルタリングするか、**【注意が必要なステータスの選択】**をクリックして、関心のあるステータスのジョブのみを表示します。次の例は、注意が必要なステータスのすべてのジョブを表示する**【概要】**タブを示しています。

Instance Name	Location	Task Type	Runtime Environment	Start Time	Duration	Status
CDC_HikaruRef_Om_00593	Krakra/Crakra_Target	Database Ingestion Task	EMGAAREP0001	Apr 27, 2022, 3:58:34 AM	00:03:24	Failed
SEC_ORACLE_TOT_KAFKA_30588	Aldi/Kafka	Database Ingestion Task	EMGAAREP0001	Apr 27, 2022, 3:46:59 AM	00:02:36	Failed

【概要】 タブに表示されるステータスボタンを制御するには、**【編集】**（鉛筆）アイコンをクリックします。次に、**【ジョブステータスの並べ替え】** ダイアログボックスで、ボタンとジョブを表示するそれぞれのジョブステータスの横にある**【表示】** チェックボックスをオンにします。

ジョブステータスボタンの順序を変更するには、**【編集】** アイコンをクリックします。次に、**【ジョブステータスの並べ替え】** ダイアログボックスで、ジョブステータスの行を選択して上下にドラッグします。

【概要】 タブでジョブのリストにフィルタを適用するには、次のいずれかの方法を使用します。

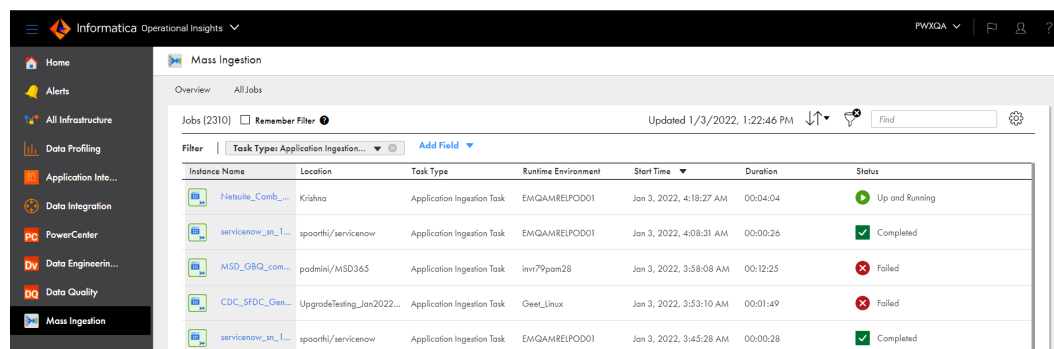
- アプリケーション取り込みジョブ、データベース統合ジョブ、ファイル取り込みジョブ、またはストリーミング統合ジョブのみを表示するには、ジョブタイプのボタンをクリックします。選択したボタンは青色で強調表示されます。すべてのタイプの取り込みジョブを再度表示するには、選択したボタンをもう一度クリックします。ジョブタイプのステータスフィルタを選択した場合、ジョブタイプの選択を解除すると、それらのフィルタもクリアされます。
- 特定のジョブステータスに一致するジョブを表示するには、ステータスボタンをクリックします。特定のジョブタイプとステータスのジョブを表示する場合は、まずジョブタイプを選択してから、ステータスを選択します。**【概要】** タブで複数のステータスボタンを同時に選択することはできません。フィルタをクリアするには、選択したステータスボタンをもう一度クリックします。
- 注意が必要なステータスのすべてのジョブを表示するには、ジョブステータスボタンの上にある**【注意が必要なステータスの選択】**をクリックします。このオプションにより、**【失敗】** または **【実行中（警告あり）】** 状態のアプリケーション取り込みジョブあるいはデータベース統合ジョブ、または **【失敗】** 状態のファイル取り込みジョブ、あるいは **【実行中（エラーあり）】** または **【実行中（警告あり）】** 状態のストリーミング統合ジョブが一覧表示されます。フィルタをクリアするには、もう一度**【注意が必要なステータスの選択】** をクリックします。特定のジョブタイプの注意が必要なジョブを表示する場合は、まずジョブタイプを選択してから、**【注意が必要なステータスの選択】** をクリックします。

注: [概要] タブまたは [ジョブステータスの並べ替え] ダイアログボックスで設定したすべてのフィルタは、現在のセッションでのみ、またはセッション中に変更するまでアクティブです。

[すべてのジョブ] タブ

[すべてのジョブ] タブには、ジョブインスタンス名、タスクタイプ、ランタイム環境、およびステータスによるオプションのフィルタリングを使用して、すべての取り込みジョブが一覧表示されます。このタブから、ジョブに対して、デプロイ解除や再デプロイなどいくつかのアクションを実行することもできます。

例えば、次の図はアプリケーション取り込みジョブを表示するようにフィルタリングされた [すべてのタスク] タブを示しています。



The screenshot shows the 'Mass Ingestion' tab in the Informatica Operational Insights interface. The left sidebar contains navigation links: Home, Alerts, All Infrastructure, Data Profiling, Application Inte..., Data Integration, PowerCenter, Data Engineerin..., Data Quality, and Mass Ingestion. The main panel displays a table of jobs with the following columns: Instance Name, Location, Task Type, Runtime Environment, Start Time, Duration, and Status. The table is filtered by 'Task Type: Application Ingestion Task'. The jobs listed are:

Instance Name	Location	Task Type	Runtime Environment	Start Time	Duration	Status
NetSuite_Comb...	Krishna	Application Ingestion Task	EMQAMREIPOD01	Jan 3, 2022, 4:18:27 AM	00:04:04	Up and Running
servicenow_m_1...	spoorthi/servicenow	Application Ingestion Task	EMQAMREIPOD01	Jan 3, 2022, 4:08:31 AM	00:00:26	Completed
MISO_G8Q_com...	padmini/MISO365	Application Ingestion Task	invr79pom28	Jan 3, 2022, 3:58:08 AM	00:12:25	Failed
CDC_SFDC_Oen...		UpgradeTesting_Jan2022...	Geet_Linux	Jan 3, 2022, 3:53:10 AM	00:01:49	Failed
servicenow_m_1...	spoorthi/servicenow	Application Ingestion Task	EMQAMREIPOD01	Jan 3, 2022, 3:45:28 AM	00:00:28	Completed

ジョブのリストが長い場合は、次のいずれかの方法を使用して、ジョブを見つけやすくします。

- 一覧表示されたジョブをソートするには、カラムの見出しをクリックするか、[ソート] の上/下矢印アイコンをクリックして、ソートするフィールドを選択します。アプリケーション取り込みジョブ、データベース統合ジョブ、ストリーミング統合ジョブのデフォルトのソート順は、タスクがデプロイされた時刻の順です（最新のものから表示）。ファイル取り込みジョブのデフォルトのソート順は、ジョブが開始された時刻の順です（最新のものから表示）。
- ジョブインスタンス名に基づいてジョブを検索するには、[検索] テキストボックスにジョブ名または名前の一部を入力します。名前の一部を入力すると、検索操作はインスタンス名の任意の場所にその文字列があるかどうかを検索します。オペレーションインサイトでは、インスタンス名の検索文字列にパーセント記号 (%) ワイルドカードを含めて、「ing2%798」などの 1 つ以上の文字を表すことができます。次の記号は含めないでください: 疑問符 (?), 番号記号 (#), またはアンパサンド (&)。これらの記号のいずれかを含めると、検索操作は結果を返しません。
- ジョブのリストをフィルタするには、[フィルタ] アイコンをクリックします。[フィルタの追加] をクリックし、1 つ以上のフィールドのフィルタ条件を入力します。[インスタンス名] フィールドに、完全なジョブインスタンス名または名前的一部分を入力できます。オペレーションインサイトでは、インスタンス名の値にパーセント記号 (%) ワイルドカードを含めて、「vp%test3」など名前の中の 1 つ以上の文字を表すようにすることができます。フィルタは、変更されるまで、現在のセッションの自分のユーザー名に対してのみ保存されます。オペレーションインサイトでは、[フィルタを記憶] チェックボックスを選択することで、今後のセッション用にフィルタを保存できます。既存のフィルタ条件をクリアするには、フィルタアイコンをもう一度クリックします。

注: リスト内の行の間隔を変更するには、[検索] ボックスの右にある [設定] アイコンをクリックします。

ジョブのステータスとタスクタイプに応じて、ジョブに対していくつかのアクションを実行できます。各ジョブ行の右端にあるアクション (...) メニューから、アクションタイプを選択します。

ジョブのプロパティ

一括取り込みサービスの【マイジョブ】ページとオペレーションインサイトの【一括取り込み】ページの【すべてのジョブ】タブの取り込みジョブリストには、各ジョブのプロパティが表示されます。プロパティには、ジョブステータスの概要が表示されます。

以下の表に、ジョブのプロパティを示します。

プロパティ	説明
インスタンス名	生成されるジョブインスタンスの名前の形式は、<task_name>_<instance_number>です。 インスタンス名をクリックすると、ジョブに関する詳細情報を表示できます。 注: 関連する取り込みタスクの名前を編集しても、ジョブ名は同じままです。
場所	ジョブに関連付けられたタスク定義があるプロジェクトまたはプロジェクト\サブフォルダ。例: Myproject\Oracle 注: このプロパティは、Fall 2020 リリースよりも以前にデプロイされたジョブでは空白になります。 タスク定義を別のフォルダに移動した場合、【ロケーション】値は更新されません。
タスクタイプ	取り込みタスクのタイプ。この値は、 アプリケーション取り込みタスク 、 データベース取り込みタスク 、 ファイル取り込みタスク 、または ストリーミング取り込みタスク である必要があります。
ランタイム環境	ジョブが実行するランタイム環境の名前。
開始時刻	アプリケーション取り込みジョブおよびデータベース統合ジョブの場合、ジョブがデプロイされた日時。 ファイル取り込みジョブの場合、ジョブが開始された日時。 ストリーミング統合ジョブの場合、ジョブがデプロイされた日時。
継続時間	アプリケーション取り込みジョブおよびデータベース統合ジョブの場合、デプロイ後にジョブが実行された時間。完了、停止、失敗、または強制終了状態のジョブの場合、ジョブがデプロイされた日時から現在の状態を取得した時点までの時間。 ファイル取り込みジョブの場合、ジョブが実行された時間。 ストリーミング統合ジョブの場合、ジョブが実行された時間。
ステータス	デプロイ中、稼働中、またはアンデプロイ済みなどの、ジョブの現在のステータス。 有効なステータスのセットは、取り込みタスクのタイプにより異なります。詳細については、 「データベース統合ジョブの詳細」 (ページ 85)または 「ストリーミング統合ジョブの詳細」 (ページ 93)の「[ジョブの概要] タブ」の節または 「ファイル取り込みジョブの詳細」 (ページ 91)の「結果」の節を参照してください。

取り込みジョブの詳細の表示

一括取り込みサービスの【マイジョブ】ページ、またはオペレーションインサイトサービスの【一括取り込み】ページの【すべてのジョブ】タブで、特定の取り込みジョブをドリルダウンしてジョブの詳細を表示できます。

ジョブの詳細を表示するには、ジョブリストのジョブ名をクリックします。そのジョブのページが表示されます。表示される詳細は、取り込みジョブのタイプによって変わります。

アプリケーション取り込みジョブの詳細

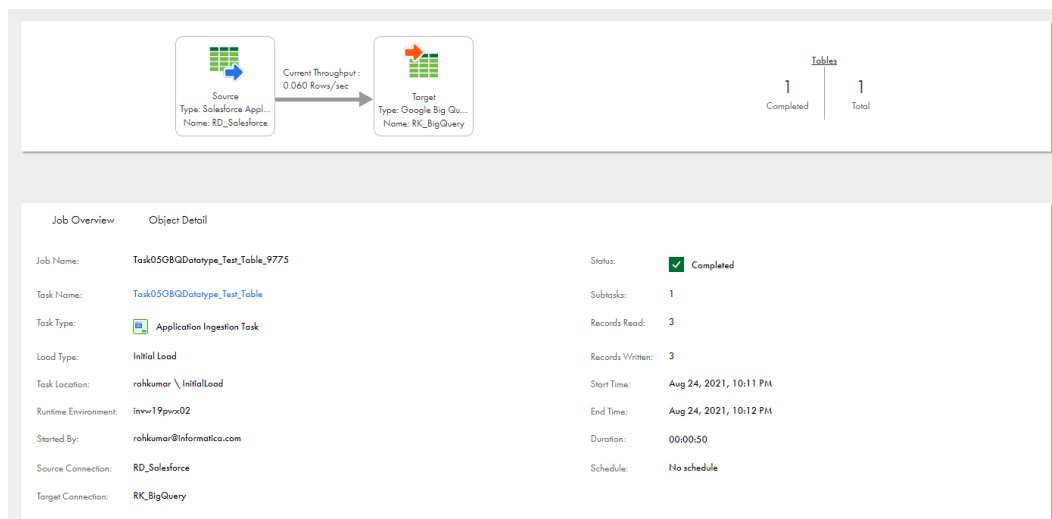
アプリケーション取り込みジョブでは、[ジョブの概要]、[オブジェクトの詳細]、および [警告] タブでジョブ固有の詳細を表示できます。これらのタブにアクセスするには、一括取り込みの [マイジョブ] ページ、またはオペレーションインサイトの一括取り込みページの [すべてのジョブ] タブから、ジョブをドリルダウンします。

[ジョブの概要] タブ

[ジョブの概要] タブには、ジョブ全体の詳細情報が表示されます。例えば、関連タスクの名前、ロードタイプ、ソースおよびターゲット接続名、現在のステータス、読み込みおよび書き込みレコード数、開始および終了時刻、実行時間などが含まれます。増分ロードジョブと初期および増分ロードジョブの組み合わせの場合、ジョブログをダウンロードすることもできます。

次の図に、完了したアプリケーション取り込みジョブの [ジョブの概要] タブを示します。

注: ページ上部の図は、ジョブの現在のステータスに関係なく、ジョブによってデータがターゲットに正常にプロパゲートされた場合に算出されたデータスループット（行/秒）を表示します。算出値が 0 の場合は、データがターゲットに流れ込まれていないことを示し、スループットは表示されません。



以下の表で、ジョブの概要プロパティについて説明します。

プロパティ	説明
ジョブ名	ジョブの名前。 アプリケーション取り込みジョブ名の形式は、 <i>task name-job instance number</i> です。
タスク名	関連取り込みタスクの名前。必要に応じて、タスク名のリンクをクリックして、一括取り込みでタスクの詳細を表示または編集できます。タスクを編集する場合は、更新されたタスク定義をジョブで使用するために、タスクを再デプロイする必要があります。
タスクタイプ	タスクのタイプ。アプリケーション取り込みタスクです。

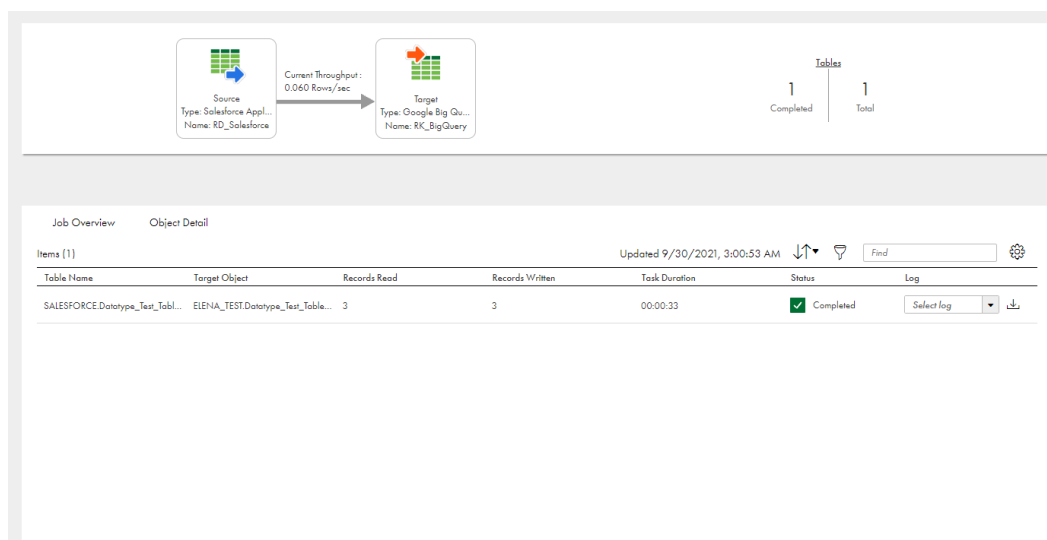
プロパティ	説明
ロードタイプ	<p>ジョブが実行するロード操作のタイプ。次のオプションがあります。</p> <ul style="list-style-type: none"> - 【初期ロード】。特定のポイントインタイムでターゲットに読み込まれるソースデータのスナップショットをロードします。 - 増分ロード。ジョブが停止または終了するまで、ターゲットに対する増分データ変更を継続的にロードします。 - 【初期および増分ロード】。初期ロードを実行し、次に増分ロードに自動的に切り替えます。
タスクの場所	取り込みタスク定義を含むプロジェクトまたはプロジェクトフォルダ。
ランタイム環境	ジョブの実行で使用するランタイム環境の名前。
開始したユーザー名	ジョブを開始したユーザーの名前。
ソース接続	ソース接続の名前。
ターゲット接続	ターゲット接続の名前。
ステータス	<p>ジョブのステータス。以下のいずれかの値になります。</p> <ul style="list-style-type: none"> - 稼働中。ジョブは実行中です。 - 実行中（警告あり）。ジョブは実行中ですが警告があります。この状態は、1 つ以上のテーブル固有サブタスクは失敗したものの、一部のサブタスクがまだ実行中であるときにも発生します。 - 保留。一括取り込みデータベース（DBMI）エージェントの更新中にジョブが一時停止状態になっています。 - 停止中。停止要求への応答として、ジョブを停止中です。 - 停止。ジョブが意図的に停止されました。 - 失敗。ジョブは異常終了しました。ジョブへのタスクのデプロイが失敗したか、1 つ以上のオブジェクト固有のサブタスクが失敗しました。また、初期ロードジョブの場合は、ジョブが停止しました。 - デプロイ中。ジョブはデプロイ中です。 - デプロイ。ジョブはデプロイされました。 - 強制終了中。強制終了要求への応答として、ジョブは直ちに停止中です。 - 強制終了。ジョブは強制終了されました。 - 配置の解除（アンデプロイ）。ジョブはアンデプロイ中です。 - デプロイされていない。ジョブはアンデプロイされました。 - 完了。ジョブが正常に完了しました。
サブタスク	データをソースオブジェクトからターゲットにプロパゲートするためにアプリケーション取り込みジョブが使用したサブタスクの数。ジョブが実行されると、各ソースオブジェクトを処理するために個別のサブタスクが使用されます。
読み取ったレコード数	<p>ソースから読み取られたレコード数。</p> <p>注: 初期ロードタスクと増分ロードタスクを組み合わせたアプリケーション取り込みに関連付けられたジョブを初めて実行するときに、【読み取ったレコード数】のカウン트가、読み取られたオブジェクトレベルの DML 変更レコードの総数よりも大きい場合があります。この動作は、変更データキャプチャが開始された後に、組み合わせた処理の初期ロードの部分が常に開始されるために発生します。その結果、初期ロード処理が開始されてカウントにレコードを追加する前に、いくつかの変更レコードが【読み取ったレコード数】のカウン트에含まれます。</p>

プロパティ	説明
書き込んだレコード数	Microsoft Azure Synapse Analytics ターゲットの場合、中間 Microsoft Azure Data Lake Storage ファイルに書き込まれレコード数。 Snowflake ターゲットの場合、ジョブの実行時に作成される内部ステージング領域に書き込んだレコード数。
開始時刻	ジョブがデプロイされた日付と時刻。
終了時刻	処理完了、停止、または失敗したためにジョブが終了した日時。このフィールドは、実行中のジョブの場合は表示されません。
継続時間	ジョブが終了するまでの実行時間 (hh:mm:ss 形式)。
スケジュール	初期ロードジョブについては、ジョブの実行に使用されるスケジュールの名前、またはジョブを手動で実行する場合は「スケジュールなし」。
ログ	<p>増分ロードジョブと初期および増分ロードジョブの組み合わせの場合、ジョブの実行全体についてジョブ実行ログをダウンロードできます。次のいずれかのログタイプを選択します。</p> <ul style="list-style-type: none"> - 完全なログ。ログ全体。すべてのタイプのメッセージを含みます。状態に関係なく、実行した任意のジョブに利用できます。 - エラー。エラーログ。発生したエラーに関するメッセージのみを含みます。失敗したジョブに対してのみ利用できます。このログを使用して、デプロイ失敗などジョブが失敗した理由を判断します。ログファイルの末尾に省略記号 (...) が付いている場合、このログは長いため切り詰められています。この場合、すべてのエラーメッセージを確認するには完全なログをダウンロードします。 <p>ログをローカルシステムにダウンロードするには、[ダウンロード] アイコンをクリックします。</p> <p>注: 初期ロードジョブの場合、[オブジェクトの詳細] タブから特定のソースオブジェクトのジョブログを取得できます。</p>

【オブジェクトの詳細】 タブ

【オブジェクトの詳細】 タブには、アプリケーション取り込みジョブの最後の実行から、ソースオブジェクト別の統計とステータス情報が表示されます。

次の図に、アプリケーション取り込みジョブの【オブジェクトの詳細】 タブを示します。



次の表に、各オブジェクトで表示されるプロパティを示します。

カラム	説明
テーブル名	<p>ターゲットにプロパゲートされたデータのソースオブジェクトまたはビューの名前。</p> <p>増分ロードジョブまたは初期および増分ロードジョブの組み合わせの場合、オブジェクト名の左にある矢印アイコンをクリックすると、処理された LOB、挿入、削除、更新、および DDL 文の数の詳細が表示されます。初期および増分ロードジョブの組み合わせの場合は「アンロード数」フィールドも表示され、処理の初期ロード部分によってソースから読み取られたレコード数が示されます。詳細な CDC カウントを使用する場合は以下の点に注意してください。</p> <ul style="list-style-type: none"> - 現在のジョブ実行のみカウントされます。ジョブを停止して再開すると、カウントはゼロから再開されます。これらのカウントを使用してターゲットに書き込まれた行数を確認しないでください。 - カウントはソースから読み取られた行数に基づいており、ターゲットに書き込まれたレコード数を反映していません。ターゲットの書き込み操作は、操作を組み合わせる物理的な書き込み回数を減らすことで最適化される場合があります。この場合、カウントは書き込み操作数と一致しないことがあります。 - 値 N/A は、カウント値がそのカウントタイプで使用できないか、値がまだ計算されていないことを示しています。 - アンロード処理の開始には遅延が発生するため、「アンロード数」にはジョブの開始時や再同期時のソースレコード数が反映されない場合があります。アンロード要求からアンロード処理の開始までの間に、行がソーステーブルに追加されたり、ソーステーブルから削除されることがあります。
ターゲットオブジェクト	ソースオブジェクトにマッピングされているターゲットテーブルの名前。
読み取ったレコード数	初期ロードジョブの場合、ソースから読み取られたレコード数。その他のロードタイプの場合、この情報は「 ジョブの概要 」タブでジョブレベルでのみ利用できます。
書き込んだレコード数	<p>この情報は「ジョブの概要」タブでジョブレベルでのみ利用できます。</p> <p>Microsoft Azure Synapse Analytics ターゲットの場合、中間 Microsoft Azure Data Lake Storage ファイルに書き込まれたレコード数。</p> <p>Snowflake ターゲットの場合、ジョブの実行時に作成される内部ステージング領域に書き込んだレコード数。</p>
タスク時間	<p>初期ロードジョブの場合、ソーステーブルを処理したサブタスクが完了または停止するまでの実行時間。その他のロードタイプの場合、この情報は「ジョブの概要」タブでジョブレベルでのみ利用できます。</p> <p>ジョブが実行されると、各ソーステーブルを処理するために個別のサブタスクが使用されます。</p>

カラム	説明
ステージ	<p>初期および増分ロードジョブの組み合わせの場合、このカラムには、テーブル固有のジョブサブタスクの初期ロード処理から CDC 処理への遷移におけるステージが表示されます。その他のロードタイプの場合、このカラムは表示されません。</p> <p>ステージは、以下の値のいずれかになります。</p> <ul style="list-style-type: none"> - 開始されていません。 テーブルの初期ロード処理がまだ開始していません。または、エラーが発生し、オブジェクトが 【再試行時にエラー】 状態である場合、次のオブジェクト処理がまだ開始していません。 - 開始。 初期ロード処理が開始しました。 - アンロード中。 サブタスクは、初期ロード処理の一環として、オブジェクトからデータをアンロード中です。 - アンロード済み。 サブタスクは、初期ロード処理の一環として、オブジェクトからデータのアンロードを終了しました。 - 完了。 サブタスクは、オブジェクトの初期ロード処理を完了しました。 - ノーマル。 サブタスクは、オブジェクトの初期ロード処理を完了し、オブジェクトの CDC 処理を開始しました。 - キャンセル済み。 初期ロード処理がキャンセルまたは停止しました。 - エラー。 サブタスクは、ソーステーブルでエラーを検出しました。
ステータス	<p>ソースオブジェクトのジョブサブタスクのステータス。</p> <p>注: ジョブが実行を停止した場合、サブタスクのステータスには、ジョブの終了前に最後に収集されたステータスが反映されます。例えば、ジョブが強制終了される場合がありますが、サブタスクのステータスは 【実行中】 です。</p> <p>状態は、以下の値のいずれかになります。</p> <ul style="list-style-type: none"> - キューに格納。 サブタスクはまだ実行を開始していません。 - 開始中。 サブタスクは開始中です。 - 開始。 初期および増分ロードジョブの組み合わせの場合、サブタスクが開始されました。 - 実行中。 サブタスクは実行中です。 - 保留。 一括取り込みデータベース (DBMI) エージェントの更新中にジョブだけでなくサブタスクも一時停止状態になっています。 - 完了。 サブタスクは処理を正常に完了しました。 - 停止中。 停止要求への応答として、サブタスクを停止中です。 - 停止。 サブタスクは停止されました。 - 強制終了中。 強制終了要求への応答として、サブタスクは直ちに終了中です。 - 強制終了。 サブタスクは強制終了されました。 - 失敗。 サブタスクは予期せず終了しました。 - エラー。 サブタスクでエラーが発生したため、データがターゲットテーブルに書き込まれなくなりました。初期および増分ロードジョブの組み合わせの場合、サブタスクは実行中で増分変更データを処理している可能性があります。データはターゲットに送信されていません。 - 再試行時にエラー。 サブタスク処理の最後の再試行時にエラーが発生し、現在は、サブタスクは処理の再試行を待機中です。 <p>注: ソーステーブルで DDL の変更が行われた後にジョブを再開すると、テーブルサブタスクの状態は最初の DML 操作がソーステーブルで実行されるまで正しく反映されない場合があります。</p>

カラム	説明
ログ	<p>初期ロードジョブの場合、ソースオブジェクトのジョブ実行ログをダウンロードできます。次のいずれかのログタイプを選択します。</p> <ul style="list-style-type: none"> - 完全なログ。ジョブの実行で生成されるオブジェクトサブタスクの完全なログ。 - エラー。エラーメッセージを含むログ。このログタイプは、失敗したサブタスクのみに利用できます。 <p>増分ロードジョブの場合、【ジョブの概要】 タブからジョブ実行全体の完全なログを取得できます。</p> <p>初期および増分ロードジョブの組み合わせの場合、【ステージログ】 をダウンロードできます。このログには、ソースオブジェクトの初期ロードから増分ロードへの遷移が示されています。</p> <p>ログをローカルにダウンロードするには、[ダウンロード] アイコンをクリックします。</p> <p>注: ジョブをアンデプロイした場合、テーブルのログをダウンロードできるのは関連タスクを削除していない場合のみです。</p>
[アクション] メニューの [再同期]	<p>初期および増分ロードジョブの組み合わせにおけるサブタスクについて、サブタスクのステージが 【ノーマル】 でサブタスクの状態が 【キューに格納】 または 【開始中】 以外の状態の場合は、サブタスク行の右端に [アクション] メニューが表示されます。[アクション] メニューから 【再同期】 を選択すると、ソースオブジェクトとターゲットオブジェクトを再同期できます。詳細については、一括取り込みのヘルプにあるソースオブジェクトとターゲットオブジェクトの再同期に関する説明を参照してください。</p>

注: このタブには、最新のジョブ実行に関する情報が表示されます。実行されていないジョブまたは再開中のジョブの場合、このタブは空白です。

[警告] タブ

[警告] タブには、特定のイベントに関する警告メッセージが表示されます。

注: ソーススキーマの変更が検出されると、**[警告]** タブに警告メッセージが表示されます。関連タスクの [スキーマの誤差] オプションを [無視] に設定した場合でも、検出されたすべてのスキーマの変更についてメッセージが表示されます。

重要度または日付範囲に基づいて警告のリストをフィルタリングできます。日付範囲を指定するには、**[フィルタ]** フィールドに次のいずれかのタイプの値を入力します。

- 選択した開始日時と終了日時で構成される **【カスタム】** 日付範囲。
- 保存されたすべての警告に対する **【任意の時間】**。
- 本日午前 0 時から午後 11 時 59 分までに発行された警告に対する **【今日】**。
- 先週、先月、または昨年の初めから現在までの警告を示す **【先週】**、**【先月】**、または **【昨年】**。

次の表に、各警告メッセージで表示される情報のカラムを示します。

カラム	説明
レベル	警告メッセージの重要度レベル。
コード	警告タイプを識別する英数字コード。
詳細	警告メッセージを生成したイベントの説明。
時間	イベントの発生日時。

注: オペレーションインサイトの **【アラート】** > **【一括取り込みアラート】** ページから、アプリケーション取り込みジョブおよびデータベース統合ジョブのアラート通知を設定することもできます。その後、オペレーシ

オンラインサイトは、取り込みジョブが特定のステータスを取得するか、DDLの変更を検出したときに、管理者が選択したユーザーとユーザーグループに一括取り込みアラート通知を送信します。

データベース統合ジョブの詳細

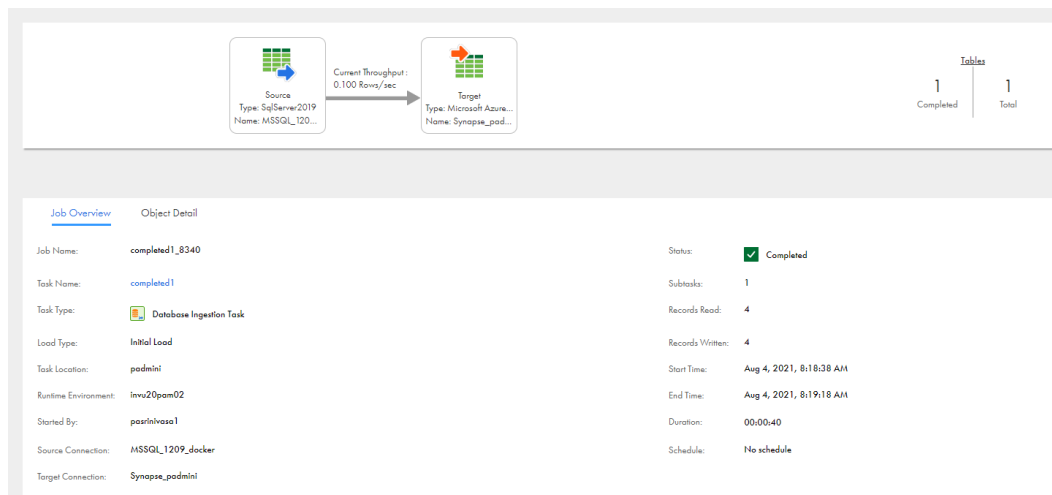
データベース統合ジョブでは、[ジョブの概要]、[オブジェクトの詳細]、および[警告] タブでジョブに特有の詳細を表示できます。これらのタブにアクセスするには、一括取り込みの【マイジョブ】 ページ、またはオペレーションインサイトの一括取り込みページの【すべてのジョブ】 タブから、ジョブをドリルダウンします。

[ジョブの概要] タブ

[ジョブの概要] タブには、ジョブ全体の詳細情報が表示されます。例えば、関連タスクの名前、ロードタイプ、ソースおよびターゲット接続名、現在のステータス、読み込みおよび書き込みレコード数、開始および終了時刻、実行時間などが含まれます。増分ロードジョブと初期および増分ロードジョブの組み合わせの場合、ジョブログをダウンロードすることもできます。

次の図に、完了したデータベース統合ジョブの [ジョブの概要] タブを示します。

注: ページ上部の図は、ジョブの現在のステータスに関係なく、ジョブによってデータがターゲットに正常にプロパゲートされた場合に算出されたデータスループット（行/秒）を表示します。算出値が 0 の場合は、データがターゲットに流れ込まれていないことを示し、スループットは表示されません。



以下の表で、ジョブの概要プロパティについて説明します。

プロパティ	説明
ジョブ名	ジョブの名前。 データベース統合ジョブ名の形式は、 <i>task name-job instance number</i> です。
タスク名	関連取り込みタスクの名前。必要に応じて、タスク名のリンクをクリックして、一括取り込みでタスクの詳細を表示または編集できます。タスクを編集する場合は、更新されたタスク定義をジョブで使用するために、タスクを再デプロイする必要があります。
タスクタイプ	タスクのタイプ。データベース取り込みタスクです。

プロパティ	説明
ロードタイプ	<p>ジョブが実行するロード操作のタイプ。次のオプションがあります。</p> <ul style="list-style-type: none"> - 【初期ロード】。特定のポイントインタイムでターゲットに読み込まれるソースデータのスナップショットをロードします。 - 増分ロード。ジョブが停止または終了するまで、ターゲットに対する増分データ変更を継続的にロードします。 - 【初期および増分ロード】。初期ロードを実行し、次に増分ロードに自動的に切り替えます。
タスクの場所	取り込みタスク定義を含むプロジェクトまたはプロジェクトフォルダ。
ランタイム環境	ジョブの実行で使用するランタイム環境の名前。
開始したユーザー名	ジョブを開始したユーザーの名前。
ソース接続	ソース接続の名前。
ターゲット接続	ターゲット接続の名前。
ステータス	<p>ジョブのステータス。以下のいずれかの値になります。</p> <ul style="list-style-type: none"> - 稼働中。ジョブは実行中です。 - 実行中（警告あり）。ジョブは実行中ですが警告があります。この状態は、1 つ以上のテーブル固有サブタスクは失敗したものの、一部のサブタスクがまだ実行中であるときにも発生します。 - 保留。一括取り込みデータベース（DBMI）エージェントの更新中にジョブが一時停止状態になっています。 - 停止中。停止要求への応答として、ジョブを停止中です。 - 停止。ジョブが意図的に停止されました。 - 失敗。ジョブは異常終了しました。ジョブへのタスクデプロイメントが失敗したか、1 つ以上のテーブル固有サブタスクが失敗しました。また、初期ロードジョブの場合は、ジョブが停止しました。 - デプロイ中。ジョブはデプロイ中です。 - デプロイ。ジョブはデプロイされました。 - 強制終了中。強制終了要求への応答として、ジョブは直ちに停止中です。 - 強制終了。ジョブは強制終了されました。 - 配置の解除（アンデプロイ）。ジョブはアンデプロイ中です。 - デプロイされていない。ジョブはアンデプロイされました。 - 完了。ジョブが正常に完了しました。
サブタスク	データをソーステーブルからターゲットにプロパゲートするためにデータベース統合ジョブが使用したサブタスクの数。ジョブが実行されると、各ソーステーブルを処理するために個別のサブタスクが使用されます。
読み取ったレコード数	<p>ソースから読み取られたレコード数。</p> <p>注: 初期ロードタスクと増分ロードタスクを組み合わせたデータベース取り込みに関連付けられたジョブを初めて実行するときに、【読み取ったレコード数】 のカウントが、読み取られたオブジェクトレベルの DML 変更レコードの総数よりも大きい場合があります。この動作は、変更データキャプチャが開始された後に、組み合わせた処理の初期ロードの部分が常に開始されるために発生します。その結果、初期ロード処理が開始されてカウントにレコードを追加する前に、いくつかの変更レコードが 【読み取ったレコード数】 のカウントに含まれます。</p>

プロパティ	説明
書き込んだレコード数	Amazon S3、Apache Kafka、フラットファイル、または Microsoft Azure Data Lake Storage ターゲットに正常にプロパゲートされたレコード数。 Microsoft Azure Synapse Analytics ターゲットの場合、中間 Microsoft Azure Data Lake Storage ファイルに書き込まれレコード数。 Snowflake ターゲットの場合、ジョブの実行時に作成される内部ステージング領域に書き込んだレコード数。
開始時刻	ジョブがデプロイされた日付と時刻。
終了時刻	処理完了、停止、または失敗したためにジョブが終了した日時。このフィールドは、実行中のジョブの場合は表示されません。
継続時間	ジョブが終了するまでの実行時間 (hh:mm:ss 形式)。
スケジュール	初期ロードジョブについては、ジョブの実行に使用されるスケジュールの名前、またはジョブを手動で実行する場合は「スケジュールなし」。
ログ	<p>増分ロードジョブと初期および増分ロードジョブの組み合わせの場合、ジョブの実行全体についてジョブ実行ログをダウンロードできます。次のいずれかのログタイプを選択します。</p> <ul style="list-style-type: none"> - 完全なログ。ログ全体。すべてのタイプのメッセージを含みます。状態に関係なく、実行した任意のジョブに利用できます。 - エラー。エラーログ。発生したエラーに関するメッセージのみを含みます。失敗したジョブに対してのみ利用できます。このログを使用して、デプロイ失敗などジョブが失敗した理由を判断します。ログファイルの末尾に省略記号 (...) が付いている場合、このログは長い場合め切り詰められています。この場合、すべてのエラーメッセージを確認するには完全なログをダウンロードします。 <p>ログをローカルシステムにダウンロードするには、[ダウンロード] アイコンをクリックします。</p> <p>注: 初期ロードジョブの場合、[オブジェクトの詳細] タブから特定のソースオブジェクトのジョブログを取得できます。</p>

[オブジェクトの詳細] タブ

[オブジェクトの詳細] タブには、データベース統合ジョブの最後の実行からソースオブジェクトによる統計およびステータス情報が表示されます。

次の図に、データベース統合ジョブの [オブジェクトの詳細] タブを示します。

Table Name	Target Object	Stage	Status	Log
AUSGKA_SRC_ALINDM_BR	AUSGKA1.DHAWC_SRC_ALINDM_BR	Normal	Running	View Log

Inserts	Updates	Deletes	LOBs	Unload Count
4	5	1	0	0

注: このタブには、最新のジョブ実行に関する情報が表示されます。実行されていないジョブまたは再開中のジョブの場合、このタブは空白です。

次の表に、ロードタイプとステータスに応じて、各テーブルで表示されるプロパティを示します。

カラム	説明
テーブル名	<p>ターゲットにプロパゲートされたデータのソーステーブルまたはビューの名前。</p> <p>増分ロードジョブまたは初期および増分ロードジョブの組み合わせの場合、オブジェクト名の左にある矢印アイコンをクリックすると、処理された挿入、削除、更新、LOB および DDL 文の数の詳細が表示されます。初期および増分ロードジョブの組み合わせの場合は [アンロード数] フィールドも表示され、処理の初期ロード部分によってソースから読み取られたレコード数が示されます。詳細な CDC カウントを使用する場合は以下の点に注意してください。</p> <ul style="list-style-type: none"> - 現在のジョブ実行のみカウントされます。ジョブを停止して再開すると、カウントはゼロから再開されます。これらのカウントを使用してターゲットに書き込まれた行数を確認しないでください。 - カウントはソースから読み取られた行数に基づいており、ターゲットに書き込まれたレコード数を反映していません。ターゲットの書き込み操作は、操作を組み合わせる物理的な書き込み回数を減らすことで最適化される場合があります。この場合、カウントは書き込み操作数と一致しないことがあります。 - 値 N/A は、カウント値がそのカウントタイプで使用できないか、値がまだ計算されていないことを示しています。 - アンロード処理の開始には遅延が発生するため、[アンロード数] にはジョブの開始時や再同期時のソースレコード数が反映されない場合があります。アンロード要求からアンロード処理の開始までの間に、行がソーステーブルに追加されたり、ソーステーブルから削除されることがあります。
ターゲットオブジェクト	ソーステーブルにマッピングされているターゲットオブジェクトの名前。
読み取ったレコード数	初期ロードジョブの場合、ソースから読み取られたレコード数。その他のロードタイプの場合、この情報は [ジョブの概要] タブでジョブレベルでのみ利用できます。
書き込んだレコード数	<p>初期ロードジョブの場合、Amazon S3、Apache Kafka、フラットファイル、または Microsoft Azure Data Lake Storage ターゲットに正常にプロパゲートされたレコード数。その他のロードタイプの場合、この情報は [ジョブの概要] タブでジョブレベルでのみ利用できます。</p> <p>Microsoft Azure Synapse Analytics ターゲットの場合、中間 Microsoft Azure Data Lake Storage ファイルに書き込まれたレコード数。</p> <p>Snowflake ターゲットの場合、ジョブの実行時に作成される内部ステージング領域に書き込んだレコード数。</p>
タスク時間	<p>初期ロードジョブの場合、ソーステーブルを処理したサブタスクが完了または停止するまでの実行時間。その他のロードタイプの場合、この情報は [ジョブの概要] タブでジョブレベルでのみ利用できます。</p> <p>ジョブが実行されると、各ソーステーブルを処理するために個別のサブタスクが使用されます。</p>

カラム	説明
ステージ	<p>初期および増分ロードジョブの組み合わせの場合、このカラムには、テーブル固有のジョブサブタスクの初期ロード処理から CDC 処理への遷移におけるステージが表示されます。その他のロードタイプの場合、このカラムは表示されません。</p> <p>ステージは、以下の値のいずれかになります。</p> <ul style="list-style-type: none"> - 開始されていません。 テーブルの初期ロード処理がまだ開始していません。または、エラーが発生し、テーブルが【再試行時にエラー】状態である場合、次のテーブル処理がまだ開始していません。 - 開始。 初期ロード処理が開始しました。 - アンロード中。 サブタスクは、初期ロード処理の一環として、テーブルからデータをアンロード中です。 - アンロード済み。 サブタスクは、初期ロード処理の一環として、テーブルからデータのアンロードを終了しました。 - 完了。 サブタスクは、テーブルの初期ロード処理を完了しました。 - ノーマル。 サブタスクは、テーブルの初期ロード処理を完了し、テーブルの CDC 処理を開始しました。 - キャンセル済み。 初期ロード処理がキャンセルまたは停止しました。 - エラー。 サブタスクは、ソーステーブルでエラーを検出しました。
ステータス	<p>ソースオブジェクトのジョブサブタスクのステータス。</p> <p>注: ジョブが実行を停止した場合、サブタスクのステータスには、ジョブの終了前に最後に収集されたステータスが反映されます。例えば、ジョブが強制終了される場合がありますが、サブタスクのステータスは【実行中】です。</p> <p>状態は、以下の値のいずれかになります。</p> <ul style="list-style-type: none"> - キューに格納。 サブタスクはまだ実行を開始していません。 - 開始中。 サブタスクは開始中です。 - 開始。 初期および増分ロードジョブの組み合わせの場合、サブタスクが開始されました。 - 実行中。 サブタスクは実行中です。 - 保留。 一括取り込みデータベース (DBMI) エージェントの更新中にジョブだけでなくサブタスクも一時停止状態になっています。 - 完了。 サブタスクは処理を正常に完了しました。 - 停止中。 停止要求への応答として、サブタスクを停止中です。 - 停止。 サブタスクは停止されました。 - 強制終了中。 強制終了要求への応答として、サブタスクは直ちに終了中です。 - 強制終了。 サブタスクは強制終了されました。 - 失敗。 サブタスクは予期せず終了しました。 - エラー。 サブタスクでエラーが発生したため、データがターゲットテーブルに書き込まれなくなりました。初期および増分ロードジョブの組み合わせの場合、サブタスクは実行中で増分変更データを処理している可能性があります。データはターゲットに送信されていません。 - 再試行時にエラー。 サブタスク処理の最後の再試行時にエラーが発生し、現在は、サブタスクは処理の再試行を待機中です。 <p>注: ソーステーブルで DDL の変更が行われた後にジョブを再開すると、テーブルサブタスクの状態は最初の DML 操作がソーステーブルで実行されるまで正しく反映されない場合があります。</p>

カラム	説明
ログ	<p>初期ロードジョブの場合、ソースオブジェクトのジョブ実行ログをダウンロードできます。次のいずれかのログタイプを選択します。</p> <ul style="list-style-type: none"> - 完全なログ。ジョブの実行で生成されるオブジェクトサブタスクの完全なログ。 - エラー。エラーメッセージを含むログ。このログタイプは、失敗したサブタスクのみに利用できます。 <p>増分ロードジョブの場合、【ジョブの概要】 タブからジョブ実行全体の完全なログを取得できます。</p> <p>初期および増分ロードジョブの組み合わせの場合、【ステージログ】 をダウンロードできます。このログには、ソースオブジェクトの初期ロードから増分ロードへの遷移が示されています。</p> <p>ログをダウンロードするには、【ダウンロード】 アイコンをクリックします。</p> <p>注: ジョブをアンデプロイした場合、テーブルのログをダウンロードできるのは関連タスクを削除していない場合のみです。</p>
【アクション】メニューの【再同期】	<p>初期および増分ロードジョブの組み合わせにおけるサブタスクについて、サブタスクのステージが【ノーマル】でサブタスクのステータスが【キューに格納】または【開始中】以外のステータスの場合は、サブタスク行の右端に【アクション】メニューが表示されます。【アクション】メニューから【再同期】を選択すると、ソースオブジェクトとターゲットオブジェクトを再同期できます。詳細については、一括取り込みのヘルプにあるソースオブジェクトとターゲットオブジェクトの再同期に関する説明を参照してください。</p>

注: リスト内の行の間隔を制御するには、**【検索】** ボックスの横にある**【設定】** アイコンをクリックします。

【警告】 タブ

【警告】 タブには、特定のイベントに関する警告メッセージが表示されます。

注: ソーススキーマの変更が検出されると、**【警告】** タブに警告メッセージが表示されます。関連タスクの**【スキーマの誤差】** オプションを**【無視】** に設定した場合でも、検出されたすべてのスキーマの変更についてメッセージが表示されます。

重要度または日付範囲に基づいて警告のリストをフィルタリングできます。日付範囲を指定するには、**【フィルタ】** フィールドに次のいずれかのタイプの値を入力します。

- 選択した開始日時と終了日時で構成される**【カスタム】** 日付範囲。
- 保存されたすべての警告に対する**【任意の時間】**。
- 本日午前 0 時から午後 11 時 59 分までに発行された警告に対する**【今日】**。
- 先週、先月、または昨年の初めから現在までの警告を示す**【先週】**、**【先月】**、または**【昨年】**。

次の表に、各警告メッセージで表示される情報のカラムを示します。

カラム	説明
レベル	警告メッセージの重要度レベル。
コード	警告タイプを識別する英数字コード。
詳細	警告メッセージを生成したイベントの説明。
時間	イベントの発生日時。

注: オペレーションインサイトの**【アラート】** > **【一括取り込みアラート】** ページから、アプリケーション取り込みジョブおよびデータベース統合ジョブのアラート通知を設定することもできます。その後、オペレーシ

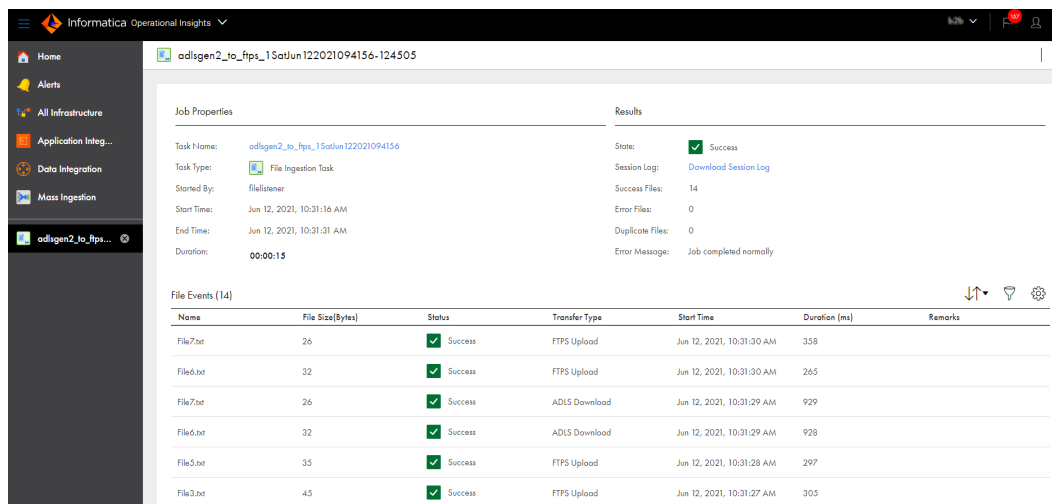
オンラインサイトは、取り込みジョブが特定のステータスを取得するか、DDL の変更を検出したときに、管理者が選択したユーザーとユーザーグループに一括取り込みアラート通知を送信します。

ファイル取り込みジョブの詳細

各ファイル取り込みタスクインスタンスのジョブの結果には、ジョブのステータスと、成功およびエラー統計が表示されます。

ファイル取り込みタスクの詳細を表示するには、一括取り込みの【マイジョブ】ページまたはオペレーションインサイトの一括取り込みページの【すべてのジョブ】タブで、タスク名をクリックします。

ジョブをダウンロードできます。次の図にファイル取り込みジョブの詳細を示します。



Job Properties		Results	
Task Name:	adlgen2_to_fps_1SatJun122021094156	State:	Success
Task Type:	File Ingestion Task	Session Log:	Download Session Log
Started By:	filelanner	Success Files:	14
Start Time:	Jun 12, 2021, 10:31:16 AM	Error Files:	0
End Time:	Jun 12, 2021, 10:31:31 AM	Duplicate Files:	0
Duration:	00:00:15	Error Message:	Job completed normally

Name	File Size(Bytes)	Status	Transfer Type	Start Time	Duration (ms)	Remarks
File7.txt	26	Success	FTPS Upload	Jun 12, 2021, 10:31:30 AM	358	
File6.txt	32	Success	FTPS Upload	Jun 12, 2021, 10:31:30 AM	265	
File7.txt	26	Success	ADLS Download	Jun 12, 2021, 10:31:29 AM	929	
File6.txt	32	Success	ADLS Download	Jun 12, 2021, 10:31:29 AM	928	
File5.txt	35	Success	FTPS Upload	Jun 12, 2021, 10:31:28 AM	297	
File3.txt	45	Success	FTPS Upload	Jun 12, 2021, 10:31:27 AM	305	

ジョブのプロパティ

ファイル取り込みタスクインスタンスのジョブのプロパティでは、インスタンスの全般プロパティが表示されます。

以下の表に、ジョブのプロパティを示します。

プロパティ	説明
タスク名	関連取り込みタスクの名前。タスク名のリンクをクリックして、一括取り込みでタスクの詳細を表示または編集できます。
タスクタイプ	タスクのタイプ。この場合はファイル取り込みタスク。
開始したユーザー名	ジョブを開始したユーザーまたはスケジュールの名前。
開始時刻	ジョブが開始された日時。
終了時刻	ジョブが完了または停止した日時。
継続時間	完了または停止するまでにジョブが実行された時間。

比較結果

ファイル取り込みタスクインスタンスのジョブの結果には、ジョブのステータスとエラー統計が表示されます。

ジョブの結果には次のプロパティが含まれます。

プロパティ	説明
状態	ジョブステータス。ジョブは、次のいずれかの状態になります。 <ul style="list-style-type: none">- 実行中。ジョブは継続して実行中です。- 成功。ジョブが正常に完了しました。- 失敗。エラーが発生したため、ジョブは完了しませんでした。- 強制終了。ジョブは強制終了されました。
セッションログ	セッションログファイルをダウンロードできます。デフォルトでは、Informatica Intelligent Cloud Services は、10 回の実行のセッションログを格納してから、最新の実行でログを上書きします。以前の実行のセッションログが必要な場合は、セッションログファイルを保持するディレクトリのバックアップを取ります。 セッションログファイルは、次のディレクトリに書き込まれます。 <Secure Agent installation directory>/apps/Data_Integration_Server/logs
成功ファイル	ターゲットへの転送、ダウンロード、アップロードが成功したファイルの数。
エラーファイル	ターゲットに転送されなかったファイルの合計数。
重複するファイル	重複として特定されたファイルの数。
エラーメッセージ	ジョブに関連付けられているエラーメッセージ（存在する場合）。

ファイルイベント

このセクションには、ファイル取り込みタスクで転送されたファイルの合計数と各ファイルの情報が表示されます。

[ファイルイベント] セクションは、ファイル取り込みタスクがファイルを転送するたびに更新され、ファイル転送プロセス全体でファイルの状態が更新されます。ファイルの転送の進行状況は、ファイルの状態に基づいて追跡できます。

[ファイルイベント] セクションには、各ファイルの次のプロパティが表示されます。

プロパティ	説明
名前	ファイルの名前。
ファイルサイズ	ファイルのサイズ（バイト単位）。

プロパティ	説明
ステータス	<p>ファイル転送のステータス。ファイルは、次のいずれかの状態になります。</p> <ul style="list-style-type: none"> - 成功。ファイル転送は正常に完了しました。 - 失敗。エラーが発生したため、ファイル転送は完了しませんでした。 - 処理中。ファイル転送が実行中です。 - 重複。以前に同じ名前、ディレクトリの場所、サイズのファイルを転送したタスクです。 - 中断。ファイル転送中にネットワークの問題が発生したか、サーバーの資格情報が変更されたため、ファイル転送が中断されました。ファイル取り込みタスクを実行して、中断されたファイルの転送を再開します。 <p>注: この状態は、ファイル取り込みタスクが高度な FTP ソース、高度な SFTP ソース、または高度な FTPS ソースとの間でファイルを転送するときに適用されます。</p> <ul style="list-style-type: none"> - 不明。ファイルの転送中に、前のタスクインスタンスがエラーを検出しました。ソースが重複ファイルをスキップするように設定されているタスクに適用できます。 - 隔離。タスクは、ソースから検出した感染ファイルを隔離済みとしてマークします。 <p>状態プロパティを監視して、各ファイルのファイル転送の進行状況を追跡できます。</p>
転送タイプ	<p>ファイル転送のタイプ。ファイルは、次のいずれかの転送タイプになります。</p> <ul style="list-style-type: none"> - <source_name>ダウンロード。ファイルはソースからダウンロードされます。<source_name>はソースの名前です。 - <target_name>アップロード。ファイルはターゲットにアップロードされます。<target_name>はターゲットの名前です。 - ソースからコピー。ファイル取り込みタスクはファイル処理アクションを実行しています。 - ターゲットへコピー。ファイルはローカルディレクトリからローカルディレクトリに転送されます。
開始時刻	ファイル転送が開始された日時。
継続時間	ファイル転送の時間（ミリ秒単位）。
コメント	失敗ステータスのファイルイベントに適用されます。メッセージには、ファイル転送タイプに基づくイベントの失敗の理由が含まれています。

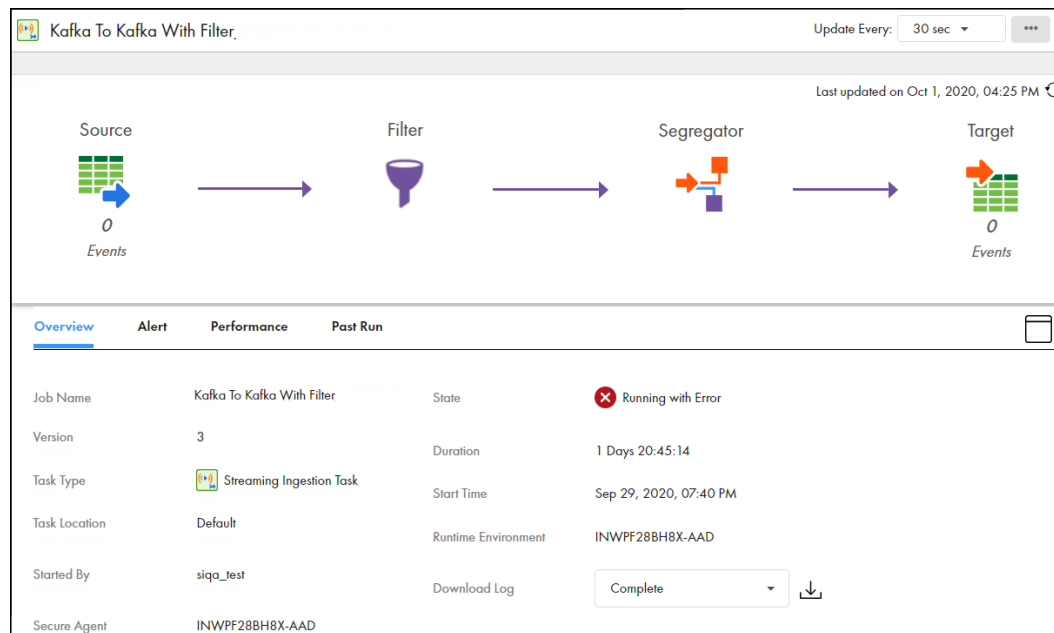
ストリーミング統合ジョブの詳細

ストリーミング統合ジョブの詳細を表示するには、一括取り込みの **【マイジョブ】** ページまたはオペレーションインサイトの一括取り込みページの **【すべてのジョブ】** タブで、ジョブ名をクリックします。

【概要】 タブ

【概要】 タブにはジョブの全般プロパティが表示されます。ジョブログをダウンロードする事もできます。

次の図に、ストリーミング統合ジョブの【概要】タブを示します。



以下の表で、ジョブの概要プロパティについて説明します。

プロパティ	説明
ジョブ名	ジョブの名前。
バージョン	ジョブのバージョン番号。
タスクタイプ	ストリーミング統合タスクのタスクタイプ。
タスクの場所	ストリーミング統合タスクを含むプロジェクトまたはプロジェクトフォルダ。
開始したユーザー名	ジョブをデプロイしたユーザーの名前。
Secure Agent	Secure Agent が実行されている場所。 Secure Agent の横に警告記号がある場合は、Secure Agent がオフラインかアクセスできないことを示します。
状態	ジョブの状態。 ジョブは、次のいずれかの状態になります。 <ul style="list-style-type: none"> - デプロイ中。ジョブはデプロイ中です。 - 稼働中。ジョブは実行中です。 - 実行中（警告あり）。ジョブは実行中ですが警告があります。 - 実行中（エラーあり）。ジョブは実行中ですがエラーがあります。警告が発生した状態でジョブが 7 分間またはランタイムオプションで指定した時間、継続的に実行すると、ジョブの状態は「実行中（エラーあり）」に変わります。 - アンデプロイ済み。ジョブはアンデプロイされています。 - 停止。ジョブが意図的に停止されました。
継続時間	ジョブがアンデプロイされるまでに実行した合計時間。合計時間は hh:mm:ss の形式で表示されます。

プロパティ	説明
開始時刻	ジョブがデプロイされた日付と時刻。
ランタイム環境	ジョブの実行で使用されるランタイム環境の名前。
ログのダウンロード	<p>実行中のジョブに対してダウンロードするログレベル。 次のいずれかのログをダウンロードすることができます。</p> <ul style="list-style-type: none"> - 完全。ログ全体。すべてのタイプのメッセージを含みます。状態に関係なく、実行した任意のジョブに利用できます。 - 最新。ログの最新バージョン。 <p>ログをローカルシステムにダウンロードするには、【ダウンロード】 アイコンをクリックします。</p>

【アラート】 タブ

【アラート】 タブには、イベントが発生したときのアラートメッセージが表示されます。

次の図に、ストリーミング統合ジョブの【アラート】 タブを示します。

KafkaToFlatfileTargetWithFormatConverterWithXML_FormatConverter

Source

499021 Events

FormatConverter

Overview Alert Performance Past Run

Alert

⚠ KafkaToFlatfileTargetWithFormatConverterWithXML_FormatConverter : ConvertRecord[id=6ee4a30e-9ed9-4e00-87bf-d6cc0e0... Show M...

⚠ KafkaToFlatfileTargetWithFormatConverterWithXML_FormatConverter : ConvertRecord[id=6ee4a30e-9ed9-4e00-87bf-d6cc0e0... Show M...

⚠ KafkaToFlatfileTargetWithFormatConverterWithXML_FormatConverter : ConvertRecord[id=6ee4a30e-9ed9-4e00-87bf-d6cc0e0... Show M...

⚠ KafkaToFlatfileTargetWithFormatConverterWithXML_FormatConverter : ConvertRecord[id=6ee4a30e-9ed9-4e00-87bf-d6cc0e0... Show M...

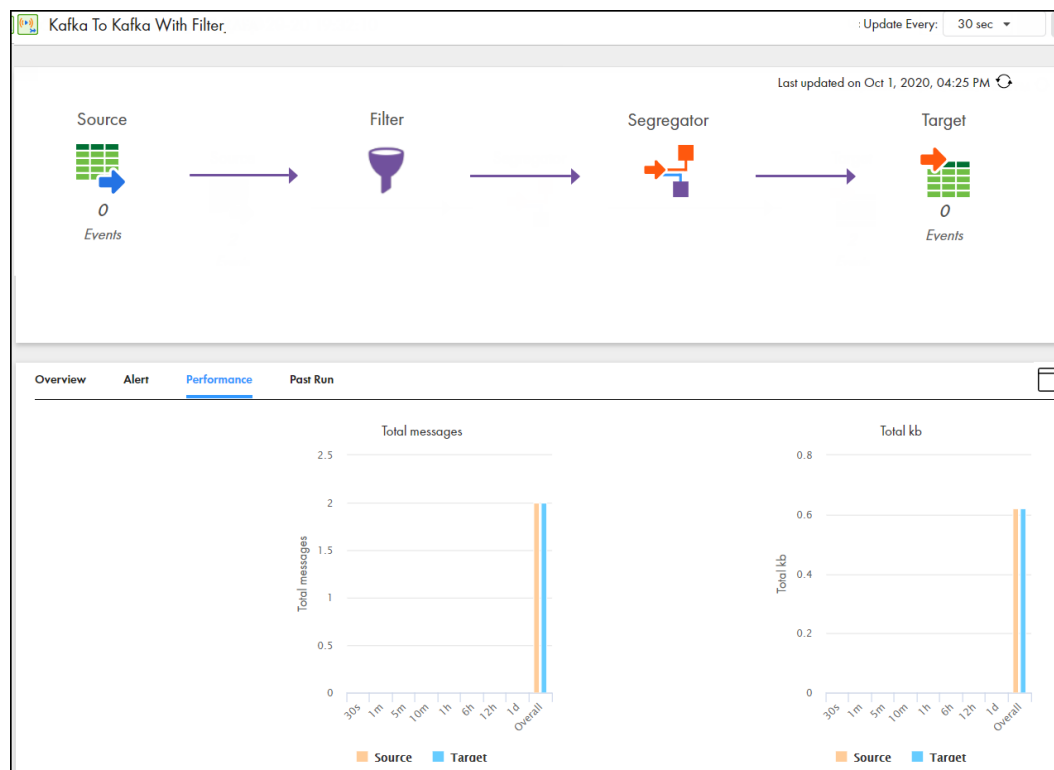
以下の表で、ジョブのアラートプロパティについて説明します。

プロパティ	説明
アラート	デプロイされたジョブに警告が発生したときにジョブが返すメッセージまたはメッセージのグループ。
時間	イベントが発生したときの日付と時刻。

[パフォーマンス] タブ

[パフォーマンス] タブには、ジョブのソースおよびターゲットのスループット情報のグラフが表示されます。

次の図に、ストリーミング統合ジョブの [パフォーマンス] タブを示します。



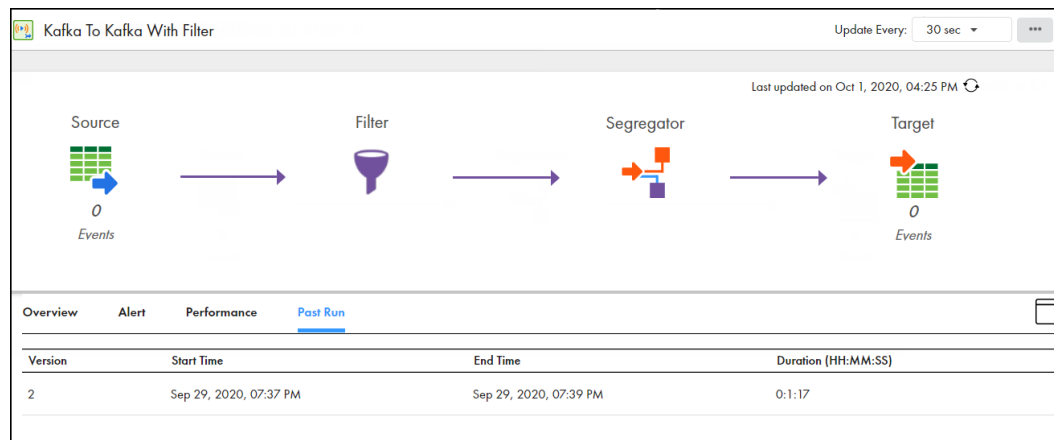
以下の表で、ジョブのパフォーマンスプロパティについて説明します。

プロパティ	説明
合計メッセージ	1 秒間にストリーミングされたメッセージ数の平均。
合計 KB	1 秒間にストリーミングされたメッセージのキロビット数の平均。

[過去の実行] タブ

[過去の実行] タブには、ストリーミング統合ジョブの以前の実行に関連する統計およびステータス情報が表示されます。

次の図に、ストリーミング統合ジョブの【過去の実行】タブを示します。



以下の表に、過去の実行のプロパティを示します。

カラム	説明
バージョン	ジョブのバージョン番号。
開始時刻	ジョブがデプロイされた日付と時刻。
終了時刻	ジョブがアンデプロイされたときの日付と時刻。
継続時間	ジョブがアンデプロイされるまでに実行した合計時間。合計時間は hh:mm:ss の形式で表示されます。

一括取り込みアラート

アプリケーション取り込みジョブまたはデータベース取り込みジョブが特定のステータス変更または DDL 変更を検出したときに、一括取り込みアラート通知をユーザーに送信するようにオペレーションインサイトを設定できます。例えば、ジョブのステータスが【失敗】または【実行中（警告あり）】に変わったときに、管理者に警告することができます。

ユーザーがアラートを設定するには、組織にジョブアラート機能を備えた

OperationalInsightsAdvancedEdition ライセンスが必要です。また、アラートを作成または変更するすべてのユーザーは、管理者またはオペレータのロール、あるいはオペレーションインサイトサービスに対する一括取り込みジョブのアラート機能が有効なカスタムロールを持っている必要があります。これらのロール要件は、アラートの確認だけを行うユーザーには関係ありません。

【アラート】 ページの【一括取り込みアラート】 タブから、アラートルールを作成、編集、または削除できます。アラートルールを作成するには、【アラートの作成】 をクリックします。リストされたアラートルールを集または削除するには、リストのルール行の右端にある鉛筆またはゴミ箱のアイコンをクリックします。

次のタイプのイベントのいずれかまたは両方が発生したときにアラートを送信するアラートルールを設定できます。

- アプリケーション取り込みジョブまたはデータベース取り込みジョブのステータスが、アラート用に選択したステータスに変わります

- DDL スキーマ変更イベントは、スキーマドリフトが有効な増分ロードジョブまたは初期および増分ロードジョブの組み合わせに対して発生します。

また、アラート通知の受信者、およびアラートルールを組織全体に適用するか、または選択した取り込みタスクに適用するかを指定します。

オペレーションインサイトは、アプリケーション取り込みとデータベース取り込みのアラートを 5 分ごとにポーリングします。

一括取り込みジョブのアラートの設定

アプリケーション取り込みジョブとデータベース取り込みジョブのアラートを設定して、ジョブのステータスと DDL の変更についてユーザーに通知できます。ファイル取り込みジョブとストリーミング取り込みジョブでは、アラートはサポートされていません。

1. **【アラート】** ページで、**【一括取り込みアラート】** タブをクリックします。
2. **【アラートの作成】** をクリックします。
3. **【アラートルールの作成】** ページで、アラートの詳細を設定します。
 - a. **【アラートルール名】** フィールドに、アラートの名前を入力します。最大長は 255 文字です。
 - b. **【アラートルールの説明】** フィールドに、必要に応じてアラートの説明を入力します。最大長は 255 文字です。
 - c. **【取り込みタイプ】** フィールドで、**【アプリケーション一括取り込み】** または **【データベース一括取り込み】**、あるいは両方のオプションを選択します。
 - d. **【ルールの適用先】** フィールドで、次のオプションのいずれかを選択して、アラートの範囲を設定します。
 - **組織全体**。アラートルールを組織内のすべてのジョブに適用します。
 - **タスクアセット**。選択した取り込みタスクに関連付けられたジョブにアラートルールを適用します。
4. **【アラート有効】** フィールドで、アラートルールを有効または無効にします。アラートの送信をすぐに開始しない場合は、アラートを無効にします。デフォルトでは、このアラートは有効になっています。
5. 次のいずれかまたは両方の方法でアラート条件を設定します。
 - ジョブステータスの変化に基づいてアラートを送信するには、アラートを送信する各ジョブステータスを選択します。デフォルトでは、**【失敗】** のみが選択されています。
 - ソーススキーマの変更が検出されたときにアラートを送信するには、**【DDL】** を選択します。このオプションは、スキーマドリフトオプションが有効になっている増分ロードジョブと、初期ロードジョブおよび増分ロードジョブの組み合わせに適用されます。
6. **【電子メールの送信先】** フィールドで、設定したアラートの電子メール通知を受信する Informatica Intelligent Cloud Services ユーザーまたはユーザーグループを選択します。

複数のユーザーを個別に選択するか、1 つ以上のユーザーグループを選択することができます。また、個々のユーザーとユーザーグループを任意に組み合わせで選択することもできます。選択できるようにするには、ユーザーとユーザーグループが Administrator サービスで事前に定義されている必要があります。

パート III: オンプレミスアプリケーションの監視

この部には、以下の章があります。

- [ドメインの登録と管理, 100 ページ](#)
- [Data Engineering Integration ドメインの監視, 114 ページ](#)
- [Data Quality ドメインの監視, 118 ページ](#)
- [PowerCenter ドメインの監視, 122 ページ](#)

第 8 章

ドメインの登録と管理

オペレーションインサイトを使用して監視する各 Informatica ドメインを登録する必要があります。ウィザードの案内に従って、処理を進めます。ドメインの登録は、オンプレミス製品にのみ必要となります。Informatica Intelligent Cloud Services のドメインは登録しません。

ドメインの登録プロセスの主な手順は次のとおりです。

1. ドメインへの接続を設定します。
2. ユーザーがドメインをより簡単に見つけられるように詳細を指定します。
3. コレクタを設定します。

登録プロセスを完了して最後のステップとして【保存】をクリックすると、コレクタでは、オペレーションインサイトで使用できるようにデータの収集と Informatica Intelligent Cloud Services へのアップロードが開始されます。

注: Informatica ドメインを以前のバージョンから 10.4.0 にアップグレードした場合は、オペレーションインサイトに登録されているドメインを編集して、アップグレードされた Informatica ドメインバージョンの詳細を反映させる必要があります。Data Engineering Integration バージョン 10.2.2 のドメインの統計を収集するには、ドメイン内の各 Data Engineering Integration ノードに EBF-14386 を適用する必要があります。

監視モデルリポジトリサービスの有効化

ドメインをオペレーションインサイトに登録する前に、監視モデルリポジトリサービスおよび関連するモデルリポジトリをドメインに設定する必要があります。

オペレーションインサイトは、ドメインの監視設定で指定されたモデルリポジトリから、ドメインノードの CPU およびメモリ消費メトリックを抽出します。モデルリポジトリで管理するモデルリポジトリサービスは、監視モデルリポジトリサービスと呼ばれます。

インストーラを実行してドメインを作成するときに、監視モデルリポジトリサービスを作成できます。詳細については、Informatica の『Data Engineering インストールガイド』の「アプリケーションサービスとデータベースの準備」の章を参照してください。

Administrator ツールを使用して、ドメイン内の監視モデルリポジトリサービスを設定することもできます。詳細については、『Informatica アプリケーションサービスガイド』の「監視モデルリポジトリサービス」を参照してください。

ドメイン接続の設定

オペレーションインサイトがドメインに接続できるようにするために必要な情報を入力します。オペレーションインサイトが、Informatica Administrator としてドメインに接続できる必要があります。

1. オペレーションインサイトのナビゲーション バーで **【すべてのインフラストラクチャ】** をクリックします。
2. **【ドメイン】 > 【ドメインの登録】** をクリックします。
3. 次の全般プロパティを入力します。

プロパティ	説明
ドメイン表示名	オペレーションインサイトのユーザーインターフェースに表示するドメイン名。任意の名前を割り当てることができますが、名前はオペレーションインサイト内で一意である必要があります。
ドメイン名	Informatica Administrator (Administrator ツール) に表示されるドメイン名。
マスターゲートウェイノードのホスト	マスターゲートウェイノードマシンのホスト名。Administrator ツールのノードの 【全般プロパティ】 > 【ホスト名】 プロパティに示されている値を正確に入力します。 Administrator ツールでこの値を見つけるには、次の手順を実行します。 <ul style="list-style-type: none">- 【サービスおよびノード】 ビューを選択し、ドメインナビゲータでノードを選択します。- 【全般プロパティ】 で、【ホスト名】 プロパティを見つけます。
ゲートウェイノードのポート	ゲートウェイノードが使用する HTTP ポート。
ドメインバージョン	ドメインにインストールされている Informatica リリース。オペレーションインサイトは、すべての Informatica リリース 10.x ドメイン内のアセットを監視できます。
製品	オペレーションインサイトを使用して監視する Informatica 製品。製品はドメインバージョンに基づいて選択されます。

4. ドメインからデータを収集して Informatica Intelligent Cloud Services にアップロードする Secure Agent を選択します。

プロパティ	説明
Secure Agent グループ	ドメインにインストールされている Secure Agent が属するグループ。
Secure Agent 名	ドメインにインストールされている Secure Agent の名前。

5. 次のドメインセキュリティの詳細を入力します。

プロパティ	説明
セキュリティドメイン	ドメインが使用するセキュリティドメインを選択します。
管理者ユーザー名	Informatica ドメイン管理者アカウントのユーザー名。
管理者パスワード	Informatica ドメイン管理者アカウントのパスワード。
TLS が有効	ドメインが Transport Layer Security (TLS) プロトコルで保護されているかどうかを選択します
トラストストアのパス	ドメインが TLS で保護されている場合は、infa_truststore.jks ファイルをドメインノードから Secure Agent ホストにコピーし、Secure Agent ホスト上のファイルのパスとファイル名を指定します。 デフォルトでは、ファイルは各ドメインノードの次のディレクトリにインストールされます。 <Informatica インストールディレクトリ>\services\shared\security
トラストストアのパスワード	ドメインでカスタムのトラストストアファイルが使用されている場合は、暗号化されたトラストストアのパスワードを指定します。

6. 次のドメイン自動スケーリングの詳細を入力して、グリッドに追加されたエラスティックノードがドメインと通信できるようにします。

プロパティ	説明
sitekey のパス	sitekey ファイルをドメインノードから Secure Agent ホストにコピーし、Secure Agent ホスト上のファイルのパスとファイル名を指定します。 デフォルトでは、ファイルは各ドメインノードの次のディレクトリにインストールされます。 <Informatica インストールディレクトリ>\isp\config\keys
キーストアのパス	ドメインが TLS で保護されている場合は、infa_keystore.jks ファイルをドメインノードから Secure Agent ホストにコピーし、Secure Agent ホスト上のファイルのパスとファイル名を指定します。 デフォルトでは、ファイルは各ドメインノードの次のディレクトリにインストールされます。 <Informatica インストールディレクトリ>\services\shared\security
キーストアのパスワード	ドメインでカスタムキーストアファイルが使用されている場合は、暗号化されたキーストアパスワードを指定します。

7. **【テスト接続】** をクリックして、マスターゲートウェイノードへの接続をテストします。

ドメインの詳細の入力

ユーザーがオペレーションインサイト内でドメインを見つけられるように、詳細を入力します。

タグを使用してドメインを分類できます。ユーザーはタグを使用してドメインを検索できます。また、ドメインの使用法を示すためのドメインタイプの選択を行います。

また、インタラクティブマップ上の地理的な場所ごとにドメインを整理することもできます。マップは、オペレーションインサイトのホームページに表示されます。ドメインを場所に割り当てると、パフォーマンスを分析し、企業全体の容量と処理能力を決定するために役立ちます。

1. [ドメインの詳細] でドメインにタグを割り当てます。複数のタグをドメインに割り当てることができます。
 - 既存のタグを割り当てするには、リストから選択します。
 - 新しいタグを追加するには、入力フィールドにタグを入力してから、キーボードの **Enter** キーを押します。
2. 組織内でのドメインの使用法に最も適したドメインタイプを選択します。
3. マップ上のドメインの場所を指定します。
 - ドメインを既存の場所に割り当てするには、マップ上の場所をクリックします。
 - ドメインを新しい場所に割り当てするには、マップ上で場所を追加する場所をクリックし、場所の名前を入力します。
4. [次へ] をクリックして、入力した情報を保存します。

ドメインの設定設定コレクタ

ドメインおよびすべてのドメインアセットの設定メタデータを収集してアップロードするドメイン設定コレクタを設定します。

デフォルトの収集頻度は 24 時間ごとです。必要に応じて、要件に合わせてカスタムスケジュールを作成できます。

このコレクタはデフォルトで有効になっています。コレクタを無効にすることはできません。

コレクタスケジュールの設定

コレクタにカスタムスケジュールを設定できます。作成したスケジュールによって、デフォルトのコレクタスケジュールが上書きされます。

以下のプロパティを入力します。

プロパティ	説明
繰り返す	収集を繰り返す間隔。
繰り返し頻度	収集を実行する頻度。 頻度は、選択した繰り返し値に基づきます。例えば、2 時間ごとにデータを収集するには、繰り返しとして [毎時] を選択し、頻度の値を 2 に設定します。

プロパティ	説明
開始	カスタムスケジュールが有効になる日時。
タイムゾーン	スケジュールの基準となるタイムゾーン。

ドメインの設定健全性統計コレクタ

ドメインアセットの可用性の統計を収集してアップロードするドメイン健全性統計コレクタを設定します。

デフォルトの収集頻度は 5 分ごとです。必要に応じて、要件に合わせてカスタムスケジュールを作成できます。

このコレクタはデフォルトで有効になっています。コレクタを無効にするには、**【有効】** チェックボックスをオフにします。

コレクタスケジュールの設定

コレクタにカスタムスケジュールを設定できます。作成したスケジュールによって、デフォルトのコレクタスケジュールが上書きされます。

以下のプロパティを入力します。

プロパティ	説明
繰り返す	収集を繰り返す間隔。
繰り返し頻度	収集を実行する頻度。 頻度は、選択した繰り返し値に基づきます。例えば、2 時間ごとにデータを収集するには、繰り返しとして [毎時] を選択し、頻度の値を 2 に設定します。
開始	カスタムスケジュールが有効になる日時。
タイムゾーン	スケジュールの基準となるタイムゾーン。

ドメインの設定リソース使用率統計コレクタ

ドメイン内のすべてのノードの CPU とメモリの消費量メトリックを収集してアップロードするドメインリソース使用率統計コレクタを設定します。

このメトリックは、ドメインの監視設定で指定されたモデルリポジトリから抽出されます。モデルリポジトリへの接続を設定する必要があります。

デフォルトの収集頻度は 1 時間ごとです。必要に応じて、要件に合わせてカスタムスケジュールを作成できます。

このドメインはデフォルトで有効になっています。コレクタを無効にするには、**【有効】** チェックボックスをオフにします。

履歴データの収集

オペレーションインサイトに最大 60 日間の履歴データを入力するようにコレクタを設定できます。

デフォルトでは、過去 30 日間の履歴データが収集されます。ただし、1 から 60 までの任意の日数を指定できます。

データ収集は、ドメインがオペレーションインサイトに追加された時点で開始されます。1 時間ごとに約 24 時間分のデータが収集されます。つまり、オペレーションインサイトに前月のデータを入力するには、約 30 時間が必要です。

履歴データの収集はデフォルトで有効になっています。履歴データの収集を無効にするには、**【履歴データの収集】** チェックボックスをオフにします。

監視統計モデルリポジトリへの接続

監視モデルリポジトリに関連付けられたモデルリポジトリから、ドメインノードの CPU およびメモリ消費量メトリックを収集するために必要な情報を入力します。

接続情報を入力する必要があるのは、ドメインリソース使用率統計コレクタまたは Data Engineering Integration コレクタのいずれかを設定するときのみです。両方のコレクタで同じ情報が使用されます。

ドメインの管理に使用する Administrator ツールを使用して、必要なプロパティ値を見つけます。

- **【サービスとノード】** ビューを選択します。
- **【監視設定】** タブをクリックし、モデルリポジトリサービスの名前をメモします。
- ドメインナビゲータでモデルリポジトリサービスインスタンスを選択し、**【リポジトリデータベースプロパティ】** の下に表示されているプロパティをメモします。

必要なプロパティ値を見つけたら、次の手順を実行して、モデルリポジトリへの接続を設定します。

1. 次の必須プロパティを入力します。

プロパティ	説明
データベースタイプ	モデルリポジトリデータベースのタイプ。
ユーザー名	モデルリポジトリデータベースのユーザー名。
パスワード	モデルリポジトリデータベースのパスワード。
JDBC 接続文字列	<p>モデルリポジトリデータベースへの接続に使用される JDBC 接続文字列。</p> <p>必要に応じて、名前付きインスタンスの JDBC URL を指定して、SQL Server データベースに接続できます。文字列を次のように書式設定します。</p> <pre>jdbc:informatica:sqlserver://<データベースのホスト名>\<名前付きインスタンス名>;databaseName=<データベース名></pre> <p>Windows 認証接続文字列を指定して、Windows 認証を使用して SQL Server データベースに接続することもできます。文字列を次のように書式設定します。</p> <pre>jdbc:informatica:sqlserver://<データベースのホスト名>:<データベースのポート>;DatabaseName=<データベース名>;SnapshotSerializable=true;AuthenticationMethod=ntlmjava;Domain=<SQL Server のドメイン名></pre> <p>接続には NTLM 認証スキームが使用されることに注意してください。</p>

2. 次のオプションのプロパティを入力します。

プロパティ	説明
セキュア JDBC パラメータ	モデルリポジトリデータベースが SSL プロトコルで保護されている場合は、セキュアデータベースパラメータ。
スキーマ名	監視データを含むモデルリポジトリデータベース内のスキーマ名。
テーブルスペース名	モデルリポジトリデータベースが IBM DB2 データベースの場合は、監視データを含むテーブルスペースの名前を指定できます。

3. **【テスト接続】** をクリックし、接続設定を確認します。

コレクタスケジュールの設定

コレクタにカスタムスケジュールを設定できます。作成したスケジュールによって、デフォルトのコレクタスケジュールが上書きされます。

以下のプロパティを入力します。

プロパティ	説明
繰り返す	収集を繰り返す間隔。
繰り返し頻度	収集を実行する頻度。 頻度は、選択した繰り返し値に基づきます。例えば、2 時間ごとにデータを収集するには、繰り返しとして 【毎時】 を選択し、頻度の値を 2 に設定します。
開始	カスタムスケジュールが有効になる日時。
タイムゾーン	スケジュールの基準となるタイムゾーン。

PowerCenter リポジトリコレクタの設定

ドメイン内の PowerCenter リポジトリからランタイムワークフローとセッションメトリックを収集してアップロードする PowerCenter リポジトリコレクタを設定します。このコレクタを設定するには、**【ドメイン接続】** パネルのドメインで使用する製品のリストで **【PowerCenter】** を選択する必要があります。

ドメイン内の各 PowerCenter リポジトリデータベースへの接続を設定する必要があります。

デフォルトの収集頻度は 1 時間ごとです。必要に応じて、要件に合わせてカスタムスケジュールを作成できます。

このコレクタはデフォルトで無効になっています。コレクタを有効にするには、**【有効】** チェックボックスを選択します。

履歴データの収集

オペレーションインサイトに最大 60 日間の履歴データを入力するようにコレクタを設定できます。

デフォルトでは、過去 30 日間の履歴データが収集されます。ただし、1 から 60 までの任意の日数を指定できます。

データ収集は、ドメインがオペレーションインサイトに追加された時点で開始されます。1 時間ごとに約 24 時間分のデータが収集されます。つまり、オペレーションインサイトに前月のデータを入力するには、約 30 時間が必要です。

履歴データの収集はデフォルトで有効になっています。履歴データの収集を無効にするには、**【履歴データの収集】** チェックボックスをオフにします。

PowerCenter リポジトリの追加

ドメインが PowerCenter ドメインである場合は、ドメイン内の各 PowerCenter リポジトリデータベースへの接続を設定します。PowerCenter リポジトリデータベースへの接続に使用する JDBC 接続文字列を指定します。必要に応じて、セキュアなデータベースへの接続に必要なパラメータを指定できます。

1. **【PowerCenter リポジトリの追加】** をクリックします。
2. 次の必須プロパティを入力します。

プロパティ	説明
データベースタイプ	PowerCenter リポジトリデータベースのタイプ。
サービス名	PowerCenter リポジトリデータベースを管理する PowerCenter リポジトリサービスの名前。
ユーザー名	PowerCenter リポジトリデータベースのユーザー名。
パスワード	PowerCenter リポジトリデータベースのパスワード。
JDBC 接続文字列	<p>PowerCenter リポジトリデータベースへの接続に使用される JDBC 接続文字列。必要に応じて、名前付きインスタンスの JDBC URL を指定して、SQL Server データベースに接続できます。文字列を次のように書式設定します。</p> <p><code>jdbc:informatica:sqlserver://<データベースのホスト名>\<名前付きインスタンス名>;databaseName=<データベース名></code></p> <p>Windows 認証接続文字列を指定して、Windows 認証を使用して SQL Server データベースに接続することもできます。文字列を次のように書式設定します。</p> <p><code>jdbc:informatica:sqlserver://<データベースのホスト名>:<データベースのポート>;DatabaseName=<データベース名>;SnapshotSerializable=true;AuthenticationMethod=ntlmjava;Domain=<SQL Server のドメイン名></code></p> <p>接続には NTLM 認証スキームが使用されることに注意してください。</p>

3. 次のオプションのプロパティを入力します。

プロパティ	説明
セキュア JDBC パラメータ	PowerCenter リポジトリデータベースが SSL プロトコルで保護されている場合は、データベースパラメータを保護します。
スキーマ名	監視データを含む PowerCenter リポジトリデータベース内のスキーマ名。 Administrator ツールでこの値を見つけるには、[サービスとノード] ビューを選択し、ドメインナビゲータで PowerCenter リポジトリサービスインスタンスを選択します。
テーブル名	監視データを含む PowerCenter リポジトリデータベース内のテーブル。 Administrator ツールでこの値を見つけるには、[サービスとノード] ビューを選択し、ドメインナビゲータで PowerCenter リポジトリサービスインスタンスを選択します。

4. [リポジトリを有効にする] チェックボックスを選択して、コレクタがリポジトリからデータを収集できるようにします。
5. [テスト接続] をクリックし、接続設定を確認します。
6. [保存] をクリックし、接続の詳細を保存します。
7. ドメイン内の PowerCenter リポジトリごとに、このプロセスを繰り返します。

コレクタスケジュールの設定

コレクタにカスタムスケジュールを設定できます。作成したスケジュールによって、デフォルトのコレクタスケジュールが上書きされます。

以下のプロパティを入力します。

プロパティ	説明
繰り返す	収集を繰り返す間隔。
繰り返し頻度	収集を実行する頻度。 頻度は、選択した繰り返し値に基づきます。例えば、2 時間ごとにデータを収集するには、繰り返しとして [毎時] を選択し、頻度の値を 2 に設定します。
開始	カスタムスケジュールが有効になる日時。
タイムゾーン	スケジュールの基準となるタイムゾーン。

Data Engineering Integration コレクタの設定

クラスタで実行されるジョブの統計を含む、ドメインで使用する Hadoop クラスタの統計を収集してアップロードするように、Data Engineering Integration コレクタを設定します。コレクタを設定するには、[ドメイン接続] パネルのドメインで使用する製品のリストで [Data Engineering Integration] を選択する必要があります。

デフォルトの収集頻度は 1 時間ごとです。要件に合わせて、カスタムスケジュールを作成できます。

このコレクタはデフォルトで有効になっています。コレクタを無効にするには、**【有効】** チェックボックスをオフにします。

コレクタの設定が完了したら、**【完了】** をクリックします。

注: Data Engineering Integration バージョン 10.2.2 のドメインの統計を収集するには、ドメイン内の各 Data Engineering Integration ノードに EBF-14386 を適用する必要があります。

履歴データの収集

オペレーションインサイトに最大 60 日間の履歴データを入力するようにコレクタを設定できます。

デフォルトでは、過去 30 日間の履歴データが収集されます。ただし、1 から 60 までの任意の日数を指定できます。

データ収集は、ドメインがオペレーションインサイトに追加された時点で開始されます。1 時間ごとに約 24 時間分のデータが収集されます。つまり、オペレーションインサイトに前月のデータを入力するには、約 30 時間が必要です。

履歴データの収集はデフォルトで有効になっています。履歴データの収集を無効にするには、**【履歴データの収集】** チェックボックスをオフにします。

クラスタ設定の選択

ドメインが Data Engineering Integration ドメインである場合は、ドメインが Hadoop クラスタに接続するために使用するクラスタ設定を選択します。Data Engineering Integration コレクタは、クラスタ設定を使用して、クラスタのジョブ実行の統計とオペレーションメトリックを収集します。

ドメインで作成されたクラスタ設定は、Informatica Administrator (Administrator ツール) の **【接続】** タブで表示できます。

1. **【クラスタ設定の選択】** をクリックします。
2. メニューから、Hadoop クラスタへの接続に使用するクラスタ設定を選択します。
3. **【クラスタ設定を有効にする】** チェックボックスを選択して、コレクタがクラスタからデータを収集できるようにします。
4. セキュアなクラスタに接続するには、**【TLS が有効】** をクリックし、クラスタのトラストストアファイルのパスとパスワードを指定します。
5. **【保存】** をクリックして設定を保存します。

コレクタスケジュールの設定

コレクタにカスタムスケジュールを設定できます。作成したスケジュールによって、デフォルトのコレクタスケジュールが上書きされます。

以下のプロパティを入力します。

プロパティ	説明
繰り返す	収集を繰り返す間隔。
繰り返し頻度	収集を実行する頻度。 頻度は、選択した繰り返し値に基づきます。例えば、2 時間ごとにデータを収集するには、繰り返しとして 【毎時】 を選択し、頻度の値を 2 に設定します。

プロパティ	説明
開始	カスタムスケジュールが有効になる日時。
タイムゾーン	スケジュールの基準となるタイムゾーン。

Kerberos 認証を使用した、保護されたクラスタへの接続

Data Engineering Integration コレクタが、Kerberos 認証を使用して保護されたクラスタから分析を収集する場合は、Data Engineering Integration ドメインが使用する Secure Agent の設定にカスタム Kerberos プロパティを追加する必要があります。

コレクタが使用する Secure Agent をを見つけるには、次の手順を実行します。

1. オペレーションインサイトにログインします。
2. ドメインを選択してから **【詳細】** タブをクリックします。
3. [Secure Agent グループ] プロパティで、ドメインが使用する Secure Agent の名前を見つけます。
4. 左側のナビゲーションバーにある **【Secure Agent】** をクリックします。
5. Secure Agent を選択してから **【管理】** をクリックします。
Administrator アプリケーションで Secure Agent の **【詳細】** ページが開きます。
6. **【編集】** をクリックします。
7. このページの [カスタム設定] セクションのプロパティの横にあるプラス記号 (+) をクリックして、新しいカスタムプロパティを追加します。
8. プロパティごとに、[サービス] メニューから **【OpsInsights データコレクタ】** を選択し、[タイプ] メニューから **【OpsInsights】** を選択します。
9. 次のカスタムプロパティを入力します。以下の表に、追加するプロパティを示します。

名前	値
kerberosPrincipal	クラスタでデータ統合サービスのジョブを実行するユーザーに Active Directory で割り当てられたサービスプリンシパル名 (SPN)。
kerberosKeyTabFile	Secure Agent が実行されているノード上の keytab ファイルのパスとファイル名。 Linux ホストおよび Windows ホストの両方で、次のように値を指定します。 /<Secure Agent インストールディレクトリ>/<ファイル名>.keytab
kerberosConfFile	Secure Agent が実行されているノード上の krb5.conf ファイルへのパス。 Linux ホストおよび Windows ホストの両方で、次のように値を指定します。 /<Secure Agent インストールディレクトリ>/krb5.conf

10. **【保存】** をクリックします。

Data Quality コレクタの設定

クラスタで実行される Data Quality ジョブの統計を収集してアップロードするように Data Quality コレクタを設定します。コレクタを設定するには、[ドメイン接続] パネルのドメインで使用する製品のリストで [Data Quality] を選択する必要があります。

デフォルトの収集頻度は 1 時間ごとです。要件に合わせて、カスタムスケジュールを作成できます。

このコレクタはデフォルトで有効になっています。コレクタを無効にするには、**[有効]** チェックボックスをオフにします。

コレクタの設定が完了したら、**[完了]** をクリックします。

コレクタスケジュールの設定

コレクタにカスタムスケジュールを設定できます。作成したスケジュールによって、デフォルトのコレクタスケジュールが上書きされます。

以下のプロパティを入力します。

プロパティ	説明
繰り返す	収集を繰り返す間隔。
繰り返し頻度	収集を実行する頻度。 頻度は、選択した繰り返し値に基づきます。例えば、2 時間ごとにデータを収集するには、繰り返しとして [毎時] を選択し、頻度の値を 2 に設定します。
開始	カスタムスケジュールが有効になる日時。
タイムゾーン	スケジュールの基準となるタイムゾーン。

オンボーディング設定の最終処理

オンボーディングプロセスが完了すると、コレクタはオペレーションインサイトで使用できるようにデータの収集と Informatica Intelligent Cloud Services へのアップロードを開始します。

[保存] をクリックして、ドメインのオンボーディングプロセスを完了し、データの収集を開始します。

ドメインの検索

ドメインに割り当てられた属性またはタグを検索パラメータとして使用して、特定のドメインを検索できます。

キー値ペアとしてドメイン属性を指定します。タグの場合は、タグ値のみを指定します。複数のパラメータはカンマで区切ります。

例えば、「Production」というタグが割り当てられたロンドンのドメインを検索するには、次のようなクエリを入力します。

loc:London,Production

検索条件に一致するドメインが、ページに動的に表示されます。

ドメインの編集または登録解除

ドメインの登録詳細を編集できます。ドメインの登録を解除することもできます。

ドメインの登録を解除すると、収集されたすべての運用データが削除され、復元できなくなります。また、ドメインで自動スケーリングが有効になっている場合は、自動スケーリングの設定も削除されます。ただし、クラウドで実行されているエラスティックノードは削除されません。クラウドからエラスティックノードを手動で削除する必要があります。

1. ページの左側にあるナビゲーションバーで **【すべてのインフラストラクチャ】** をクリックします。
2. ドメインをクリックします。
3. **【監視】** タブまたは **【詳細】** タブをクリックします。
4. 編集メニューから、**【ドメインの編集】** または **【ドメインの登録解除】** を選択します。

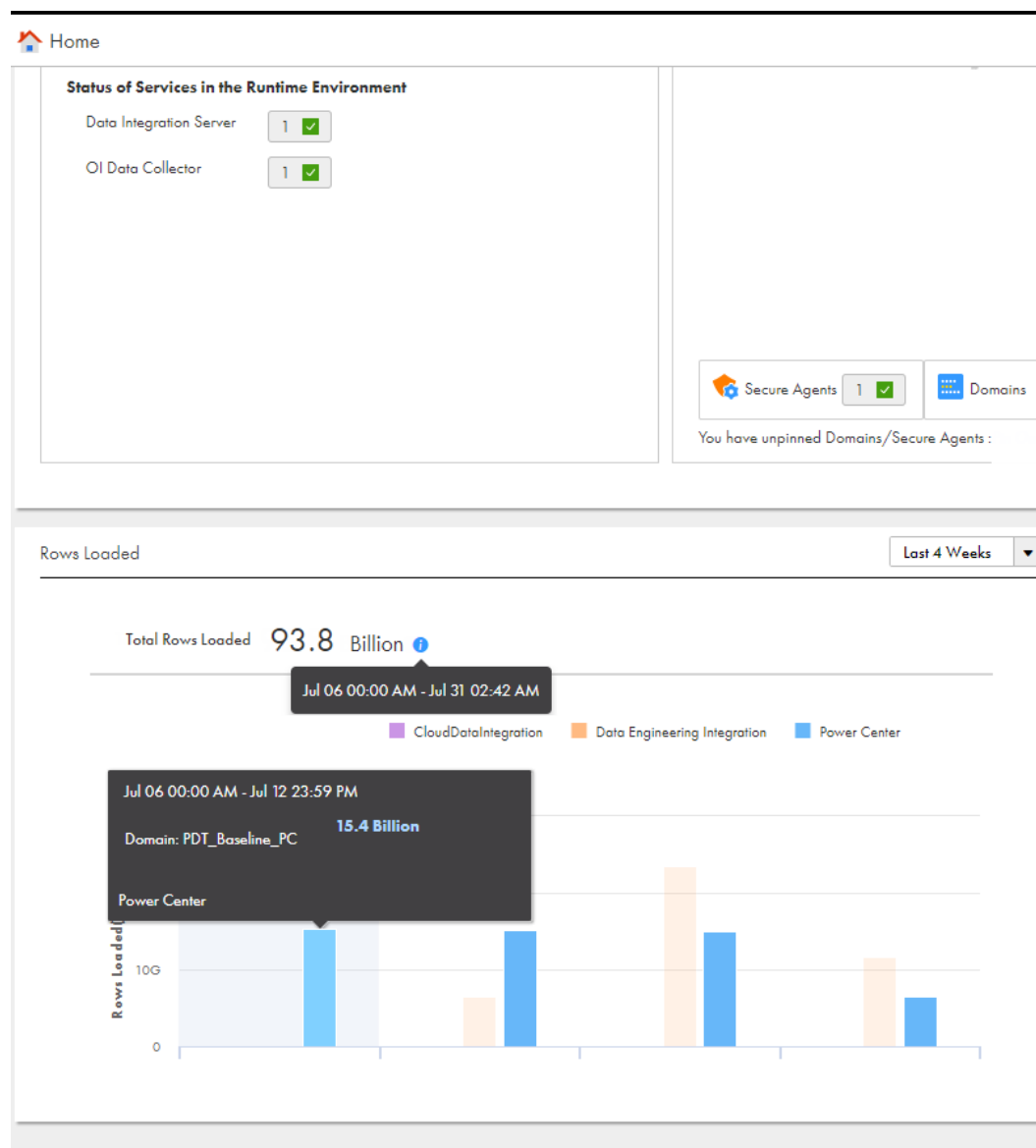
タイムゾーンの設定

オペレーションインサイトは、時間を協定世界時（UTC）形式で保存します。

ログインすると、オペレーションインサイトは時間を変換し、ユーザープロファイルに関連付けられたタイムゾーンの時間が表示されます。ユーザープロファイルを編集し、要件に基づいてタイムゾーンを選択できます。ユーザープロファイルの時間を設定していない場合、または時間が利用できない場合、タイムゾーンは PDT で表示されます。

すべてのオペレーションインサイトページにあるグラフのデータにカーソルを合わせると、統計のサマリーに、ユーザープロファイルで設定されたタイムゾーンのデータが表示されます。さらに、ツールチップには、Data Engineering Integration、Data Quality、および PowerCenter のジョブの時間範囲が表示されます。

例えば、次の図では、ユーザプロフィールで設定されたタイムゾーンでインフラストラクチャ内のすべてのサービスとドメインについて、過去 4 週間または過去 6 か月間に読み込まれた合計行数のサマリを確認できます。



第 9 章

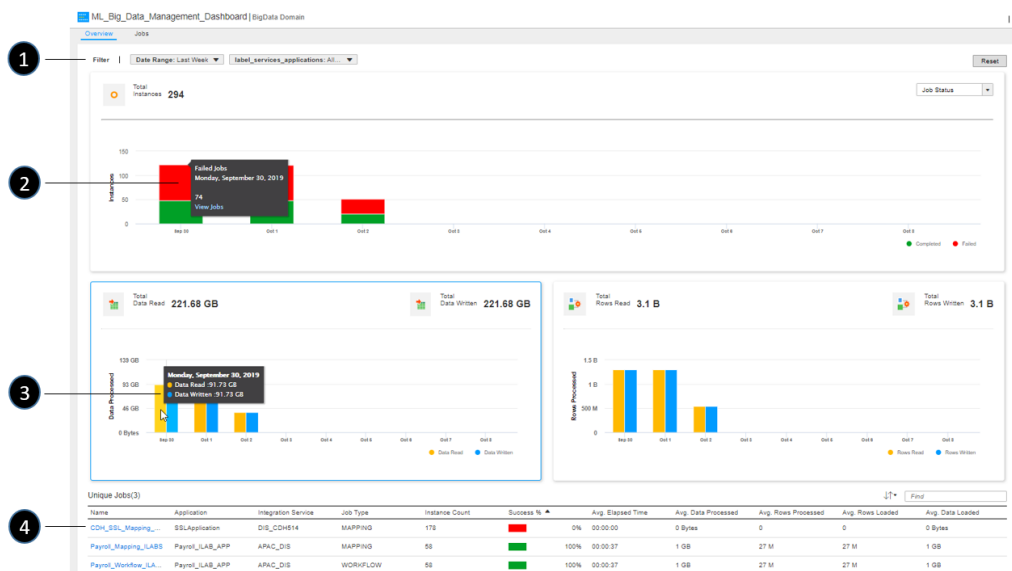
Data Engineering Integration ドメインの監視

オペレーションインサイトを使用して、Data Engineering Integration ドメインを監視できます。[概要] ページを使用して、特定の Data Engineering Integration ドメインのジョブ実行の統計とデータ処理の傾向を表示します。

ページを表示するには、次の手順を実行します。

1. 左側のナビゲーションバーにある **[Data Engineering Integration]** をクリックします。
2. **[ドメイン]** パネルでドメインをクリックします。
3. **[概要]** タブをクリックします。

ページの上部には、選択した日付範囲、データ統合サービスインスタンス、およびクラスタのジョブ実行とデータ処理の統計が表示されます。デフォルトでは、このテーブルには、過去 7 日間に登録済みクラスタにジョブを送信するデータ統合サービスインスタンスによって実行されたマッピングおよびワークフロージョブのデータが表示されます。



次の表に、このページから実行できるタスクを示します。

タ ス ク	説明
1	フィルタを使用して、データを表示する日付範囲、データ統合サービスインスタンス、および Hadoop クラスタを選択します。ページに表示されるデータは、フィルタ設定に基づいて更新されます。デフォルトでは、ドメイン内のすべてのデータ統合サービスインスタンスおよび Hadoop クラスタについて、過去 7 日間のデータが表示されます。
2	[合計インスタンス数] グラフで、ジョブの完了ステータス、ジョブタイプ、または実行エンジン別にジョブを表示するかどうかを選択します。グラフのバーセグメントにカーソルを合わせ、 [ジョブを表示] をクリックして詳細を表示します。
3	カーソルを [合計データ読み取り] グラフと [合計行数読み取り] グラフに移動して、フィルタで指定された時間範囲の詳細を表示します。
4	[一意のジョブ] リージョンのリンクをクリックして、選択した日付範囲、サービスおよびクラスタの一意のワークフローおよびマッピングの詳細を表示します。詳細については、 「Data Engineering Integration ジョブの分析の表示」 (ページ 115) を参照してください。

Data Engineering Integration ジョブの分析の表示

Data Engineering Integration ジョブ実行の統計を使用して、ジョブ実行パフォーマンスを評価し、失敗したジョブや長時間実行されているジョブを特定して、問題をトラブルシューティングします。

フィルタを使用して、表示するジョブ実行データをドリルダウンします。各ページに表示されるデータは、設定したフィルタの組み合わせに基づきます。

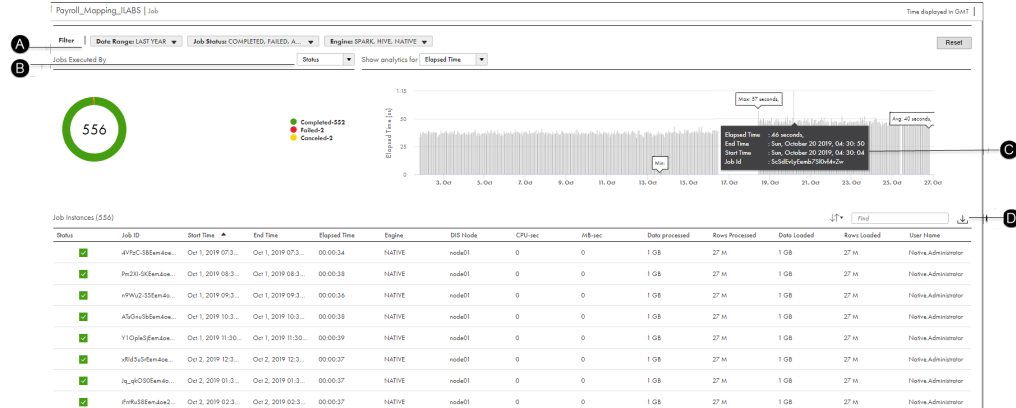
ジョブ実行データの表示

ジョブ実行時に収集されたサマリデータを使用して、ジョブ実行のパフォーマンスを把握できます。指定した時間範囲のジョブの全体的なパフォーマンスを、データ統合サービス別、およびジョブタイプ別に表示できます。また、失敗率が増加しているジョブや、実行時間が増加しているジョブを特定することもできます。

- ドメインをクリックします。
- [ジョブ]** タブをクリックします。
- フィルタを使用して、データを表示するジョブを選択します。
フィルタ設定に従ってテーブルが更新されます。デフォルトでは、このテーブルには過去 7 日間に実行されたすべてのジョブのデータが表示されます。
- 詳細を表示するには、テーブル内のジョブをクリックします。
個々のジョブインスタンスの統計を表示するページがロードされます。フィルタを使用して、表示するデータを選択します。**[フィールドの追加]** メニューからフィルタリングする追加のカラムを選択できます。

5. テーブル内のジョブをクリックします。

ジョブ実行の統計を表示するグラフがページにロードされます。経過した実行時間、処理済みのデータの量、ソース行から読み取られたデータ量、およびターゲット行に書き込まれたデータ量ごとに統計を表示できます。グラフには、設定したフィルタに基づいたデータが表示されます。



- A. フィルタを使用して、表示するジョブデータを選択します。
- B. ジョブをステータス別に表示するか、実行エンジン別に表示するかを選択します。
- C. グラフ上でカーソルを移動すると、特定の詳細が表示されます。グラフを拡大して、特定のタイムフレームの詳細を表示できます。詳細については、「[グラフの詳細の拡大](#)」(ページ 32)を参照してください。
- C. グラフ上でカーソルを移動すると、特定の詳細が表示されます。グラフを拡大して、特定のタイムフレームの詳細を表示できます。詳細については、「Informatica Intelligent Cloud Services の監視」を参照してください。
- D. アイコンをクリックして、テーブルデータをカンマ区切り値 (.csv) ファイルにダウンロードします。

Data Engineering Integration プロジェクトの作成

オペレーションインサイトで作成して、Data Engineering Integration アセットを監視することができます。

プロジェクトとは、Data Engineering Integration ドメインにデプロイされたサービスとアプリケーションのグループです。作成した各プロジェクトのサービスとアプリケーションのデータ処理分析およびジョブ実行の統計を表示できます。

1. 左側のナビゲーションバーにある **[Data Engineering Integration]** をクリックします。
2. **[プロジェクト]** タブをクリックします。
Data Quality プロジェクトが表示された **[プロジェクト]** ページが開きます。各プロジェクトのパネルには、過去 7 日間に実行されたジョブのサマリデータが表示されます。
3. **[プロジェクトの作成]** をクリックします。
4. プロジェクトの名前を入力します。
アプリケーションの **[プロジェクト]** ページに名前が表示されます。
5. タグを追加または選択して、ユーザーがプロジェクトを検索できるようにします。
6. プロジェクトに含めるドメインを選択します。

7. プロジェクトに含めるドメイン内のサービスを選択します。
サービスを展開して個々のアプリケーションを選択します。

第 10 章

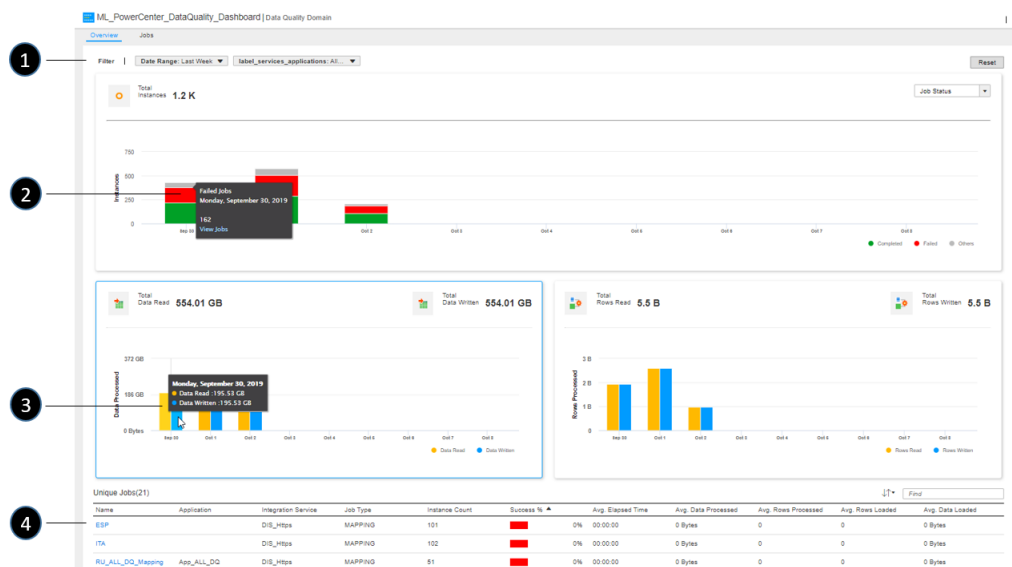
Data Quality ドメインの監視

オペレーションインサイトを使用して、Data Quality ドメインを監視できます。【概要】ページを使用して、特定の Data Quality ドメインのジョブ実行の統計とデータ処理の傾向を表示します。

ページを表示するには、次の手順を実行します。

1. 左側のナビゲーションバーにある **[Data Quality]** をクリックします。
2. **[ドメイン]** パネルでドメインをクリックします。
3. **[概要]** タブをクリックします。

ページの上部には、選択した日付範囲、およびデータ統合サービスのジョブ実行とデータ処理の統計が表示されます。デフォルトでは、このテーブルには、過去 7 日間にクラスタにジョブを送信するデータ統合サービスによって実行されたマッピングおよびワークフロージョブのデータが表示されます。



次の表に、このページから実行できるタスクを示します。

タ ス ク	説明
1	フィルタを使用して、データを表示する日付範囲、データ統合サービスインスタンス、および Hadoop クラスタを選択します。ページに表示されるデータは、フィルタ設定に基づいて更新されます。デフォルトでは、ドメイン内のすべてのデータ統合サービスインスタンスおよび Hadoop クラスタについて、過去 7 日間のデータが表示されます。
2	[合計インスタンス数] グラフで、ジョブの完了ステータス、ジョブタイプ、または実行エンジン別にジョブを表示するかどうかを選択します。グラフのバーセグメントにカーソルを合わせ、 [ジョブを表示] をクリックして詳細を表示します。
3	カーソルを [合計データ読み取り] グラフと [合計行数読み取り] グラフに移動して、フィルタで指定された時間範囲の詳細を表示します。
4	[一意のジョブ] リージョンのリンクをクリックして、選択した日付範囲、サービスおよびクラスタの一意のワークフローおよびマッピングの詳細を表示します。詳細については、 「Data Quality ジョブ分析の表示」 (ページ 119) を参照してください。

Data Quality ジョブ分析の表示

ジョブ実行の統計を使用して、ジョブ実行のパフォーマンスを評価し、失敗したジョブや長時間実行されているジョブを特定して、問題をトラブルシューティングします。

フィルタを使用して、表示するジョブ実行データをドリルダウンします。各ページに表示されるデータは、設定したフィルタの組み合わせに基づきます。

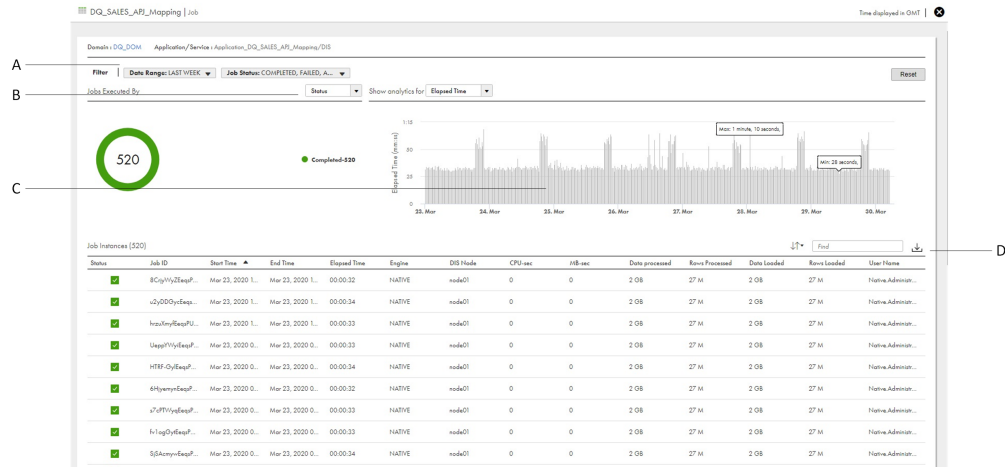
ジョブ実行サマリデータの表示

ジョブ実行時に収集されたサマリデータを使用して、ジョブ実行のパフォーマンスを把握できます。指定した時間範囲のジョブの全体的なパフォーマンスを、データ統合サービス別、およびジョブタイプ別に表示できます。また、失敗率が増加しているジョブや、実行時間が増加しているジョブを特定することもできます。

1. **【概要】** タブをクリックします。
2. ドメインをクリックします。
場合によっては、最初に場所を選択してから、その場所内のドメインを選択する必要があります。
3. **【ジョブ】** タブをクリックします。
ジョブ実行を表示するページがロードされます。
4. フィルタを使用して、表示するジョブデータを選択します。
フィルタ設定に従ってページが更新されます。デフォルトでは、このページには過去 7 日間に実行されたすべてのジョブのデータが表示されます。
5. 詳細を表示するには、テーブル内のジョブをクリックします。
個々のジョブインスタンスの統計を表示するページがロードされます。フィルタを使用して、表示するデータを選択します。**【フィールドの追加】** メニューからフィルタリングする追加のカラムを選択できます。

6. テーブル内のジョブをクリックします。

ジョブ実行の統計を表示するグラフがページにロードされます。経過した実行時間、処理済みのデータの量、ソース行から読み取られたデータ量、およびターゲット行に書き込まれたデータ量ごとに統計を表示できます。グラフには、設定したフィルタに基づいたデータが表示されます。



A. フィルタを使用して、表示するジョブデータを選択します。

B. ジョブをステータス別に表示するか、実行エンジン別に表示するかを選択します。

C. グラフ上でカーソルを移動すると、特定の詳細が表示されます。グラフを拡大して、特定のタイムフレームの詳細を表示できます。詳細については、「[グラフの詳細の拡大](#)」(ページ 32)を参照してください。

C. グラフ上でカーソルを移動すると、特定の詳細が表示されます。グラフを拡大して、特定のタイムフレームの詳細を表示できます。詳細については、「Informatica Intelligent Cloud Services の監視」を参照してください。

D. アイコンをクリックして、テーブルデータをカンマ区切り値 (.csv) ファイルにダウンロードします。

Data Quality プロジェクトの作成

オペレーションインサイトでプロジェクトを作成して、Data Quality アセットを監視することができます。

プロジェクトとは、Data Quality ドメインにデプロイされたサービスとアプリケーションのグループです。作成した各プロジェクトのサービスとアプリケーションのデータ処理分析およびジョブ実行の統計を表示できます。

1. 左側のナビゲーションバーにある **[Data Quality]** をクリックします。

2. **[プロジェクト]** タブをクリックします。

Data Quality プロジェクトが表示された **[プロジェクト]** ページが開きます。各プロジェクトのパネルには、過去 7 日間に実行されたジョブのサマリーデータが表示されます。

3. **[プロジェクトの作成]** をクリックします。

4. プロジェクトの名前を入力します。

アプリケーションの **[プロジェクト]** ページに名前が表示されます。

5. タグを追加または選択して、ユーザーがプロジェクトを検索できるようにします。

6. プロジェクトに含めるドメインを選択します。

7. プロジェクトに含めるドメイン内のサービスを選択します。
サービスを展開して個々のアプリケーションを選択します。

第 11 章

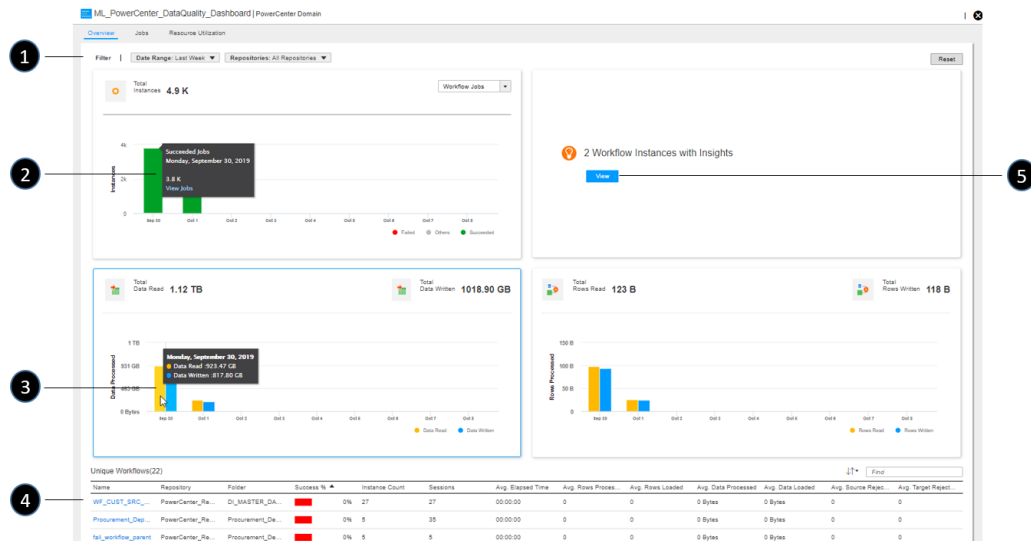
PowerCenter ドメインの監視

オペレーションインサイトを使用して、PowerCenter ドメインを監視できます。【概要】 ページを使用して、特定のドメインのワークフローの統計とデータ処理の傾向を表示します。

【概要】 ページを表示するには、次の手順を実行します。

1. オペレーションインサイトのナビゲーション バーで **[PowerCenter]** をクリックします。
2. **[ドメイン]** パネルでドメインをクリックします。
3. **[概要]** タブをクリックします。

【概要】 ページに、選択した日付範囲およびリポジトリとフォルダのワークフローの実行とデータ処理の統計が表示されます。処理されたデータボリュームと移動された合計行数に基づいてデータを表示できます。デフォルトでは、このページには過去 7 日間に実行されたワークフロージョブで処理されたデータボリュームが表示されます。



次の表に、このページから実行できるタスクを示します。

タ ス ク	説明
1	フィルタを使用して、データを表示する日付範囲とリポジトリおよびフォルダを選択します。 【概要】 ページに表示されるデータは、フィルタ設定に基づいて更新されます。
3	【合計インスタンス数】 グラフで、ワークフロージョブまたはセッションタスクに基づいてデータを表示するかどうかを選択します。グラフのパーセグメントにカーソルを合わせ、 【ジョブを表示】 をクリックして詳細を表示します。
3	カーソルを 【合計データ読み取り】 グラフと 【合計行数読み取り】 グラフに移動して、フィルタで指定された時間範囲の詳細を表示します。
4	【一意のワークフロー】 リージョンでワークフローをクリックして、選択した日付範囲とリポジトリの詳細なワークフローインスタンスの統計を表示します。詳細については、 「PowerCenter ワークフロー分析の表示」 (ページ 123) を参照してください。
5	【表示】 をクリックして、CLAIRE エンジンが異常または異常な動作を検出したワークフローインスタンスのリストを表示します。詳細については、 「異常なワークフロー実行動作の表示」 (ページ 124) を参照してください。

PowerCenter ワークフロー分析の表示

PowerCenter ワークフローの統計を使用して、ワークフローインスタンスのパフォーマンスを評価し、失敗したワークフローや長時間実行されているワークフローの実行を特定して、問題をトラブルシューティングします。

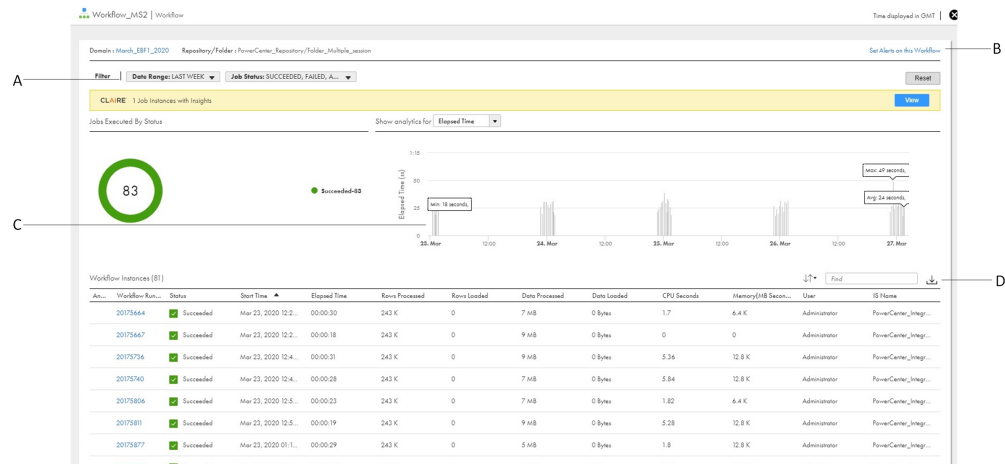
フィルタを使用して、表示するデータをドリルダウンします。各ページに表示されるデータは、設定したフィルタの組み合わせに基づきます。

PowerCenter ワークフロー実行データの表示

ワークフロー実行の実行時に収集されたデータを使用して、ジョブ実行のパフォーマンスを把握します。特定の時間範囲、特定のリポジトリとフォルダ、インスタンス数、および経過時間とデータ処理の平均ごとに、ワークフローの全体的なパフォーマンスを表示できます。また、失敗率が増加しているジョブや、実行時間が増加しているジョブを特定することもできます。

1. 左側のナビゲーションバーにある **【PowerCenter】** をクリックします。
PowerCenter ダッシュボードページが表示されます。
2. ダッシュボードページで PowerCenter ドメインをクリックします。
3. **【ジョブ】** タブをクリックします。
ワークフローの実行を表示するページが表示されます。
4. フィルタを使用して、表示するワークフローデータを選択します。**【フィールドの追加】** メニューからフィルタリングする追加のカラムを選択できます。
フィルタ設定に応じたテーブルページ。
5. テーブル内のワークフローをクリックして、ワークフローインスタンスの詳細を表示します。

ジョブ実行の統計を表示するグラフがページにロードされます。経過した実行時間、処理済みのデータの量、ソース行から読み取られたデータ量、およびターゲット行に書き込まれたデータ量ごとに統計を表示できます。グラフには、設定したフィルタに基づいたデータが表示されます。



A. フィルタを使用して、表示するワークフローデータを選択します。

B. ワークフローのアラートを設定します。

C. グラフ上でカーソルを移動すると、特定の詳細が表示されます。グラフを拡大して、特定のタイムフレームの詳細を表示できます。詳細については、「[グラフの詳細の拡大](#)」(ページ 32)を参照してください。

C. グラフ上でカーソルを移動すると、特定の詳細が表示されます。グラフを拡大して、特定のタイムフレームの詳細を表示できます。詳細については、「Informatica Intelligent Cloud Services の監視」を参照してください。

D. アイコンをクリックして、「ワークフローインスタンス」テーブルのデータをカンマ区切り値 (.csv) ファイルにダウンロードします。

ワークフローの実行で異常が検出された場合は、異常な動作をしているワークフローインスタンスのリストを表示できます。

6. 「ワークフローインスタンス」テーブルで実行 ID をクリックして、タスクの詳細を表示します。

異常なワークフロー実行動作の表示

オペレーションインサイトは、統計的アプローチおよび機械学習アプローチを使用してデータの異常値と異常を検出する CLAIRE エンジンを用いて、異常な PowerCenter ワークフロー実行動作について通知するためのインサイトを提供します。

CLAIRE は、経過した実行時間、処理およびロード済みのデータ、ワークフローのために毎日処理およびロードされる行を分析することにより、異常を検出します。このデータを使用して、異常または異常な動作が発生した期間を特定し、根本原因を特定できます。

1. 左側のナビゲーションバーにある **[PowerCenter]** をクリックします。

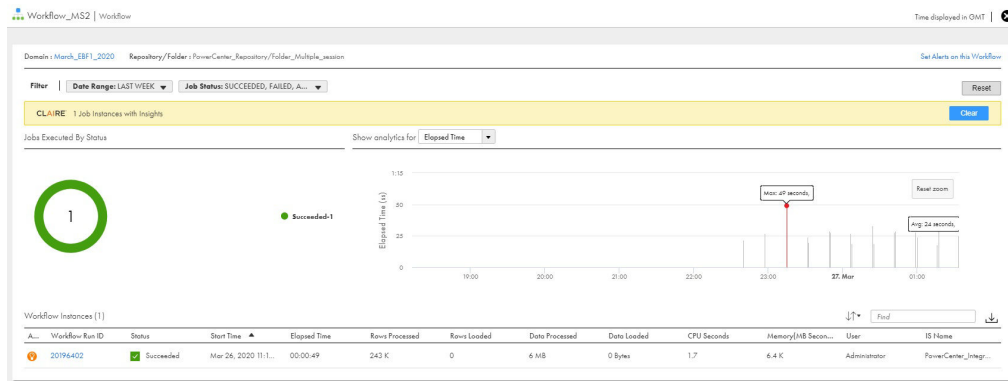
2. 次のいずれかの手順を実行します。

- ドメインのパネルで **[新規インサイト]** リンクをクリックします。
- ダッシュボードページで PowerCenter ドメインをクリックし、インサイトを含むワークフローが検出されたことを示すパネルで **[表示]** をクリックします。

[ジョブ] ページが開き、異常な動作をするワークフローインスタンスのリストが表示されます。

3. 異常値は赤いボックスで囲まれます。赤いボックスで囲まれた値をクリックし、**[このジョブの異常をすべて表示]** をクリックします。

【処理済みのデータ】などの異常な実行データを含むメトリックのグラフの上のタブをクリックします。ワークフローインスタンスのデータでグラフが更新されます。異常な動作に関連するグラフのバーは、赤い点で示されます。



4. グラフ内の赤い点をクリックして、異常の詳細を表示します。

推奨事項の表示

推奨事項という形でインサイトを使用して、パフォーマンスを改善し、エラーを解決して、PowerCenter ドメイン内の潜在的な問題を回避します。

エラー修復の推奨事項は、企業全体のすべての PowerCenter ドメインおよび PowerCenter プロジェクトに対して毎日生成されます。表示される推奨事項は、過去 7 日間で最も頻繁に発生したエラーに関するものです。この推奨事項には、推奨事項で報告されたエラー コードに関連する Informatica Knowledge Base の記事へのリンクが含まれます。

推奨事項を表示するには、次の手順を実行します。

1. 左側のナビゲーションバーにある **【PowerCenter】** をクリックします。
2. **【インサイト】** タブをクリックします。
3. フィルタを使用して、推奨事項を表示するドメイン、日付範囲、およびステータスを選択します。1 つ以上のカンマ区切りのエラー ID 値を入力して、エラーコードごとにフィルタリングすることもできます。
このページには、最大 25 件の推奨事項が表示されます。**【さらに表示】** をクリックすると、次の 25 件の推奨事項が表示されます。
4. 推奨事項カードで **【表示】** をクリックして、エラーの影響を受けたワークフローを表示します。
ワークフローが一覧で表示されたダイアログボックスが開きます。ワークフローをクリックして詳細を表示します。
5. **【さらに表示】** をクリックすると、追加の詳細が表示されます。複数の推奨事項を同時に展開できます。
6. 推奨事項を評価します。
 - 高評価アイコンをクリックすると、いいねの数が 1 増えます。
 - 低評価アイコンをクリックすると、コメントダイアログが開き、推奨事項の評価が低い理由に関する説明を記入することができます。
記入したフィードバックは、他のオペレーションインサイトユーザーには表示されません。これは、推奨事項の品質または有用性を向上させるために Informatica によって使用されます。

7. エラー解決の進捗状況を追跡する場合に役立つ、推奨事項のステータスを示します。
推奨事項が使用環境に当てはまらない場合は、**【破棄】** ステータスを選択して、リストから推奨事項を削除します。
8. **【ここから記事を読む】** をクリックして、エラーコードに関連する Informatica Knowledge Base の記事を新しいブラウザで開きます。

リソース使用率のヒートマップの表示

ヒートマップを使用して、PowerCenter ドメイン内のリソース競合の問題をすばやく特定し、同じ時間内に実行されているワークフロージョブが多すぎるために発生するボトルネックを分析します。

ヒートマップは、リソース消費が最も多い期間と最も少ない期間を示すカレンダービューを提供します。メモリ消費または CPU 使用率に基づいてデータを表示できます。ヒートマップには、デフォルトで、CPU 使用率データが表示されます。

カレンダーの各タイルは 4 時間という期間を表します。最も濃い色のタイルは消費量が 71%以上の期間を表し、明るい色は消費量が少ない期間を表します。タイルをクリックして、期間内に実行されたジョブの詳細を読み込みます。

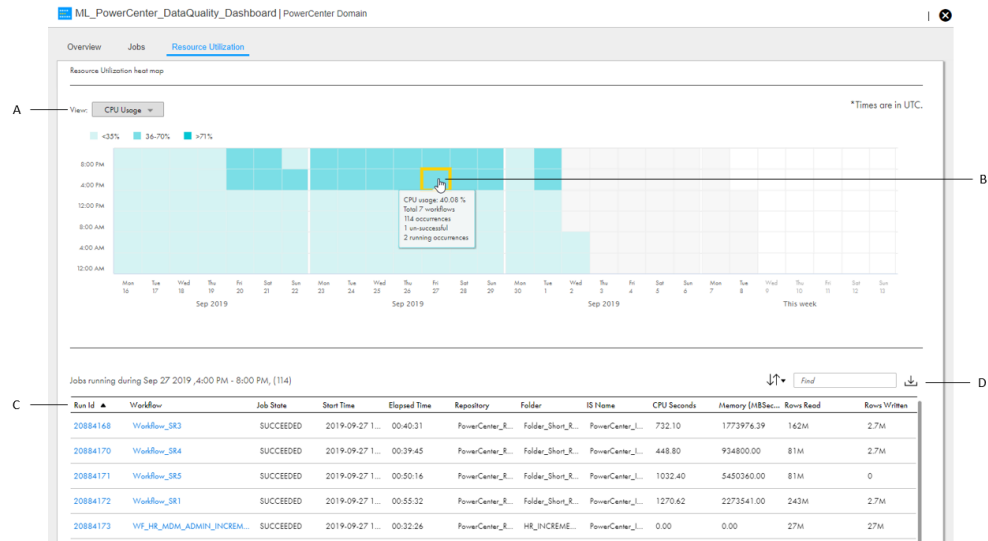
選択したタイルのデータを含むテーブルをカンマ区切り値 (.CSV) ファイルにダウンロードできます。ある一日の期間における消費量が多く、別の日の同じ期間における消費量が少ない場合は、両方のタイルのテーブルをダウンロードして、それぞれのデータを比較し、考えられる原因を特定することをお勧めします。

PowerCenter ドメインのリソース使用率のヒートマップを有効にする前に、該当する EBF を適用するか、カスタムプロパティを設定する必要があります。詳細については、次の Knowledge Base の記事を参照してください: [563791](#)

リソース使用率のヒートマップを表示するには、次の手順を実行します。

1. 左側のナビゲーションバーにある **【PowerCenter】** をクリックします。
PowerCenter ダッシュボードページが表示されます。
2. ダッシュボードページで PowerCenter ドメインをクリックします。
3. **【概要】** タブをクリックします。
4. PowerCenter ドメインをクリックします。

5. [リソース使用率] タブをクリックします。



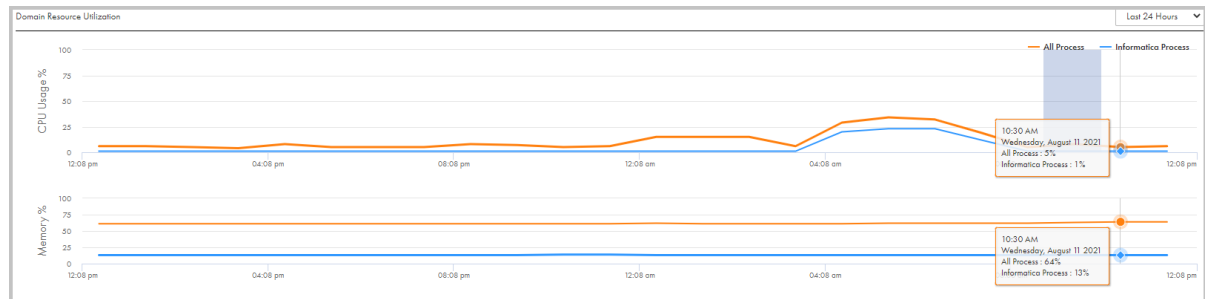
- CPU 使用率データまたはメモリ消費量データの表示を選択します。
- 期間のタイルをクリックします。この期間内に実行されたジョブの詳細が、下のテーブルにロードされます。
- 実行 ID をクリックして、ジョブ実行タスクの詳細を表示します。
- ここをクリックして、テーブルデータをカンマ区切り値 (.csv) ファイルにダウンロードします。

ドメインリソース使用率の表示

ドメインリソース使用率グラフを使用して、ドメインのリソース消費の統計を表示します。グラフを拡大して、特定のタイムフレームの詳細を表示できます。

- [すべてのインフラストラクチャ] をクリックします。
- [モニタ] タブをクリックします。
- ドメインをクリックします。
ドメインリソース使用率グラフがページの下部に表示されます。
- グラフで詳細を表示する期間を選択します。過去 24 時間、先週、または先月の統計を表示するように選択できます。
- グラフ上でカーソルを移動すると、特定の詳細が表示されます。
- グラフの詳細を拡大するには、カーソルをグラフのタイムフレームの開始点に移動します。

7. 次の図に示すように、始点で左クリックし、カーソルを終点までドラッグします。



リソース使用率グラフが更新され、指定したタイムフレームのデータのみが表示されます。

8. グラフを元の状態に戻すには、**【ズームのリセット】** をクリックします。

PowerCenter プロジェクトの作成

オペレーションインサイトでプロジェクトを作成して、PowerCenter アセットを監視することができます。

プロジェクトとは、PowerCenter ドメイン内のリポジトリとフォルダのグループです。作成した各プロジェクトのリポジトリとフォルダのデータ処理分析とワークフロー実行統計を表示できます。

オペレーションインサイトは、統計的アプローチおよび機械学習アプローチを採用してデータの異常値と異常を検出する CLAIRE エンジンを活用して、プロジェクト内の異常な PowerCenter ワークフロー実行動作を検出します。異常な動作が検出されたときに電子メール通知を送信するようにアプリケーションを設定できます。異常アラートを受信するユーザーおよびユーザーグループを指定するか、すべてのプロジェクトユーザーがデフォルトでアラートを受信できるようにすることができます。

1. 左側のナビゲーションバーにある **【PowerCenter】** をクリックします。
2. **【プロジェクト】** タブをクリックします。

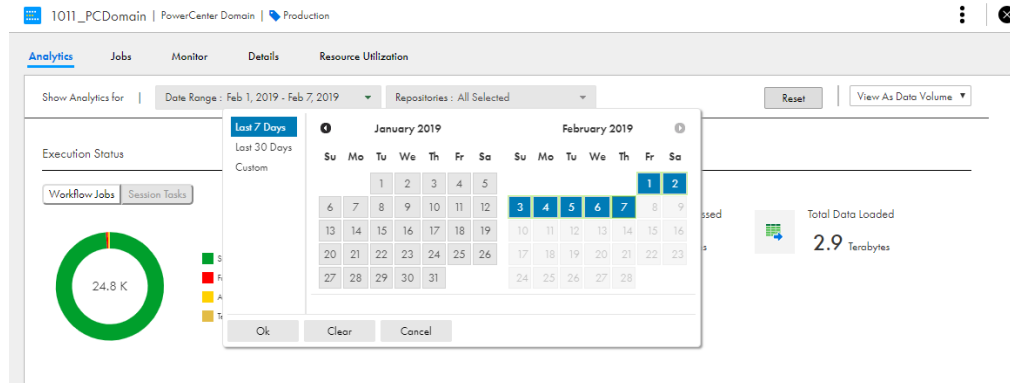
すべての PowerCenter プロジェクトが表示された **【プロジェクト】** ページが開きます。各プロジェクトのパネルには、過去 7 日間に実行されたワークフローのサマリデータが表示されます。

3. **【プロジェクトの作成】** をクリックします。
4. プロジェクトの名前を入力します。
アプリケーションの **【プロジェクト】** ページに名前が表示されます。
5. タグを追加または選択して、ユーザーがプロジェクトを検索できるようにします。
6. プロジェクトに含めるドメインを選択します。
7. プロジェクトに含めるドメイン内の PowerCenter リポジトリフォルダを選択します。
リポジトリを展開して個々のフォルダを選択します。
8. 必要に応じてアラートを有効にし、電子メール通知を受け取るユーザーまたはユーザーグループを指定します。

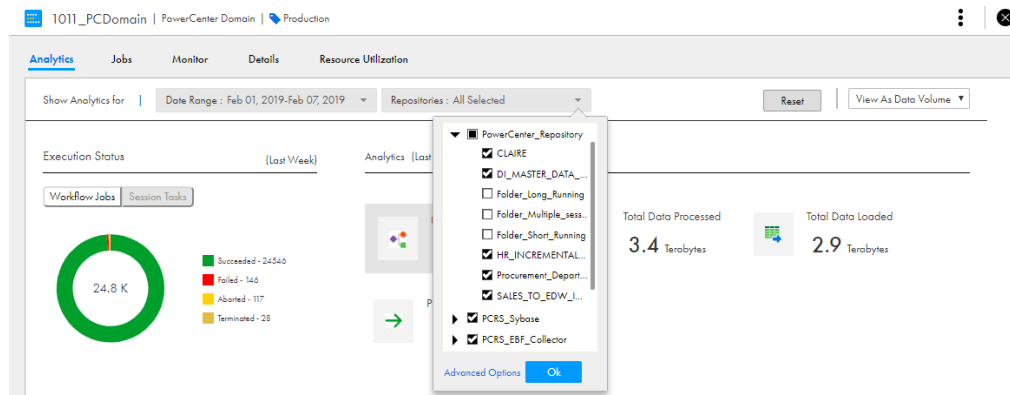
PowerCenter リポジトリフィルタの使用

PowerCenter リポジトリフィルタを使用して、特定の期間に収集されたランタイムワークフロー分析を表示します。各リポジトリ内の特定の PowerCenter リポジトリおよびフォルダを選択して、データを表示することもできます。詳細フィルタを使用して、結果をさらに絞り込むことができます。

1. [日付範囲] メニューから、統計情報を表示する日付範囲を選択します。



2. [リポジトリ] メニューから、データを表示するリポジトリを選択します。デフォルトではすべてのリポジトリが選択されているため、必要のないリポジトリをクリアします。



3. 必要に応じて、データを表示する各リポジトリ内のフォルダを選択します。デフォルトではすべてのフォルダが選択されているため、必要のないフォルダをクリアします。

[詳細オプション] をクリックして、データを表示する各リポジトリ内のフォルダを選択することもできます。

4. [OK] をクリックします。
5. [適用] をクリックして、選択した日付範囲とリポジトリの分析データを含むページを再読み込みします。

PowerCenter アラート

PowerCenter ワークフローで問題が発生したときに、Informatica Intelligent Cloud Services ユーザー、ユーザー グループ、または組織外の電子メール受信者に電子メール通知を送信するようにオペレーションインサ

イトを設定できます。例えば、ワークフローの実行が停止した場合、または CPU 使用率がアラート条件で指定した値と一致した場合に、ユーザーにアラートを送信する条件を設定できます。

[PowerCenter のアラート] タブで、設定されたアラートを表示できます。オペレーションインサイトが監視するアラートを有効化または無効化することができます。

次のような PowerCenter のアラートを設定できます。

CLAIRE アラート

CLAIRE™エンジンによって検出された PowerCenter プロジェクトの異常または異常な動作に関するアラート。PowerCenter プロジェクトの作成時に CLAIRE アラートを有効にしてから、電子メール通知を受信する必要があります。あるユーザーまたはユーザーのグループを指定します。

CLAIRE アラートの設定に関する詳細については、[「PowerCenter プロジェクトの作成」 \(ページ 128\)](#)を参照してください。

ワークフローアラート

PowerCenter ドメイン内のワークフローまたはオペレーションインサイトで作成されたプロジェクトで発生した問題に関するアラート。

PowerCenter ワークフローのアラートルールを作成するには、アラートを生成するアラート条件を指定します。ドメインまたはプロジェクトでリポジトリとフォルダのフィルタを指定して、特定のワークフローのアラートを設定できます。リポジトリフィルタとフォルダフィルタを指定しない場合、アラートはドメインまたはプロジェクト内のすべてのワークフローに適用されます。

アラートの設定時には、Informatica Intelligent Cloud Services のユーザー、ユーザーグループ、または指定したアラート条件と問題が一致したときにアラート通知を受信する組織外の電子メール受信者も指定する必要があります。

また、アラートがトリガされたときにオペレーションインサイト実行するアラートスクリプトを作成して、追加のアクションを実行することもできます。アラートスクリプトの作成と使用に関する詳細については、[「アラートスクリプトの使用」 \(ページ 34\)](#)を参照してください。

また、アラートがトリガされたときにオペレーションインサイト実行するアラートスクリプトを作成して、追加のアクションを実行することもできます。アラートスクリプトの作成と使用に関する詳細については、「Informatica Intelligent Cloud Services の監視」を参照してください。

索引

C

Cloud Application Integration コミュニティ
URL [13](#)
Cloud 開発者コミュニティ
URL [13](#)

I

Informatica Intelligent Cloud Services
Web サイト [13](#)
Informatica グローバルカスタマサポート
連絡先情報 [14](#)

L

Linux
Secure Agent のアンインストール [27](#)
プロキシの設定 [26](#)

S

Secure Agent
Linux でのアンインストール [27](#)
Linux での権限 [24](#)
Linux での登録 [24](#)
Linux での要件 [23](#)
Linux へのインストール [24](#)
Windows サービスログインの設定 [22](#)
Windows でのアンインストール [23](#)
Windows での起動 [18](#)
Windows での権限 [18](#)
Windows での登録 [19](#)
Windows での要件 [18](#)
Windows へのインストール [19](#)
Secure Agent Manager
起動 [18](#)

W

Web サイト [13](#)
Windows
プロキシの設定 [21](#)
Windows サービス
Secure Agent ログインの設定 [22](#)

あ

アップグレード通知 [14](#)

アラート
アプリケーション取り込みジョブ [97](#)
データベース取り込みジョブ [97](#)
データ統合ジョブ [49](#)
アラートの設定
Secure Agent [34](#)
インフラストラクチャ [34](#)
データ統合 [49](#)
ドメイン [34](#)

し

システムステータス [14](#)
ジョブデータ
エクスポート [43](#)
ジョブの監視 [40](#), [71](#)
ジョブの詳細 [44](#), [72](#)
ジョブの詳細の表示 [44](#), [72](#)

す

スケジュール済みのジョブ
データ統合 [48](#)
ステータス
Informatica Intelligent Cloud Services [14](#)
ストリーミング取り込みジョブ [93](#)

て

ディレクトリ
アクセスする Secure Agent ログインの設定 [22](#)
データプロファイリングジョブ [71](#)
データプロファイリングジョブの監視 [71](#)
データプロファイリングジョブの詳細 [72](#)
データ統合ジョブ [40](#)
データ統合ジョブの監視 [40](#)
データ統合ジョブの詳細 [44](#)

ふ

プロキシ設定
Linux での設定 [26](#)
Windows 上での設定 [21](#)

め

メンテナンスの停止 [14](#)