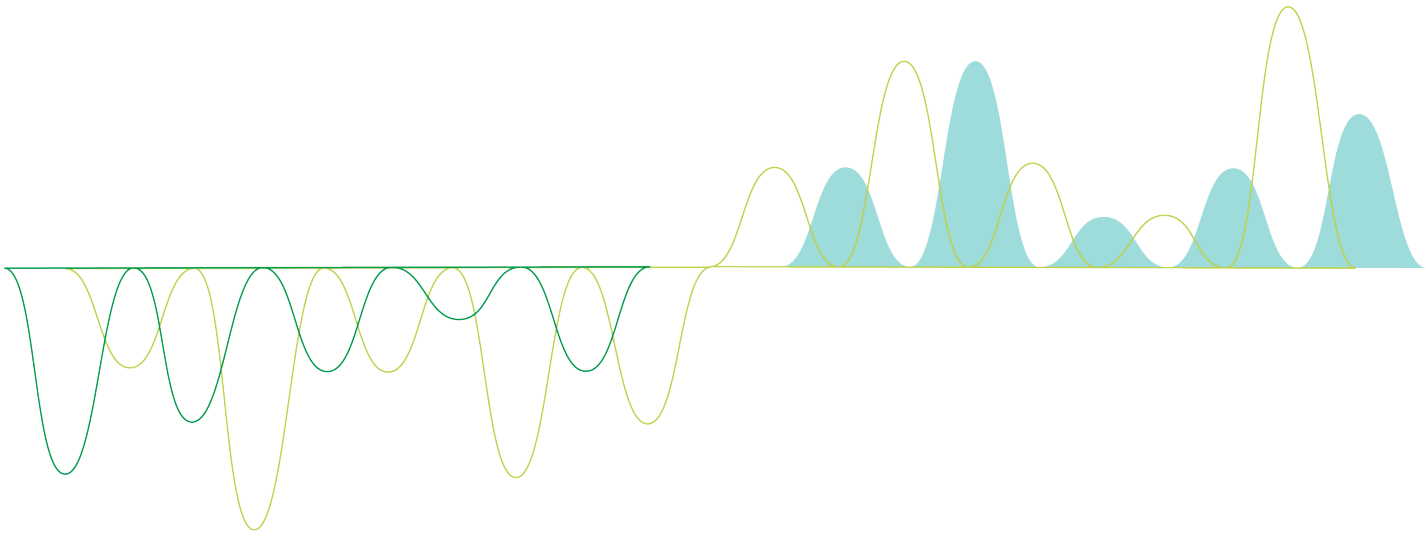
Windows 上での Qlik Sense Enterprise の管理

Qlik Sense®
August 2022
Copyright © 1993-2023 QlikTech International AB. All rights reserved.



© 2023 QlikTech International AB. All rights reserved. All company and/or product names may be trade names, trademarks and/or registered trademarks of the respective owners with which they are associated.

Contents

1 Qlik Sense Enterprise on Windows サイトの管理 ... 9

1.1 QMC の重要な概念 ... 9

アプリ ... 9

関連するアイテム ... 10

監査 ... 10

カスタム プロパティとQMC タグ ... 10

データ接続 ... 10

複数 選択 ... 10

ストリームへの公開 ... 10

セキュリティ ルール ... 11

アクセス タイプ ... 11

ユーザー ... 12

リソース所有者 ... 12

1.2 リソース ワークフロー ... 12

1.3 QMC の起動 ... 13

インストール後、初めて QMC を起動する場合 ... 13

QMC からのログアウト ... 14

1.4 QMCでのナビゲーション ... 15

QMC でのキーボード ショートカット ... 15

UI アイコンと記号 ... 17

QMC スタート ページ ... 20

リソース概要 ページ ... 21

リソース編集 ページ ... 24

QMCでの検索とフィルタリング ... 25

テーブル ビューでのカスタム フィルターの管理 ... 27

1.5 QMC リソース概要 ... 30

アプリ ... 36

コンテンツ ライブラリ ... 43

データ接続 ... 49

分析接続 ... 52

アプリ オブジェクト ... 54

ストリーム ... 57

タスク ... 61

ユーザー ... 66

システム通知 ... 68

システム通知 ポリシー ... 70

監査 ... 72

セキュリティ ルール ... 75

カスタム プロパティ ... 88

ライセンス管理 ... 90

拡張機能 ... 111

タグ ... 114

On-Demand アプリ ... 116

ユーザー ディレクトリ コネクタ ... 118

監視 アプリ ... 142

サービス クラスター ... 143

ノード ... 145

エンジン ... 147

Printing ... 152
プロキシ ... 153
仮想プロキシ ... 157
スケジューラ ... 165
リポジトリ ... 168
負荷分散ルール ... 171
例と結果 ... 174
クラウドの配布 ... 175
証明書 ... 179
Log Collector ... 179
サービス証明書 ... 181
暗号化証明書 ... 185
1.6 QMC リソースの管理 ... 194
ライセンスの管理 ... 195
アプリの管理 ... 203
On-demand アプリの管理 ... 252
ストリームの管理 ... 257
データ接続および拡張機能の管理 ... 262
ユーザーの管理 ... 272
タスクとトリガーの管理 ... 349
システム通知の管理 ... 367
システム通知ポリシーの管理 ... 370
ノードおよびサービスの管理 ... 375
カスタム プロパティの使用 ... 438
タグを使用する ... 445
1.7 QMC パフォーマンス – ベストプラクティス ... 449
パフォーマンス向上のための提案 ... 449
セキュリティルール ... 449
1.8 Qlik Sense Enterprise on Windowsの構成 ... 453
デフォルトの構成 ... 454
セキュリティの設定 ... 454
凡例 ... 458
ユーザー ログアウト ... 473
セッション タイムアウト ... 473
シングル サインオンをサービス プロバイダーから開始する場合 ... 478
シングル サインオンを ID プロバイダーから開始する場合 ... 478
シングル サインオンをサービス プロバイダーから開始する場合 ... 482
シングル サインオンを ID プロバイダーから開始する場合 ... 482
証明書の PowerShell 設定 ... 486
シングル サインオンをサービス プロバイダーから開始する場合 ... 486
ヘッダー ... 487
ペイロード ... 487
シグネチャー ... 487
Settings.ini の SSO 設定 ... 501
Settings.iniのシステム関数計算の設定 ... 503
負荷分散ルールを設定する ... 512
コンテンツのキャッシュ制御の構成 ... 517
1.9 アクセス制御の設計 ... 518

プロパティ 518
プロパティベースのアクセス制御 519
セキュリティルールのしくみ 522
Qlik Sense に含まれるセキュリティルール 540
セキュリティルール エディタ 566
セキュリティルールの作成 568
リソース フィルターの定義 572
複合ユーザー イベントにおける複数の許可 573
利用可能なリソース フィルター 577
利用可能なリソース条件 582
演算子と条件の関数 588
セキュリティルールの編集 594
セキュリティルールの削除 595
セキュリティルールの評価 596
セキュリティルールの例 601
1.10 配布ポリシー - はじめに 623
配布ポリシーの作成 624
配布ポリシーの作成 624
配布ポリシー - カスタム プロパティの使用 625
配布ポリシーの編集 629
1.11 アクセス制御の監査 630
監査クエリの定義 631
監査クエリ結果の表示とフィルタリング 632
1.12 トラブルシューティング - QMC 633
トラブルシューティング - QMC の起動 633
トラブルシューティング - QMC リソースの管理 636
トラブルシューティング - QMC での移動 644
トラブルシューティング - アクセス制御の設計 645
トラブルシューティング - 一般 647
1.13 Insight Advisor の参照元機械学習 647
1.14 Qlik Sense Enterprise on Windows での Qlik Insight Advisor Chat の構成 647
Qlik Insight Advisor Chat のアクセス制御の作成 648
外部チャネル用の Qlik Insight Advisor Chat の構成 649
Microsoft Azure Bot Service の作成 651
Microsoft Teams の通信チャネルの構成 652
Slack の通信チャネルの構成 653
Bot チャネル サービスの構成 658
2 Qlik Sense Enterprise on Windows サイトの監視 662
2.1 監視アプリの構成 662
シングル ノード環境の構成 662
マルチ ノード環境の構成 663
プレフィックス付きの既定の仮想プロキシ 664
新しい監視アプリのインポート 664
アプリのカスタマイズ 665
2.2 QMC からの監視アプリの起動 665
2.3 監視アプリのアップグレード 665
Qlik SenseFebruary 2019 以前から Qlik SenseApril 2019 以降へのアップグレード 665

Qlik Sense 3.2.x から Qlik Sense June 2017 へのアップグレード ... 666
同期持続性から共有持続性へのアップグレード ... 666
2.4 Operations Monitor ... 667
Operations Monitor シート ... 667
2.5 License Monitor ... 668
License Monitor シート ... 669
2.6 Log Monitor ... 670
QMC の監視アプリへの Log Monitor アプリのインポート ... 670
Log Monitor シート ... 670
2.7 Reloads Monitor ... 671
QMC の監視アプリへの Reloads Monitor アプリのインポート ... 671
Reloads Monitor シート ... 671
2.8 Sessions Monitor ... 672
QMC の監視アプリへの Sessions Monitor アプリのインポート ... 672
Sessions Monitor シート ... 672
2.9 Sense Connector Logs Analyzer ... 673
QMC の監視アプリへの Sense Connector Logs Analyzer アプリのインポート ... 673
一般構成 ... 673
マルチノード展開構成 ... 674
Sense Connector Logs Analyzer シート ... 675
2.10 App Metadata Analyzer ... 675
QMC の監視アプリへの App Metadata Analyzer アプリのインポート ... 676
一般構成 ... 676
オプションでのしきい値の設定 ... 676
App Metadata Analyzer シート ... 677
2.11 トラブルシューティング: Qlik Senseサイトの監視 ... 677
監視アプリが適切にバックアップされていない ... 677
間違って監視アプリを削除してしまった ... 678
監視アプリが破損した ... 678
監視アプリのリロードに失敗した ... 678
マルチノード環境でリロードに失敗する監視アプリ ... 681
データベース ログをオフにした後、Operations Monitor アプリでリロードが失敗する ... 682
Qlik RESTコネクタ経由でのQRSへの接続に失敗した ... 683
3 ログを使用した Qlik Sense Enterprise on Windows のトラブルシューティング ... 684
3.1 表記規則 ... 684
コーディング スタイル ... 684
環境変数 ... 685
3.2 Qlik Sense Repository Service ... 685
ユーザーの更新 ... 685
ユーザーの削除 ... 685
アプリを開く ... 686
アプリの追加 ... 686
アプリの削除 ... 687
アプリの公開 ... 687
アプリのエクスポート ... 688
アプリのインポート ... 688
アプリのリロード ... 689

アプリの複製 690
アプリオブジェクトの追加 691
アプリオブジェクトの更新 691
アプリオブジェクトの削除 691
アプリオブジェクトの公開 692
アプリオブジェクトの公開中止 692
拡張機能の追加 692
拡張機能の作成 692
拡張機能のアップロード 693
拡張機能の削除 693
拡張コンテンツの追加 694
拡張コンテンツの削除 694
コンテンツ ライブラリの追加 694
コンテンツ ライブラリの削除 694
コンテンツ ライブラリのコンテンツのアップロード 695
コンテンツ ライブラリのコンテンツの削除 695
ユーザー アクセスの追加 696
ユーザー アクセスの更新 696
ユーザー アクセスの削除 696
ユーザー アクセス リクエストの許可 697
ユーザー アクセスの許可 697
ライセンスからのユーザー アクセスの追加 698
アプリの権限の追加 698
証明書のエクスポート 698
ライセンスのダウンロード 699
ライセンスの追加 699
Update license (ライセンスの更新) 700
ライセンスの削除 700
ルールの追加 700
ルールの更新 701
ルールの削除 701
ストリームの追加 701
ストリームの削除 701
サーバー ノード登録 702
サーバー ノード構成 702
タスクの作成 702
タスクの更新 703
タスクの削除 703
タスクの開始 703
タスクの停止 704
ユーザー ディレクトリの同期 704
リポジトリの開始 705
リポジトリの停止 705
サービスの状態のチェック 706
プラグインのロード 706
ルールの監査 706
セキュリティの監査 707
ライセンスの監査 707

ライセンス ルールの監査 707
ライセンスのメンテナンス 707
証明書の配布 708
3.3 Qlik Sense Proxy Service 708
プロキシの開始 708
プロキシの停止 709
接続を開く 710
接続の終了 712
セッションの開始 713
セッションの停止 713
ログアウト 714
ログイン 714
証明書のインストール 715
3.4 Qlik Sense Engine Service 715
タスクの開始 715
タスクの終了 718
タスクの実行 720
マネージャーの開始 721
ワーカーの開始 721
マネージャーの再開 722
ワーカーの再開 722
初期設定の読み取り 722
サービス起動時のハードウェア情報の記録 722
マネージャーの停止 723
ワーカーの停止 723
マネージャーの一時停止 723
ワーカーの一時停止 724
ワーカーの設定の変更 724
3.5 Qlik Sense Engine Service 724
アプリを開く 724
アプリの追加 725
アプリの削除 726
アプリのエクスポート 727
アプリのインポート 727
アプリのリロード 728
アプリの複製 728
アプリの公開 729
アプリの公開中止 730
アプリの置換 731
エンジンの開始 731
エンジンの停止 732

1 Qlik Sense Enterprise on Windows サイトの管理

QMC は Web ベースのアプリケーションで、Qlik Sense Enterprise on Windows サイトの設定と管理を行います。QMC では、特に以下を実行することができます。

- ライセンスの管理
- アクセス タイプの管理
- ノードの構成
- データ接続の管理
- コンテンツのセキュリティの管理 (セキュリティ ルールによる)
- タスクとトリガーの管理
- ユーザーの同期

マルチノードのインストールでは、セントラル ノードの QMC から Qlik Sense Enterprise on Windows サイト全体を管理します。リム ノードから QMC にアクセスすることはできますが、QMC からリポジトリへのリクエストがセントラル ノードのリポジトリに転送されます。

QMC は、異なる QMC 管理者およびそのハブにアクセスする異なるユーザー グループ用に、異なるアクセス パターンを作成する非常に強力なツール一式を備えています。

- セキュリティ ルール
- 管理者ロール
- カスタム プロパティ

QMC での作業に有用なヒントについては、「QMC パフォーマンス – ベスト プラクティス (page 449)」を参照してください。

1.1 QMC の重要な概念

アプリ

適切なアクセス権限がある場合は、Qlik Sense ハブからアプリを作成し、ストリームに公開することができます。アプリは、QMC から公開することもできます。インストールされている Qlik Sense Desktop で作成されるアプリを公開するには、まずそのアプリを QMC からインポートする必要があります。アプリ、ストリーム、ユーザーに適用されるセキュリティ ルールによって、コンテンツにアクセスできるユーザーおよびそのユーザーが実行できる内容が決まります。アプリは公開後ロックされます。サーバー デプロイメントの Qlik Sense ハブを介してコンテンツを公開済みのアプリに追加することは可能ですが、オリジナルのアプリで公開されたコンテンツは編集できません。アプリは、QMC のアプリ概要ページからのみ削除できます。

関連するアイテム

QMC のリソースは連想構造になっています。このため、QMC の異なるリソース間を容易に移動できます。QMC は連想構造になっているため、複数の方法でリソースを選択できます。たとえば、アプリが属するストリームでは、アプリ概要または [**Associated items**] のいずれかからアプリを選択できます。同様に、タスク概要、またはタスクが属するアプリの [**Associated items**] からタスクを選択できます。

監査

QMC 監査ページで、リソースとユーザーのクエリや、Qlik Sense システムで定義されたセキュリティルールや負荷分散ルール、ライセンス ルールの監査を行うことができます。

カスタム プロパティとQMC タグ

QMC では、リソースに接続できるカスタマイズされたプロパティを作成できます。カスタム プロパティの主な目的はセキュリティルールで使用することです。また、リソースの概要ページでフィルタリングに使用できる QMC タグを作成し、接続することができます。セキュリティルールではタグを使用できません。

カスタム プロパティの適用例:

- **部門ごとのストリームのグループ化**
  組織に適した値のある、*[Departments]* というカスタム プロパティを作成します。カスタム プロパティをストリームに適用し、ストリームごとにセキュリティルールを管理する代わりに *Department* プロパティに応じてストリームにセキュリティルールを適用できます。

ユーザー ディレクトリ コネクタを作成して同期すると、グループのメンバーシップは中央リポジトリにアップロードされます。つまり、カスタム プロパティを定義してユーザーに適用する代わりにセキュリティ ルールをグループ メンバーシップに適用することができます。

データ接続

QMC からすべてのデータ接続のセキュリティルールを管理できます。ユーザーは Qlik Sense からデータ接続を作成できますが、データ接続 (セキュリティルール) の共有は QMC から管理されます。

複数 選択

概要から複数のリソースを選択することができます。これを行うと、複数のリソースを同時に編集または削除できます。これにより、QMC 管理作業の効率が向上します。

ストリームへの公開

適切なアクセス権限がある場合は、Qlik Sense ハブからアプリを作成し、ストリームに公開することができます。アプリは、QMC から公開することもできます。インストールされている Qlik Sense Desktop で作成されるアプリを公開するには、まずそのアプリを QMC からインポートする必要があります。アプリ、ストリーム、ユーザーに適用されるセキュリティルールによって、コンテンツにアクセスできるユーザーおよびそのユーザーが実行できる内容が決まります。アプリは公開後ロックされます。サーバー デプロイメントの Qlik Sense ハブを介してコンテンツを公開済みのアプリに追加することは可能ですが、オリジナルのアプリで公開されたコンテンツは編集できません。

既定で、Qlik Sense には次の 2 つのストリームが含まれます。**Everyone** および **Monitoring apps** 。

*すべての認証ユーザーには [**Everyone**] ストリームの読み取りと公開権限があり、すべての匿名ユーザーには読み取り専用権限があります。*

あらかじめ定義された管理者のロールの 3 つ (RootAdmin、ContentAdmin、SecurityAdmin) には、Monitoring apps ストリームの読み取り権限と公開権限があります。

セキュリティルール

コンテンツのセキュリティは、Qlik Sense Enterprise on Windows システムの設定と管理の重要な要素です。QMC を使うと、すべての Qlik Sense リソースのセキュリティルールを集約的に作成して管理できます。セキュリティルールは、ユーザーがリソースを用いて実行できること (読み取り、更新、作成、削除など) を定義します。

セキュリティルールはユーザーを除外するのではなく包含するようデザインされています。セキュリティルールに含まれていないユーザーはアクセスを拒否されます。このため、ユーザーが Qlik Sense のコンテンツやデータ接続、その他のリソースを使用できるようにセキュリティルールを作成する必要があります。

QMC には、あらかじめ定義された管理者ロールが含まれます。RootAdmin ユーザーで、Qlik Sense Enterprise on Windows システムへの完全なアクセス権があるユーザーなどです。これにより、RootAdmin ユーザーはセキュリティルールを設定することができます。

アクセス タイプ

ライセンス モデルには、シリアル番号とコントロール ナンバー、および署名付きのライセンス キーの 2 つがあります。これらのモデルで、ライセンスの契約条件およびユーザーに割り当て可能なアクセス タイプを定義します。ユーザーの割り当て、分析時間消費および製品のアクティベーションには、クラウドベースのライセンス バックエンドにアクセスするために、署名済みのライセンス キーとともにインターネット アクセス (直接またはプロキシ経由) が必要となります。

主なライセンス タイプには、アクセス タイプに基づくものと、トークンに基づくものの 2 つがあります。

- アクセス タイプのライセンスは、Professional User と Analyzer User ライセンス (ユーザーベース) および Analyzer Capacity ライセンス (キャパシティベース) です。Professional User および Analyzer User ライセンスは、Professional アクセスおよび Analyzer アクセスを割り当てることができます。Analyzer Capacity ライセンスでは、Analyzer Capacity ライセンスを割り当てることができます。ここでは消費が時間ベース (Analyzer タイム) となっています。
- Qlik Sense Token ライセンスでは、トークンを使用してアクセス パスをユーザーに割り当てます。User アクセスおよび Login アクセスを割り当てることができます。

アクセス タイプを使うと、ユーザーは Qlik Sense Enterprise on Windows サイト内のハブとアプリにアクセスできます。

Qlik Sense Enterprise SaaS をセットアップする場合は、Qlik 代理店または Qlik サポートに連絡してセットアップのための有効なライセンスを入力してください。

各アクセス タイプは Qlik Sense ユーザーに Qlik Sense アプリへの特定のタイプのアクセス権を与えます。アクセス タイプのないユーザーはストリームを表示できません。

> *アプリケーション アクセス権では、マッシュアップのアプリオブジェクトにのみアクセスできます。Qlik Sense ハブやストリームにはアクセスできません。*

ユーザー

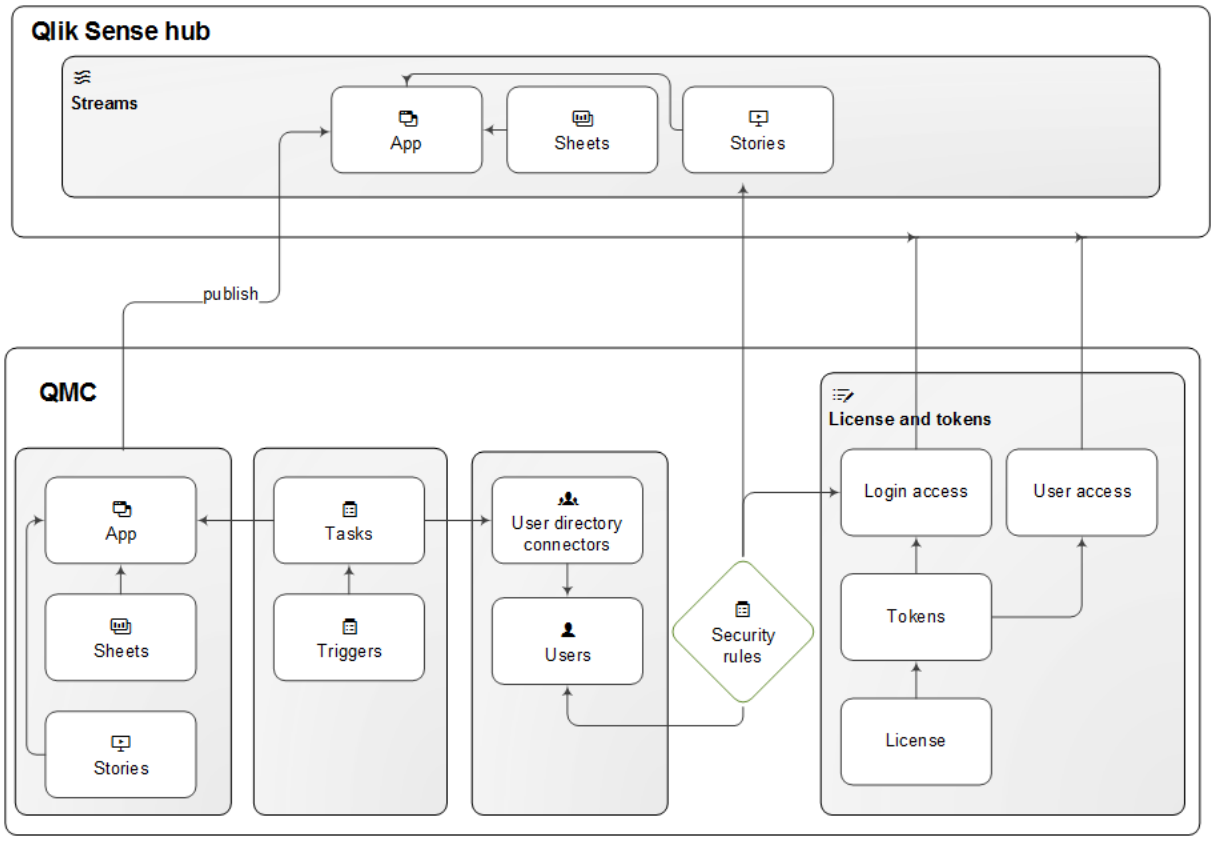
ユーザー データはすべて、Qlik Sense Repository Service (QRS) データベースに保存されます。QMCでユーザーディレクトリコネクタを作成し、構成されているディレクトリサービスからユーザー データを同期および取得できるようにします。ユーザーがQlik SenseまたはQMCにログインすると、ユーザー データが自動的に取得されます。Qlik Sense ユーザーの認証を扱う認証方法は変更できます。

リソース所有者

リソース (アプリやストリームなど) の作成者は既定でそのリソースの所有者になります。リソースの所有権は QMC で変更できます。

1.2 リソース ワークフロー

以下の図は、リソース ワークフローの概要を示しています。



トークンベースのライセンスに関するリソースの概要およびワークフロー

アプリ、シートおよびストーリーは、Qlik Senseハブから作成されます。アプリは、Qlik Sense ハブまたは QMC からストリームに公開されます。

アプリとユーザー ディレクトリ コネクタでタスクを利用できます。リロード タスクは、ソースからアプリにデータを完全にリロードするために使われます。ユーザー同期タスクはユーザー ディレクトリ コネクタに適用され、ユーザー ディレクトリからユーザーを同期します。トリガーはタスクを実行できます。

ストリーム セキュリティ ルールはストリームに適用され、ユーザーの アクセス権に影響します。

トークンベースのライセンス: サイト ライセンスは、アクセス タイプに割り当てられている数多くのトークンを提供します。ユーザーには、ログイン アクセスまたはユーザー アクセスによりハブでストリームとアプリへのアクセスが与えられます。セキュリティ ルールはログイン アクセスに適用され、どのユーザーがログイン アクセスを利用できるか指定します。

ユーザーベースのライセンス: サイト ライセンスによって、数多くのプロフェッショナルおよびアナライザー アクセスを割り当てます。ユーザーには、自身のアクセスによりハブでストリームとアプリへのアクセスが与えられます。

ハブは、QMC の一部ではありません。ハブは、Qlik Sense アプリとシートを開いて管理するところです。

1.3 QMC の起動

Qlik Management Console (QMC) にログインすると、新規セッションが開始します。以下のいずれかの状態からスタートできます。

- 以前のセッションのインターネット ブラウザがまだ開いている場合は、ページの中央に [**ログイン**] ダイアログがあるはずです。[**ログイン**] ボタンをクリックして新しいセッションをスタートしてください。
- または、[**スタート**] メニューの Qlik Sense プログラム グループから QMC を起動するか、インターネット ブラウザのアドレス フィールドに QMC のアドレスを入力します。
  - QMC の既定のアドレスは、*https://<QPS サーバー名>/qmc*です.
  - プロキシのプロパティ[**Allow HTTP**] を選択する場合、暗号化されていない通信が許可されます。つまり、https (セキュアな通信) とhttp (暗号化されていない通信) の両方が許可されます。その後、QMC アドレスは *https://<QPS server name>:Service listen port HTTP/qmc* になります(ここで、*https* は *http* で置換できます)。

    ユーザー名とパスワードを入力するよう指示されます。

*Windows 以外では、ブラウザにログイン ウィンドウが開きます。[**ユーザー名**] は、DOMAIN\user の形式で入力する必要があります。*

QMC は [**スタート**] ページで開きます。

インストール後、初めて QMC を起動する場合

Qlik Senseのインストール後、初めてQMCにアクセスするときには、ライセンスをアクティブ化する必要があります。

次の手順を実行します。

1. インターネットブラウザのアドレス フィールドに QMC のアドレスを入力します。
   QMC が [**サイト ライセンス**] ページで開きます。

   ユーザー名とパスワードを入力するよう指示されます。

2. ライセンスをアクティブにします。
   これにより、Qlik Sense サイトのルート管理者になり、RootAdmin ロールが割り当てられます。
   ライセンス モデルには、シリアル番号とコントロール ナンバー、および署名付きのライセンス キーの 2 つがあります。これらのモデルで、ライセンスの契約条件およびユーザーに割り当て可能なアクセス タイプを定義します。ユーザーの割り当て、分析時間消費および製品のアクティベーションには、クラウドベースのライセンス バックエンドにアクセスするために、署名済みのライセンス キーとともにインターネット アクセス (直接またはプロキシ経由) が必要となります。
   主なライセンス タイプには、アクセス タイプに基づくものと、トークンに基づくものの 2 つがあります。
   - アクセス タイプのライセンスは、Professional User とAnalyzer User ライセンス (ユーザーベース) および Analyzer Capacity ライセンス (キャパシティベース) です。Professional User および Analyzer User ライセンスは、Professional アクセスおよび Analyzer アクセスを割り当てることができます。Analyzer Capacity ライセンスでは、Analyzer Capacity ライセンスを割り当てることができます。ここでは消費が時間ベース (Analyzer タイム) となっています。
   - Qlik Sense Token ライセンスでは、トークンを使用してアクセス パスをユーザーに割り当てます。User アクセスおよび Login アクセスを割り当てることができます。

   アクセス タイプを使うと、ユーザーは Qlik Sense Enterprise on Windows サイト内のハブとアプリにアクセスできます。

   Qlik Sense Enterprise SaaS をセットアップする場合は、Qlik 代理店または Qlik サポートに連絡してセットアップのための有効なライセンスを入力してください。

*署名入りのライセンス キーの場合、ライセンス キーを入力して[**適用**] で保存した後、QMC でライセンス情報を確認することができます。*

これで最初の QMC セッションが開始されました。次に、ユーザー アクセスまたはプロフェッショナル アクセスを自分自身に割り当てます。

ユーザー アクセスの管理 (page 319)

Professional アクセスの管理 (page 309)

QMC からのログアウト

QMC からは手動でログアウト、あるいは自動的にログアウトすることができます。自動ログアウトは、あらかじめ設定された制限時間よりも、QMC セッションで非アクティブだった時間が長かった場合に発生します。この時間制限は、[**仮想プロキシの編集**] ページで仮想プロキシごとに設定されます。

次の手順を実行します。

1. ページの右上にある **username**▼ をクリックします。
   [**ログアウト**] がドロップダウン リストに表示されます。
2. [**ログアウト**] をクリックします。
   [**ログイン**] ボタンが掲載されている QMC のようこそページが表示されます。

*ようこそページで [**ログイン**] をクリックすると、QMC のスタート ページが開きます。ユーザー名とパスワードを入力するよう指示されます。*

1.4 QMCでのナビゲーション

QMC は連想構造になっているため、複数の方法でリソースを選択できます。たとえば、アプリが属するストリームでは、アプリ概要または [**Associated items**] のいずれかからアプリを選択できます。同様に、タスク概要、またはタスクが属するアプリの [**Associated items**] からタスクを選択できます。

インターネットのブラウザの戻るボタンと進むボタンを使用して、QMC 内のページを移動することができます。また、アドレス フィールドに URL を入力することもできます。例えば、*https://<QPS server name>/qmc/Users* と入力すると、ユーザーの概要ページを開くことができます。また、インターネット ブラウザで、QMC のページをブックマークすることも可能です。

特定のリソースを頻繁に管理する場合、そのページをブックマークすることをお勧めします (アプリの概要ページをブックマークするなど)。

QMC でカスタム フィルターとしてよく使用するビューを保存できます。これにより、必要なデータにすばやくアクセスできます。

QMC でのキーボード ショートカット

Qlik Sense はキーボードによるアクセスに対応しており、キーボード コントロールを使用して、Qlik Management Console (QMC) およびマルチクラウド セットアップ コンソール (MSC) をナビゲートすることができます。

キーボード ショートカットは、Windows での作業を前提としています。Mac OS については、Ctrl の代わりに Cmd を使用してください。

Qlik Management Console

主なアクション

ショートカットとそのアクション

ショートカット	アクション
Esc	フィルター ダイアログを閉じます
↑	表を上にスクロールします

ショートカットとそのアクション

ショートカット	アクション
↓	表を下にスクロールします
Tab	編集ページの次のフィールドに移動します
Shift+Tab	編集ページの前のフィールドに移動します
Esc	ダイアログ ボックスを閉じます
Ctrl+C	選択したテキストをクリップボードにコピーします
Ctrl+H	Qlik Sense ヘルプを開きます
Ctrl+V	最後にコピーしたテキストをクリップボードから貼り付けます
Ctrl+X	選択したテキストを切り取り、クリップボードにコピーします
Ctrl+Z	操作 (コピー、貼り付け、切り取り) を元に戻します
Ctrl+Y	操作 (コピー、貼り付け、切り取り) をやり直します
Backspace	PC 上で: ナビゲーションへ戻ります。Mac 上で: 選択したアイテムを削除します。

テーブルで

*オプション[**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション[**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*

ショートカットとそのアクション

ショートカット	アクション
Ctrl+A	テーブルのすべての行を選択します
Esc	選択したすべての行の選択を解除します
S	**検索** ポップオーバーを開きます
C	列セレクターを開きます
R	テーブルを更新します

概要ページで

ショートカットとそのアクション

ショートカット	アクション
Enter	選択した行を編集します
Delete	選択した行を削除します

編集ページで

ショートカットとそのアクション

ショートカット	アクション
Esc	**キャンセル**をクリックしたときと同様に、すべての変更を元に戻します
Ctrl+S	**適用**をクリックしたときと同様に、すべての変更を保存し適用します

確認ダイアログで

ショートカットとそのアクション

ショートカット	アクション
Esc	キャンセル
Enter	OK

マルチクラウド セットアップ コンソール

コンソール

ショートカットとそのアクション

ショートカット	アクション
左矢印と右矢印	メニュー タイトル間を移動します
Enter/Space キー	オブジェクトを選択します

展開

ショートカットとそのアクション

ショートカット	アクション
Tab	次の項目に移動します
上矢印と下矢印	リスト項目間を移動します
Enter/Space キー	オブジェクトを選択します

UI アイコンと記号

記号は複数のコンテキストで使用できます。次は、Qlik Management Console (QMC) ユーザー インターフェイス全体で使用するアイコンと記号のリストです。

UI アイコン

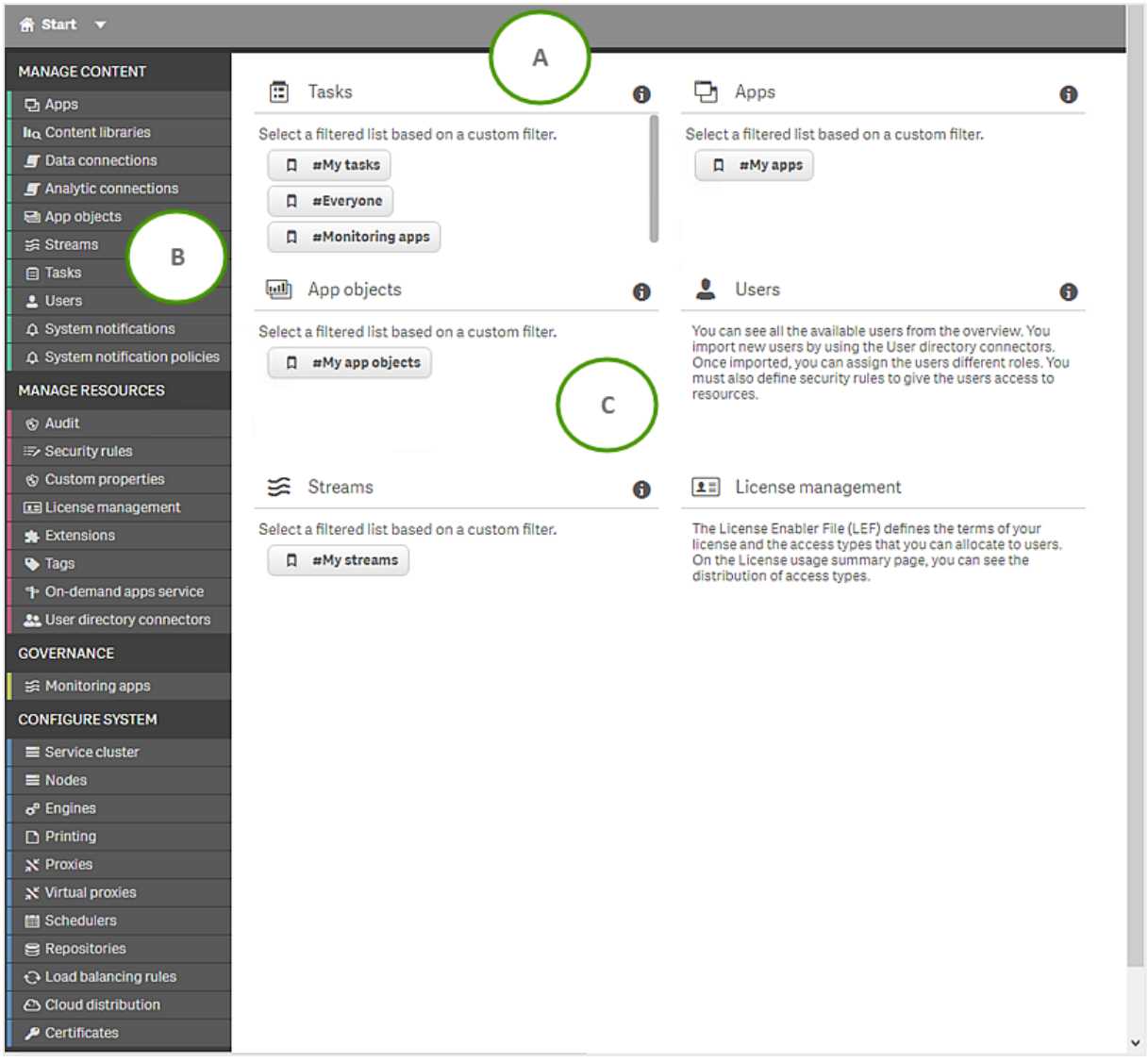
アイコン	意味
	新規作成
	アプリ
	コンテンツ ライブラリ
	データ接続
	分析接続
	アプリオブジェクト
	ストリーム
	タスク
	ユーザー
	アプリの配布 ステータス/クラウドの配布
	監査
	セキュリティルール
	カスタム プロパティ
	ライセンス管理
	拡張機能
	タグ
	On-Demand アプリ サービス
	ユーザー ディレクトリ コネクタ
	監視 アプリ
	サービス クラスター
	ノード
	エンジン
	印刷
	プロキシ
	仮想プロキシ
	スケジューラ

	リポジトリ
	配布ポリシー
	負荷分散ルール
	証明書
	タスクチェーン
	タスクチェーン
	タスクの状態: 未開始、スキップ済み、リセット
	タスクの状態: トリガー済み、開始済み、中止の開始、中止中、再試行中
	タスクの状態: キュー
	タスクの状態: 中止
	タスクの状態: 成功
	タスクの状態: 失敗、エラー
	読み取りアクセス (セキュリティルールによる)
	更新/書き込み/編集アクセス (セキュリティルールによる)
	削除アクセス (セキュリティルールによる)、ログアウト、キャンセル、閉じる、終了
	その他のアクセス (セキュリティルールによる)、作成、所有者の変更、エクスポートなど
	フィルター
	ヘルプ
	情報
	情報
	ロック
	ロック解除
	検索
	元に戻す
	設定
	上向き矢印
	下向き矢印

◀	左向き矢印
▶	右向き矢印
🔖	カスタム フィルター

QMC スタート ページ

Qlik Management Console (QMC) のスタート ページには、Qlik Sense サイトで管理できるすべてのリソースが含まれています。管理できるリソースはアクセス権によって異なります。



QMC スタート ページ

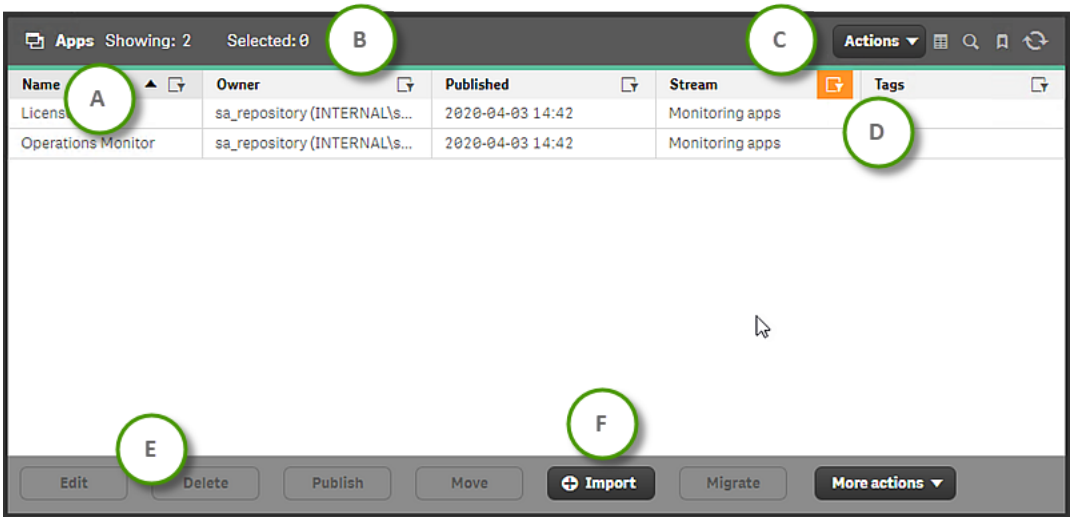
QMC スタートページのインターフェースの凡例の説明

凡例の文字	説明
ライン番号の隣にある	すべてのページで最上部にバーが表示され、QMC を効率よくナビゲートできます。以下が可能です。 [**スタート**] をクリックして、QMC スタートページにアクセスしてください。 [**スタート**] の横にある▼をクリックして、すべてのリソースのドロップダウン リストを表示します。これにより、最初にスタートページにアクセスしなくても別のリソースを選択できます。 [**ヘルプ**] をクリックして、(QMC) ヘルプにアクセスします。 右上には、誰が (QMC) にログインしているのか表示されます。ドロップダウン▼をクリックし、ログイン名の横にある [**ログアウト**] ダイアログをクリックしてログアウトします。
B	左側のパネルには、グループの QMC リソースがすべて含まれています。 Qlik Sense のサービスがダウンしている場合、稼働していないサービスの数が数字で表示されます。
C	スタートページの中央では基本的なリソースも利用できます。リソースごとにカスタム フィルターが一覧表示されます。シャープ記号 (#) は、定義済みのカスタム フィルターを示します。カスタム フィルターをクリックして、保存されたテーブル ビューに移動します。 クリックすると、リソースに関する情報が表示されます。

リソース概要ページ

スタートページでリソースを選択すると、リソース概要が表示されます。概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

既定では [overview] ページには最も一般的に使用される列が表示されます。列セレクターで列を追加したり、削除できます。テーブルのヘッダー バーで、 をクリックして列セレクターを開きます。[**アクション**] メニューでは、フィルターや検索をクリアしたり、すべての行を選択/選択解除したり、折り返しを切り替えたりできます。



アプリ概要ページ

アプリ概要ページの凡例の説明

凡例の文字	説明
ライン番号の隣にある	列見出しをクリックして、その列を昇順▼または降順▲に並べ替えます。 並び替えの横の をクリックして、列のフィルタダイアログを表示します。フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。
B	テーブルのヘッダーには、現在のデータセットのステータスの概要が表示されます。 [**Total**] には、リソースの総数が表示されます。 [**Showing**] には、現在表示されているリソースの数が表示されます。 [**Selected**] には、選択したリソースの数が表示されます。

C	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション[**Select all rows**]は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション[**Deselect all rows**]はフィルターが適用された行を含むすべての行に適用されています。* をクリックして[**列セレクター**]を開きます。ここでは概要に表示する列を選択できます。をクリックすると既定の列にリセットされます。 をクリックして[**カスタム フィルター**]メニューを開き、カスタム フィルターを選択、作成、削除できます。カスタム フィルターが適用されると、ボタンが強調表示されます。 をクリックしてテーブルのデータを更新します。データに変更があった場合は、ボタンが強調表示されます。
D	QMC のコンテンツを効率よく検索して管理できるように、タグを作成してリソースに適用することができます。
E	ページ最下部のアクション バーには、選択したリソースのタイプに応じて異なる操作ボタンが含まれます。例えば、概要でアプリを選択して、[**編集**]をクリックし、[**アプリの編集**]ページを開きます。 選択したアイテムに対する更新権限を持っていない場合、[**Edit**]は[**View**]に置き換わります。 選択したアイテムに対する削除権限を持っていない場合、[**Delete (削除)**]は無効となります。リソースが削除されると、そのリソースに関連付けられている負荷分散ルールとセキュリティルールはすべて自動的に削除されます。
F	アクション バーの をクリックして、リソースのインスタンスを新規に作成します。 この例では、[**インポート**]をクリックすると、[**アプリのインポート**]ダイアログが開きます。 *新しい行がテーブルの下部に追加されます。これは、ソート順がキャッシュに保存されるためです。ソートまたはフィルターを使用してテーブル全体のリロードをトリガーします。*

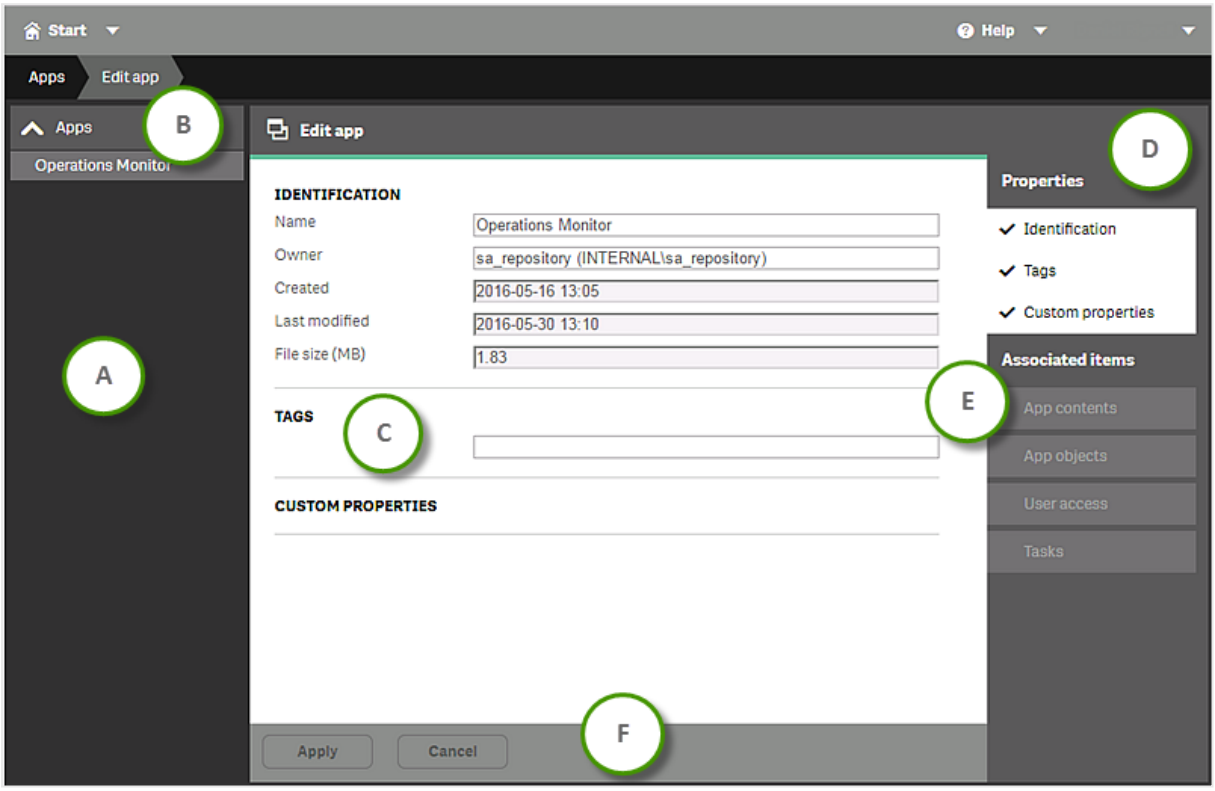
選択

以前に行った選択は、リソース概要を表示している間は、それを選択した後に別のリソース タイプで作業を行っていた場合でもアクティブです。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

リソース編集ページ

リソースは編集ページで編集できます。編集するには、更新権限が必要です。更新権限がなければ、このページを表示することは可能ですが、編集はできません。この例は、[**アプリの編集**] ページです。



例: [アプリの編集] ページ

[**アプリの編集**] インターフェースの凡例の説明

凡例の文字	説明
ライン番号の隣にある	左側の選択パネルには、現在編集しているリソースが表示されます。複数のリソースを同時に編集して、QMC のコンテンツを効率よく管理することができます。
B	[**アプリ**] をクリックして、選択アプリを変更できる概要ページに戻ります。
C	編集ページには、右側のパネルのプロパティグループから選択したプロパティが表示されます。概要で複数の項目を選択し、特定の項目に異なる値がある場合は、項目値として*複数の値*が表示されます。項目の横の ↩ をクリックすると、その項目の変更内容が取り消されます。QRS との通信に失敗すると、編集ページはロックされます。ページから離れるにはトップバーを使用します。
D	[**Properties**] セクションには、リソースのプロパティを含むプロパティグループが表示されます。編集ページではプロパティを表示または非表示にできます。
E	[**関連するアイテム**] セクションには、この特定のリソースに関連するアイテムが表示されます。

F	ページの最下部にあるアクション バーには、[**適用**] および [**キャンセル**] ボタンが含まれています。[**キャンセル**] をクリックすると、全項目値がリセットされます。必須項目が空欄の場合、[**適用**] は無効になります。[**適用**] をクリックしないで編集ページから移動しようとすると、未保存の変更内容を示すダイアログが表示されます。[**続行**] を選択するか (編集ページを終了して変更をすべて元に戻す)、[**キャンセル**] します (編集ページにとどまる)。[**適用**] をクリックした場合、QRS との通信に失敗すると、エラー メッセージが表示されます。編集を続けるか、再び [**適用**] をクリックします。

QMCでの検索とフィルタリング

内蔵されている検索ツールを使用して、QMC のほとんどのテーブルで検索できます。簡単な検索をすぐに実行でき、いくつかの検索条件を使ってサブグループに設定する、より高度な検索を作成することもできます。検索と列のフィルタリングを組み合わせて、結果のリストをさらに絞り込むこともできます。フィルター処理されたテーブル ビューをカスタム フィルターとして保存できます。

検索オプション

検索時には、以下の 4 つのオプションを利用できます。

検索オプション

検索オプション	説明
A	検索する属性を選択します。
B	検索条件を選択します。ほとんどの場合、その条件は [=]、[!=]、[**次を含む**]、[**次で始まる**]、[**次で終わる**] です。時間に関する列には、[**以降**]、[**より前**]、[**より後**] の条件があります。
C	利用可能な値の 1 つをクリックして選択するか、文字列を入力します。
D	他の検索条件を追加します。

簡単な検索

次の手順を実行します。

1. テーブル ヘッダーの右にある をクリックします。
   検索が開きます。
2. 最初のドロップダウン リストで、検索する属性を選択します。
3. 2 番目のドロップダウン リストで、検索条件を選択します。

4. 3 番目のリストをクリックして、利用可能なオプションの 1 つをクリックするか、文字列を入力します。
5. [**検索**] をクリックします。

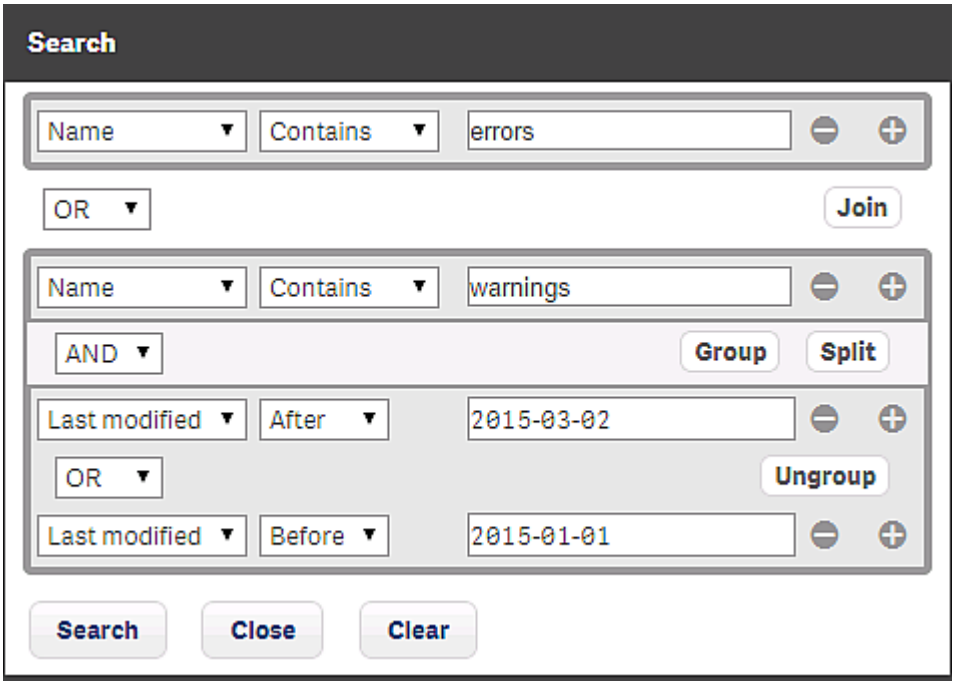
テーブルには、一致したアイテムが表示されます。

テーブル ヘッダーで をクリックして、検索とフィルタをクリアします。

高度な検索

より高度な検索をする場合は、複数の検索条件を組み合わせることができます。条件は、OR (または) か AND (および) のいずれかで接続します。[**グループ**]、[**結合**]、[**分割**] を使用して行間の論理関係を調整できます。既定では、行はグループ化されます。

以下の検索は、4 つの条件で構成されています。



最初の条件は、[**分割**] オプションで他の条件と区別されます。

2 番目の条件は、[**結合**] で 3 番目と4 番目の条件を接続し、3 番目と4 番目の条件は順番にグループ化されます。

これらの条件を満たすには、3 つの方法があります。

- 最初の条件を満たしている。
- 2 番目の条件を3 番目の条件とともに満たしている。
- 2 番目の条件を4 番目の条件とともに満たしている。

フィルタリング

フィルタリングは、単独でまたは検索と一緒に使用できます。複数の列を同時にフィルタできます。

次の手順を実行します。

1. 列見出しの ▼ をクリックします。
   列のフィルタダイアログが表示されます。
2. フィルターダイアログで、フィルターする文字列を入力します。利用可能な場合は、代わりに事前定義された値を選択できます。
3. フィルタダイアログの外側をクリックして (または「Esc」を押して) ダイアログを閉じます。
   アイコンは、フィルタが列に適用されたことを示しています。

テーブルには、一致したアイテムが表示されます。

テーブル ビューでのカスタム フィルターの管理

カスタム フィルターを使用すると、操作するコンテンツを簡単に見つけることができます。例えば、特定のタスクセットを毎日見る必要がある場合があります。タスクをフィルターし、テーブル ビューをカスタム フィルターとして保存します。次回は、カスタム フィルターを使用して、タスクのセットに直接移動します。追加の利点は、フィルターに含まれるアイテムのみがロードされることです。これにより、ロード時間が短縮されます。

次の設定をカスタム フィルターに保存できます。

- 検索フィルター
- 列フィルター
- ソート順
- ソート列
- 列の定義 (表示する列と列の幅)

リソース概要ページの [**カスタム フィルター**] メニューから、すべてのリソースのカスタム フィルターを作成および管理します。

事前定義のカスタム フィルター

QMC スタートページでは、事前定義されたカスタム フィルターを使用できます。これらは番号記号 (#) で示されます。

- **#マイ アプリ**、**#マイ アプリオブジェクト**、**#マイ ストリーム**には、所有しているオブジェクトが表示されます。
- **#マイ タスク**には、所有しているアプリに関連付けられているタスクが表示されます。
- **タスク**の概要には、ストリームごとに 1 つのカスタム フィルターがあります。それらは、そのストリームに公開されているアプリに接続されているタスクを示します。

定義済みのカスタム フィルターには、列レイアウトの設定はありません。フィルターとソート順のみを定義します。特定のレイアウトを保存する場合は、事前定義のカスタム フィルターを更新します。

事前定義のカスタムフィルターを一時的に削除できますが、ブラウザーを更新すると再作成されます。

カスタム フィルターの適用

カスタム フィルターを適用すると、カスタム フィルター アイコンが強調表示されます。現在適用されているカスタム フィルターの [**カスタム フィルター**] メニューにチェック マークがあります。これは、テーブルに変更を加えるとリセットされます。

適用するカスタム フィルターにフィルターが含まれている場合、テーブル データのサブセットのみがロードされます。

次の手順を実行します。

1. リソースの概要ページで、 をクリックして [**カスタム フィルター**] メニューを開きます。
2. 適用するカスタム フィルターの横にある [**使用**] をクリックします。

アプリ、アプリオブジェクト、タスク、ストリームの場合、QMC スタート ページでカスタム フィルターを利用できます。

カスタム フィルターの作成

最初にテーブルに必要な編集を行い、次に結果を保存することにより、カスタム フィルターを作成します。

次の手順を実行します。

1. リソース概要ページに移動します。
2. フィルター、ソート、または列の調整を行って、カスタム フィルターに保存します。
3. [ ] をクリックして [**カスタム フィルター**] メニューを開きます。
4. 新しいカスタム フィルターの名前を入力し、説明を追加します。
5. をクリックします。

カスタム フィルターの削除

次の手順を実行します。

1. リソース概要ページで、 をクリックして [**カスタム フィルター**] メニューを開きます。
2. ストーリー ツール パネルのストーリーテリング ビューで します。

*[**クリア**] オプションは何も削除せず、適用されたカスタム フィルターを削除するだけです。*

カスタム フィルターの更新

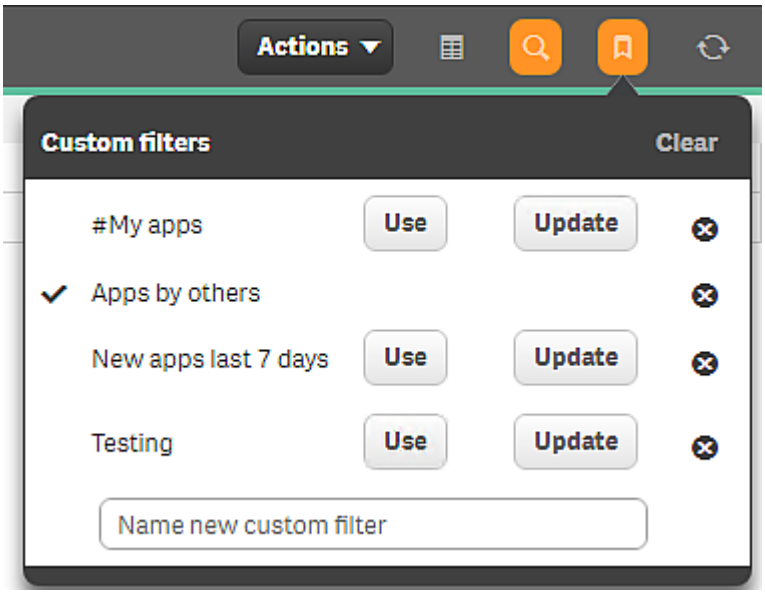
カスタム フィルターは、現在のレイアウト、フィルター、ソート順で更新できます。

次の手順を実行します。

1. リソース概要ページで、 をクリックして [**カスタム フィルター**] メニューを開きます。
2. 更新するカスタム フィルターの横にある [**更新**] をクリックします。

選択したカスタム フィルターが新しい設定で更新されます。

カスタム フィルターのユーザー インターフェイス



次のユーザー インターフェイスでは、カスタム フィルター [**他の人によるアプリ**] が使用されています。[**クリア**] をクリックして、現在のフィルターをクリアします。何も削除されません。

別のフィルターを適用するには、そのフィルターの [**使用**] をクリックします。[**更新**] をクリックすると、カスタム フィルターが現在の設定で更新されます。

をクリックしてフィルターを削除します。

例: 他の人が所有するアプリのカスタム フィルターの作成

このフィルターには、他のユーザーが作成したアプリのみが表示されます。

次の手順を実行します。

1. QMC スタート ページで、[**アプリ**] をクリックします。
   アプリ概要セクションが開きます。
2. をクリックして検索を開きます。
3. 最初のリストで、[**所有者**] を選択します。
4. 2 番目のリストで、[**!=**] を選択します。
5. テキスト ボックスに、ユーザー名を入力します。
6. [**検索**] をクリックします。
   他の人が所有するアプリのみが表示されるようになりました。
7. をクリックして [**カスタム フィルター**] メニューを開きます。
8. 新しいカスタムフィルターに [*他の人によるアプリ*] という名前を付けます。
9. をクリックします。
   新しいカスタム フィルターが保存され、チェック マークはそれが現在使用中であることを示します。

例: カスタム フィルターの更新

この例では、事前定義されたカスタム フィルター [**#My apps**] を更新して、アプリをサイズでソートします。

次の手順を実行します。

1. QMC スタート ページで、カスタム フィルター [**#My apps**] を選択します。
   アプリ セクションが開き、カスタム フィルターが適用されます。アプリのみが表示されます。
2. をクリックして列セレクターを開き、[**ファイル サイズ (MB)**] を選択します。
3. [**ファイル サイズ (MB)**] ヘッダーをクリックして、ソート順を変更します。
4. をクリックして [**カスタム フィルター**] メニューを開きます。
5. [**#My apps**] の行で、[**更新**] をクリックします。
6. [**#My apps**] フィルターが更新され、チェック マークが現在使用中であることを示します。

1.5 QMC リソース概要

以下のテーブルで Qlik Management Console (QMC) で利用できるリソースすべてについて簡単に説明します。

QMC リソースの説明

リソース	説明
Apps	Qlik Senseアプリは、タスク固有の、目的に沿って構築されたアプリです。アプリを作成したユーザーは、自動的にアプリの所有者に割り当てられます。アプリを再利用、変更、共有することができます。 適切なアクセス権限がある場合は、Qlik Sense ハブからアプリを作成し、ストリームに公開することができます。アプリは、QMC から公開することもできます。インストールされている Qlik Sense Desktop で作成されるアプリを公開するには、まずそのアプリを QMC からインポートする必要があります。アプリ、ストリーム、ユーザーに適用されるセキュリティ ルールによって、コンテンツにアクセスできるユーザーおよびそのユーザーが実行できる内容が決まります。アプリは公開後ロックされます。サーバー デプロイメントの Qlik Sense ハブを介してコンテンツを公開済みのアプリに追加することは可能ですが、オリジナルのアプリで公開されたコンテンツは編集できません。
[コンテンツ ライブラリ]	コンテンツ ライブラリは Qlik Sense ユーザーがアプリに共有コンテンツを追加することができるストレージです。 コンテンツ ライブラリを作成するユーザーは自動的にそのライブラリの所有者になります。ライブラリおよびライブラリ オブジェクトは、QMC で定義されたセキュリティ ルールを使用して他のユーザーと共有できます。

データ接続	データ接続により、データ ソースからデータを選択およびロードすることができます。すべてのデータ接続は、QMC から集中的に管理されています。データ接続は、Qlik Sense データ ロード エディタで作成されますデータ接続を作成したユーザーは自動的に、その接続の所有者となり、既定ではそのデータ接続にアクセスできる唯一のユーザーです。データ接続は、QMC で定義されたセキュリティ ルールを使用して他のユーザーと共有できます。 Qlik Sense Desktop で開発されたアプリをインポートすると、既存のデータ接続が QMC にインポートされます。サーバーからアプリをエクスポートすると、既存のデータ接続はそのアプリとともにはエクスポートされません。 *インポートされるアプリのデータ接続名が、既存のデータ接続の名前と同じ場合、データ接続はインポートされません。つまり、インポートされたアプリは、インポートされたアプリのデータ接続ではなく、同一名のすでに存在するデータ接続を使用します。*
分析接続	分析接続を使用すると、外部分析をビジネス ディスカバリと統合することができます。分析接続は、外部計算エンジンの呼び出し (このとき外部計算エンジンはサーバーサイド拡張 (SSE) として動作) によって、ロード スクリプトおよびチャートで使用可能な数式を拡張します。たとえば、R への分析接続を作成し、データのロード時に統計数式を使用できます。
[アプリ オブジェクト]	以下のアプリ オブジェクトを管理できます。 • シート • ストーリー アプリを作成したユーザーは自動的にアプリおよびアプリ オブジェクトの所有者に割り当てられます。アプリ オブジェクトは、属するアプリが公開されると公開されます。ユーザーは、Qlik Sense からアプリ オブジェクトを公開することで、未公開のアプリ オブジェクトをアプリに追加し、共有することができます。

[ストリーム]	ストリームを利用すると、ユーザーはアプリ、シート、ストーリーを読み取ったり公開したりできます。ストリームへの公開アクセス権があるユーザーは、その特定のストリームのコンテンツを作成できます。Qlik Senseサイトでのストリーム アクセス パターンは、各ストリームのセキュリティルールによって決まります。既定で、Qlik Senseには次の2つのストリームが含まれます。**Everyone** および **Monitoring apps** 。 1つのアプリは、1つのストリームにしか公開できません。ただし、アプリを複製してコピーを作成する場合は、コピーを別のストリームに公開することができます。アプリはストリーム間で移動できます。 ハブでは、アプリを持たないストリーム (空のストリームまたはユーザーの既存のセキュリティ規則によりアプリが表示されないストリーム) は表示されません。アプリを公開、別のストリームから移動、または削除すると、ストリームのリストが動的に更新され、アプリが1つ以上あるか否かによって、ストリームはハブから表示または非表示になります。QMC など、ハブ外での変更は、ハブ内のストリームのリストの更新をトリガーしません。 *すべての認証ユーザーには [**Everyone**] ストリームの読み取りと公開権限があり、すべての匿名ユーザーには読み取り専用権限があります。あらかじめ定義された管理者のロールの3つ (RootAdmin、ContentAdmin、SecurityAdmin) には、Monitoring apps ストリームの読み取り権限と公開権限があります。*
[タスク]	タスクは幅広い作業を行うために使用され、任意のパターンでの連動が可能です。タスクは、Qlik Sense Engine Service (QSS) によって処理されます。4種類のタスクがあります。 • リロード • ユーザー同期化 • 外部プログラム • 配布 タスク概要のページから、トリガーまたは手動で、タスク実行を開始します。タスクを実行する追加のトリガーを作成できます。トリガーには以下の2種類があります。 • スケジュールによるもの • タスク イベント
ユーザー	ユーザーは、QMC のユーザー ディレクトリ コネクタを介してユーザー ディレクトリからインポートされます。

システム通知	モバイル デバイス上の Qlik Sense Mobile Client Managed アプリからユーザーにプッシュされるカスタム通知を作成することができます。 *システム通知およびシステム通知ポリシーの機能は、署名付きキーでライセンスが付与された Qlik Sense Enterprise on Windows インストールでのみ使用できます。ライセンスの詳細については、Qlik Sense ライセンスの資料。*
システム通知ポリシー	システム通知ポリシーを作成して、システム通知の配布対象とするユーザーを指定することができます。システム通知ポリシーの作成によって、モバイル デバイス上で通知を受信するユーザーのプールまたはユーザーのグループをカスタマイズすることができます。 *システム通知およびシステム通知ポリシーの機能は、署名付きキーでライセンスが付与された Qlik Sense Enterprise on Windows インストールでのみ使用できます。ライセンスの詳細については、Qlik Sense ライセンスの資料。*
監査	QMC 監査ページで、リソースとユーザーのクエリや、Qlik Sense システムで定義されたセキュリティルールや負荷分散ルール、ライセンス ルールの監査を行うことができます。
[セキュリティ ルール]	Qlik Sense システムには、属性ベースのセキュリティルール エンジンが組み込まれており、このエンジンでは、ルールを数式として使用して、ユーザーに付与するリソースに対するアクセス権のタイプを評価します。
[カスタム プロパティ]	カスタム プロパティを作成して、セキュリティルールに自分自身の値を使用できるようにします。カスタム プロパティに 1 つまたは複数の値を定義して、リソースのセキュリティルールで使用します。

ライセンス管理	ライセンス モデルには、シリアル番号とコントロール ナンバー、および署名付きのライセンス キーの 2 つがあります。これらのモデルで、ライセンスの契約条件およびユーザーに割り当て可能なアクセス タイプを定義します。ユーザーの割り当て、分析時間消費および製品のアクティベーションには、クラウドベースのライセンス バックエンドにアクセスするために、署名済みのライセンス キーとともにインターネット アクセス (直接またはプロキシ経由) が必要となります。 主なライセンス タイプには、アクセス タイプに基づくものと、トークンに基づくものの 2 つがあります。 • アクセス タイプのライセンスは、Professional User とAnalyzer User ライセンス (ユーザーベース) および Analyzer Capacity ライセンス (キャパシティベース) です。Professional User および Analyzer User ライセンスは、Professional アクセスおよび Analyzer アクセスを割り当てることができます。Analyzer Capacity ライセンスでは、Analyzer Capacity ライセンスを割り当てることができます。ここでは消費が時間ベース (Analyzer タイム) となっています。 • Qlik Sense Token ライセンスでは、トークンを使用してアクセス パスをユーザーに割り当てます。User アクセスおよび Login アクセスを割り当てることができます。 アクセス タイプを使うと、ユーザーは Qlik Sense Enterprise on Windows サイト内のハブとアプリにアクセスできます。 *Qlik Sense Enterprise SaaS をセットアップする場合は、Qlik 代理店または Qlik サポートに連絡してセットアップのための有効なライセンスを入力してください。*
[拡張機能]	拡張機能には、ウィジェット ライブラリ、カスタム テーマ、またはビジュアライゼーション エクステンションなどさまざまなものがあり、これらを使用して、たとえば、多様な地域を選択できるインタラクティブ マップで、データを可視化します。
タグ	QMC のリソース概要ページから効率よく環境を検索して管理できるようにするには、タグを作成してリソースに適用します。
On-demand アプリ	On-Demand アプリはもちろん、選択アプリとテンプレート アプリも QMC からストリームに公開されます。

[ユーザー ディレクトリ コネクタ]	ユーザー ディレクトリ コネクタ(UDC) は構成済みのディレクトリ サービスに接続してユーザーを取得します。インストールされる Qlik Sense に組み込まれている UDC は、Generic と高度な LDAP、Active Directory、ApacheDS、ODBC、Access (ODBC 経由)、Excel (ODBC 経由)、SQL (ODBC 経由)、および Teradata (ODBC 経由) です。 *ローカル ユーザーが Qlik Sense にログオンする場合、UDC は不要です。ただし、ローカル ユーザーがアプリにアクセスできるようにするには、アクセスを割り当てる必要があります。ユーザーベースのライセンスでは、プロフェッショナルまたはアナライザーのアクセス ルールを使用できます。トークンベースのライセンスでは、ユーザーまたはログイン アクセス ルールを使用してアクセスを割り当てることができます。あるいは、まずローカル ユーザーがログオンしてユーザーとして認識され、それからトークンが割り当てられるようにすることもできます。* 新しいユーザー ディレクトリ コネクタは QMC で作成します。
監視 アプリ	Qlik Sense ログ ファイルからのデータを表示する統治アプリ、License Monitor と Operations Monitor を含むストリーム。
[サービス クラスター]	マルチ ノード サイトの場合、サービス クラスターは、すべての ノードの場合に、永続タイプ、データベース接続、および静的コンテンツ フォルダーなどの構成を保存します。設定を統一できるように、すべての ノードがサービス クラスターにリンクされています。
[ノード]	ノードは構成済みの Qlik Sense サービスを使用しているサーバーです。どの実装にも必ずセントラル ノードがあり、異なるサービスの構成用にノードを追加できます。どのノードにも必ずリポジトリがあります。 Qlik Sense のサイトは、共通の論理リポジトリあるいはセントラル ノードに接続された 1 つ以上のサーバー マシン (ノード) の集まりです。 *Shared Persistence マルチ ノード環境を設置している場合、1 つ以上のノードをフェールオーバー候補にすることができます。セントラル ノードでエラーが発生すると、フェールオーバー候補がセントラル ノードのロールを担います。* *マルチノードのインストールでは、セントラル ノードの QMC から Qlik Sense Enterprise on Windows サイト全体を管理します。リム ノードから QMC にアクセスすることはできますが、QMC からリポジトリへのリクエストがセントラル ノードのリポジトリに転送されます。*
[エンジン]	Qlik Sense Engine Service (QES) は、アプリケーションのすべての計算とロジックを処理するアプリケーション サービスです。

[印刷]	Qlik Sense Printing Service (QPR) は、PDF ファイルや画像ファイルへのオブジェクトのエクスポートと印刷を管理します。
[プロキシ]	Qlik Sense Proxy Service (QPS) は、Qlik Sense の認証、セッション ハンドリング、負荷分散を管理します。
[仮想プロキシ]	1 つ以上の仮想プロキシが各 Qlik Sense Proxy Service (QPS) で実行され、複数のサイトの認証、セッションの処理、シングル プロキシ ノードの負荷分散方法をサポートできるようにします。
[スケジューラ]	Qlik Sense Engine Service (QSS) はスケジュール済みのタスク (Qlik Sense アプリまたはユーザー同期化のリロード) とタスク チェーンを管理します。Qlik Sense の実装のタイプにより、QSS は、マネージャーとして、あるいはワーカーとして、あるいはその両方として、ノード上で稼働します。
[リポジトリ]	Qlik Sense Repository Service (QRS) は、Qlik Sense アプリ、ライセンス、セキュリティ、サービス構成データの持続性と同期を管理します。QRS は Qlik Sense Repository Database に付属し、Qlik Sense アプリを稼働および提供するその他すべての Qlik Sense サービスで必要です。さらに、QRS には Qlik Sense アプリの構造およびバイナリファイル (ローカル ファイル システムに保存されているアプリのデータ) へのパスが保存されています。
負荷分散ルール	負荷分散ルールは、リソースへのノードのアクセス権を定義します。
クラウドの配布	マルチクラウドのライセンスを持っている場合、次のセクションを利用できます。 • **アプリの配布 ステータス**: アプリの配布を監視します。 • **配布 ポリシー**:Qlik Sense Enterprise SaaS の展開に公開アプリを配布できるかどうかを決定します。配布するには、公開アプリに接続されている配布 ポリシーがあることが必要です。 • **展開の設定**:Qlik Sense Enterprise on Windows で展開を構成。
証明書	Qlik Sense は認証のために証明書を使用します。証明書により、Qlik Sense サイト内のノード間における信頼性が保たれています。証明書は、複数のノード上にあるサービス間の通信を認証するために、Qlik Sense サイト内で使用されます。
Log Collector	ログコレクタを使用すると、定義した期間のログファイルを収集およびエクスポートできます。このログは、Qlik サポートのトラブルシューティングを容易にします。

アプリ

Qlik Senseアプリは、タスク固有の、目的に沿って構築されたアプリです。アプリを作成したユーザーは、自動的にアプリの所有者に割り当てられます。アプリを再利用、変更、共有することができます。

適切なアクセス権限がある場合は、Qlik Sense ハブからアプリを作成し、ストリームに公開することができます。アプリは、QMC から公開することもできます。 インストールされている Qlik Sense Desktop で作成されるアプリを公開するには、まずそのアプリを QMC からインポートする必要があります。 アプリ、ストリーム、ユーザーに適用されるセキュリティルールによって、コンテンツにアクセスできるユーザーおよびそのユーザーが実行できる内容が決まります。アプリは公開後ロックされます。サーバー デプロイメントの Qlik Sense ハブを介してコンテンツを公開済みのアプリに追加することは可能ですが、オリジナルのアプリで公開されたコンテンツは編集できません。

QMC からアプリを複製、リロード、インポート、エクスポートまたは削除することもできます。

[**アプリ**] 概要では、利用可能なアプリすべてが一覧表示されます。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (⊞) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

アプリのプロパティ

プロパティ	説明
名前	アプリの名前。
所有者	アプリの所有者。
公開済み	アプリが公開された日付です。
ストリーム	アプリの公開先のストリーム。
タグ	アプリに紐付けられているタグ。
Target app ID (ターゲット アプリID)	複製済みの公開された元のアプリのアプリID です。公開されたアプリのコピーを作成し、元のアプリを交換する場合は、ターゲット アプリID を使用してそのアプリを特定します。
説明	アプリの説明 (ある場合)。
ファイル サイズ	アプリのファイル サイズ。 *QMC に表示されるアプリのファイル サイズは、ディスク上のファイル サイズとは異なります。これは、QMC でのサイズには、項目、テーブル、およびドキュメントプロパティなどのデータ オブジェクトのみが含まれており、.qvf ファイルにも含まれているビジュアライゼーション、ブックマーク、メジャーなどはこのサイズに含まれないためです。*
最後のリロード	アプリが最後にリロードされた時期。
ID	アプリID。
作成日	アプリが作成された日時。

プロパティ	説明
最終変更日	この項目は以下の条件によって更新されます。 • アプリのタイトルの変更。 • アプリの説明の変更。 • アプリのサムネイルの変更。 • アプリの公開。 • ストリーム間でのアプリの移動。 • アプリデータのリロード。 この項目は、以下の条件では更新されません。 • シート、ビジュアライゼーション、ストーリー、ブックマークの変更。 • ビジュアライゼーション設定の変更。 • アプリオプションの変更。
変更者	アプリを最後に変更した者。
<Custom properties>	カスタムプロパティがある場合はここに一覧表示されます。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション[**Select all rows**]は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション[**Deselect all rows**]はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*

プロパティ	説明
↻	ページを更新します。
編集	選択したアプリを編集します。[**Edit (編集)**] の横の数字は、選択したアイテムの中で編集できるアイテムの数を示します。選択したアイテムに対する更新権限を持っていない場合、[**Edit**] は [**View**] に置き換わります。
表示	選択したアプリを表示します。選択したアイテムに対する更新権限を持っていない場合、[**Edit**] は [**View**] に置き換わります。
削除	選択したアプリを削除します。[**Delete (削除)**] の横にある数字は削除されるアイテム数を示しています。選択したアイテムに対する削除権限を持っていない場合、[**Delete (削除)**] は無効となります。
公開	選択したアプリを公開します。
⊕ **インポート**	新しいアプリをインポートします。
[**More actions**] > [**Export**]	選択したアプリをエクスポートします。
[**More actions**] > [**Duplicate**]	選択したアプリを複製します。
[**More actions**] > [**Reload now**]	選択したアプリをリロードします。 *マルチノードサイトでは、セントラル ノードの Qlik Sense Engine Service (QSS) はマネージャーとして、リム ノードの QSS はワーカーとして稼働し、[**すぐにリロード**] から初めてトリガーされるときにタスクが失敗することがあります。これは、まだマネージャー QSS からワーカー QSS にタスクが同期されていないためです。2 度目はアクションが実行され、タスクが動作します。*
[**その他のアクション**] > [**新しいリロード タスクの作成**]	新しいリロード タスクを作成します。
[**その他のアクション**] > [**配布のトリガー**]	選択したアプリの配布をトリガーします。 *マルチノードサイトでは、セントラル ノードの Qlik Sense Engine Service (QSS) はマネージャーとして、リム ノードの QSS はワーカーとして稼働し、[**配布のトリガー**] から初めてトリガーされるときにタスクが失敗することがあります。これは、まだマネージャー QSS からワーカー QSS にタスクが同期されていないためです。2 度目はアクションが実行され、タスクが動作します。*

プロパティ	説明
さらに表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

アプリ: 関連するアイテム

本書の表に、[**コンテンツ**] プロパティグループと[**セキュリティルール**] プロパティグループで利用可能な項目を示します。

既定では項目の一部のみが表示されます。列セレクター ( ) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

アプリのコンテンツ

[**アプリ コンテンツ**] はアプリを編集する際に [**関連するアイテム**] から利用できます。概要には 、選択したアプリに関連付けられるアプリコンテンツ (画像) のリストが含まれます。

アプリコンテンツプロパティ

プロパティ	説明
[**ファイル名**]	アプリコンテンツ ファイルの名前。
場所	アプリコンテンツ ファイルが保存されている場所。 例: *%RepositoryRoot%\AppContent\[App ID]\[App content file]*
[**URL パス**]	アプリコンテンツ ファイルのパス。 例: */AppContent/[App ID]/[App content file]*。
[**ファイル サイズ (KB)**]	アプリコンテンツ ファイルのサイズ。
[**アプリ**]	アプリコンテンツが含まれるアプリ。
ID	アプリコンテンツの ID。
作成日	アプリコンテンツが作成された日時。
[**最終変更日**]	アプリコンテンツが最後に変更された日時。
[**変更者**]	アプリコンテンツを最後に変更した人物。

アプリオブジェクト

[**アプリオブジェクト**] はアプリを編集する際に [**関連するアイテム**] から利用できます。概要には、選択したスアプリに関連付けられるアプリオブジェクトのリストが含まれます。

アプリオブジェクトプロパティ

プロパティ	説明
[名前]	アプリオブジェクトの名前。
[タイプ]	アプリオブジェクトのタイプ: シートまたはストーリー。
[所有者]	アプリオブジェクトの所有者。
[承認済み]	アプリオブジェクトのステータス: • **Not approved**: アプリオブジェクトは公開済みアプリに追加されたため、承認されていません。 • [**Approved**]: アプリオブジェクトは、アプリが公開された際にそのアプリに含まれていたため、承認されています。
[公開済み]	アプリオブジェクトのステータス: • **Not published** (未公開): アプリオブジェクトはストリームに公開されていません。 • **公開済み**: アプリオブジェクトはストリームに公開されています。2 つの公開方法があります。アプリオブジェクトそのものを Qlik Sense から公開するか、アプリオブジェクトが属するアプリを Qlik Sense または Qlik Management Console から公開する方法があります。
[最終変更日]	アプリオブジェクトが最後に変更された日時。
[アプリ]	アプリオブジェクトが含まれるアプリ。
[タグ]	アプリオブジェクトのタグ。
[ID]	アプリオブジェクトの ID。
[作成日時]	アプリオブジェクトが作成された日時。
[変更者]	アプリオブジェクトを最後に変更した者。

概要で選択してアクション バーの [**Edit**] をクリックすると、アプリオブジェクトの編集ページが表示されます。

ユーザー アクセス

[**ユーザー アクセス**] は、リソースを編集する際に [**関連するアイテム**] から利用できます。

プレビューには、ターゲット リソースと選択したアイテムにアクセスできるソース ユーザーが表示されます。

権限に応じて、ユーザーやリソース、関連するルールを編集したり、表示することができます。

タスク

[**タスク**] はアプリを編集する際に [**関連するアイテム**] から利用できます。概要には、選択したアプリに関連付けられるタスクのリストが含まれます。

タスクのプロパティ

プロパティ	説明
名前	タスクの名前。
タイプ	タスクのタイプ。
[**アプリ**]	タスクと関連付けられたアプリの名前。
有効化済み	ステータス値:**Yes** または **No**
ステータス	タスクの状態。
タグ	タスクと関連付けられたアプリの名前。
部分的なリロード	最近変更されたデータのみを読み込む。
最大再試行回数	リロード リトライの最大数。
ID	タスクの ID。
作成日	タスクが作成された日時。
[**最終変更日**]	タスクが最後に変更された日時。
[**変更者**]	タスクを最後に変更した者。
カスタム プロパティ	カスタム プロパティがある場合はここに一覧表示されます。

概要で選択してアクション バーの [**Edit**] をクリックすると、タスクの編集ページが表示されます。

アプリのコンテンツ

Qlik Senseアプリは、タスク固有の、目的に沿って構築されたアプリです。アプリを作成したユーザーは、自動的にアプリの所有者に割り当てられます。アプリを再利用、変更、共有することができます。

サーバーにアプリをインポートする場合やサーバーからアプリをエクスポートする場合は、画像などの .qvf ファイルに保存されていない関連コンテンツも移動します。関連コンテンツは、*%ProgramData%\Qlik\Sense\Repository\AppContent\<App ID>* フォルダに個別に保存されます。各アプリには、アプリID をフォルダ名とする独自のアプリ コンテンツ フォルダがあります。

*AppContent フォルダにアップロードされたコンテンツは、その特定のアプリでのみ使用できます。他のアプリでコンテンツを使用できるようにするには、[**コンテンツ ライブラリ**] を使用します。*

アプリ コンテンツ フォルダに画像をアップロードする

QMC の [**App contents**] ページでは、特定のアプリで使用するファイル (画像) をアップロードできます。このファイルは、アプリ コンテンツ フォルダに保存されます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**アプリ**] を選択して、概要を表示します。
3. 画像をアップロードする先のアプリを選択し、[**Edit**] をクリックします。
4. [**App edit**] ページの [**Associated items**] で、[**App contents**] を選択します。
5. [**アップロード**] をクリックします。
   ファイル選択ダイアログが表示されます。
6. アップロードするファイルを選択するボタンをクリックし、ファイルを選択して [**Upload**] をクリックします。

ファイルがアップロードされ、[**App contents**] リストに表示されます。

> *Qlik Sense Repository Service は、AppContent またはコンテンツ ライブラリにアップロードされた XML ファイルにあるスクリプト タグをスキャンします。*

アプリ コンテンツ フォルダの画像を削除する

QMC の [**App contents**] ページでは、特定のアプリからファイル (画像) を削除できます。このファイルは、アプリ コンテンツ フォルダから削除されます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**アプリ**] を選択して、概要を表示します。
3. 画像を削除するアプリを選択し、[**Edit**] をクリックします。
4. [**App edit**] ページの [**Associated items**] で、[**App contents**] を選択します。
5. [**App contents**] リストで、削除するファイルを選択します。
   (URL のパスには、ファイル名が含まれます。)
6. [**削除**] をクリックします。
   確認のダイアログが表示されます。
7. [**OK**] をクリックします。

コンテンツ ライブラリ

コンテンツ ライブラリは Qlik Sense ユーザーがアプリに共有コンテンツを追加することができるストレージです。

コンテンツ ライブラリを作成するユーザーは自動的にそのライブラリの所有者になります。ライブラリおよびライブラリ オブジェクトは、QMC で定義されたセキュリティ ルールを使用して他のユーザーと共有できます。

[**コンテンツ ライブラリ**] の概要には、Qlik Sense サイトにあるすべてのコンテンツ ライブラリが一覧表示されます。

次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (▦) を使用して項目を追加できます。

> *列幅は、ヘッダーの線をドラッグすることで調整できます。*

コンテンツ ライブラリの項目と値

項目	値
名前	コンテンツ ライブラリの名前。
[**所有者**]	コンテンツ ライブラリの所有者。
タグ	コンテンツ ライブラリに紐付けられているタグ。
ID	コンテンツ ライブラリの ID。既定では、表示されていない状態です。
作成日	コンテンツ ライブラリが作成された日時。
[**最終変更日**]	コンテンツ ライブラリが最後に変更された日時。
[**変更者**]	コンテンツ ライブラリを最後に変更した人物。
[**<カスタム プロパティ>**]	カスタム プロパティがある場合はここに一覧表示されます。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
▽	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、▽ が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
▦	列セレクター: 概要で表示する列を選択します。↩ をクリックすると既定の列にリセットされます。

🔍	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
🔄	ページを更新します。
[**編集**]	選択したコンテンツ ライブラリを編集します。選択したアイテムに対する更新権限を持っていない場合、[**Edit**] は [**View**] に置き換わります。
[**表示**]	選択したコンテンツ ライブラリを表示します。選択したアイテムに対する更新権限を持っていない場合、[**Edit**] は [**View**] に置き換わります。
[**削除**]	選択したコンテンツ ライブラリを削除します。選択したアイテムに対する削除権限を持っていない場合、[**Delete (削除)**] は無効となります。
[**アップロード**]	選択したコンテンツ ライブラリにライブラリオブジェクトをアップロードします。 *Qlik Sense Repository Service は、AppContent または コンテンツ ライブラリにアップロードされた XML ファイルにあるスクリプト タグをスキャンします。*
⊕ [**新規作成**]	新しいコンテンツ ライブラリを作成します。
さらに表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

コンテンツ ライブラリ: 関連するアイテム

本書の表に、[**コンテンツ**] プロパティグループと [**セキュリティ ルール**] プロパティグループで利用可能な項目を示します。

既定では項目の一部のみが表示されます。列セレクター (⊞) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

コンテンツ

[**コンテンツ**] はコンテンツ ライブラリを編集する際に [**関連するアイテム**] から利用できます。

概要には、選択したコンテンツ ライブラリに関連付けられるコンテンツのリストが含まれます。

[**コンテンツ**] プロパティグループの項目

プロパティ	**説明**
[**ファイル名**]	オブジェクト ファイルの名前。
[**場所**]	オブジェクトが保存されたロケーション: *\Content\<コンテンツ ライブラリ名>\<ファイル名>*。
[**URL パス**]	オブジェクトの URL パス: */content/<コンテンツ ライブラリ名>/<ファイル名>*。
[**ファイル サイズ (KB)**]	キロバイト単位のファイル サイズ。
[**ID**]	オブジェクトの ID。
作成日時	オブジェクトが作成された日時。
最終変更日	オブジェクトが最後に変更された日時。
変更者	オブジェクトを最後に変更した人物。

コンテンツのキャッシュ制御

キャッシュされたコンテンツには潜在的なセキュリティ リスクがあります。ブラウザは、ウェブ サーバーから受信したコンテンツのローカル キャッシュ コピーを保存する場合があります。一部のブラウザは、HTTP/HTTPS を介してアクセスされるコンテンツをキャッシュします。アプリケーション応答の機密情報がローカル キャッシュに保存されている場合、この情報は将来同じコンピューターにアクセスできる他のユーザーが取得できます。

コンテンツのキャッシュ制御を使用すると、ブラウザのキャッシュ動作を変更して、このようなリスクを防ぐことができます。

[**コンテンツのキャッシュ制御**] プロパティグループの項目

プロパティ	**説明**
名前	コンテンツのキャッシュ制御の名前。

プロパティ	説明

regex フィルター	キャッシュ設定が適用されるURLの一致を除外するための正規表現。
	
	(.*?) - すべてに一致します(.*?)
	
	(resources|appcontent) - URIに「resources」または「appcontent」を含むリクエストに一致します。次に例を示します。
	
	/resources/hub/img/core/static/Default_thumbnail_app.svg
	
	/appcontent/126610c6-1a6f-4d1b-8126-a7fbb040b44d/Icon_License_grey.png
	
	キャッシュ設定が適用されるURLの一致を除外するための正規表現。リポジトリには、標準の `System.Text.RegularExpressions.Regex` クラスを使用します。比較は次の方法で行います:
	
	`regex = new Regex(contentCacheControl.Filter)`
	
	`regex.IsMatch(httpRequest.RawUrl);`
	
	hubの場合は、標準のnodejs RegExp:
	
	`regex = new RegExp(contentCacheControl.Filter)`
	`regex.test("/api/hub" + res.req.originalUrl);`

maxAge	キャッシュされたコンテンツが含まれる最大経過時間。既定値の3600 (秒) を編集できます。
cachePolicy	**公開、最大経過時間**: キャッシュされた応答は、再検証なしで送信されます。 **公開、再検証必要あり、最大経過時間 =0**: キャッシュされた応答を使用する前に、古い応答を再検証するためにキャッシュが必要です。 **プライベート、最大経過時間**: キャッシュされた応答は、再検証なしで送信されます。応答メッセージの全部または一部は1人のユーザーを対象としており、共有キャッシュによってキャッシュされてはなりません。 **プライベート、再検証必要あり、最大経過時間 =0**: 通常はキャッシュできない応答はキャッシュ可能ですが、キャッシュされた応答を使用する前に、古い応答を再検証するためにキャッシュが必要です。応答メッセージの全部または一部は1人のユーザーを対象としており、共有キャッシュによってキャッシュされてはなりません。 **保存なし**: 応答は再利用できません。
ID	オブジェクトのID。
作成日時	オブジェクトが作成された日時。
[**最終変更日**]	オブジェクトが最後に変更された日時。
[**変更者**]	オブジェクトを最後に変更した人物。

キャッシュ制御を変更する前に

キャッシュ コントロール ヘッダーを変更する前に、次の点に注意してください。

- 通常、キャッシュ制御ヘッダーを手動で変更することはお勧めしません。
- ブラウザのキャッシュ動作が変更によってどのように影響を受けるかを理解してください。
- 実稼働環境に変更を適用する前に、変更のリスクを評価してください。

新しいコンテンツ キャッシュ制御のリンク

キャッシュ制御には所有者がいません。コンテンツ ライブラリへの必須の参照があり、[**regex フィルター**] 設定の正規表現に一致するそのライブラリ内のリソースにのみ影響します。

次の手順を実行します。

1. QMC で、[**コンテンツ ライブラリ**] を開きます。
2. コンテンツ キャッシュ制御を追加するコンテンツ ライブラリをダブルクリックします。
3. [**関連するアイテム**] で、[**コンテンツ キャッシュ制御**] を開きます。
4. [**新しいコンテンツ キャッシュ コントロールのリンク**] をクリックします。
5. フィールドに入力します。
   [**name**] と[**regex filter**] は必須です。[**maxAge**] は秒単位で表示され、編集できます。
6. [**追加**] をクリックします。

関連項目: *コンテンツのキャッシュ制御の構成 (page 517)*

ユーザー アクセス

[**ユーザー アクセス**] は、リソースを編集する際に [**関連するアイテム**] から利用できます。

プレビューには、ターゲット リソースと選択したアイテムにアクセスできるソース ユーザーが表示されます。

権限に応じて、ユーザーやリソース、関連するルールを編集したり、表示することができます。

セキュリティ ルール

[**セキュリティ ルール**] はコンテンツ ライブラリを編集する際に [**関連するアイテム**] から利用できます。概要には、選択したコンテンツ ライブラリに関連付けられるセキュリティ ルールのリストが含まれます。

[**セキュリティ ルール**] プロパティ グループにはユーザー条件プロパティが含まれます。

ユーザー条件プロパティ

プロパティ	説明
[**名前**]	セキュリティ ルールの名前。
[**説明**]	ルールの説明。
[**リソース フィルター**]	ルールの ID。
[**アクション**]	ルールで許可されたアクション。
[**無効化**]	ステータス値:**Yes** または **No**
[**コンテキスト**]	セキュリティ ルールのコンテキスト ([**QMC**]、[**Hub**]、[**Both**])。
[**タイプ**]	セキュリティ ルール タイプ ([**Default**]、[**Read only**]、[**Custom**])。
[**条件**]	セキュリティ ルールの条件。

プロパティ	説明
[**ID**]	セキュリティルールの ID。
[**作成日時**]	セキュリティルールが作成された日時。
[**最終変更日**]	セキュリティルールが最後に変更された日時。
[**変更者**]	セキュリティルールを最後に変更した者。

*概要で選択してアクションバーの [**Edit**] をクリックすると、セキュリティの編集ページが表示されます。*

データ接続

データ接続により、データソースからデータを選択およびロードすることができます。すべてのデータ接続は、QMC から集中的に管理されています。データ接続は、Qlik Sense データロードエディタで作成されますデータ接続を作成したユーザーは自動的に、その接続の所有者となり、既定ではそのデータ接続にアクセスできる唯一のユーザーです。データ接続は、QMC で定義されたセキュリティルールを使用して他のユーザーと共有できます。

Qlik Sense Desktop で開発されたアプリをインポートすると、既存のデータ接続が QMC にインポートされます。サーバーからアプリをエクスポートすると、既存のデータ接続はそのアプリとともにはエクスポートされません。

インポートされるアプリのデータ接続名が、既存のデータ接続の名前と同じ場合、データ接続はインポートされません。つまり、インポートされたアプリは、インポートされたアプリのデータ接続ではなく、同一名のすでに存在するデータ接続を使用します。

*所有者以外のユーザーにデータ接続へのアクセス権を付与するには、接続を編集するか、[**セキュリティルール**] のページに進みます。*

[**データ接続**] 概要には、利用可能なデータ接続がすべて一覧表示されます。

既定では、QMC にはArchivedLogsFolder とServerLogFolder の 2 つのデータ接続が含まれています。これらは QMC に一緒にインストールされている監視アプリ「License Monitor」と「Operations Monitor」に対するデータ接続です。管理者ロール (ルート、セキュリティ、コンテンツ、実装) のユーザーは、Qlik Sense ハブのデータロードエディタでデータ接続が利用できます。

次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (⊞) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

項目の説明

項目	説明
[**名前**]	データ接続名。

[**所有者**]	データ接続の所有者。
タグ	データ接続に紐付けられているタグ。
[**接続文字列**]	データ接続の接続文字列。通常はデータソースやドライバー、パスの名前が含まれています。
[***タイプ***]	データ接続のタイプ。ODBC、OLEDB およびフォルダーなど標準的なデータ接続。
[**ユーザー ID**]	接続文字列で使用されているユーザー ID。
[**ID**]	データ接続の ID。既定では、表示されていない状態です。
[**作成日時**]	データ接続が作成された日時。
[**最終変更日**]	データ接続が最後に変更された日時。
[**変更者**]	データ接続を最後に変更した者。
[***<カスタム プロパティ>***]	カスタム プロパティがある場合はここに一覧表示されます。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
[***アクション***]	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
[**編集**]	選択したデータ接続を編集します。

[**削除**]	選択したデータ接続を削除します。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

データ接続: 関連するアイテム

本書の表に、[**コンテンツ**] プロパティグループと[**セキュリティルール**] プロパティグループで利用可能な項目を示します。

既定では項目の一部のみが表示されます。列セレクター ( ) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

ユーザー アクセス

[**ユーザー アクセス**] は、リソースを編集する際に [**関連するアイテム**] から利用できます。

プレビューには、ターゲット リソースと選択したアイテムにアクセスできるソース ユーザーが表示されます。

権限に応じて、ユーザーやリソース、関連するルールを編集したり、表示することができます。

セキュリティルール

[**セキュリティルール**] はデータ接続を編集する際に [**関連するアイテム**] から利用できます。概要には、選択したデータ接続に関連付けられるセキュリティルールのリストが含まれます。

[**セキュリティルール**] プロパティグループにはユーザー条件プロパティが含まれます。

ユーザー条件プロパティ

プロパティ	**説明**
[**名前**]	セキュリティルールの名前。
[**説明**]	ルールの説明。
[**リソース フィルター**]	ルールの ID。
[**アクション**]	ルールで許可されたアクション。
[**無効化**]	ステータス値:**Yes** または **No**
[**コンテキスト**]	セキュリティルールのコンテキスト ([**QMC**]、[**Hub**]、[**Both**])。
[**タイプ**]	セキュリティルール タイプ ([**Default**]、[**Read only**]、[**Custom**])。

プロパティ	説明
[**条件**]	セキュリティルールの条件。
[**ID**]	セキュリティルールの ID。
[**作成日時**]	セキュリティルールが作成された日時。
[**最終変更日**]	セキュリティルールが最後に変更された日時。
[**変更者**]	セキュリティルールを最後に変更した者。

概要で選択してアクション バーの [**Edit**] をクリックすると、セキュリティルールの編集ページが表示されます。

分析接続

分析接続を使用すると、外部分析をビジネスディスカバリと統合することができます。分析接続は、外部計算エンジンの呼び出し (このとき外部計算エンジンはサーバーサイド拡張 (SSE) として動作) によって、ロード スクリプトおよびチャートで使用可能な数式を拡張します。たとえば、R への分析接続を作成し、データのロード時に統計数式を使用できます。

[**分析接続**] 概要には、利用可能な分析接続がすべて一覧表示されます。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (▦) を使用して項目を追加できます。

> *[**分析接続**] をスタートページで表示するには、QMC へのアクセスに使用する仮想プロキシに負荷分散サーバーがあることが前提条件となります。[**仮想プロキシの編集**] ページの [**負荷分散**] で、負荷分散のサーバー ノードがあることを確認します。*

分析接続プロパティ

プロパティ	説明
[**名前**]	分析接続の名前。一意である必要があり、数字で始まってはなりません。プラグイン関数 (例えば、Python プラグインの場合の SSEPython または R プラグインの場合の R) により、アプリの数式内から使用されるプラグインへのマッピング/エイリアス。
ホスト	分析接続のホストは、例えば同じマシン上では *localhost*、別のマシン上にある場合は *mymachinename.qlik.com* です。
ポート	接続時に使用するポート (整数)。

プロパティ	説明
証明書ファイルのパス	証明書へのフル パス:*C:\ProgramData\Qlik\Sense\Repository\Exported Certificates\<サーバー名>*。このパスは、クライアントおよびサーバーの両方の証明書とキーを含むフォルダーを指し示す必要があります。このパスは、証明書が配置されているフォルダーを指し示しているだけです。証明書が実際にこのフォルダーにコピーされていることを確認する必要があります。3 つの証明書の名前は、*root_cert.pem*、*sse_client_cert.pem*、*sse_client_key.pem* とする必要があります。許可されているのは相互認証のみです (サーバーとクライアント間の認証)。 *証明書のファイル パスの設定は任意ですが、パスがないと接続は安全ではありません。*
再接続タイムアウト (秒)	既定値: 20
要求タイムアウト (秒)	既定値: 0
ID	分析接続の ID。
作成日時	分析接続が作成された日時。
最終変更日	分析接続が最後に変更された日時。
変更者	分析接続を最後に変更した者。
[<カスタム プロパティ>]	カスタム プロパティがある場合はここに一覧表示されます。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。

プロパティ	説明
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
[**編集**]	選択した接続を編集します。
削除	選択した接続を削除します。
[**新規作成**]	新しい接続を作成します。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

アプリオブジェクト

[**アプリオブジェクト**] 概要には、Qlik Sense サイトにあるアプリオブジェクトが一覧表示されます。

以下のアプリオブジェクトを管理できます。

- シート
- ストーリー

アプリを作成したユーザーは自動的にアプリおよびアプリオブジェクトの所有者に割り当てられます。アプリオブジェクトは、属するアプリが公開されると公開されます。ユーザーは、Qlik Sense からアプリオブジェクトを公開することで、未公開のアプリオブジェクトをアプリに追加し、共有することができます。

アプリオブジェクトの概要では、利用可能なアプリオブジェクトがすべて一覧表示されます。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (⊞) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

アプリオブジェクトプロパティ

プロパティ	説明
[名前]	アプリオブジェクトの名前。
[タイプ]	アプリオブジェクトの タイプ: シートまたは ストーリー。
[所有者]	アプリオブジェクトの所有者。
[承認済み]	アプリオブジェクトのステータス: • **Not approved**: アプリオブジェクトは公開済みアプリに追加されたため、承認されていません。 • [**Approved**]: アプリオブジェクトは、アプリが公開された際にそのアプリに含まれていたため、承認されています。
[公開済み]	アプリオブジェクトのステータス: • **Not published** (未公開): アプリオブジェクトはストリームに公開されていません。 • **公開済み**: アプリオブジェクトはストリームに公開されています。2 つの公開方法があります。アプリオブジェクトそのものを Qlik Sense から公開するか、アプリオブジェクトが属するアプリを Qlik Sense または Qlik Management Console から公開する方法があります。
[最終変更日]	アプリオブジェクトが最後に変更された日時。
[アプリ]	アプリオブジェクトが属するアプリの名前。

プロパティ	説明
[ストリーム]	アプリオブジェクトが属するストリームの名前。
タグ	アプリオブジェクトに紐付けられているタグ。
[ID]	アプリオブジェクトの ID。
[作成日時]	アプリオブジェクトが作成された日時。
[変更者]	アプリオブジェクトを最後に変更した者。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
[アクション]	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
[編集]	選択したアプリオブジェクトを編集します。選択したアイテムに対する更新権限を持っていない場合、[**Edit**] は [**View**] に置き換わります。
[表示]	選択したアプリオブジェクトを表示します。選択したアイテムに対する更新権限を持っていない場合、[**Edit**] は [**View**] に置き換わります。

プロパティ	説明
[削除]	選択したアプリオブジェクトを削除します。選択したアイテムに対する削除権限を持っていない場合、[**Delete (削除)**] は無効となります。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

アプリオブジェクト: 関連するアイテム

本書の表に、[**コンテンツ**] プロパティグループと[**セキュリティルール**] プロパティグループで利用可能な項目を示します。

既定では項目の一部のみが表示されます。列セレクター (⊞) を使用して項目を追加できます。

ユーザー アクセス

[**ユーザー アクセス**] は、リソースを編集する際に [**関連するアイテム**] から利用できます。

プレビューには、ターゲット リソースと選択したアイテムにアクセスできるソース ユーザーが表示されます。

権限に応じて、ユーザーやリソース、関連するルールを編集したり、表示することができます。

ストリーム

ストリームを利用すると、ユーザーはアプリ、シート、ストーリーを読み取ったり公開したりできます。ストリームへの公開アクセス権があるユーザーは、その特定のストリームのコンテンツを作成できます。Qlik Senseサイトでのストリーム アクセス パターンは、各ストリームのセキュリティルールによって決まります。既定で、Qlik Sense には次の 2 つのストリームが含まれます。**Everyone** および **Monitoring apps** 。

1 つのアプリは、1 つのストリームにしか公開できません。ただし、アプリを複製してコピーを作成する場合は、コピーを別のストリームに公開することができます。アプリはストリーム間で移動できます。

ハブでは、アプリを持たないストリーム (空のストリームまたはユーザーの既存のセキュリティ規則によりアプリが表示されないストリーム) は表示されません。アプリを公開、別のストリームから移動、または削除すると、ストリームのリストが動的に更新され、アプリが 1 つ以上あるか否かによって、ストリームはハブから表示または非表示になります。QMC など、ハブ外での変更は、ハブ内のストリームのリストの更新をトリガーしません。

*すべての認証ユーザーには [**Everyone**] ストリームの読み取りと公開権限があり、すべての匿名ユーザーには読み取り専用権限があります。あらかじめ定義された管理者のロールの 3 つ (RootAdmin、ContentAdmin、SecurityAdmin) には、Monitoring apps ストリームの読み取り権限と公開権限があります。*

ユーザーがストリーム内の公開されたアプリを編集できるようなルールを作成することは推奨されません。

[**ストリーム**] 概要には利用可能なストリームすべてが一覧表示されます。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (▦) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

名前	ストリームの名前。
所有者	ストリームの所有者。デフォルトでは、ストリームの作成者です。
タグ	ストリームに紐付けされているタグ。
最後に開始された同期	最後に開始されたクラウド環境との同期の日時。
最後に完了した同期	最後に正常に終了したクラウド環境との同期の日時。
同期ステータス	Qlik Senseとの同期の最新ステータス。
ID	ストリームのID。
作成日時	ストリームが作成された日時。
最終変更日	ストリームが最後に変更された日時。
変更者	ストリームを最後に変更した者。
<カスタム プロパティ>	カスタム プロパティがある場合はここに一覧表示されます。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
⧩	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、⧩ が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*

アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション[**Select all rows**]は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション[**Deselect all rows**]はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
編集	選択したストリームを編集します。
削除	選択したストリームを削除します。
[新規作成]	新しいストリームを作成します。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**]をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl]キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

ストリーム: 関連するアイテム

本書の表に、[**コンテンツ**]プロパティグループと[**セキュリティルール**]プロパティグループで利用可能な項目を示します。

既定では項目の一部のみが表示されます。列セレクター( )を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

アプリ

[**アプリ**]はストリームを編集する際に[**関連するアイテム**]から利用できます。概要には、選択したストリームに関連付けられているアプリのリストが含まれます。

関連するアイテムのプロパティ

プロパティ	説明
[名前]	アプリの名前。
所有者	アプリの所有者。
[公開済み]	アプリが公開された日付です。
[説明]	アプリの説明。
[ファイル サイズ]	アプリのサイズ。
[最後のリロード]	アプリが最後にリロードされた日時。
[ID]	アプリの ID。
[作成日時]	アプリが作成された日時。
[最終変更日]	アプリが最後に変更された日時。
[変更者]	アプリを最後に変更した者。
[カスタム プロパティ]	カスタム プロパティがある場合はここに一覧表示されます。

概要で選択して操作バーの [**編集**] をクリックすると、アプリの編集ページが表示されます。

ユーザー アクセス

[**ユーザー アクセス**] は、リソースを編集する際に [**関連するアイテム**] から利用できます。

プレビューには、ターゲット リソースと選択したアイテムにアクセスできるソース ユーザーが表示されます。

権限に応じて、ユーザーやリソース、関連するルールを編集したり、表示することができます。

セキュリティ ルール

[**セキュリティ ルール**] はストリームを編集する際に [**関連するアイテム**] から利用できます。概要には、選択したストリームに関連付けられるセキュリティ ルールのリストが含まれます。

[**セキュリティ ルール**] プロパティ グループにはユーザー条件プロパティが含まれます。

ユーザー条件プロパティ

プロパティ	説明
[名前]	セキュリティ ルールの名前。
[説明]	ルールの説明。
[リソース フィルター]	ルールの ID。
[アクション]	ルールで許可されたアクション。
[無効化]	ステータス値:**Yes** または **No**
[コンテキスト]	セキュリティ ルールのコンテキスト ([**QMC**]、[**Hub**]、[**Both**])。
[タイプ]	セキュリティ ルール タイプ ([**Default**]、[**Read only**]、[**Custom**])。

プロパティ	説明
[**条件**]	セキュリティルールの条件。
[**ID**]	セキュリティルールの ID。
[**作成日時**]	セキュリティルールが作成された日時。
[**最終変更日**]	セキュリティルールが最後に変更された日時。
[**変更者**]	セキュリティルールを最後に変更した者。

概要で選択してアクション バーの [**Edit**] をクリックすると、セキュリティルールの編集ページが表示されます。

タスク

タスクは幅広い作業を行うために使用され、任意のパターンでの連動が可能です。タスクは、Qlik Sense Engine Service (QSS) によって処理されます。4 種類のタスクがあります。

- リロード
- ユーザー同期化
- 外部プログラム
- 配布

[**Tasks**] 概要では利用可能なタスクがすべて一覧表示されます。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (⊞) を使用して項目を追加できます。

> *列幅は、ヘッダーの線をドラッグすることで調整できます。*

タスクのプロパティ

項目/ボタン	説明
名前	タスクの名前。クリックして、🔗 タスクチェーン概要を表示します(タスクチェーン トリガーが適用されているリロード タスクにのみ該当します) 。
[**Associated resource**]	アプリ名あるいは タスクを使用するユーザー ディレクトリコネクタ。
タイプ	タスクのタイプ: • リロード (アプリ用) • ユーザー同期化 (ユーザー ディレクトリコネクタ用) • External program (外部プログラム) (サード パーティのプログラムのトリガー) • 配布 タスク (Qlik Cloud へのアプリの配布 トリガー)
有効化済み	ステータス値:**Yes** または **No**

ステータス	タスクの状態。 ••• 未開始: タスクは開始されていません。 🔄 トリガー: タスクを実行する要求がスケジューラに送信されました。 🔄 開始: タスクが開始されました。 ⏳ キュー: タスクはキューに入れられ、先行するタスクが処理されると開始されます。キューイングは、**最大同時リロード**の値によって制御されます。*スケジューラの編集 (page 422)* を参照してください。 🔄 中止の開始: マネージャー スケジューラは中止要求を受け取りましたが、処理を開始していません。 🔄 中止中: マネージャー スケジューラが中止要求の処理を開始しました。 ⛔ 中止: タスクは中止されました。 ✔成功: タスクの実行は成功しました。 ✕ 失敗: タスクは実行のためにワーカー スケジューラに送信されましたが、完了できませんでした。例えば、データ接続に対する読み取り権限がないか、リロード スクリプトにエラーがあるため、リロードが失敗する可能性があります。 ••• スキップ: タスクの開始が要求されましたが、何らかの理由でタスクの実行が開始されていません。例えば、タスクが有効になっていない可能性があります。 🔄 再試行中: タスクの開始に失敗し、新しい試行が開始されました。 ✕ エラー: タスクは実行のためにワーカー スケジューラに正常に送信されず、エラーが返されました。例えば、タスクを実行するために使用できるワーカー スケジューラがない場合、またはアプリケーションが別のタスクによってすでに更新されている場合に、エラーが発生する可能性があります。 ••• リセット: 現在のステータスが非ターミナルの場合、つまり実行がまだ終了していないトリガー、起動、キューなどの状態の場合に、マネージャー スケジューラが起動時にタスクに設定する状態。 クリックして、ℹ 最後のリロードやユーザー同期タスクの概要を開きます。 *タスクの状態の情報 (page 65)*
[**Last execution**]	タスクの最後の実施日と時間。実施されなかった場合、情報は表示されません。

[**Next execution**]	次回のタスク実施を開始するトリガーのタイプ。 • [**On task event trigger**]: 別のタスクが完了するとタスクの実行が開始されます。 • [**On multiple triggers**]: タスクには、適用されるトリガーが 2 つ以上含まれています。 • タスクにスケジュール トリガーが適用されている場合、タスクの次の実行日時が表示されます。 • 項目が空の場合、タスクにトリガーが作成されていないことを示します。
タグ	タスクに紐付けされているタグ。
ID	タスクの ID。
作成日	タスクが作成された日時。
[**Last modified**]	タスクが最後に変更された日時。
[**Modified by**]	タスクを最後に変更した者。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。

[**編集**]	選択したタスクを編集します。
[**Delete**]	選択したタスクを削除します。
[**Start**]	選択したタスクを開始します。
[**Stop**]	選択したタスクを停止します。
⊕ [**タスクのリロード**]	新しいリロード タスクを作成します。
⊕ [**外部プログラムのタスク**]	新規の外部プログラムタスクを作成します。
⊕**配布 タスク**	新規の配布タスクを作成します。
[**More actions > Enable**]	選択したタスクを有効にします。
[**More actions > Disable**]	選択したタスクを無効にします。
さらに表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

タスク: 関連するアイテム

次の関連するアイテムはリロード タスク、外部プログラム タスク、および配布タスクで利用できます。

ユーザー アクセス

[**ユーザー アクセス**] は、リソースを編集する際に [**関連するアイテム**] から利用できます。

プレビューには、ターゲット リソースと選択したアイテムにアクセスできるソース ユーザーが表示されます。

権限に応じて、ユーザーやリソース、関連するルールを編集したり、表示することができます。

ユーザー同期化タスク: 関連するアイテム

次の関連するアイテムはユーザー同期化タスクで利用できます。

ユーザー アクセス

[**ユーザー アクセス**] は、リソースを編集する際に [**関連するアイテム**] から利用できます。

プレビューには、ターゲット リソースと選択したアイテムにアクセスできるソース ユーザーが表示されます。

権限に応じて、ユーザーやリソース、関連するルールを編集したり、表示することができます。

トリガー

[**トリガー**] はタスクを編集する際に [**関連するアイテム**] から利用できます。概要には、選択したタスクに関連付けられるトリガーのリストが含まれます。

トリガー

プロパティ	**説明**
[**名前**]	トリガー名。
[**有効期間の開始日**]	トリガー作成時に入力された [**開始**] の値に従い、年 ·日 ·時刻が表示されます。
[**有効期間の終了日**]	トリガー作成時に入力された [**終了**] 値に従い、年 ·日 ·時間が表示されます。
[**スケジュール**]	トリガー作成時に選択された [**スケジュール**] の値に従い、繰り返しのパターンが表示されます。
[**有効化**]	ステータス値:**Yes** または **No**
[**ID**]	トリガーの ID。
[**作成日時**]	トリガーが作成された日時。
[**最終変更日**]	トリガーが最後に変更された日時。
[**変更者**]	トリガーを最後に変更した人物。

トリガーは概要から管理できます。トリガーを選択してアクション バーでボタンをクリックしてください。

[**Edit**] をクリックすると、トリガーの編集ページが表示されます。

タスクの状態の情報

On the tasks overview page, in the **Status** column, each task has an information icon (ⓘ) that you can click to get a summary of the latest task execution. 概要には次の情報が含まれています。

タスク実行の概要

項目	**説明**
タスクのステータス	タスク状態ウィンドウと状態列とで表示されている状態が異なる場合があります。データ マネージャーでテーブルの ↻ in the task status window to refresh the status for that specific task, or click ↻ to the far right on the tasks overview page to update the status for all tasks. さまざまなタスク ステータスの説明については、*タスク(page 61)* を参照してください。
ホスト名	タスクを前回起動したサーバー ノード。

日付およびタイムスタンプ	タスク実施ステップが実行された日時。ステップが最近実施された順に表示されます。 タスクテーブル実行列では、時間でタイムゾーンの違いが考慮されます。そのため、ポップアップと違う表示になります。
実行されたタスクステップ	実行されたタスク実施ステップの説明。

タスクのリロードにも [**スクリプトログのダウンロード**] ボタンがあり、スクリプトログに簡単にアクセスできます。ボタンが淡色表示されている場合は、セントラルノードとスクリプトログのノード間の同期が完了していません。

ユーザー

ユーザーディレクトリからユーザーをインポートします。インポートすると、ユーザーアクセス権を管理できます。

- セキュリティルールエディタを使用し、ユーザーID と名前に基づいてルールを作成し、へのアクセス権を付与します。Qlik Sense
- QMC 管理者ロールを割り当てます。ロールは、セキュリティ規則のページで定義する必要があります。

*ストリームやデータ接続に関連するユーザーを編集できます。[**ストリーム**] 概要または [**データ接続**] 概要からストリームまたはデータ接続を選択し、[**関連するアイテム**] で [**ユーザーアクセス**] をクリックします。ユーザーを選択して、[**ユーザーを編集**] をクリックします。*

[**ユーザー**] 概要には、利用可能なユーザーがすべて一覧表示されます。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (▦) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

ユーザー

項目/ボタン	説明
名前	ユーザーの氏名。データマネージャーでテーブルの ⓘ to view user information in a separate window.
ユーザーディレクトリ	ユーザーと関連のあるディレクトリ。
[**ユーザーID**]	ユーザーに関連付けられているユーザーID。
[**管理者ロール**]	ユーザーに関連付けられている QMC 管理者ロール。
[**非アクティブ**]	ステータス値:**Yes** または **No**
[**ブロック**]	ステータス値:**Yes** または **No**

[**削除禁止**]	ステータス値:**Yes** または **No**
[**外部から削除**]	ステータス値:**Yes** または **No** [**Yes**] の場合、通常はユーザーがユーザー ディレクトリから削除されているためです。
タグ	ユーザーに紐付けされているタグ。
[**ID**]	ユーザーの ID。
[**作成日時**]	ユーザーが作成された日時。
[**最終変更日**]	ユーザーが最後に変更された日時。
[**変更者**]	ユーザーを最後に変更した者。
[***<カスタム プロパティ>***]	カスタム プロパティがある場合はここに一覧表示されます。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション[**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション[**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
[**編集**]	選択したユーザーを編集します。
[**削除**]	選択したユーザーを削除します。

詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

ユーザー: 関連するアイテム

次の関連アイテムはユーザーで利用できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

ユーザー アクセス

[**ユーザー アクセス**] は、リソースを編集する際に [**関連するアイテム**] から利用できます。

プレビューには、ターゲット リソースと選択したアイテムにアクセスできるソース ユーザーが表示されます。

権限に応じて、ユーザーやリソース、関連するルールを編集したり、表示することができます。

所有アイテム

[**所有アイテム**] はユーザーを編集する際に [**関連するアイテム**] から利用できます。概要には、選択したユーザーが所有しているリソースのリストが含まれています。

リソース

プロパティ	**説明**
[**名前**]	リソース名。
[**所有者**]	リソース所有者のユーザー ID。
[**タイプ**]	アプリやストリームといったリソースのタイプ。

概要で選択してアクション バーの [**Edit**] をクリックすると、所有アイテムの編集ページが表示されます。編集ページが同じ場合、複数の所有アイテムのみ同時に編集できます。

システム通知

システム通知の概要には、使用可能なシステム通知がすべてリストされています。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (▦) を使用して項目を追加できます。

システム通知およびシステム通知ポリシーの機能は、署名付きキーでライセンスが付与された Qlik Sense Enterprise on Windows インストールでのみ使用できます。ライセンスの詳細については、Qlik Sense ライセンスの資料。

システム通知

項目/ボタン	説明
タイトル	通知のタイトル。
メッセージ	通知のテキスト。
Application link (アプリケーション リンク)	Qlik Sense アプリへのリンク。
User groups (ユーザー グループ)	システム通知を受け取るユーザー グループのリスト。
ユーザー	システム通知を受け取るユーザーのリスト。
Last triggered (最終トリガー日)	通知の配布が最後にトリガーされた日時。トリガーされたことがない場合は、通知は表示されません。
ID	システム通知の ID。
作成日時	通知が作成された日時。
最終変更日	通知が最後に変更された日時。
変更者	通知の変更者。
[**カスタム プロパティ**]	カスタム プロパティがある場合はここに一覧表示されます。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*

アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション[**Select all rows**]は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション[**Deselect all rows**]はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
編集	選択された通知を編集します。
削除	選択された通知を削除します。
トリガー	通知の配布をトリガーします。
[新規作成]	新しいシステム通知を作成します。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**]をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

参照先:

システム通知の作成 (page 367)

システム通知の編集 (page 368)

システム通知の削除 (page 369)

システム通知ポリシー

システム通知ポリシーの概要には、使用可能なシステム通知ポリシーがすべてリストされています。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター ( ) を使用して項目を追加できます。

システム通知およびシステム通知ポリシーの機能は、署名付きキーでライセンスが付与された Qlik Sense Enterprise on Windows インストールでのみ使用できます。ライセンスの詳細については、Qlik Sense ライセンスの資料。

システム通知ポリシー

項目/ボタン	説明
名前	ポリシーの名前。
説明	システム通知ポリシーの説明。
リソース フィルター	ルールが適用されるリソースのタイプ。アスタリスク (*) は、ルールがリソースすべてに適用されることを示します。
アクション	[**Notify**] (通知する) を選択して通知を配布します。[**Notify**] (通知する) を選択しなかった場合、通知は表示されません。
無効化	ステータス値:**Yes** または **No**
タイプ	[**既定**] または [**カスタム**]。
タグ	通知に接続されているタグ。
[**カスタム プロパティ**]	カスタム プロパティがある場合はここに一覧表示されます。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
編集	選択した通知ポリシーを編集します。

削除	選択した通知ポリシーを削除します。
[新規作成]	新しいシステム通知ポリシーを作成します。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、**[Show more (詳細を表示)]** をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

参照先:

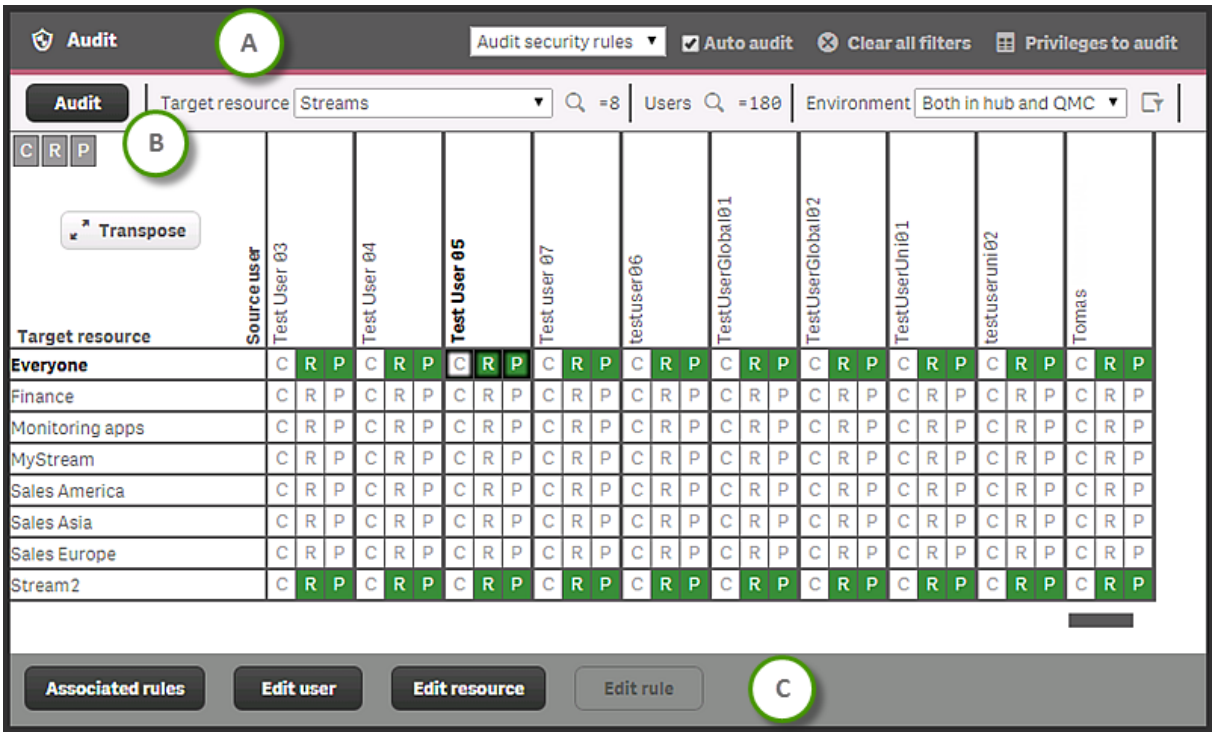
システム通知ポリシーの作成 (page 371)

システム通知ポリシーの編集 (page 373)

システム通知ポリシーの削除 (page 374)

監査

QMC 監査ページで、リソースとユーザーのクエリや、Qlik Sense システムで定義されたセキュリティルールや負荷分散ルール、ライセンスルールの監査を行うことができます。



*[**ストリーム**] に関するクエリを含む監査ページ。上に見出しバー(A) と監査バー(B)、下に操作バー(C) があります。*

監査ページ見出しバーのオプション

- [**セキュリティルールの監査**] ドロップダウン リスト: 監査するルール (セキュリティルール、負荷分散ルール、ライセンス ルール) を選択します。
- [**自動監査**]: これを選択すると、リソースまたはユーザー、ルールの編集ページで適用されたすべての変更が監査テーブルに自動的に反映されます。また、編集中にセキュリティルールを開くと、リソース タイプを抽出できる場合には自動的にプレビューが生成されます。
- [**すべてのフィルタを消去**]: リソースの選択とユーザー検索クエリをクリアします。グリッドを更新するには、[**監査**] をクリックする必要があります。
- [**監査の権限**]: セキュリティルール監査では、監査に適用される複数の異なる権限を選択できます。どの権限が特定の監査で利用可能かは、選択したリソースにより異なります。データ マネージャーでテーブルの↩をクリックして、既定の権限にリセットします。

権限アクションの監査

アクション	説明
C:作成	リソースの作成
R:読み取り	リソースの読み込み
U:更新プログラム	リソースの更新
D:削除	リソースの削除
E:エクスポート	アプリのエクスポート
A:データのエクスポート	アプリデータのエクスポート
T:複製	アプリの複製
M:オフラインでアクセス	オフラインでアプリにアクセス
P:公開	リソースをストリームに公開
O:所有者の変更	リソースの所有者の変更
B:負荷分散	アプリの負荷分散が行われるノードの管理
L:Allow access (アクセスの許可)	リソースへのログイン アクセス
V:承認	アプリシートのプロモーションの承認

監査ページ監査バーのオプション

- [**監査**]: ターゲット リソースおよびユーザー、環境を選択した場合、[**監査**] をクリックします。
- [**ターゲット リソース**]: 監査するリソースを選択します。リソースには次のものが含まれます。
  - 分析接続
  - アプリ
  - コンテンツ ライブラリ
  - データ接続
  - アプリ オブジェクト
  - ストリーム

- タスクのリロード
- ユーザー同期タスク
- ユーザー
- セキュリティルール
- 拡張機能
- ユーザーディレクトリコネクタ
- ノード
- ログインアクセス(ライセンスルールの監査のみ)

ライセンスルールの監査は、ログインアクセスに対し常に有効になっています。

- **ユーザー**: [🔍] をクリックし、検索を使用してユーザーのセットを減らします。多数のユーザーやリソースの監査を行う場合には、サーバーの処理量が増えるため、時間がかかります。
  詳細については、*QMC での検索とフィルタリング (page 25)* を参照してください。
- **環境**: 監査のコンテキストを選択します。
  : ユーザー環境をシミュレートします。
  オペレーティング システムやブラウザ、IP アドレスを設定して、ユーザー環境をシミュレートします。利用可能な設定は、システムの設定や、どのブラウザのヘッダーを利用可能かにより異なります。

```
OS=Windows;
IP=10.88.3.35;
ブラウザ = Firefox;
```

監査ページ操作バーのオプション

- [**関連ルール**]: クリックすると、ユーザー/ターゲットの組み合わせにアクセスするセキュリティルールが表示されます。
- [**ユーザーを編集**]: クリックして選択したユーザーを編集します。
- [**リソースを編集**]: クリックして選択したリソースを編集します。
- [**ルールを編集**]: クリックして選択したルールを編集します。(関連するルールが選択されている場合のみ)
- [**詳細を表示**]: ユーザーおよび/またはリソースのフィルタリングが行われていない場合、監査結果が 1000 件を超えると表示されます。[**ターゲット リソース**] と [**ユーザー**] の両方がフィルタリングされている場合、すべての監査結果が表示されます。

> *編集権限がない場合は、[**ユーザーを編集**] および [**リソースを編集**] ボタンの代わりに [**ユーザーを表示**] および [**リソースを表示**] ボタンが表示されます。*

監査

> *読み取りアクセス権があるユーザーとリソース、ルールのみが表示されます。*

[**監査**] をクリックすると、監査テーブルが表示されます。[**行列の入れ替え**] をクリックして、テーブルを回転させることができます。

緑および黄、赤、青色のセルには、次のようなルールがあります。

- 緑色: ルールは有効で使用中です。
- 黄色: ルールは有効ですが使用されていません。
- 赤色: ルールは無効です。
- 青色: ルールはプレビュー表示されています。
- 淡色表示の値: パフォーマンス上の理由から、監査結果が完全に取得されていません。詳しい情報については、[**詳細を表示**] をクリックしてください。

セルを選択し、[**関連ルール**] をクリックしてルールの詳細を表示します。ユーザーやリソースを編集するためのボタンもあります。

セキュリティルール、負荷分散ルール、またはライセンスルールの編集

監査を完了したら、セルをクリックして関連するルール (編集可能) を表示するか、ユーザーまたはリソース、ルールを編集します。編集の際、監査ページの左側に編集パネルが表示されます。この編集パネルには、編集しているアイテムの全プロパティが記載されています。

セキュリティルールの編集 (page 594)、*負荷分散ルールを編集する (page 514)*、および *ライセンスルールの編集 (page 333)*

セキュリティルール

Qlik Sense システムには、属性ベースのセキュリティルール エンジンが組み込まれており、このエンジンでは、ルールを数式として使用して、ユーザーに付与するリソースに対するアクセス権のタイプを評価します。

[**セキュリティルール**] の概要には、利用可能なセキュリティルールがすべて一覧表示されます。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター ( ) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

セキュリティルールの概要

項目/ボタン	**説明**
名前	ルール名。生成されたルールの名前の構文は、[resource type]_ [access type]_ [resource name] となっています。
[**説明**]	ルールの説明。
[**リソース フィルター**]	規則が適用されるリソースのタイプ。アスタリスク ([*****]) は、規則がリソースすべてに適用することを示しています。 生成されたルール、リソースの列には、ルールの ID が含まれています。
[**無効化**]	ステータス値:**Yes** または **No**
[**コンテキスト**]	ルールの対象が、**QMC** か [**ハブ**]、またはその [**両方**] かどうかを表示します。
[**タイプ**]	[**読み取り専用**]、[**既定**]、[**カスタム**]。

タグ	ルールに紐付けされているタグ。
[**条件**]	セキュリティルールの条件を表示します。
[**ID**]	セキュリティルール の ID。
[**作成日時**]	セキュリティルールが作成された日時。
[**最終変更日**]	セキュリティルールが最後に変更された日時。
[**変更者**]	セキュリティルールを最後に変更した者。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
[**アクション**]	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション[**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション[**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
[**編集**]	選択したセキュリティルールを編集します。
[**削除**]	選択したセキュリティルールを削除します。
[**新規作成**]	新しいセキュリティルールを作成します。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

リソースが削除されると、そのリソースに関連付けられている負荷分散ルールとセキュリティルールはすべて自動的に削除されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl]キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

アクション (基本ビュー)

ユーザーがリソースに対して実行できるアクションを選択します。最低 1 つのアクションを指定する必要があります。

アクセス ルールの説明

アクション	説明
Create	リソースを作成します。
Read	リソースを読み取ります。
Update	リソースを更新します。
Delete	リソースを削除します。
Export	Qlik Sense Enterpriseからqvfファイルにアプリをエクスポートします。
Duplicate	アプリの複製。
Publish	リソースをストリームに公開します。
Approve	アプリに属するオブジェクトを承認します。
Change owner	リソースの所有者を変更します。
Change role	ユーザー ロールを変更します。

アクション	説明
Export data	オブジェクトからデータをエクスポートします。これには、次のアクションが含まれます。 • ビジュアライゼーションの「画像としてエクスポート」。 • ビジュアライゼーションの「PDF としてエクスポート」。 • ビジュアライゼーションの「データのエクスポート」。 • メニューの「シートのエクスポート」。 • ストーリーテリングの「ストーリーのエクスポート」。 *これらのアクションのサブセットのみにアクセス権を付与することはできません。* *匿名ユーザーがデータをエクスポートできるようにするには、セキュリティルール ExportAppData のコピーを作成し、そのコピーを変更して、`resource.HasPrivilege("read")` のみを[**条件**]に含めるようにします。「Qlik Sense に含まれるセキュリティルール (page 540)」を参照してください。*
Access offline	アプリにオフラインでアクセスします。

条件 (詳細ビュー)

ルールを適用すべきリソースやユーザー条件を定義します。

構文

```
resource.resourcetype = <resourcetypevalue> [OPERATOR resource.<property> =
<propertyvalue> [OPERATOR resource.<property> = <propertyvalue> ...]]
```

シンプルな条件は、最初の部分の `resource.resourcetype = <resourcetypevalue>` のみで構成されます。上記の例にある後続の演算子、プロパティ、およびプロパティ値は省略可能です。

[**基本**] ビューのドロップダウン リストからリソースおよびリソース条件を選択すると、[**詳細**] ビューの [**Conditions (条件)**] 項目には、選択したリソース タイプに対応するコードが自動的に入力されます。

条件は、プロパティ値のペアを使用して定義されます。リソースやユーザー条件を指定する必要はありません。実際、[**条件**] 項目は空欄のままにしておくことができます。

条件を定義する順序は関係ありません。リソースを最初に定義してからユーザーやリソース条件を定義したり、その逆の順序で定義したりできます。ただし、リソースと条件を定義する順序は一貫させるようお勧めします。トラブルシューティングが容易になります。

複数の条件を使用すると、[**Group**] をクリックして 2 つの条件をグループ化できます。条件のグループ化後、[**Ungroup**] をクリックして、グループ化を解除できます。 この他に、サブグループ化オプションには [**Split**] および [**Join**] があります。条件間の既定の演算子は、OR です。これは、演算子のドロップダウン リストで変更できます。AND が OR より上位になるように、条件をグループ化します。

[**基本**] セクションと[**詳細**] セクションの間での同期 (いわゆるバックトラッキング) を有効にするには、[**基本**] セクションで作成された条件にかっこを追加します。同様に、[**基本**] セクションでリソースを追加すると、[**Conditions (条件)**] テキストフィールドに、条件が空欄のユーザー定義が自動的に設定されます。ただし、[**詳細**] セクションのみでルールを作成し、バックトラッキングの必要がなければ、上記の方法に従う必要はありません。

引数

引数の説明

引数	説明
resource	条件がリソースに適用されることを示唆します。
resourcetype	条件が [**resourcetypevalue**] で定義されたタイプのリソースに適用されることを示唆します。 また、プロパティ値を返す条件に対してあらかじめ定義された関数を使用することもできます。
resourcetypevalue	使用される演算子に応じて (=、!=、または like)、一致または不一致を検索するために条件で使用される値です。少なくとも 1 つのリソース タイプを指定してください。
property	リソース条件のプロパティ名。使用可能な名前については、*プロパティ(page 79)* を参照してください。
propertyvalue	選択されたプロパティ名の値。
user	条件がユーザーに適用されることを示唆します。

プロパティ

次のプロパティグループを使用できます。

基本設定

基本プロパティの説明と例

プロパティ	説明	例
resource.@<customproperty>	リソースに関連付けられているカスタム プロパティ。この例では、@Department はカスタム プロパティ名です。	`resource.@Department = Finance`。 `resource.@Department = user.userDirectory`
resource.name	リソース名。	`resource.name like "*US*"`。「US」を含む文字列が条件に一致します。
resource.id	リソースの ID。	`resource.id=5dd0dc16-96fd-4bd0-9a84-62721f0db427`。この場合のリソースはアプリです。

リソース ユーザーとオブジェクトの所有者

リソース ユーザーとオブジェクトの所有者 のプロパティ

プロパティ	説明	例
user.email owner.email	ユーザーの メール。 所有者の メール。	`user.email="user@domain.com"` `owner.email="owner@domain.com"`
user.environment.browser	ブラウザのセッション ベースの属性。「=」ではなく「like」演算子を使用します。ブラウザ データは、「Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0」のように、バージョンとその他の詳細を含む形式で送信されるためです。代わりに「=」演算子を使用することはできますが、その場合は値全体を指定する必要があります。	`user.environment.browser like "*Firefox*"`
user.environment.context	コンテキストのセッション ベースの属性。(QMC にはコンテキスト用の個別の設定があります)。	`user.environment.context="Management Access"`
user.environment.device	デバイスのセッション ベースの属性。	`user.environment.device="iPhone"`
user.environment.ip	IP アドレスのセッション ベースの属性。	*セキュリティルールの例: IP アドレス別のストリーム アクセス権 (page 613)*
user.environment.os	オペレーティング システムのセッション ベースの属性。	`user.environment.os like "Windows*"`
user.environment.secureRequest	secureRequest のセッション ベースの属性。値 true - SSL が使用される場合。それ以外の場合は false。	`user.environment.secureRequest="true"`
user.environment.[SAML attribute]	認証時に入力されたセッションベースの属性 (user.environment.group など)。	`user.environment.xxx="<attribute name>"`

プロパティ	説明	例
user.environment.[ticket attribute]	認証時に入力されたセッションベースの属性 (user.environment.group など)。	`user.environment.xxx="<attribute name>"`
user.environment.[session attribute]	認証時に入力されたセッションベースの属性 (user.environment.group など)。	`user.environment.xxx="<attribute name>"`

user.group
owner.group
	ユーザーが属するグループ。
	所有者が属するグループ。
		`user.group=resource.app.stream.@AdminGroup`
		
		`owner.group=@Developers`

user.userdirectory
owner.userdirectory
	ユーザーが属するユーザーディレクトリ。
	所有者が属するユーザーディレクトリ。
		`user.userdirectory="Employees"`
		
		`owner.userdirectory="Employees"`

user.userId
owner.userId
	ユーザーの ID。
	所有者の ID。
		`user.userId="<userID>"`
		
		`owner.userId="<ownerID>"`

user.roles
owner.roles
	ユーザーのロール。
	所有者のロール。
		`user.roles="AuditAdmin"`
		
		`owner.roles="SystemAdmin"`

*user.environment 条件を使用するには、仮想プロキシ内の [**仮想セキュリティ環境**] を有効にする必要があります。*

参照先: 仮想プロキシ (page 157)

リソース アプリ

リソース アプリのプロパティ

プロパティ	説明	例
stream.name	アプリの公開先のストリームの名前。	`stream.name="Finance"`

app.object リソース

app.object リソースのプロパティ

プロパティ	説明	例
app.stream.name	アプリオブジェクトの公開先のストリームの名前。	`app.stream.name="Test"`

プロパティ	説明	例
app.name	オブジェクトが属するアプリの名前。	`app.name="Q3_Report"`
approved	そのオブジェクトが、アプリの公開時のオリジナルアプリの一部であったかどうかを示すインジケーター。値: true または false。	`resource.approved="true"`
description	オブジェクトの説明。	`resource.description="old"`
objectType	考えられる値: • app_appscript • bookmark • dimension • embeddedsnapshot • genericvariableentry • hiddenbookmark • loadmodel • masterobject • measure • odagapplink • sheet • snapshot • story	`resource.objectType="sheet"`
published	オブジェクトが公開されているかどうかを示すインジケーター。値: true または false。	`resource.published="false"`

app.content や reloadtask などのアプリ関連のリソース

app.content や reloadtask などのアプリ関連リソースのプロパティ

プロパティ	説明	例
app.stream.name	アプリの公開先のストリームの名前。	`app.stream.name="Test"`
app.name	アプリの名前。	`app.name="Q3_Report"`

リソース DataConnection

リソース DataConnection のプロパティ

プロパティ	説明	例
Type	データ接続のタイプ。 考えられる値: • OLEDB • ODBC • フォルダ • Internet • カスタム (すべてのカスタム コネクター向け)	`resource.type!="folder"`

SystemRule リソース

SystemRule リソースのプロパティ

プロパティ	説明	例
Category	システム ルール カテゴリ。 考えられる値: • セキュリティ • ライセンス • 同期	`resource.category="license"`
ResourceFilter	ルールのリソース フィルター。	`resource.resourcefilter matches "DataConnection_\w{8}-\w{4}-\w{4}-\w{4}-\w{12}"`
RuleContext	ルールのコンテキスト。 考えられる値: • BothQlikSenseAndQMC • QlikSenseOnly • QMCOnly	`resource.rulecontext="BothQlikSenseAndQMC"`
Type	ルールのタイプ。 考えられる値: • 初期設定 • Read only (読み取り専用) • Custom (カスタム)	`resource.type!="custom"`

ContentLibrary リソース

ContentLibrary リソースのプロパティ

プロパティ	説明	例
Type	考えられる値: • media	resource.type="media"

ServerNodeConfiguration リソース

ServerNodeConfiguration リソースのプロパティ

プロパティ	説明	例
IsCentral	セントラル ノードのインジケーター。値: true または false。	resource.iscentral="true"
nodePurpose	ノードの目的。development または production。	resource.nodepurpose="production"

UserDirectory リソース

UserDirectory リソースのプロパティ

プロパティ	説明	例
userDirectoryName	ユーザー ディレクトリの名前。	resource.userDirectoryname="Employees"

UserSyncTask リソース

UserSyncTask リソースのプロパティ

プロパティ	説明	例
userDirectory.name	ユーザー ディレクトリ コネクタの名前。	resource.userDirectory.name="Employees"
userDirectory.userDirectoryName	ユーザー ディレクトリの名前。	userDirectory.userdirectoryname="Employees"

Widget リソース

Widget リソースのプロパティ

プロパティ	説明	例
library.name	そのウィジェットが属するライブラリの名前。	resource.library.name="Dev"

OS やブラウザのタイプなど外部コールから受け取った環境データは、Qlik Sense システムによって安全を確保されません。

例と結果

リソース フィルターの例と結果

例	結果
Resource filter: App* **Conditions:**resource.resourcetype="App" and (resource.name like "*")	このルールはすべてのアプリに適用されます。 *[リソース] 項目を「App*」に設定し、[条件] 項目を空にしておくだけで同じルールを定義できます。*
リソース フィルター: App*、App.Object*、または Stream* **条件:**resource.resourcetype="App" or resource.resourcetype="Stream" or (resource.resourcetype="App.Object" and resource.objectType="sheet") and resource.name like "My*"	このルールは、名前が「My」で始まっているすべてのアプリ、ストリーム、シートに適用されます。
resource.resourcetype="ServerNodeConfiguration" and (resource.@Department="Finance")	このルールはカスタム プロパティ「Department」が「Finance」に設定されているすべてのノードに適用されます。
resource.resourcetype="ServerNodeConfiguration" and !(resource.@Department="Finance")	このルールはカスタム プロパティの「Department」が「Finance」に設定されているノード以外のすべてのノードに適用されます。
[**リソース フィルター**]= resource.resourcetype="App.Object" and (((resource.objectType="sheet" or resource.objectType="story")) and ((user.name="Myname")))	このルールは、「MyName」という名前のアプリ、シート、ストーリー、ユーザーすべてに適用されます。
[**リソース フィルター**]=Stream_* user.@Department="Finance" and !user.IsAnonymous()	このルールは、ユーザーが匿名としてログインしていない場合、カスタム プロパティの「Department」が「Finance」に設定されているストリームとユーザーすべてに適用されます。
[**リソース フィルター**]=* and Conditions field empty	このルールは、あらゆるリソースとユーザーに適用されます。

例	結果
user.name="MyUserName"	このルールは、ユーザー名が「MyUserName」のユーザーに適用されます。 *個人に適用されるルールはなるべく作成しないようにしてください。ユーザーグループのメンバーシップ、ユーザーのロール、またはカスタムプロパティを使用して、ルールをユーザーのグループに適用します。*
user.group="DL-MyDepartment"	このルールは、「MyDepartment」分布グループのあらゆるメンバーに適用されます。
user.@Department="Sales"	このルールは、カスタムプロパティ「@Department」が「Sales」に設定されているユーザー全員に適用されます。
user.roles="Developer"	リソース、条件、アクションフィールドで定義されているアクセス権は、ユーザーロール「Developer」に適用されます。ユーザー編集ページの [Roles (ロール)] ドロップダウンリストでこのロールを利用できるようになります。
resource.resourcetype="App" and resource.name="My*" and user.role="QlikSenseAdmin"	user.role を演算子と併用して、ユーザーに特定のユーザーロールがある場合にルールを適用するよう指定することもできます。
user.environment.os="Windows"	このルールは、オペレーティングシステムが Windows の場合、その外部環境すべてに適用されます。

リソース フィルタ(詳細 ビュー)

セキュリティルールが適用される、リソースのタイプの必須定義。

構文

```
resourcetype1[*][_*][, resourcetype2[*][_*], ...]
```

[**ID**] セクションの [**テンプレート リストからルールを作成する**] でリソースを選択すると、[**基本**] の [**リソース フィルター**] 項目に選択したリソースが自動的に取り込まれます。デフォルトで、オプションのアンダースコアとアスタリスク ('**_***') が追加されます。[**基本**] セクションのルールウィザード ドロップダウン リストでの選択項目は、[**詳細**] の [**条件**] ボックスに自動的に追加されます。

引数

引数

引数	説明
resourcetype1	必須。少なくとも 1 つのリソース タイプ名を指定してください。
*	オプションのワイルドカード。これが含まれている場合、指定されたテキストで始まるリソースのタイプすべてにルールが適用されます。たとえば、**「App*」**であれば、**"App"** で始まるすべてのリソース タイプ、つまり、**App** と**App.Object** といったタイプのリソースすべてにルールが適用されます。 これが省略されている場合、セキュリティルールは リソース フィールドで指定された正確な名前のリソース タイプに適用されます。ルールが機能するには、GUID、または GUID のテンプレートを提供する必要があります。 **「_*」**オプションと併用することはできません。
_*	オプションのワイルドカード。これが含まれている場合、指定されたタイプのリソースすべてにルールが適用されます。たとえば、**「App_*」**の場合、すべてのアプリにルールが適用されます。同様に**「App.Object_*」**であれば、ルールはすべてのアプリオブジェクトに適用されます。 これが省略されている場合、セキュリティルールは リソース フィールドで指定された正確な名前のリソース タイプに適用されます。ルールが機能するには、GUID、または GUID のテンプレートを提供する必要があります。 **'*'** オプションとともに使用することはできません。

プロパティ

セキュリティルールのプロパティ

プロパティ	セキュリティ規則が適用されます
App	アプリ
App.Object	オブジェクト シート、ストーリー、ブックマーク、メジャー、軸など、オブジェクトのオブジェクト タイプ。
ContentLibrary	コンテンツ ライブラリ
DataConnection	データ接続
Extension	拡張機能
ReloadTask	タスクのリロード
ServerNodeConfiguration	Qlik Sense ノードの構成
Stream	ストリーム
SystemRule	セキュリティルール

プロパティ	セキュリティ規則が適用されます
User	ユーザー
UserDirectory	ユーザー ディレクトリ コネクタ
UserSyncTask	ユーザー同期タスク

例と結果

例と結果

例	結果
`App*`	ルールはアプリとアプリオブジェクトに適用されます。
`App_*`	ルールはアプリのみに適用されます。
`App*, Streams*, App.Object* resource.resourcetype="App.Object" and (((resource.objectType="sheet")))`	ルールはアプリ、ストリーム、シートに適用されます。 *この例では「AppSheet* ... 」を除外できます。「App* 」でアプリとシートの双方にルールが適用されるためです。*
`Stream_88ee46c6-5e9a-41a7-a66a-f5d8995454ec`	ルールは、GUID が指定されているストリームに適用されます。
`Stream_\w{8}-\w{4}-\w{4}-\w{4}-\w{12}`	ルールは既存のストリームすべてに適用されます。
[**アプリ**] を [**リソース**] ドロップダウン リストから選択します。	以下のテキストが詳細ビューに表示されます。 **Resource (リソース)***`App*` **Conditions (条件)***`resource.resourcetype="App" and ( )` *かっこ内にリソースまたはユーザー条件を入力しなければ、デフォルトでセキュリティルールはすべてのアプリとユーザーに適用されます。*

カスタム プロパティ

カスタム プロパティを作成して、セキュリティルールに自分自身の値を使用できるようにします。カスタム プロパティに 1 つまたは複数の値を定義して、リソースのセキュリティルールで使用します。

カスタム プロパティの QMC チェックは、20 秒毎に変更されます。
[**カスタム プロパティ**] 概要には、利用可能なカスタム プロパティがすべて一覧表示されます。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター ( ) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

カスタム プロパティ

プロパティ名	説明
名前	QMC で定義されたカスタム プロパティの名前です。
説明	ルールの説明。オプション。
リソース タイプ	カスタム プロパティを利用できるリソースの種類です。
ID	カスタム プロパティの ID です。
作成日時	カスタム プロパティが作成された日時。
最終変更日	カスタム プロパティが最後に変更された日時。
変更者	カスタム プロパティを最後に変更した者。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
編集	選択したカスタム プロパティを編集します。
削除	選択したカスタム プロパティを削除します。
新規作成	新しいカスタム プロパティを作成します。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

ライセンス管理

ライセンス モデルには、シリアル番号とコントロール ナンバー、および署名付きのライセンス キーの 2 つがあります。これらのモデルで、ライセンスの契約条件およびユーザーに割り当て可能なアクセス タイプを定義します。ユーザーの割り当て、分析時間消費および製品のアクティベーションには、クラウドベースのライセンス バックエンドにアクセスするために、署名済みのライセンス キーとともにインターネット アクセス (直接またはプロキシ経由) が必要となります。

主なライセンス タイプには、アクセス タイプに基づくものと、トークンに基づくものの 2 つがあります。

- アクセス タイプのライセンスは、Professional User とAnalyzer User ライセンス (ユーザーベース) および Analyzer Capacity ライセンス (キャパシティベース) です。Professional User および Analyzer User ライセンスは、Professional アクセスおよび Analyzer アクセスを割り当てることができます。Analyzer Capacity ライセンスでは、Analyzer Capacity ライセンスを割り当てることができます。ここでは消費が時間ベース (Analyzer タイム) となっています。
- Qlik Sense Token ライセンスでは、トークンを使用してアクセス パスをユーザーに割り当てます。User アクセスおよび Login アクセスを割り当てることができます。

アクセス タイプを使うと、ユーザーは Qlik Sense Enterprise on Windows サイト内のハブとアプリにアクセスできます。

Qlik Sense Enterprise SaaS をセットアップする場合は、Qlik 代理店または Qlik サポートに連絡してセットアップのための有効なライセンスを入力してください。

- [**ライセンス使用の概要**] ページには、さまざまなアクセス タイプの分布が表示されます。
- [**プロフェッショナル アクセスの割り当て**] ページには概要が表示され、ユーザーへのプロフェッショナル アクセス権の割り当て、割り当て解除、回復が可能です。
- [**プロフェッショナル アクセス ルール**] ページには概要が表示され、プロフェッショナル アクセス ルールの編集、削除、新規作成が可能です。プロフェッショナル アクセスを自動的に割り当てるために、プロフェッショナル アクセス ルールが使用されます。
- [**アナライザー アクセスの割り当て**] ページには概要が表示され、ユーザーへのアナライザー アクセス権の割り当て、割り当て解除、回復が可能です。
- [**アナライザー アクセス ルール**] ページには概要が表示され、アナライザー アクセス ルールの編集、削除、新規作成が可能です。アナライザー アクセスを自動的に割り当てるために、アナライザー アクセス ルールが使用されます。
- [**Analyzer Capacity ルール**] ページには概要が表示され、Analyzer Capacity ルールの編集、削除、新規作成が可能です。Analyzer Capacity アクセスを自動的に割り当てるために、Analyzer Capacity ルールが使用されます。
- [**ユーザー アクセスの割り当て**] ページには概要が表示され、ユーザーへのユーザー アクセス権の割り当て、割り当て解除、回復が可能です。

- [**ユーザー アクセス ルール**] ページには概要が表示され、ユーザー アクセス ルールの編集、削除、新規作成が可能です。ユーザー アクセスを自動的に割り当てるために、ユーザー アクセス ルールが使用されます。
- [**ログイン アクセス ルール**] ページには概要が表示され、ログイン アクセス ルールの編集、削除、新規作成が可能です。
- [**サイト ライセンス**] ページでは、LEF をアクティブ化するか、変更を適用します。

プロフェッショナル アクセスの割り当て

識別されたユーザーに Professional アクセス権を割り当て、Qlik Sense サイト内のストリームとアプリにアクセスできるようにします。プロフェッショナル アクセスは、Qlik Sense インストールのすべての機能にアクセスする必要があるユーザーが対象です。プロフェッショナル アクセス権のあるユーザーは、シートまたはアプリを作成、編集、公開でき、Qlik Sense サイトの管理などの使用可能な機能をすべて使うことができます。

シルアル番号とコントロール ナンバーでライセンスが付与された Qlik Sense インストールでは、ユーザーから Professional アクセスの割り当てを削除すると、アクセス権が直近 7 日間で使用されていた場合、そのアクセス タイプは検疫のため隔離されます。直近 7 日間で使用されていない場合、プロフェッショナル アクセス権は直ちに解放されます。7 日以内であれば、同一のユーザーに検疫状態のプロフェッショナル アクセス権を復元することができます。

検疫は、署名済みライセンス キーでライセンス付与されている Qlik Sense のインストールでは強制されません。

このアクセス パスのタイプでは、単一ユーザーが行える並列ユーザー接続の最大数は、5 回です。署名付きライセンス キーでライセンスを使用する場合、QMC にアクセスすると、並列セッションの最大数がカウントされて追加され、5 つとなります。セッションの不必要な消費を避けるには、ルート管理者にどのタイプのアクセスも割り当てないでください。

最大数の並列ユーザー接続を持つユーザーが接続を終了する (たとえば、ログアウト) 場合、別の接続を追加する (たとえば、ログイン) には、アクセス パスが使用可能になる前に 5 分が経過する必要があります。

詳しくは「**ステータス**」の内容をお読みください。

[**プロフェッショナル アクセスの割り当て**] 概要には、プロフェッショナル アクセスを持つすべてのユーザーがリストに表示されています。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (⊞) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

プロフェッショナル アクセスの割り当てのプロパティ

項目	詳細
名前	割り当て済み (あるいは検疫済みの) プロフェッショナル アクセスがあるユーザーの名前。 [**削除されたユーザー**] は、ユーザーが削除され、検疫中になると表示されます。検疫期間が終了すると、削除されたユーザーは概要から削除されます。

項目	詳細
ユーザー ディレクトリ	ユーザーのインポート元のユーザー ディレクトリ。
状態	プロフェッショナル アクセスの状態: [**割り当て済み**] は、特定のユーザーにプロフェッショナル アクセス権が割り当てられていて、そのユーザーがハブやアプリにアクセス可能であることを示しています。 [**検疫済み**] (シリアル番号付きライセンスの場合のみ) は以下を意味します。 • ユーザーはハブのストリームおよびアプリにアクセスできません。 • 以前、該当するユーザーにプロフェッショナル アクセスが割り当てられ、その後、割り当てが解除されました。 • 検疫期間中、元のユーザーはプロフェッショナル アクセス権を回復できます。 署名付きライセンス キーを使用しており、割り当ての数がライセンスで定義されている数より多くなると、**「除外済み」**と表示されます。この場合は、それらのユーザーは、割り当て数がライセンスで定義されている数と一致するまで、直近に割り当てらえたユーザーが除外されます。割り当て可能なアクセス権の数が増えた場合、または管理者が他のユーザーのアクセス権を削除した場合には、除外されたユーザーにアクセス権が再割り当てされます。除外は、例えばライセンスでの割り当て数が減った場合に発生することがあります。
最後の使用	ユーザーが最後にハブにアクセスした日時。 署名付きラインセンス キーでライセンスを使用する場合、QMC にアクセスすると、並列セッションの最大数がカウントされて追加され、5 つとなります。セッションの不必要な消費を避けるには、ルート管理者にどのタイプのアクセスも割り当てないでください。
ID	ユーザー アクセス権の ID。
作成日時	プロフェッショナル アクセス権が作成された日時。
最終変更日	プロフェッショナル アクセス権が最後に変更された日時。
変更者	プロフェッショナル アクセス権を変更した人物。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*

項目	詳細
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション[**Select all rows**]は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション[**Deselect all rows**]はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
割り当て解除	選択したユーザーからプロフェッショナル アクセス権の割り当てを解除します。
回復	検疫済みの場合、選択したユーザーへのプロフェッショナル アクセス権を回復します。
割り当て	特定のユーザーにプロフェッショナル アクセス権を割り当てます。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl]キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

プロフェッショナル アクセス ルール

プロフェッショナル アクセス ルールでは、ログイン時にプロフェッショナル アクセスを自動的に割り当てるユーザーを定義します。

[**プロフェッショナル アクセス ルール**] 概要には、プロフェッショナル アクセス ルールがすべてリストに表示されています。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター ( ) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

プロフェッショナル アクセス ルールの項目

項目	説明
名前	プロフェッショナル アクセス ルールの名前。
説明	プロフェッショナル アクセス ルールの説明。
リソース フィルター	プロフェッショナル アクセス ルールが適用されるリソースのタイプ。
無効化	ステータス値:**Yes** または **No**
タイプ	プロフェッショナル アクセス ルールのタイプ。
条件	ルールを適用するために満たす必要のあるリソース/ユーザーの定義。
コンテキスト	プロフェッショナル アクセス ルールが適用されるコンテキストを指定します。[**ハブ**]、[**QMC**]、または [**Both**] (両方) になります。
ID	プロフェッショナル アクセス ルールの ID。
作成日時	プロフェッショナル アクセス ルールが作成された日時。
最終変更日	プロフェッショナル アクセス ルールが最後に変更された日時。
変更者	プロフェッショナル アクセス ルールを変更した人物。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*

項目	説明
↻	ページを更新します。
編集	選択したプロフェッショナル アクセス ルールを編集します。
削除	選択したプロフェッショナル アクセス ルールを削除します。
⊕**新規作成**	新しいプロフェッショナル アクセス ルールを作成します。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

アナライザー アクセスの割り当て

識別されたユーザーに割り当てられた Analyzer アクセス権によって、ハブ内のストリームとアプリにアクセスできるようにします。アナライザー アクセスは、他のユーザーによって作成されたシートとアプリを使用するユーザーが対象です。アナライザー アクセス権を持つユーザーは、シートやアプリを作成、編集、または公開することはできませんが、アプリ内のデータに基づいて、ストーリー、ブックマーク、スナップショットを作成できます。また、ユーザーは、ブックマーク、印刷オブジェクト、ストーリー、シートを作成したり、オブジェクトから Excel にデータをエクスポートしたりすることもできます。

シルアル番号とコントロール ナンバーでライセンスが付与された Qlik Sense インストールでは、ユーザーから Analyzer アクセスの割り当てを削除すると、アクセス権が直近 7 日間で使用されていた場合、そのアクセス タイプは検疫のため隔離されます。直近 7 日間で使用されていない場合、アナライザー アクセス権は直ちに解放されます。7 日以内であれば、同一のユーザーに検疫状態のアナライザー アクセス権を復元することができます。

検疫は、署名済みライセンス キーでライセンス付与されている Qlik Sense のインストールでは強制されません。

このアクセス パスのタイプでは、単一ユーザーが行える並列ユーザー接続の最大数は、5 回です。最大数の並列ユーザー接続を持つユーザーが接続を終了する (たとえば、ログアウト) 場合、別の接続を追加する (たとえば、ログイン) には、アクセス パスが使用可能になる前に 5 分が経過する必要があります。

除外については、[**ステータス**] の内容をお読みください。

[**アナライザー アクセスの割り当て**] の概要には、アナライザー アクセスを有するユーザーがすべて一覧表示されています。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (▦) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

アナライザー アクセス割り当てのプロパティ

プロパティ	説明
名前	割り当て済み (あるいは検疫済みの) アナライザー アクセスがあるユーザーの名前。 [**削除されたユーザー**] は、ユーザーが削除され、検疫中になると表示されます。検疫期間が終了すると、削除されたユーザーは概要から削除されます。
ユーザー ディレクトリ	ユーザーのインポート元のユーザー ディレクトリ。
状態	アナライザー アクセスの状態: [**割り当て済み**] は、識別されたユーザーにアナライザー アクセス権が割り当てられていて、そのユーザーがハブやアプリにアクセスできることを示します。 [**検疫済み**] は、以下の状態を示します。 • ユーザーはハブのストリームおよびアプリにアクセスできません。 • 以前、該当するユーザーにアナライザー アクセス権が割り当てられ、その後、割り当てが解除されました。 • 検疫期間中、元のユーザーはアナライザー アクセス権を回復できます。 署名付きライセンス キーを使用しており、割り当ての数がライセンスで定義されている数より多くなると、**「除外済み」**と表示されます。この場合は、それらのユーザーは、割り当て数がライセンスで定義されている数と一致するまで、直近に割り当てらえたユーザーが除外されます。割り当て可能なアクセス権の数が増えた場合、または管理者が他のユーザーのアクセス権を削除した場合には、除外されたユーザーにアクセス権が再割り当てされます。除外は、例えばライセンスでの割り当て数が減った場合に発生することがあります。
最後の使用	ユーザーが最後にハブにアクセスした日時。
ID	ユーザー アクセス権の ID。
作成日時	アナライザー アクセス権が作成された日時。
最終変更日	アナライザー アクセス権が最後に変更された日時。
変更者	アナライザー アクセス権を最後に変更した者。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。

プロパティ	説明
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
割り当て解除	選択したユーザーからアナライザー アクセス権の割り当てを解除します。
回復	検疫済みの場合、選択したユーザーへのアナライザー アクセス権を回復します。
[割り当て]	識別されたユーザーに アナライザー アクセス権を割り当てます。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

アナライザー アクセス ルール

アナライザー アクセス ルールでは、ログイン時にアナライザー アクセスを自動的に割り当てるユーザーを定義します。

[**アナライザー アクセス ルール**] の概要には、アナライザー アクセス ルールのすべてが一覧表示されています。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター ( ) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

アナライザー アクセス ルールのプロパティ

プロパティ	説明
名前	アナライザー アクセス ルールの名前。
説明	アナライザー アクセス ルールの説明。
リソース フィルター	アナライザー アクセス ルールが適用されるリソースのタイプ。
無効化	ステータス値:**Yes** または **No**
タイプ	アナライザー アクセス ルールのタイプ。
条件	ルールを適用するために満たす必要のあるリソース/ユーザーの定義。
[**コンテキスト**]	ユーザー アクセス ルールが適用されるコンテキストを指定します。[Hub]、[QMC]、[Both] になります。[**ハブ**]、[**QMC**]、または [**Both**] (両方) になります。
ID	アナライザー アクセス ルールの ID。
作成日時	アナライザー アクセス ルールが作成された日時。
最終変更日	アナライザー アクセス ルールが最後に変更された日時。
変更者	アナライザー アクセス ルールを最後に変更した者。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。

プロパティ	説明
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
編集	選択したアナライザー アクセス ルールを編集します。
削除	選択したアナライザー アクセス ルールを削除します。
[新規作成]	新しいアナライザー アクセス ルールを作成します。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブル クリックすると、リソースの編集 ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

Analyzer Capacity ライセンス

アナライザー キャパシティは消費ベースのライセンス タイプで、使用可能な機能に関してアナライザー アクセスに似ています。ユーザーは、ハブ内のストリームとアプリにアクセスし、他のユーザーによって作成されたシートとアプリを消費できます。Analyzer Capacity アクセスでは、アプリ内のデータに基づいてストーリー、ブックマーク、スナップショットを作成することができます。シートまたはアプリの作成、編集、または公開はできません。

アナライザー キャパシティ ライセンスにより、アナライザー時間 (毎月の定義済み分数 (カレンダー日付)) に対してサブスクライブします。これらの分時間は、ユーザー間で共有され、匿名ユーザーを含むユーザー グループの一員になっている任意のユーザーが消費可能です。消費は 6 分単位で測定されます。新しい 6 分間ごとに、1 単位が消費されます。

Analyzer Capacity の消費

Analyzer Capacity の消費は、ユーザーとQlik Sense アプリ間にアクティビティが存在する場合に開始されます。アイドル時間 (アプリが表示されているかどうかに関係なく) に追加時間が消費されることはありません。

次のインタラクションは、ユーザーとQlik Sense 間のアクティビティ例です。

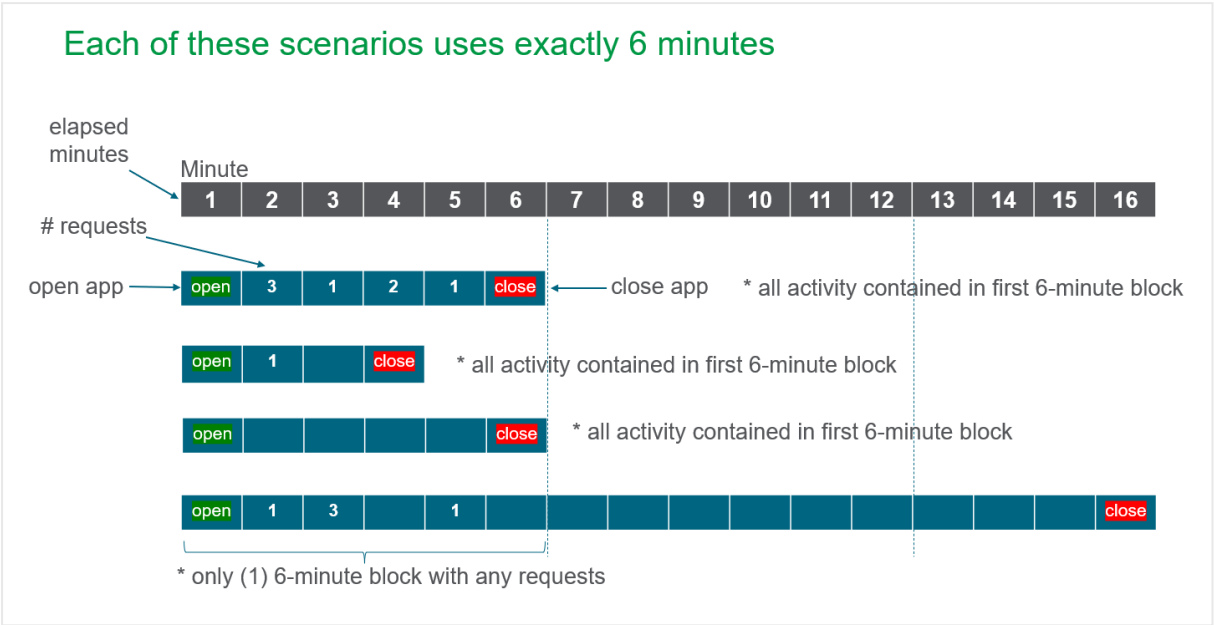
- アプリを開くとき。
- アプリで選択を行うとき。例えば、データ カタログ で Insight Advisor Chat またはデータプロファイリングを使用する場合。
- 新しいシートに移動するとき。
- アプリをリロードするとき、またはスケジュールされたリロードが発生するとき。

消費の 1 単位は 6 分です。6 分が経過し、アプリでなんからのユーザー アクティビティがあると、新しい 6 分の単位が消費されます。6 分間が経過してもアクティビティがない場合、アイドルとみなされ、単位数が消費されます。

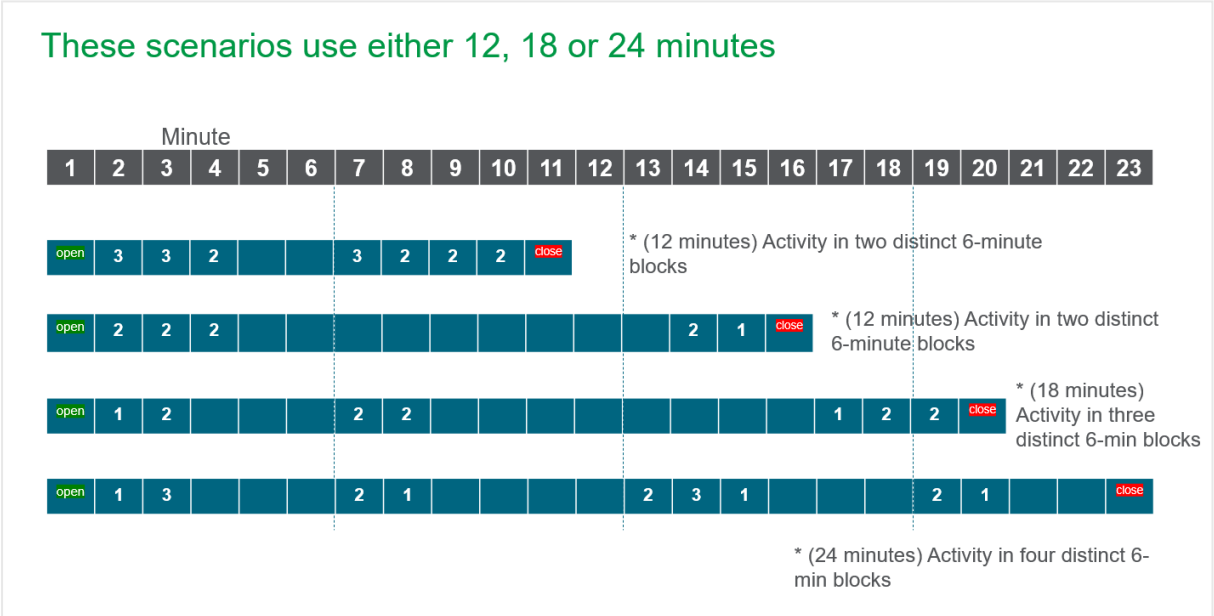
単位の消費はアクティブである限り続きます。26 分間アクティブであった場合は、5 単位 (30 分) が消費されます。Analyzer Capacity は、アラートが評価されるときなど、バックグラウンド サービスの実行時に消費される可能性があります。ただし、継続的なユニット消費がまだない場合は、ユーザーが接続しているapp でスケジュールされたリロードが発生すると、追加のユニットが消費されます。

次の図は、Analyzer Capacity がどのように測定されるか、そしていつ単位数が消費されるかを示しています。

1 単位を使用した Capacity 消費の図。



複数単位を使用した Capacity 消費の図。



主な違いは、Qlik Sense Enterprise Client-Managed と Qlik Sense Enterprise SaaS が Analyzer Capacity の使用状況を計算する方法にあります。Qlik Sense Enterprise Client-Managed では、Analyzer Capacity の使用状況に対する評価の一部に、デバイスの台数を使用します。Qlik Sense Enterprise SaaS では、Analyzer Capacity の使用状況に対する評価の一部に、開かれているアプリの数を使用します。計算方法の例のいくつかを次のテーブルに示します。

デバイスによって消費される単位

例 - アプリおよびデバイス	Qlik Sense Enterprise Client-Managed
Qlik Sense アプリケーション x 1 - デバイス x 1	1 単位
Qlik Sense アプリケーション x 2 - デバイス x 1	1 単位
Qlik Sense アプリケーション x 3 - デバイス x 2	2 単位
Qlik Sense アプリケーション x 5 - デバイス x 2	2 単位

デバイスは、ノートPC またはモバイル デバイスなど、個別のデバイスとして定義されます。これには、2 つ目のブラウザーが含まれる場合があります。

時間によって消費される単位

例 - アプリおよび時間	Qlik Sense Enterprise Client-Managed
Qlik Sense アプリケーション x 1 - アクティビティ 6 分間	1 単位
Qlik Sense アプリケーション x 1 - アクティビティ 14 分間	3 単位
Qlik Sense アプリケーション x 2 - アクティビティ 6 分間	1 単位
Qlik Sense アプリケーション x 2 - アクティビティ 14 分間	3 単位

Analyzer Capacity 超過分

該当月の Analyzer Capacity すべてが消費された場合、Analyzer Capacity を使用して Qlik Sense にアクセスしているユーザーは、アクセスを拒否されます。Analyzer Capacity の消費量は、月始めごとにリセットされます。

Analyzer Capacity 超過分によって、想定よりも多い使用量が原因でユーザーがロックアウトされないように、お客様が該当月の消費割り当て量を超えて消費できるようにします。Analyzer Capacity 超過分は、サブスクリプションに追加すると有効になります。既定では、Analyzer Capacity パックの数と超過分パックがマッチするようになっていますが、必要に応じて調整することができます。

Analyzer Capacity の消費の監視

Analyzer Capacity の消費を監視するには、いくつかの方法があります。

Qlik Sense Enterprise Client-Managed システムで、次を使用して Analyzer Capacity の消費を監視できます。

- Qlik Management Console の **License Management Usage Summary** (ライセンス管理使用状況の概要) タブ
- **License Monitor** アプリの **Usage Snapshot** タブ
- **License Monitor** アプリの **Unified License History** タブです。このタブを使用して、個別ユーザーの消費を表示します。

アナライザー キャパシティアクセスの概要

- アナライザー アクセスでも同じ機能を利用可能です。
- 匿名ユーザーを含むユーザー グループに割り当てられます。
- 定義された時間に対する毎月のサブスクリプション。

- 6 分ブロック内の消費。
- 余分の時間をサブスクリプションに追加可能。

Analyzer Capacity ルール

Analyzer Capacity ルールでは、ログイン時に Analyzer Capacity アクセスを自動的に割り当てるユーザーを定義します。

[**Analyzer Capacity ルール**] の概要には、Analyzer Capacity ルールのすべてが一覧表示されています。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター () を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

Analyzer Capacity ルール項目

プロパティ	説明
名前	Analyzer Capacity ルールの名前。
説明	Analyzer Capacity ルールの説明。
リソース フィルター	Analyzer Capacity ルールが適用されるリソースのタイプ。 *リソース フィルターの定義 (page 572)*
無効化	ステータス値:**Yes** または **No**
タイプ	Analyzer Capacity ルール タイプ。
条件	ルールを適用するために満たす必要のあるリソース/ユーザーの定義。
[**コンテキスト**]	ユーザー アクセス ルールが適用されるコンテキストを指定します。[Hub]、[QMC]、[Both] になります。[**ハブ**]、[**QMC**]、または [**Both**] (両方) になります。
ID	Analyzer Capacity ルール ID。
作成日時	Analyzer Capacity ルールが作成された日時。
最終変更日	Analyzer Capacity ルールが最後に変更された日時。
変更者	Analyzer Capacity ルールを最後に変更した者。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。

プロパティ	説明
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
編集	選択した Analyzer Capacity ルールを編集します。
削除	選択した Analyzer Capacity ルールを削除します。
[新規作成]	新しい Analyzer Capacity ルールを作成します。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

ユーザー アクセス割り当て

識別されたユーザーにユーザー アクセス権を割り当て、Qlik Sense サイト内のストリームおよびアプリにアクセスできるようにします。アクセス タイプ (ユーザー アクセス) とユーザーとは、直接的に関係していますユーザーからユーザー アクセスの割り当てを解除すると、アクセス権が直近 7 日間で使用されていなければ、そのアクセス タイプは検疫のため隔離されます。直近 7 日間で使用されていないユーザー アクセス権は削除され、トークンは直ちに解放されます。7 日以内であれば、同一のユーザーに検疫状態のユーザー アクセス権を回復させることができます。その場合、ユーザーには、追加のトークンを使用せずに、再びアクセス権が付与されます。

[**ユーザー アクセス割り当て**] の概要には、ユーザー アクセスを有するユーザーがすべて一覧表示されています。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター ( ) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

ユーザー アクセス割り当てのプロパティ

名前	割り当て済み (あるいは検疫済みの) ユーザー アクセスがあるユーザーの名前。 [**削除されたユーザー**] は、ユーザーが削除され、検疫中になると表示されます。検疫期間が終了すると、削除されたユーザーは概要から削除されます。
ユーザー ディレクトリ	ユーザーがインポートされたユーザー ディレクトリ。
[**状態**]	ユーザー アクセスの状態: [**割り当て済み**] は、特定のユーザーにユーザー アクセス権が割り当てられていて、そのユーザーがハブやアプリにアクセス可能であることを示しています。 [**検疫済み**] は、以下の状態を示します。 • ユーザーはハブのストリームおよびアプリにアクセスできません。 • 以前、該当するユーザーにユーザー アクセスが割り当てられ、その後、割り当てが解除されました。 • トークンは、検疫期間 (7 日間) が終了するまで、新しい割り当てに使用できません。 • 検疫期間中、元のユーザーはユーザー アクセス権を回復できます。
[**最後の使用**]	ユーザーが最後にハブにアクセスした日時。
[**ID**]	ユーザー アクセス権の ID。
[**作成日時**]	ユーザー アクセス権が作成された日時。
[**最終変更日**]	ユーザー アクセス権が最後に変更された日時。
[**変更者**]	ユーザー アクセス権を最後に変更した者。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*

[**アクション**]	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション[**Select all rows**]は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション[**Deselect all rows**]はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
[**割り当て解除**]	選択したユーザーからユーザー アクセス権の割り当てを解除します。
[**回復**]	検疫済みの場合、選択したユーザーへのユーザー アクセス権を回復します。
割り当て	特定のユーザーにユーザー アクセス権を割り当てます。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**]をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl]キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

ユーザー アクセス ルール

ユーザー アクセス ルールでは、ログイン時にユーザー アクセスを自動的に割り当てるユーザーを定義します。

[**ユーザー アクセス ルール**]の概要では、ユーザー アクセス ルールのすべてが一覧表示されています。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター ( )を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

ユーザー アクセス ルールのプロパティ

プロパティ	**説明**
名前	ユーザー アクセス ルールの名前です。
[**説明**]	ユーザー アクセス ルールの説明。

[**リソース フィルター**]	ユーザー アクセス ルールが適用されるリソースのタイプ。
[**無効化**]	ステータス値:**Yes** または **No**
[**タイプ**]	ユーザー アクセス ルールのタイプ。
[**条件**]	ルールを適用するために満たす必要のあるリソース/ユーザーの定義。
[**コンテキスト**]	ユーザー アクセス ルールが適用されるコンテキストを指定します。[Hub]、[QMC]、[Both] になります。[**ハブ**]、[**QMC**]、または [**Both**] (両方) になります。
[**ID**]	ユーザー アクセス ルールの ID。
[**作成日時**]	ユーザー アクセス ルールが作成された日時。
[**最終変更日**]	ユーザー アクセス ルールが最後に変更された日時。
[**変更者**]	ユーザー アクセス ルールを最後に変更した者。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
[**アクション**]	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
[**編集**]	選択したユーザー アクセス ルールを編集します。
[**削除**]	選択したユーザー アクセス ルールを削除します。

新規作成	新しいユーザー アクセス ルールを作成します。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

ユーザー アクセス ルール: 関連するアイテム

[**ユーザー アクセス**] は、リソースを編集する際に [**関連するアイテム**] から利用できます。

プレビューには、ターゲット リソースと選択したアイテムにアクセスできるソース ユーザーが表示されます。

権限に応じて、ユーザーやリソース、関連するルールを編集したり、表示することができます。

ログイン アクセス ルール

トークン 1 つは、事前に定義されたボリュームのログイン アクセス パスと同等です。ログイン アクセス権がある場合、ユーザーは事前に定義した時間の間、ストリームとアプリにアクセスできます。これは、単一のユーザーが同じ日に複数のログイン アクセス パスを使用できることを意味します。どのユーザーがログイン アクセス権を利用できるのか指定したセキュリティ ルールを作成します。

ログイン アクセス (グループ) 権を削除すると、ログイン アクセスに十分な数の未使用ログイン アクセス パスが含まれていればトークンが即時リリースされます。リリースされるトークンの数は、使用されたログイン アクセス パスの数によって決まります。使用されているログイン アクセス パスは最後の使用から 28 日が経過するまでリリースされません。例: 1,000 回のログイン アクセス パスのあるトークンをグループに割り当てると、28 日間は 1,000 回を超えるログイン アクセス パスを使用できません。また、100 回のログイン アクセス パスを 1 日目に使うと、29 日目にも 100 回利用できます。使用中のアクセス パスがない場合は、ログイン アクセス インスタンスに割り当てられたすべてのトークンは、ログイン アクセス インスタンスの削除時にリリースされます。

アプリがアクティブに使用されていない場合、アプリをリロードするとセッションが延長され、アクセス パスも消費されます。アプリとともにブラウザー ページが開いている場合、アプリをリロードするとさらにアクセス パスが消費されます。

[**ログイン アクセス ルール**] 概要では、ログイン アクセス ルールのすべてが一覧表示されています。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター ( ) を使用して項目を追加できます。

ログイン アクセス グループのプロパティ

プロパティ	説明文
名前	ログイン アクセス グループの名前です。

プロパティ	説明文
[**割り当てられたトークン**]	ログイン アクセス グループに割り当てられたトークンの数で、これにより多くのアクセス パスが提供されます。
[**使用済みのログイン アクセス パス**]	グループのユーザーがハブにログインした場合に使用されたアクセス パスの数です。
[**残りのログイン アクセス パス**]	グループのユーザーがハブへのログインで利用できるアクセス パスの数です。
[**ID**]	ログイン アクセス グループの ID です。
[**作成日時**]	ログイン アクセス グループが作成された日時。
[**最終変更日**]	ログイン アクセス グループが最後に変更された日時。
[**変更者**]	ログイン アクセス グループを最後に変更した者。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
[**アクション**]	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
[**編集**]	選択したログイン アクセス グループを編集します。

プロパティ	説明文
[削除]	選択したログイン アクセス グループを削除します。
⊕新規作成	新しいログイン アクセス グループを作成します。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

Login アクセス ルールに関連するアイテム

[**Login access rules**] 概要では、ログイン アクセス ルールに関連するすべてのアイテムが一覧表示されています。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (⊞) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

ユーザー アクセス

[**ユーザー アクセス**] は、リソースを編集する際に [**関連するアイテム**] から利用できます。

プレビューには、ターゲット リソースと選択したアイテムにアクセスできるソース ユーザーが表示されます。

権限に応じて、ユーザーやリソース、関連するルールを編集したり、表示することができます。

ライセンス ルール

プロパティグループ [**ライセンス ルール**] には、アクセス パス ルールのプロパティが含まれています。

ライセンス ルールの プロパティ

プロパティ名	説明
[名前]	ライセンス ルールの名前。
[説明]	ルールの目的の説明。
[リソース フィルター]	ルールのリソース フィルター。
[アクション]	ライセンス ルールで許可されたアクション。
[無効化]	ステータス値:**Yes** または **No**
[コンテキスト]	ライセンス ルールのコンテキスト ([**QMC**]、[**Hub**]、[**Both**])。
[タイプ]	ライセンス ルールのタイプ。
[条件]	ライセンス ルールの条件。
[ID]	ライセンス ルールの ID。
[作成日時]	ライセンス ルールが作成された日時。
[最終変更日]	ライセンス ルールが最後に変更された日時。
[変更者]	ライセンス ルールを最後に変更した者。

概要で選択してアクション バーの [**Edit**] をクリックすると、ログイン アクセス ルールの編集ページが表示されます。

サイト ライセンス

Qlik Management Console (QMC) を使い始める前に、ライセンス情報を入力する必要があります。ライセンス情報が期限切れの場合は、更新する必要があります。

ライセンスの入力時には、シリアル番号とコントロール番号を使用するオプションと、署名付きライセンス キーを使用するオプションのどちらかを選択できます。アナライザー キャパシティ ライセンスには署名付きライセンス キーが必要です。

ユーザーの割り当て、分析時間消費および製品のアクティベーションには、クラウドベースのライセンス バックエンドにアクセスするために、署名済みのライセンス キーとともにインターネット アクセス (直接またはプロキシ経由) が必要となります。

*署名入りのライセンス キーの場合、ライセンス キーを入力して[**適用**] で保存した後、QMC でライセンス情報を確認することができます。*

ライセンス認証ファイル (LEF) により、Qlik Sense サイトで使用可能なトークンの数が決まります。アクセスの種類によって、Qlik Sense サイト内でのアクセス パターンが決まります。アクセスのタイプをユーザーに割り当てると、利用可能なトークンの数が減ります。

[**サイト ライセンス**] プロパティグループには、Qlik Sense システムのライセンスに関連するプロパティが含まれています。全項目が必須で、空欄のままにはできません。

サイト ライセンスのプロパティ

プロパティ名	説明
[**所有者名**]	Qlik Sense 製品所有者のユーザー名。
[**所有者の組織**]	Qlik Sense 製品所有者が所属する組織の名称。
[**シリアル番号**]	Qlik Sense ソフトウェアに割り当てられているシリアル番号。
[**コントロール番号**]	Qlik Sense ソフトウェアに割り当てられているコントロール番号。
LEF アクセス	Qlik Sense ソフトウェアに割り当てられる ライセンス認証ファイル (LEF)。

拡張機能

拡張機能には、ウィジェット ライブラリ、カスタム テーマ、またはビジュアライゼーション エクステンションなどさまざまなものがあり、これらを使用して、たとえば、多様な地域を選択できるインタラクティブ マップで、データを可視化します。

[**拡張機能**] 概要では利用可能な拡張機能がすべて一覧表示されます。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (⊞) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

拡張機能の項目

項目	説明
名前	QMC から定義される拡張機能名。
[**所有者**]	拡張機能の所有者です。既定では拡張機能をアップロードしたユーザーになっています。
タグ	拡張機能に紐付けされているタグ。
[**ID**]	拡張機能の ID。
[**作成日時**]	拡張機能が作成された日時。
[**最終変更日**]	拡張機能が最後に変更された日時。
[**変更者**]	拡張機能を最後に変更した者。
[***<カスタム プロパティ>***]	カスタム プロパティがある場合はここに一覧表示されます。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション[**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション[**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
[**編集**]	選択した拡張機能を編集します。

項目	説明
[**削除**]	選択した拡張機能を削除します。
インポート	新しい拡張機能をインポートします。 *QMCにすでに存在する拡張子をインポートする場合は、プロンプトが表示されたら、[**Replace**] (置き換え) をクリックして既存のファイルを新しいファイルに置き換えるか、[✕] をクリックしてキャンセルします。*
[**エクスポート**]	拡張機能をエクスポートします。 *アプリをエクスポートする場合、エクステンションはそのエクスポートに含められません。このため、Qlik Sense の異なるインスタンス間でアプリを移動すると、一部のビジュアライゼーションが描画されなくなる可能性がありますエクステンションは、インストール時に指定する共有フォルダー(\\<ドメイン >\QlikShare\StaticContent\Extensions など) から入手可能です。*
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

拡張機能: 関連するアイテム

本書の表に、[**コンテンツ**] プロパティグループと[**セキュリティルール**] プロパティグループで利用可能な項目を示します。

既定では項目の一部のみが表示されます。列セレクター (⊞) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

ユーザー アクセス

[**ユーザー アクセス**] は、リソースを編集する際に [**関連するアイテム**] から利用できます。

プレビューには、ターゲット リソースと選択したアイテムにアクセスできるソース ユーザーが表示されます。

権限に応じて、ユーザーやリソース、関連するルールを編集したり、表示することができます。

セキュリティルール

[**セキュリティルール**] は拡張機能を編集する際に [**関連するアイテム**] から利用できます。概要には、選択した拡張機能に関連付けられるセキュリティルールのリストが含まれます。

[**セキュリティルール**] プロパティグループにはユーザー条件プロパティが含まれます。

ユーザー条件プロパティ

プロパティ	説明
[**名前**]	セキュリティルールの名前。
[**説明**]	ルールの説明。
[**リソース フィルター**]	ルールの ID。
[**アクション**]	ルールで許可されたアクション。
[**無効化**]	ステータス値:**Yes** または **No**
[**コンテキスト**]	セキュリティルールのコンテキスト ([**QMC**]、[**Hub**]、[**Both**])。
[**タイプ**]	セキュリティルール タイプ ([**Default**]、[**Read only**]、[**Custom**])。
[**条件**]	セキュリティルールの条件。
[**ID**]	セキュリティルールの ID。
[**作成日時**]	セキュリティルールが作成された日時。
[**最終変更日**]	セキュリティルールが最後に変更された日時。
[**変更者**]	セキュリティルールを最後に変更した者。

概要で選択してアクション バーの [**Edit**] をクリックすると、セキュリティルールの編集ページが表示されます。

タグ

QMC のリソース概要ページから効率よく環境を検索して管理できるようにするには、タグを作成してリソースに適用します。

[**タグ**] 概要には、利用可能なタグがすべて一覧表示されます。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (▦) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

タグ プロパティ

項目/ボタン	説明
名前	タグの名前。QMC
[**発生数**]	タグが紐付けされているリソース数。
[**ID**]	タグの ID。

[**作成日時**]	タグが作成された日時。
[**最終変更日**]	タグが最後に変更された日時。
[**変更者**]	タグを最後に変更した者。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
[**アクション**]	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
[**編集**]	選択したタグを編集します。
[**削除**]	選択したタグを削除します。
[**新規作成**]	新しいタグを作成します。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

On-Demand アプリ

On-Demand アプリは、選択アプリをテンプレートアプリに接続するナビテーション リンクから、Qlik Sense ハブに生成されます。選択アプリとテンプレートアプリは、QMC または Qlik Sense ハブからストリームに公開することもできます。生成される On-Demand アプリは、QMC または Qlik Sense ハブから公開することもできます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

On-Demand アプリサービスのプロパティ

選択アプリおよびテンプレートアプリは、On-demand アプリサービスを有効にしなくても作成できますが、ナビゲーション リンクを作成して On-demand アプリを生成するには、このサービスを有効にする必要があります。On-Demand アプリサービスの以下のプロパティを管理できます。

プロパティの説明

プロパティ	説明
On-Demand アプリの有効化	On-Demand アプリサービスを有効化および無効化します。このサービスは、デフォルトでは無効になっています。 サービスを有効から無効に切り替えると、On-Demand アプリを生成するためにペンディング中の要求を終了することができます。ただし、いったんサービスを無効にすると、アプリを生成する新しい要求は受け入れられません。
ダイナミック ビューの有効化	ダイナミック ビューにより、チャートの更新を分析ツールの環境から実行できます。ダイナミック ビューを有効にするには、オンデマンド アプリサービスをオンにする必要があります。 ダイナミック ビューをオンにすることによって、オンデマンドのデータ ソースからロードされるチャートをアプリシートに含めることができます。 ダイナミック ビューに基づくチャートが含まれるシートがあるアプリで、[**ダイナミック ビュー**] の設定がテナントに対して無効になっている場合、アプリは次の制限付きで引き続き動作します。 • ダイナミック ビュー機能が無効になっていることを示すため、ダイナミック チャートはすべて淡色表示 (データも非表示) されます。 • ダイナミック ビュー内の情報は、シート エディターには表示されません。 ダイナミック ビューに関係のないチャートや機能はすべて正常に動作します。
ログ レベル	サービス ログ ファイルに書き込まれる詳細レベルを指定します。

プロパティ	説明
一度に作成可能なアプリ数	サービスが一度に作成できるアプリの数を指定します。デフォルトは 1、最大数は 10 です。 この設定はアプリ生成の応答時間に影響しますが、一度に生成できるアプリの数を設定するときには、ロードされるデータの量も考慮する必要があります。データのロードサイズが適度である場合は、一度に生成されるアプリの数を多くすると、各アプリの応答時間が改善されます。ただし、ロードサイズが大きいと、設定数がより少ない場合よりも応答が遅くなり、アプリ生成のためにアプリがキューで待機しなければならなくなる可能性があります。 マルチノード環境では、一度に生成できるアプリの数に関する設定は、その環境で実行されている On-Demand アプリのすべてのインスタンスに適用されます。複数のサービスが同じ Qlik associative engine を使用している場合、その Qlik associative engine へのロードは、サービスの複数のインスタンスから一度に生成できるアプリの累積数となります。
履歴データを解析するまでの日数	On-Demand アプリに関する特定の履歴データを削除するまでの保存日数を指定します。0 ~ 365 の値を指定できます。0 に設定するとデータは削除されません。既定値は 90 日です。 On-Demand アプリサービスでは、ナビゲーション リンクおよび要求に関するデータを保持して On-Demand アプリを生成およびリロードします。 On-Demand アプリのナビゲーション リンクが削除されると、デコミッション ステートに廃棄状態で維持されます。解析前に指定した日数に到達すると、ナビゲーション リンクに関する情報は削除されます。 On-Demand アプリサービスには、On-Demand アプリを生成およびリロードする要求に関する情報も維持されます。On-Demand アプリを削除すると、リロード要求に関する情報は解析前に指定した日数の間維持されます。
匿名ユーザーに対するアプリ生成の許可	公開された選択アプリのナビゲーション ポイントから匿名ユーザーが On-demand アプリを生成できるよう許可します。この設定は、匿名認証が設定されている Qlik Sense システム上でのみ適用されます。 *匿名の認証 (page 461)* 匿名ユーザーは、ナビゲーション リンクから自動的に公開されるアプリのみ生成できます。生成されたアプリが自動的に公開されない場合、匿名ユーザーにはそのアプリに対するアクセス権限がありません。

プロパティ	説明
匿名ユーザーの代わりにアプリの生成に使用されるプロキシ ユーザー	匿名ユーザーの代わりのプロキシ ユーザーとなるユーザーを選択します。On-demand アプリリクエストを作成可能な登録ユーザーを選択します。プロキシ ユーザーには、匿名ユーザーがアクセス可能な On-demand 選択アプリに対する読み取り権限も必要です。プロキシ ユーザーとして、またはルート管理者権限を持つユーザーとして管理ユーザー (*INTERNAL\sa-xxx*) を選択しないでください。 *匿名ユーザーが使用可能な On-demand 選択アプリを含むストリームを作成する場合、On-demand アプリのプロキシ ユーザーに対して読み取りアクセスを許可するセキュリティルールを設定する必要があります。プロキシ ユーザーに読み取りアクセス権限がないと、アプリナビゲーション バーのすべてのリンクが [Invalid] (無効) として表示されます。* シングル ユーザーはすべての匿名ユーザーの代わりとなりますが、匿名ユーザーはそれぞれが On-demand アプリサービスによって特定され、識別されています。これにより、各匿名ユーザーは自身が生成したアプリにアクセスできるようになりますが、他の匿名ユーザーがそのアプリにアクセスできなくなります。各匿名ユーザーは、自身が生成したアプリにのみアクセスできます。
匿名ユーザーが生成したアプリの保存期間	匿名ユーザーが生成したアプリが削除されるまでの保存期間を指定します。既定の設定は 60 分間です。 この時間は、最後にデータがロードされた時点から計測されます。 ナビゲーション リンクに対する保存期間の設定もあります。匿名ユーザーが生成したアプリの場合、2 種類の保存期間設定のうち短い期間が使用されます。 例えば、保存期間が 24 時間に設定されているナビゲーション リンクが匿名ユーザーに使用されていて、[**匿名ユーザーが生成したアプリの保存期間**] の設定が 60分間の場合、アプリは最後のデータロードから 60 分後に削除されます。ただし、ナビゲーション リンクの保存期間の設定が 30 分であれば、匿名ユーザーが生成したアプリは最後のデータロードから 30 分後に削除されます。 *[**匿名ユーザーが生成したアプリの保存期間**] がゼロ (0) に設定されている場合、アプリはできるだけ長く、すなわち 365 日間保存されます。*

ユーザー ディレクトリ コネクタ

ユーザー ディレクトリ コネクタ (UDC) は構成済みのディレクトリ サービスに接続してユーザーを取得します。インストールされる Qlik Sense に組み込まれている UDC は、Generic と高度な LDAP、Active Directory、ApacheDS、ODBC、Access (ODBC 経由)、Excel (ODBC 経由)、SQL (ODBC 経由)、および Teradata (ODBC 経由) です。

ローカル ユーザーが Qlik Sense にログオンする場合、UDC は不要です。ただし、ローカル ユーザーがアプリにアクセスできるようにするには、アクセスを割り当てる必要があります。ユーザーベースのライセンスでは、プロフェッショナルまたはアナライザーのアクセス ルールを使用できます。トークンベースのライセンスでは、ユーザーまたはログイン アクセス ルールを使用してアクセスを割り当てることができます。あるいは、まずローカル ユーザーがログオンしてユーザーとして認識され、それからトークンが割り当てられるようにすることもできます。

ユーザー属性の名前と値は、セキュリティルールで使用する場合、LDAP 標準の構文定義に準拠する必要があります。つまり、以下のような制約があります。
- *属性名: a-z、A-Z、0-9、- のみを使用できる。a-z または A-Z で始まる必要がある。*
- *帰属の値: 任意の UTF-8 文字列。*

PostgreSQL データベースを使用する場合で、テーブル名に大文字や "." などの特殊文字が含まれる場合は、テーブル名を引用符で囲む必要があります。引用符がない場合、テーブル名の検証でエラーが発生します。テーブル名の例: "table.Name"、public."Table" (または "Table")、testschema."Table"。

ユーザーを同期していて、あるユーザー属性がユーザー テーブルの列と同じ名前である場合は、その列は列セレクターで利用できなくなり、テーブルのレンダリングが不規則になる場合があります。

[**ユーザー ディレクトリ コネクタ**] の概要には、利用可能なユーザー ディレクトリ コネクタがすべて一覧表示されています。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (▦) を使用して項目を追加できます。

ユーザー ディレクトリ コネクタ

項目/ボタン	説明
名前	QMC から入力されたユーザー ディレクトリ コネクタの構成名。
ユーザー ディレクトリ	ユーザー ディレクトリ名は、ユーザー ディレクトリ構成によって異なります。 • ODBC および LDAP 用に手動で入力。 • アクティブ ディレクトリのコネクタのプロパティから生成。 *[**ユーザー ディレクトリ**] の値は一意でなければなりません。一意でなければ、コネクタは設定できません。[**ユーザー ディレクトリ**] の値は、ユーザー ディレクトリに対してセキュリティルールを作成する際に使用されます。*
タイプ	汎用 LDAP、高度な LDAP、Microsoft Active Directory、ApacheDS、ODBC、Access (ODBC 経由)、Excel (ODBC 経由)、SQL (ODBC 経由)。

[**設定済み**]	ステータス値:**Yes** または **No** ユーザー ディレクトリ名を設定する場合、固有のもので空欄でないことが必要です。
[**稼働可能**]	ステータス値:**Yes** または **No** 稼働可能とは、コネクタプロパティの構成により、ユーザー ディレクトリとのやり取りが可能になっていることを示しています。 *それぞれのコネクタには、異なるプロパティが必要です。この場所で UserManagement_Repository ログを確認します: %ProgramData%\Qlik\Sense\Log\Repository\Trace*
ステータス	ユーザー ディレクトリ コネクタの状態: • [**アイドル**]: 同期が行われなかったとき。 • [**外部フェッチ**]: ディレクトリ サービスからデータを取得する時の同期化の最初のフレーズ。 • [**データベース保管**]:QRS にデータを保管する際の同期化の 2 番目のフレーズ。 *状態が [**アイドル**] として表示され、[**前回の開始**] が [**前回の終了**] よりも後になっている場合は同期に失敗したということです。*
最後に開始された同期	ユーザー データの同期化が最後に開始された日時。同期はタスクによるトリガー、あるいはユーザー ディレクトリ コネクタ概要から手動による開始のいずれか。 *UDC または同じドメインに属するユーザーがハブ、dev-hub、または QMC にアクセスしたときなど、ユーザー同期がトリガーされると、[**最後に開始された同期**] と [**最後に完了した同期**] が更新されます。*
[**最後に完了した同期**]	ユーザー データの同期化が最後に正常に終了した日時。 *UDC または同じドメインに属するユーザーがハブ、dev-hub、または QMC にアクセスしたときなど、ユーザー同期がトリガーされると、[**最後に開始された同期**] と [**最後に完了した同期**] が更新されます。*
タグ	紐付けされたタグの名前。

[**既存のユーザーのユーザー データの同期**]	ステータス値:**Yes** または **No** このオプションを選択すると「Yes」が表示されます。 • 選択されている場合は、既存のユーザーのみが同期されます。既存のユーザーは、Qlik Sense にログインしているユーザーや、構成済みディレクトリサービスから同期されたことのあるユーザーです。 • 選択されていない場合は、UDC のプロパティで定義されているすべてのユーザーが構成済みのディレクトリサービスから同期されます。選択したユーザーのみを同期する場合は、[**Active Directory**]、[**ApacheDS**]、[**汎用 LDAP**] または [**Advanced LDAP**] でフィルターを作成できます。 *大量のユーザーとユーザー属性が格納されたユーザー ディレクトリがある場合は、このオプションを選択したままにすることをお勧めします。* *ユーザー属性は、ユーザーがハブにログインするときにのみ同期されます。QMC でユーザーを削除しても、削除されたユーザーに対してアクティブなセッションは引き続き有効です。ハブの更新のみが行われた場合、ユーザーはデータベースに追加されますが、いかなる属性も持ちません。*
ID	ユーザー ディレクトリ コネクタの ID。
作成日	ユーザー ディレクトリが作成された日時。
最終変更日	ユーザー ディレクトリ コネクタが最後に変更された日時。
変更者	ユーザー ディレクトリ コネクタを変更したユーザーのユーザー ID。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*

	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。 *新しいユーザーディレクトリコネクタタイプを追加した場合は、F5 を押して、利用可能なユーザーディレクトリコネクタのリストを更新する必要があります。*
編集	選択したユーザーディレクトリコネクタを編集します。
削除	選択したユーザーディレクトリコネクタを削除します。
[**同期**]	選択したユーザーディレクトリコネクタを通じてユーザーデータを同期します。
新規作成	新しいユーザーディレクトリコネクタを作成します。
さらに表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

[User directory connectors Generic LDAP] プロパティ

以下のプロパティグループは、汎用 LDAP タイプのユーザーディレクトリコネクタで利用できます。

ID

全項目が必須で、空欄のままにはできません。

ID プロパティ

プロパティ	説明
名前	QMC で定義された UDC プロパティの名前です。
タイプ	UDC タイプです。

ユーザー同期設定

ユーザー同期プロパティ

プロパティ	説明	既定値
[**既存のユーザーのユーザーデータの同期**]	• 選択されている場合は、既存のユーザーのみが同期されます。既存のユーザーは、Qlik Sense にログインしているユーザーや、構成済みディレクトリサービスから同期されたことのあるユーザーです。 • 選択されていない場合は、UDC のプロパティで定義されているすべてのユーザーが構成済みのディレクトリサービスから同期されます。選択したユーザーのみを同期する場合は、[**Active Directory**]、[**ApacheDS**]、[**汎用 LDAP**] または [**Advanced LDAP**] でフィルターを作成できます。 *ユーザー属性は、ユーザーがハブにログインするときにのみ同期されます。QMC でユーザーを削除しても、削除されたユーザーに対してアクティブなセッションは引き続き有効です。ハブの更新のみが行われた場合、ユーザーはデータベースに追加されますが、いかなる属性も持ちません。*	選択値

接続

接続プロパティ

プロパティ	説明	既定値
ユーザーディレクトリ名	ユーザーディレクトリは一意でなければなりません。一意でないと、コネクタは構成されません。UDC インスタンスの名前 (Active Directory のドメイン名に喩えられる)。ユーザーアカウント名と共に、この名前はユーザーを固有のものにします。 *Active Directory には手動で入力できません。*	-
パス	ディレクトリサーバーへの接続に使用する URI。SSL をサポートするため、プロトコルを LDAPS として指定します。 *カスタム ポートには対応していません。*	ldap://company.domain.com
[**ユーザー名**]	ディレクトリサーバーへの接続に使用する、オプションのユーザー ID。空の場合、Qlik Sense リポジトリを実行するユーザーを使用して、ディレクトリサーバーにログインします。	-
[**パスワード**]	ユーザー向けのオプションのパスワード。	-

ユーザーがActive Directory コネクターを作成する場合、Qlik Sense サービスを実行しているユーザーがディレクトリサーバーへのアクセスを許可されている場合のみ、そのコネクターは動作します。Qlik Sense サービスを実行しているユーザーがディレクトリサーバーへのアクセスを許可されていない場合、ディレクトリサーバーにアクセス可能なユーザー名とパスワードを入力する必要があります。

詳細設定

[**詳細設定**] プロパティグループには、Qlik Sense システムの詳細な LDAP コネクタプロパティが含まれています。

詳細設定プロパティ

プロパティ	説明	デフォルト値
[**LDAP 追加フィルター**]	LDAP クエリとして使用し、ディレクトリでユーザーを再取得します。	-
同期タイムアウト (秒)	データソースからのデータ読み取りのタイムアウト。	240
[**検索のページサイズ**]	データソースからデータを読み取るときに取得する投稿数を指定します。指定した数の投稿が検出されると検索が停止し、結果が返されます。検索を再開すると、停止した位置から検索が続行されます。 *ユーザーの同期に失敗した場合は、設定値を「0」(ゼロ) にし、ページ指定検索を行わないのと同じ設定にします。*	2000 (ApacheDS の場合: 1000)
[**最適化されたクエリを使用**]	このプロパティにより、Qlik Sense は、再取得されたユーザーの数に比例する多くのグループを含むディレクトリのクエリを最適化できます。 *最適化を使用できるようにするには、グループでユーザーを参照するようディレクトリを設定する必要があります。ディレクトリが正しく設定されていない場合、最適化されたクエリは、ユーザーに関連付けられたすべてのグループを検索しません。* このプロパティは、汎用 LDAP およびアクティブなディレクトリ検索でのみ表示されます (Active Directory は常に最適化を使用します)。	選択されていない

プロパティ	説明	デフォルト値
認証の種類	オプション。LDAP に接続するための認証タイプ。 複数の値はカンマで区切ることができます。 [値]:*Secure*、*Encryption*、*SecureSocketsLayer*、*ReadonlyServer*、*FastBind*、*Signing*、*Sealing*、*Delegation*、*ServerBind*。 *「Active Directory および汎用 LDAP UDC での LDAP チャネル バインディングと LDAP 署名」をサポートするには、次の認証タイプの値を使用します。Secure,Signing。*	資格情報の設定に基づいて、*FastBind* または *Anonymous*。

ディレクトリ入力属性

ディレクトリエントリ属性は、大文字と小文字を区別します。

ディレクトリエントリ属性のプロパティ

プロパティ	説明	デフォルト値
[**タイプ**]	ディレクトリエントリのタイプを特定する属性名 (ユーザーとグループのみを LDAP UDC で使用)。	objectClass
[**ユーザー ID**]	ユーザーを識別するディレクトリエントリの属性値。	inetOrgPerson
[**グループ ID**]	グループを識別するディレクトリエントリの属性値。	group
[**アカウント名**]	ユーザーがログインに使用する (UDC 内の) 一意のユーザー名。	sAMAccountName
[**電子メール**]	ディレクトリエントリの電子メールを含む属性名 (ユーザー)。	mail
[**表示名**]	ユーザーまたはグループ ディレクトリエントリのフルネーム。	名前
[**グループ メンバーシップ**]	この属性は、ディレクトリエントリがメンバーの直属のグループを示します。ユーザー同期化の間に、間接的なグループ メンバーシップは解消されます。 この設定または下記の設定である [**ディレクトリ エントリの メンバー**] は、空欄のままにできます。つまり、グループ メンバーシップは、2 つの設定のうちのどちらか 1 つの設定のみを使用して解消されます。	memberOf

プロパティ	説明	デフォルト値
[ディレクトリエントリのメンバー]	このディレクトリエントリの直接メンバーへの参照が入っている属性の名前。 上記の [グループ メンバーシップ] の設定も参照してください。	member
カスタム属性 (高度な LDAP のみ)	取得する追加の LDAP オブジェクト属性。	-

タグ

タグ プロパティ

プロパティ	説明
[タグ]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキストボックスの下に表示されます。

[User directory connectors Advanced LDAP] プロパティ

以下のプロパティグループは、高度な LDAP タイプのユーザー ディレクトリコネクタで利用できます。

ID

全項目が必須で、空欄のままにはできません。

ID プロパティ

プロパティ	説明
名前	QMC で定義された UDC プロパティの名前です。
タイプ	UDC タイプです。

ユーザー同期設定

ユーザー同期プロパティ

プロパティ	説明	既定値
[**既存のユーザーのユーザーデータの同期**]	• 選択されている場合は、既存のユーザーのみが同期されます。既存のユーザーは、Qlik Sense にログインしているユーザーや、構成済みディレクトリサービスから同期されたことのあるユーザーです。 • 選択されていない場合は、UDC のプロパティで定義されているすべてのユーザーが構成済みのディレクトリサービスから同期されます。選択したユーザーのみを同期する場合は、[**Active Directory**]、[**ApacheDS**]、[**汎用 LDAP**] または [**Advanced LDAP**] でフィルターを作成できます。 *ユーザー属性は、ユーザーがハブにログインするときにのみ同期されます。QMC でユーザーを削除しても、削除されたユーザーに対してアクティブなセッションは引き続き有効です。ハブの更新のみが行われた場合、ユーザーはデータベースに追加されますが、いかなる属性も持ちません。*	選択値

接続

LDAP 接続のプロパティ

プロパティ	説明	既定値
ユーザー ディレクトリ名	ユーザー ディレクトリは一意でなければなりません。一意でないと、コネクタは構成されません。UDC インスタンスの名前 (Active Directory のドメイン名に喩えられる)。ユーザー アカウント名と共に、この名前はユーザーを固有のものにします。 *Active Directory には手動で入力できません。*	

プロパティ	説明	既定値
ホスト	「:」で区切られたポートを持つホスト名 ホスト名が IP アドレスの場合、**フラグ**項目に値 *no_fqdn* を追加します。 グローバル カタログ検索にはポート 3268/(LDAP の場合: 3269) を使用します。 アクセスのための Qlik Sense がインストールされているサーバーから LDAP サーバーに開いている対応するポートをチェックします。	company.com:port
[**ユーザー名**]	ディレクトリサーバーへの接続に使用する、オプションのユーザー ID。 形式: *ドメイン名\ユーザー名* *ユーザー名とパスワードが空の場合、そのユーザーは匿名ユーザーと見なされます。*	
[**パスワード**]	ユーザー向けのオプションのパスワード。 *ユーザー名とパスワードが空の場合、そのユーザーは匿名ユーザーと見なされます。*	
タイムアウト (秒)	秒単位の接続タイムアウト。	500
ベース DN	選択する LDAP のベース DN。	cn=builtin,dc=company,dc=com

ユーザーが Active Directory コネクターを作成する場合、Qlik Sense サービスを実行しているユーザーがディレクトリサーバーへのアクセスを許可されている場合のみ、そのコネクターは動作します。Qlik Sense サービスを実行しているユーザーがディレクトリサーバーへのアクセスを許可されていない場合、ディレクトリサーバーにアクセス可能なユーザー名とパスワードを入力する必要があります。

詳細設定

[**詳細設定**] プロパティグループには、Qlik Sense システムの詳細な LDAP コネクタプロパティが含まれています。

LDAP の詳細なプロパティ

プロパティ	説明	既定値
ページ サイズ	データ ソースからデータを読み取るときに取得する投稿数を指定します。指定した数の投稿が検出されると検索が停止し、結果が返されます。検索を再開すると、停止した位置から検索が続行されます。 *ユーザーの同期に失敗した場合は、設定値を「0」(ゼロ) にし、ページ指定検索を行わないのと同じ設定にします。*	2000 (ApacheDS の場合: 1000)
[**最適化されたクエリを使用**]	このプロパティにより、Qlik Sense は、再取得されたユーザーの数に比例する多くのグループを含むディレクトリのクエリを最適化できます。 *最適化を使用できるようにするには、グループでユーザーを参照するようディレクトリを設定する必要があります。ディレクトリが正しく設定されていない場合、最適化されたクエリは、ユーザーに関連付けられたすべてのグループを検索しません。* このプロパティは、汎用 LDAP、高度な LDAP およびアクティブなディレクトリ検索でのみ表示されます (Active Directory は常に最適化を使用します)。	選択されていない
タイムアウト (秒)	データ ソースからのデータ読み取りのタイムアウト。	400
認証の種類	LDAP に接続するための認証タイプ。 *オプション:匿名、基本、ネゴシエート、NTLM、ダイジェスト、Sicily、DPA、MSN、外部、Kerberos*。	-

プロパティ	説明	既定値
フラグ	LDAP 接続セッション設定について言及するフラグ。複数の値をカンマ区切りで指定できます。 *Tcpkeepalive*: TCP keep-alive を有効にします。 *Autoreconnect*: Autoreconnect を有効にします。 *Rootdsecache*: 内部 RootDSE キャッシュを有効にします。 *封印*: Kerberos 暗号化を有効にします。 *セキュア ソケット レイヤーまたは SSL*: 接続でセキュア ソケット レイヤーを有効にします。 *署名*: Kerberos 暗号化を有効にします。 *コネクションレス*: 接続が UDP かどうかを指定します。 *No_fqdn*: [**ホスト**] 項目のホストが IP アドレスとして指定されている場合は、このフラグを使用します。 *noclientcert*: SSL 接続がの確立されたときにクライアント証明書の指定に使用されるデフォルトのコールバック関数をスキップします。 *NoCertVerify*: SSL 接続が確立されたときにサーバー証明書の検証をスキップします。 *NoCertVerify とCertdebug を一緒に使用しないでください。* *Certdebug*: デバッグのために、特定のサーバー証明書検証エラーがあれば取得します。 *AllProps*: LDAP オブジェクトのすべての属性を取得します。	-

プロパティ	説明	既定値
ロケーター フラグ	DC ロケーターのロケーター フラグ。複数の値をカンマ区切りで指定できます。 *なし* *ForceRediscovery* *DirectoryServiceRequired* *DirectoryServicePreferred* *GCRequired* *PdcRequired* *IPRequired* *KdcRequired* *TimeServerRequired* *WriteableRequired* *GoodTimeServerPreferred* *AvoidSelf* *OnlyLdapNeeded* *IsFlatName* *IsDnsName* *ReturnDnsName* *ReturnFlatName*	-
LDAP フィルターの検索	オプションの LDAP フィルター クエリ。	-
プロトコル バージョン	使用する LDAP プロトコルのバージョン。	3
Simple Authentication and Security Layer (SASL) メソッド	SASL バインディング方式: *gssapi* *外部* *gss-spnego* *digest-md5*	-
証明書のパス	認証のために送信するクライアント証明書のパス。	-

ディレクトリ入力属性

ディレクトリエントリ属性は、大文字と小文字を区別します。

LDAP ディレクトリエントリ属性のプロパティ

プロパティ	説明	デフォルト値
[タイプ]	ディレクトリエントリのタイプを特定する属性名 (ユーザーとグループのみを LDAP UDC で使用)。	objectClass
ユーザー識別子	ユーザーを識別するディレクトリエントリの属性値。	inetOrgPerson
グループ識別子	グループを識別するディレクトリエントリの属性値。	group
[アカウント名]	ユーザーがログインに使用する (UDC 内の) 一意のユーザー名。	sAMAccountName
[電子メール]	ディレクトリエントリの電子メールを含む属性名 (ユーザー)。	mail
[表示名]	ユーザーまたはグループ ディレクトリエントリのフルネーム。	名前
[グループ メンバーシップ]	この属性は、ディレクトリエントリがメンバーの直属のグループを示します。ユーザー同期化の間に、間接的なグループ メンバーシップは解消されます。 この設定または下記の設定である [**ディレクトリ エントリのメンバー**] は、空欄のままにできます。つまり、グループ メンバーシップは、2 つの設定のうちのどちらか 1 つの設定のみを使用して解消されます。	memberOf
[ディレクトリエントリのメンバー]	このディレクトリエントリの直接メンバーへの参照が入っている属性の名前。 上記の [**グループ メンバーシップ**] の設定も参照してください。	member
カスタム帰属	取得する追加の LDAP オブジェクト属性。	

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキストボックスの下に表示されます。

[User directory connectors Active Directory] プロパティ

以下のプロパティグループは、Active Directory タイプのユーザー ディレクトリコネクタで利用できます。

ID

全項目が必須で、空欄のままにはできません。

ID プロパティ

プロパティ	説明
名前	QMC で定義された UDC プロパティの名前です。
タイプ	UDC タイプです。

ユーザー同期設定

ユーザー同期プロパティ

プロパティ	説明	既定値
[**既存のユーザーのユーザーデータの同期**]	• 選択されている場合は、既存のユーザーのみが同期されます。既存のユーザーは、Qlik Sense にログインしているユーザーや、構成済みディレクトリサービスから同期されたことのあるユーザーです。 • 選択されていない場合は、UDC のプロパティで定義されているすべてのユーザーが構成済みのディレクトリサービスから同期されます。選択したユーザーのみを同期する場合は、[**Active Directory**]、[**ApacheDS**]、[**汎用 LDAP**] または [**Advanced LDAP**] でフィルターを作成できます。 *ユーザー属性は、ユーザーがハブにログインするときにのみ同期されます。QMC でユーザーを削除しても、削除されたユーザーに対してアクティブなセッションは引き続き有効です。ハブの更新のみが行われた場合、ユーザーはデータベースに追加されますが、いかなる属性も持ちません。*	選択値

接続

[**接続**] プロパティグループには、Qlik Sense システムのアクティブ ディレクトリ接続プロパティが含まれています。

接続プロパティ

プロパティ	説明	既定値
[**パス**]	AD ドメインへの接続に使われる URI。	ldap://company.domain.com
[**ユーザー名**]	AD サーバーへの接続に使用されるオプションのユーザー ID。これが空の場合、Qlik Sense リポジトリを実行しているユーザーは、AD サーバーにログオンするために使われます。	-
[**パスワード**]	上記ユーザー向けのオプションのパスワード。	-

Active Directory 内の複数のサブドメインにユーザーが属している場合、サブドメインごとに 1 つのユーザー ディレクトリ コネクタを作成する必要があります。

詳細設定

[**詳細設定**] プロパティグループには、Active Directory の詳細なプロパティが含まれています。

詳細設定プロパティ

プロパティ	説明	既定値
[**LDAP 追加フィルター**]	AD のユーザーを取得するために LDAP クエリーとして使用。	空
[**同期タイムアウト (秒)**]	データ ソースからのデータ読み取りのタイムアウト。	240
[**検索のページ サイズ**]	データ ソースからデータを読み取るときに取得する投稿数を指定します。指定した数の投稿が検出されると検索が停止し、結果が返されます。検索を再開すると、停止した位置から検索が続行されます。 *ユーザーの同期に失敗した場合は、設定値を「0」(ゼロ) にし、ページ指定検索を行わないのと同じ設定にします。*	2000

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキストボックスの下に表示されます。

[User directory connectors ApacheDS] プロパティ

以下のプロパティグループは、ApacheDS タイプのユーザーディレクトリコネクタで利用できます。

ID

全項目が必須で、空欄のままにはできません。

ID プロパティ

プロパティ	説明
名前	QMC で定義された UDC プロパティの名前です。
タイプ	UDC タイプです。

ユーザー同期設定

ユーザー同期プロパティ

プロパティ	説明	既定値
[**既存のユーザーのユーザーデータの同期**]	• 選択されている場合は、既存のユーザーのみが同期されます。既存のユーザーは、Qlik Sense にログインしているユーザーや、構成済みディレクトリサービスから同期されたことのあるユーザーです。 • 選択されていない場合は、UDC のプロパティで定義されているすべてのユーザーが構成済みのディレクトリサービスから同期されます。選択したユーザーのみを同期する場合は、[**Active Directory**]、[**ApacheDS**]、[**汎用 LDAP**] または [**Advanced LDAP**] でフィルターを作成できます。 *ユーザー属性は、ユーザーがハブにログインするときにのみ同期されます。QMC でユーザーを削除しても、削除されたユーザーに対してアクティブなセッションは引き続き有効です。ハブの更新のみが行われた場合、ユーザーはデータベースに追加されますが、いかなる属性も持ちません。*	選択値

接続

接続プロパティ

プロパティ	説明	既定値
ユーザーディレクトリ名	ユーザーディレクトリは一意でなければなりません。一意でないと、コネクタは構成されません。UDC インスタンスの名前 (Active Directory のドメイン名に喩えられる)。ユーザーアカウント名と共に、この名前はユーザーを固有のものにします。 *Active Directory には手動で入力できません。*	-
パス	ディレクトリサーバーへの接続に使用する URI。SSL をサポートするため、プロトコルを LDAPS として指定します。 *カスタム ポートには対応していません。*	ldap://company.domain.com
[**ユーザー名**]	ディレクトリサーバーへの接続に使用する、オプションのユーザー ID。空の場合、Qlik Sense リポジトリを実行するユーザーを使用して、ディレクトリサーバーにログインします。	-
[**パスワード**]	ユーザー向けのオプションのパスワード。	-

ユーザーが Active Directory コネクターを作成する場合、Qlik Sense サービスを実行しているユーザーがディレクトリサーバーへのアクセスを許可されている場合のみ、そのコネクターは動作します。Qlik Sense サービスを実行しているユーザーがディレクトリサーバーへのアクセスを許可されていない場合、ディレクトリサーバーにアクセス可能なユーザー名とパスワードを入力する必要があります。

詳細設定

[**詳細設定**] プロパティグループには、Qlik Sense システムの詳細な LDAP コネクタプロパティが含まれています。

詳細設定プロパティ

プロパティ	説明	デフォルト値
[**LDAP 追加フィルター**]	LDAP クエリとして使用し、ディレクトリでユーザーを再取得します。	-

プロパティ	説明	デフォルト値
同期タイムアウト(秒)	データソースからのデータ読み取りのタイムアウト。	240
[**検索のページサイズ**]	データソースからデータを読み取るときに取得する投稿数を指定します。指定した数の投稿が検出されると検索が停止し、結果が返されます。検索を再開すると、停止した位置から検索が続行されます。 *ユーザーの同期に失敗した場合は、設定値を「0」(ゼロ) にし、ページ指定検索を行わないのと同じ設定にします。*	2000 (ApacheDS の場合: 1000)
[**最適化されたクエリを使用**]	このプロパティにより、Qlik Sense は、再取得されたユーザーの数に比例する多くのグループを含むディレクトリのクエリを最適化できます。 *最適化を使用できるようにするには、グループでユーザーを参照するようディレクトリを設定する必要があります。ディレクトリが正しく設定されていない場合、最適化されたクエリは、ユーザーに関連付けられたすべてのグループを検索しません。* このプロパティは、汎用 LDAP およびアクティブなディレクトリ検索でのみ表示されます (Active Directory は常に最適化を使用します)。	選択されていない
認証の種類	オプション。LDAP に接続するための認証タイプ。 複数の値はカンマで区切ることができます。 [値]:*Secure*、*Encryption*、*SecureSocketsLayer*、*ReadonlyServer*、*FastBind*、*Signing*、*Sealing*、*Delegation*、*ServerBind*。 *「Active Directory および汎用 LDAP UDC での LDAP チャネル バインディングとLDAP 署名」をサポートするには、次の認証タイプの値を使用します。Secure,Signing。*	資格情報の設定に基づいて、*FastBind* または *Anonymous*。

ディレクトリ入力属性

[**ディレクトリエントリ属性**] プロパティグループには、LDAP コネクタのディレクトリエントリ属性が含まれています。

ディレクトリエントリ属性は、大文字と小文字を区別します。

ディレクトリエントリ属性のプロパティ

プロパティ	説明	デフォルト値
[**タイプ**]	ディレクトリエントリのタイプを特定する属性名 (ユーザーとグループのみを ApacheDS UDC で使用)。	objectClass
[**ユーザー ID**]	ユーザーを識別するディレクトリエントリの属性値。	inetOrgPerson
[**グループ ID**]	グループを識別するディレクトリエントリの属性値。	groupOfNames
[**アカウント名**]	ユーザーがログインに使用する (UDC 内の) 一意のユーザー名。	uid
[**電子メール**]	ディレクトリエントリの電子メールを含む属性名 (ユーザー)。	mail
[**表示名**]	ユーザーまたはグループ ディレクトリエントリのフルネーム。	cn
[**グループ メンバーシップ**]	ディレクトリエントリが直属のグループを示す属性の名前。ユーザー同期化の間に、間接的なグループ メンバーシップは解消されます。 この設定または下記の設定である [**ディレクトリ エントリのメンバー**] は、空欄のままにできます。つまり、グループ メンバーシップは、2 つの設定のうちのどちらか 1 つの設定のみを使用して解消されます。	-
[**ディレクトリ エントリのメンバー**]	このディレクトリエントリの直接メンバーへの参照が入っている属性の名前。 上記の [**グループ メンバーシップ**] の設定も参照してください。	member

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

[User directory connectors ODBC] プロパティ

新しいユーザー ディレクトリコネクタ (UDC) を作成するときには、4 つの ODBC オプションが存在します。それらのオプションすべてのプロパティと項目は同じですが、**Access (ODBC 経由)**、**Excel (ODBC 経由)**、**SQL (ODBC 経由)**、および **Teradata (ODBC 経由)** の場合には、一部の項目 にはサポートのための既定値が含まれています。通常はこれらの値を変更する必要があります。

PostgreSQL データベースを使用する場合で、テーブル名に大文字や "." などの特殊文字が含まれる場合は、テーブル名を引用符で囲む必要があります。引用符がない場合、テーブル名の検証でエラーが発生します。テーブル名の例: "table.Name"、public."Table" (または "Table")、testschema."Table"。

ユーザーを同期していて、あるユーザー属性がユーザー テーブルの列と同じ名前である場合は、その列は列セレクターで利用できなくなり、テーブルのレンダリングが不規則になる場合があります。

次のプロパティグループは ODBC UDC で利用できます。

ID

全項目が必須で、空欄のままにはできません。

ID プロパティ

プロパティ	説明
名前	QMC で定義された UDC プロパティの名前です。
タイプ	UDC タイプです。

ユーザー同期設定

ユーザー同期プロパティ

プロパティ	説明	既定値
[**既存のユーザーのユーザーデータの同期**]	• 選択されている場合は、既存のユーザーのみが同期されます。既存のユーザーは、Qlik Sense にログインしているユーザーや、構成済みディレクトリサービスから同期されたことのあるユーザーです。 • 選択されていない場合は、UDC のプロパティで定義されているすべてのユーザーが構成済みのディレクトリサービスから同期されます。選択したユーザーのみを同期する場合は、[**Active Directory**]、[**ApacheDS**]、[**汎用 LDAP**] または [**Advanced LDAP**] でフィルターを作成できます。 *ユーザー属性は、ユーザーがハブにログインするときにのみ同期されます。QMC でユーザーを削除しても、削除されたユーザーに対してアクティブなセッションは引き続き有効です。ハブの更新のみが行われた場合、ユーザーはデータベースに追加されますが、いかなる属性も持ちません。*	選択値

接続

Microsoft Access Text Driver (.txt, *.csv) を使用して .txt ファイルをロードする場合、コネクター タイプは [**ODBC**]. ではなく[**Access (ODBC 経由)**] を使用する必要があります。*

接続プロパティ

プロパティ	説明	既定値
ユーザーディレクトリ名	ユーザーディレクトリの名前。ユーザーディレクトリは一意でなければなりません。一意でないと、コネクタは構成されません。この名前にスペースを含んではいけません。	-
ユーザーテーブル名	ユーザーが一覧表示されているテーブルの名前。テーブル名にファイル拡張子を含めます。例:*Table.csv*. *Oracle ODBC ユーザーディレクトリコネクターを設定する場合、**ユーザーテーブル名**および**属性テーブル名**の前に、それらのテーブルの所有者を付ける必要があります。例: ただの USERS でなくOWNER.USERS。*	-
属性テーブル名	ユーザー属性を含むテーブルの名前。テーブル名にファイル拡張子を含めます。 例:*Table.csv*. *Oracle ODBC ユーザーディレクトリコネクターを設定する場合、**ユーザーテーブル名**および**属性テーブル名**の前に、それらのテーブルの所有者を付ける必要があります。例: ただの USERS でなくOWNER.USERS。*	-
表示されている接続文字列	データソースへの接続に使われる接続文字列関数の表示可能な部分。以下のいずれかを指定します。 • 完全な接続文字列。例: *Driver={SQL Server Native Client 11.0};Server=localhost;Database=Users;Trusted_Connection=yes;* 1. *Driver*は現在コンピュータにあるドライバを指定する必要があります。[**ODBC データ ソース アドミニストレータ**] で、指定するドライバーを確認してください。「データ ソース」を検索して、アプリケーションを見つけます。 2. *Server* は接続するサーバーを指定する必要があります。 3. *Database* はテーブルがあるデータベースを指定する必要があります。 4. *Trusted_Connection=yes* は設定によって必要になる場合があります。この例では、必要です。 • 確立されたシステム DNS へのポインタ。例えば、*dsn=MyDSN;* *データベースに接続する場合、2 つの接続文字列関数は単一の接続文字列関数に連結されます。*	-

プロパティ	説明	既定値
暗号化された接続文字列	データソースへの接続に使われる接続文字列関数の暗号化された部分。通常、この文字列にはユーザー名とパスワードが含まれます。 次の接続文字列があると見なされます: *Driver={Microsoft Access Driver (.mdb)};Dbq=C:\mydatabase.mdb;Uid=Admin;Pwd=verySecretAdminPassword;* この接続文字列は、そのままデータベースに保存すると秘密のパスワードが表示されてしまうため注意が必要です。パスワードを保護するため以下の手順に従ってください。 最初の部分 (*Driver={Microsoft Access Driver (.mdb)};Dbq=C:\mydatabase.mdb;*) を [**表示されている接続文字列**] 項目に保存し、二番目の部分 *(Uid=Admin;Pwd=verySecretAdminPassword;)* を [**暗号化された接続文字列**] 項目に保存します。このようにすれば二番目の部分がデータベースに暗号化されて保存されるため、後に編集のため UDC で開いても表示されません。 *データベースに接続する場合、2 つの接続文字列関数は単一の接続文字列関数に連結されます。*	-
同期タイムアウト (秒)	データソースからのデータ読み取りのタイムアウト。	240

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキストボックスの下に表示されます。

ユーザーディレクトリコネクタ: 関連するアイテム

次のテーブルでは、関連するアイテムで利用できる項目を示しています。既定では項目の一部のみが表示されます。You can use the column selector (⊞) to add fields.

列幅は、ヘッダーの線をドラッグすることで調整できます。

ユーザー アクセス

[**ユーザー アクセス**] は、リソースを編集する際に [**関連するアイテム**] から利用できます。

プレビューには、ターゲット リソースと選択したアイテムにアクセスできるソース ユーザーが表示されます。

権限に応じて、ユーザーやリソース、関連するルールを編集したり、表示することができます。

タスク

[**タスク**] は使用されたディレクトリコネクタを編集する際に [**関連するアイテム**] から利用できます。概要には、選択したユーザー ディレクトリコネクタと関連付けられているタスクのリストが含まれています。

タスクのプロパティ

プロパティ	**説明**
[**名前**]	タスクの名前。
[**タイプ**]	タスクのタイプ (ユーザー同期 または リロード)。
[**UDC 名**]	タスクと関連のあるユーザー ディレクトリ。
[**有効化**]	ステータス値:**Yes** または **No**
[**状態**]	タスクの状態。
[**タグ**]	タスクと関連付けられたタグ。
[**ID**]	タスクの ID。
[**作成日時**]	タスクが作成された日時。
[**最終変更日**]	タスクが最後に変更された日時。
[**変更者**]	タスクを最後に変更した者。
[**カスタム プロパティ**]	カスタム プロパティがある場合はここに一覧表示されます。

監視アプリ

統治アプリは、Qlik Sense ログ ファイルからのデータを表示します。

以下のアプリは、既定のインストールに含まれています。

- License Monitor
- Operations Monitor

Select **Monitoring apps** on the **QMC start** page, or from the **Start** drop-down menu, to open the hub for the stream **Monitoring apps** with the apps License Monitor and Operations Monitor.

Qlik Sense ログ フォルダへの既定のパスは、*%ProgramData%\Qlik\Sense\Log\<サービス>* です。

*[**Monitoring apps**] ストリームは削除しないでください。ストリームを削除すると、取り消すことができません。(RootAdmins、ContentAdmins、SecurityAdmins はストリームを削除できます。)*

サービス クラスター

サービス クラスターは ノードの集まりです。ノードをクラスターにまとめると、中央構成が可能になります。

マルチ ノード サイトの場合、サービス クラスターは、すべての ノードの場合に、永続タイプ、データベース接続、および静的コンテンツ フォルダーなどの構成を保存します。設定を統一できるように、すべての ノードがサービス クラスターにリンクされています。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. [**サービスクラスタ**] を QMC [スタート] ページまたは [**スタート**] ドロップダウン メニューから選択して、▼サービス クラスタページを表示します。

ID

ID プロパティ

プロパティ	説明
名前	サービス クラスターの名前。

クラスターの設定

クラスター設定のプロパティ

プロパティ	説明
Root folder (ルート フォルダー)	異なるパスが明示的に指定されていない限り、ルート サブフォルダーには、既定でルート フォルダー パスが使用されます。ルート フォルダーのパスが *//myhost/share* の場合、既定のルート サブフォルダーのパスは *//myhost/share/<root subfolder>* です。
App folder (アプリのフォルダー)	すべての ノードがアプリを取得するために接続するルート サブフォルダー。
Static content root folder (静的コンテンツのルート フォルダー)	静的コンテンツ (画像など) が含まれるルート サブフォルダー。
Archived logs root folder (アーカイブされたログのルート フォルダー)	ルート サブフォルダー、各ホストに 1 つ。
Failover timeout (minutes) (フェールオーバー タイムアウト (分))	フェールオーバーが発生するまで、セントラル ノードがオフライン状態であることができる時間。既定値: 10分。この値は編集可能です。

Data encryption (データの暗号化)

データベースの暗号化のプロパティ

プロパティ	説明
QVF encryption (QVF 暗号化)	[*Encryption key*] (暗号化キー) 入力項目に示されている暗号化キーを使用して、Qlik Sense アプリ (QVF) を暗号化します。 アプリのコンテンツ (データおよびブックマーク) は保存の際に暗号化されます。QVF 暗号化が有効になる前に作成されたアプリは、次にデータあるはブックマークのアップデートを行って保存する際に暗号化されます。
QVD encryption (QVD 暗号化)	データロードスクリプトで STORE コマンドを使用して作成される、新しい Qlik Sense データファイル (QVD) を暗号化します。QVD は、[*Encryption key*] (暗号化キー) 入力項目に示されている暗号化キーを使用して暗号化されます。 データファイルは保存の際に暗号化されます。QVD 暗号化が有効になる前に作成されたデータファイルは、次にデータが保存される際に暗号化されます。
Encryption key (暗号化キー)	Qlik Sense アプリおよび Qlik Sense データファイルの暗号化に使用される暗号化キー。これは、暗号化証明書の [*Thumbprint*] (サムプリント) フィールドです。

なりすまし

なりすましのプロパティ

プロパティ	説明
[**タスクのリロード**]	[**タスクのリロード**] を選択すると、借用が有効になります。借用により、アプリの所有者の権限を使用してリロードタスクを実行できるようになります。タスクチェーン内において、アプリは異なる所有者およびソースに対する権限を有することができますが、これは各所有者個人のアクセス権に依存します。 [**タスクのリロード**] が選択解除された場合、内部システム アカウントの代表として実行するリロードタスク、*sa_scheduler* の権限が昇格されるため、技術的にはあらゆるデータソースを使用できます。

Help us improve (改善へのご協力のお願い)

改善へのご協力のお願いのプロパティ

プロパティ	説明
データ コレクション	製品とサービスを向上させるため、Qlik はシステムおよび使用状況のデータを収集します。データは匿名化され、個人データは含まれません。 [データ コレクション] はインストール手順におけるチェック ボックスで、既定で選択されています。つまりQlik はデータを収集するように設定されています。[**データ コレクション**] の選択を解除することにより、インストール中とインストール後のどちらにおいてもデータが Qlik に送信されないようにすることができます。QMC でデータ コレクションの設定を変更するには、一定の権限が必要です。

ノード

ノードは構成済みの Qlik Sense サービスを使用しているサーバーです。どの実装にも必ずセントラル ノードがあり、異なるサービスの構成用にノードを追加できます。どのノードにも必ずリポジトリがあります。

Qlik Sense のサイトは、共通の論理リポジトリあるいはセントラル ノードに接続された 1 つ以上のサーバー マシン (ノード) の集まりです。

Shared Persistence マルチ ノード環境を設置している場合、1 つ以上のノードをフェールオーバー候補にすることができます。セントラル ノードでエラーが発生すると、フェールオーバー候補がセントラル ノードのロールを担います。

[**ノード**] 概要では利用可能なノードがすべて一覧表示されています。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター ( ) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

ノードのプロパティ

プロパティ	説明
名前	ノードの名前。
[**ホスト名**]	ホストの名前。
[**セントラル ノード**]	ステータス値:**Yes** または **No** ノードがセントラル ノードの場合、[**Yes**] が表示されます。
[**状態**]	サービスの状態が表示されます。次のテキストのいずれかが表示されます。 • **(x)/(y) 件のサービスが実行中** ノード上で有効なサービス (y) 件に比べて、(x) 件のサービスが実行中です。 • **(x)/(y) 件のサービスが停止** ノード上で有効なサービス (y) 件に比べて、(x) 件のサービスが停止しています。 • **(z) が停止** 停止したサービス (z) の名前です (1 つのサービスのみが停止した場合)。 *データ マネージャーでテーブルの in the **Status** column for more detailed information on the status of the node.*
タグ	ノードに紐付けされているタグ。
[**ノードの目的**]	ノードの使用目的: [**実稼働環境**]、[**開発環境**]、または [**両方**]。

プロパティ	説明
[エンジン]	ステータス値:**Yes** または **No** **Yes**:Qlik Sense Engine Service (QES) はアクティブです。
[プロキシ]	ステータス値:**Yes** または **No** **Yes**:Qlik Sense Proxy Service (QPS) はアクティブです。
[印刷]	ステータス値:**Yes** または **No** **Yes**:Qlik Sense Printing Service (QPR) はアクティブです。
[スケジューラ]	ステータス値:**Yes** または **No** **Yes**:Qlik Sense Engine Service (QSS) はアクティブです。
[**ID**]	ノードの ID。
[作成日時]	ノードが作成された日時。
[最終変更日]	ノードが最後に変更された日時。
[変更者]	ノードを最後に変更した者。
[<カスタム プロパティ>]	カスタム プロパティがある場合はここに一覧表示されます。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション[**Select all rows**]は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション[**Deselect all rows**]はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。

プロパティ	説明
🔍	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
🔄	ページを更新します。
[**編集**]	選択したノードを編集します。
[**削除**]	選択したノードを削除します。
[**再配置**]	選択したノードを再配置します。
⊕**新規作成**	新しいノードを作成します。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

ノード: 関連するアイテム

次の関連アイテムはノードで利用できます。

ユーザー アクセス

[**ユーザー アクセス**] は、リソースを編集する際に [**関連するアイテム**] から利用できます。

プレビューには、ターゲット リソースと選択したアイテムにアクセスできるソース ユーザーが表示されます。

権限に応じて、ユーザーやリソース、関連するルールを編集したり、表示することができます。

エンジン

Qlik Sense Engine Service (QES) は、アプリケーションのすべての計算とロジックを処理するアプリケーション サービスです。

[**エンジン**] の概要では、利用可能なエンジンがすべて一覧表示されています。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (▦) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

エンジン *ノード*のプロパティ

プロパティ	説明
ノード	エンジン *ノード*の名前。
ステータス	次のテキストのいずれかが表示されます。 • **実行中** サービスは正常に実行中です。 • **停止** サービスは停止されました。 • **無効化** サービスは無効になっています。 *状態の詳細については、[**状態**] 列で ⓘ をクリックしてください。* *Qlik Sense サービスの状態を確認する (page 375)*。
タグ	エンジンに紐付けされているタグ。
[**アプリ自動保存間隔 (秒)**]	アプリの自動保存間の秒数。自動保存は常にセッションの最後に実行されます。 データ以外はすべて保存されます。データを持続化するには、データ ロード エディター でリロードを実行します。
[**アプリのキャッシュ時間 (秒)**]	アプリを使用していた最後のセッションが終了した後、Qlik Sense アプリがメモリに残存できる時間 (秒数)。
[**作業フォルダ**]	関連パスがファイルの場所を決めるために使用される場合、予定されたリロードは、このディレクトリのファイルを検索します。 *この設定は、リロード中のファイルへの相対パス向けの QlikView スクリプトでレガシー機能に対応するために使用されます。この設定を使用して、アプリが保存されているディレクトリを変更することはできません。*
[**元に戻す最高回数**]	シート、オブジェクト、ブックマーク、ストーリーなどのアプリコンテンツを編集する場合の元に戻す最大回数: 最小 = 0、最大 = 999。
[**パフォーマンス ログ間隔 (分)**]	パフォーマンスのログ エントリの間隔時間 (分数)。
[**監査アクティビティ ログ レベル**]	レベル: [**オフ**] または [**基本**] (制限的なエントリ)
[**サービス ログ レベル**]	[**エラー**] から [**デバッグ**] までの各レベルには前のレベルよりも多くの情報が含まれます。

プロパティ	説明
[**システム ログ レベル**]	標準的なエンジン メッセージはすべて、このロガーに保存されます。 [**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
[**パフォーマンス ログ レベル**]	パフォーマンス メッセージはすべて、このロガーに保存されます (既定では 5 分ごとに更新)。ログにはアクティブ ユーザー数、開いているセッションの数、CPU ロードなどが含まれます。 [**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
[**QIX パフォーマンス ログ レベル**]	QIX プロトコルのパフォーマンス メッセージはすべて、このロガーに保存されます。 [**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
[**監査ログ レベル**]	ユーザーがアプリで選択する場合など、ユーザーベースの詳細 メッセージはこのロガーに保存されます。[**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
[**セッション ログ レベル**]	クライアント セッションが終了すると、ユーザー情報、マシン ID、IP アドレス、ポート番号などすべてのセッション メッセージがこのロガーに保存されます。[**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
[**トラフィック ログ レベル**]	エンジンへの JSON メッセージやエンジンからの JSON メッセージなど、すべてのトラフィック メッセージはこのロガーに保存されます。[**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
分析接続ログ レベル	分析接続 メッセージはすべて、このロガーに保存されます。[**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
[**データ系統を許可**]	ステータス値:**Yes** または **No** データ系統とは Qlik Sense にロードされたデータの元です。
[**最小 メモリ使用量**]	Qlik Sense によって使用される最小 メモリ容量。
[**最大 メモリ使用量**]	Qlik Sense によって使用される最大 メモリ容量。
[**CPU 調整**]	Qlik Sense が使用する CPU 容量。範囲: 0~100%
[**標準 モード**]	ステータス値: [**Yes**]: 標準 モード[**No**]: レガシー モード セキュリティ上の理由から、Qlik Sense の標準 モードでは、データ ロード スクリプトまたは関数、変数に含まれる絶対 パスや相対 パスはサポートされていません。これは、ファイル システムが露呈されてしまうからです。 *ただし、標準 モードを無効にすると、ファイル システムが露呈するためセキュリティ リスクが生じます。*
[**HTTP コール バック ポート**]	このコールバック ポートは、エンジンに HTTP イベントを送信するために、Qlik Sense Repository Service で使用されます。

プロパティ	説明
[**ハイパーキューブ計算に使用するメモリに対する制限 (バイト)**]	リクエスト中にハイパーキューブ (超立方体) 評価が割り当てることのできるメモリの制限です。リクエストで複数のハイパーキューブが計算されている場合、この制限はハイパーキューブの各計算に対し個別に適用されます。 この制限はあらゆる割り当てに対して強制されるのではありません。「**0**」に設定すると、エンジンは全体にヒューリスティック手法を適用し、計算に多くのメモリを要する同時実行のリクエストの数を制限します。 負の値を指定すると、制限は無効になります。 パフォーマンス上の理由から、メモリの使用/制限は、割り当てごとにではなく、定期的にチェックされます。そのため、場合によっては一時的に制限を超過することがあります。
[**メモリのリロードで使用されるメモリに対する制限 (バイト)**]	リロード リクエストに割り当てるメモリの制限です。 負の値または 0 を指定すると、制限は行われなくなります。 パフォーマンス上の理由から、メモリの使用/制限は、割り当てごとにではなく、定期的にチェックされます。そのため、場合によっては一時的に制限を超過することがあります。
[**エクスポートに使用するメモリに対する制限 (バイト)**]	データ エクスポートのリクエストの中で、エクスポートが割り当てることのできるメモリの制限です。計算に起因する割り当てはこの制限の対象になりません。 負の値または 0 を指定すると、制限は無効になります。 パフォーマンス上の理由から、メモリの使用/制限は、割り当てごとにではなく、定期的にチェックされます。そのため、場合によっては一時的に制限を超過することがあります。
[**ハイパーキューブに対する時間制限 (秒)**]	ハイパーキューブ計算で使用できる単一コア CPU 稼動時間を制限します。この単一コア CPU 稼動時間は、ヒューリスティック手法による CPU 消費時間の概算 (CPU 消費時間を計算時に使用されたコア数で除算したもの) です。これはハード リミットではなく、処理される計算の複雑さに依存します。 負の値または 0 を指定すると、制限は行われなくなります。 パフォーマンス上の理由から、CPU 時間に対する厳密な追跡は行われません。
[**エクスポートに対する時間制限 (秒)**]	データ エクスポートのリクエストで、エクスポート処理に許可される CPU 時間の制限です。 負の値または 0 を指定すると、制限は行われなくなります。
[**リロードに対する時間制限 (秒)**]	リロード リクエストで使用できる CPU 時間を制限します。 負の値または 0 を指定すると、制限は行われなくなります。
[**リロード中に検索インデックスを作成します。**]	ステータス値:**Yes** または **No** 選択すると、サーバー上のアプリがすべてリロード中にインデックス化され、最初の検索セッションの性能が向上します。

プロパティ	説明
ID	エンジンの ID。
[**作成日時**]	エンジンが作成された日時。
[**最終変更日**]	エンジンが最後に変更された日時。
[**変更者**]	エンジンを最後に変更した者。
[**<カスタム プロパティ>**]	カスタム プロパティがある場合はここに一覧表示されます。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
[**編集**]	選択したエンジンを編集します。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

Printing

Qlik Sense Printing Service (QPR) は、Qlik Sense のエクスポートを管理します。

[**印刷**] 概要では利用可能な印刷ノードがすべて一覧表示されています。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (⊞) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

利用可能な項目とボタン

項目	詳細
ノード	印刷ノードの名前
[状態]	次のテキストのいずれかが表示されます。 • **実行中** サービスは正常に実行中です。 • **停止** サービスは停止されました。 • **無効化** サービスは無効になっています。 *状態の詳細については、[状態] 列で ⓘ をクリックしてください。* *Qlik Sense サービスの状態を確認する (page 375)*。
[タグ]	印刷サービスに紐付けされているタグ。
[監査アクティビティログ レベル]	[**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
[サービス ログ レベル]	[**エラー**] から [**デバッグ**] までの各レベルには前のレベルよりも多くの情報が含まれます。
[ID]	印刷サービスの ID
[作成日時]	印刷サービスが作成された日時
[最終変更日]	印刷サービスが最後に変更された日時
[変更者]	印刷サービスを最後に変更した者

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

プロキシ

Qlik Sense Proxy Service (QPS) は、Qlik Sense の認証、セッション ハンドリング、負荷分散を管理します。

[**プロキシ**] 概要では利用可能なプロキシがすべて一覧表示されます。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (⊞) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

ノードのプロパティ

プロパティ	詳細
ノード	プロキシ ノードの名前。
状態	次のテキストのいずれかが表示されます。 • **実行中** サービスは正常に実行中です。 • **停止** サービスは停止されました。 • **無効化** サービスは無効になっています。 *状態の詳細については、[**状態**] 列で ⓘ をクリックしてください。* *Qlik Sense サービスの状態を確認する (page 375)*。
タグ	プロキシに紐付けされているタグ。
サービスの待ち受けポート HTTPS (既定)	既定のプロキシのセキュアな待ち受けポートで、Qlik Sense 通信をすべて管理します。 *ポート443 は他のソフトウェア (Web サーバーなど) によって使用されることがあるため、Qlik Sense Proxy Service (QPS) がこのポートを使用できることを確認してください。*
HTTP 許可	ステータス値:**Yes** または **No** **有効化する**: 暗号化されていない通信を許可します。これは、両方の https (セキュア通信) と (http) の暗号化されていない通信が許可されることを意味しています。

プロパティ	詳細
サービスの待ち受けポート HTTP	非暗号化待ち受けポート、HTTP 接続が許可されている場合に使用されます。
認証の待ち受けポート	内部認証モジュールの待ち受けポート。 *管理者権限のないユーザーとしてこのポートを編集する場合、変更を有効にするには、起動モードでレポジトリを実行する必要があります。*
Kerberos 認証	ステータス値:**Yes** または **No** **有効化する**: Kerberos 認証を有効にします。
REST API 待ち受けポート	プロキシ API の待ち受けポート。 *管理者権限のないユーザーとしてこのポートを編集する場合、変更を有効にするには、起動モードでレポジトリを実行する必要があります。*
SSL ブラウザ証明書捺印 (署名)	ブラウザからプロキシへのトラフィックの暗号化を扱う、セキュア ソケット レイヤー (SSL) 証明書の捺印。プロキシ証明書および管理者権限のないアカウントでの Qlik Sense サービス実行を編集する場合、以下のように証明書にプライベートキーのアクセス許可を設定する必要があります。
Keep-alive タイムアウト (秒)	接続が切断されるまでの 1 回の HTTP/HTTPS リクエストの最大タイムアウト時間。DoS 攻撃 (サービス拒否攻撃) に対する防御。リクエストがこの時間を超過した場合は、Qlik Sense プロキシによって接続が切断されることを意味しています。ユーザーが接続の遅さと接続の切断で困っている場合は、この値を増やしてください。
ヘッダーの最大サイズ (バイト)	ヘッダーの最大合計サイズ。
最大ヘッダー行数	最大ヘッダー行数。
監査アクティビティ ログ レベル	レベル: [**オフ**] または [**基本**] (制限的なエントリ)
監査セキュリティ ログ レベル	レベル: [**オフ**] または [**基本**] (制限的なエントリ)
サービス ログ レベル	[**エラー**] から [**デバッグ**] までの各レベルには前のレベルよりも多くの情報が含まれます。

プロパティ	詳細
監査ログ レベル	プロキシの呼び出しなど、より詳細なユーザーベース メッセージはこのロガーに保存されます。 [**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
パフォーマンス ログ レベル	パフォーマンス カウンター、および接続、ストリーム、セッション、チケット、ウェブ ソケットの数、負荷分散情報などです。パフォーマンス メッセージはすべて、このロガーに保存されます。 [**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
セキュリティ ログ レベル	証明書メッセージはすべて、このロガーに保存されます。 [**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
システム ログ レベル	標準的なプロキシ メッセージはすべて、このロガーに保存されます。 [**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
パフォーマンス ログ間隔 (分)	パフォーマンス ログの間隔。
ID	プロキシの ID。
作成日時	プロキシが作成された日時。
最終変更日	プロキシが最後に変更された日時。
変更者	プロキシを最後に変更したユーザー。
<Custom properties>	カスタム プロパティがある場合はここに一覧表示されます。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*

プロパティ	詳細
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
編集	選択したプロキシを編集します。
アイテムをさらに表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

プロキシ: 関連するアイテム

次の関連アイテムはプロキシで利用できます。

仮想プロキシ

[**仮想プロキシ**] プロパティグループには、Qlik Sense システムの仮想プロキシのプロパティが含まれています。

仮想プロキシのプロパティ

プロパティ	説明
[**説明**]	仮想プロキシの名前。
[**プレフィックス**]	各追加パスを定義するプロキシの URI のパス名。例: *https://[node]/prefix/*
[**セッション クッキー ヘッダー名**]	セッション クッキーのために使用される HTTP ヘッダー名。この値は必須で、空欄のままにはできません。 *February 2019 以降のリリースは、ユーザーが http を介してシステムにアクセスすると、セッションの Cookie ヘッダー名にサフィックス (-HTTP) が付加されます。* *クッキー名のサフィックスとして、上記のプレフィックス プロパティの値が含まれていると、役に立ちます。*

[**既定の仮想プロキシ**]	ステータス値:**Yes** または **No**
[**カスタム プロパティ**]	カスタム プロパティがある場合はここに一覧表示されます。

仮想プロキシ

1 つ以上の仮想プロキシが各 Qlik Sense Proxy Service (QPS) で実行され、複数のサイトの認証、セッションの処理、シングル プロキシ ノードの負荷分散方法をサポートできるようにします。

[**仮想プロキシ**] 概要では利用可能な仮想プロキシがすべて一覧表示されます。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (▦) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

仮想プロキシ

項目/ボタン	**説明**
説明	仮想プロキシの名前。
プレフィックス	各追加パスを定義するプロキシの URI のパス名。プレフィックスでは小文字のみを使用できます。
セッション クッキー ヘッダー名	セッション クッキーのために使用される HTTP ヘッダー名。 *February 2019 以降のリリースは、ユーザーが http を介してシステムにアクセスすると、セッションの Cookie ヘッダー名にサフィックス (-HTTP) が付加されます。*
既定の仮想プロキシ	ステータス値:**Yes** または **No**
認証方法	• [**Ticket**]: チケットは認証に使用されます。 • [**ヘッダー認証静的ユーザー ディレクトリ**]: 静的ヘッダー認証を許可します。QMC でユーザー ディレクトリを設定します。 • [**ヘッダー認証動的ユーザー ディレクトリ**]: 動的ヘッダー認証を許可します。ヘッダーからユーザー ディレクトリの情報を取得します。 • SAML:SAML2 は認証に使用されます。 • JWT:JSON Web Token は認証に使用されます。 • OIDC:OpenID Connect は認証に使用されます。
プロキシ サービスへリンク	ステータス値:**Yes** または **No**
タグ	仮想プロキシに紐付けされているタグ。

ヘッダー認証静的ユーザーディレクトリ	ヘッダー認証を受けたユーザーの追加情報を取得できるユーザーディレクトリ名。
ヘッダー認証動的ユーザーディレクトリ	ヘッダー認証を受けたユーザーの追加情報を取得できるユーザーディレクトリの認証に使用するパターン。
匿名アクセスモード	3 つの絞込値: • **匿名ユーザーを拒否**: ユーザは、ユーザ ID と資格情報を指定する必要があります。 • **匿名ユーザーを許可**: ユーザは匿名で入力しますが、ユーザアカウントで切り替えてログインすることができます。 • **常に匿名ユーザー**: ユーザーは常に匿名です。
Windows 認証パターン	ログイン用に選択された認証パターン。User-Agent ヘッダーに Windows 認証パターン文字列が含まれている場合、Windows 認証が使用されます。一致する文字列がない場合は、フォーム認証が使用されます。
セッション Cookie ドメイン	既定では、プロキシがインストールされたマシンに対してのみ、セッション Cookie が有効です。この (オプションの) プロパティであれば、より大きいドメインへの有効性を高められます。例: `company.com`
[**Secure 属性あり (https)**]	Secure 属性を持ち、https を使用するセッション クッキー用のオプション。
[**SameSite 属性 (https)**]	https 用の SameSite 属性値: **属性なし**、**None**、**Lax**、**Strict** 詳しくは「*SameSite クッキー属性 (page 165)*」を参照してください。
[**Secure 属性あり(http)**]	Secure 属性を持ち、http を使用するセッション クッキー用のオプション。
[**SameSite 属性 (http)**]	http 用の SameSite 属性値: **属性なし**、**None**、**Lax**、**Strict** 詳しくは「*SameSite クッキー属性 (page 165)*」を参照してください。

追加の応答ヘッダー	クライアントに返す HTTP 応答すべてに付加されるヘッダー。例:
	`Header1: value1`
	`Header2: value2`

タイムアウトまでのセッションアイドル時間(分)	タイムアウトするまでのアイドル状態の最大時間。この時間が経過すると、セッションは無効となり、ユーザーはシステムからログアウトされます。
拡張セキュリティ環境	ステータス値:**Yes** または **No** **有効化する**: クライアント環境についての情報(OS、デバイス、ブラウザー、IP) は、セキュリティヘッダーで送信されます。 **無効にする**: ユーザーは、同じエンジンセッションを複数のデバイスで同時に実行できます。
SAML メタデータ IdP	IdP からのメタデータで、サービスプロバイダーを構成する際に使用します。使用するには SAML 認証に存在している必要があります。
SAML エンティティ ID	サービスプロバイダーを識別する ID。ID は一意にする必要があります。
ユーザー ID に使用する SAML 属性	ユーザー ID を説明する属性の SAML 属性名。
ユーザーディレクトリに使用する SAML 属性	ユーザーディレクトリを説明する属性の SAML 属性名。
SAML署名アルゴリズム	署名 SAML 要求に使用されるハッシュアルゴリズム。SHA-256 を使用するには、関連する秘密キーのプロバイダーが「Microsoft Enhanced RSA and AES Cryptographic Provider」である第三者機関の証明書が必要となります。
ユーザー ID に使用する JWT 属性	ユーザー ID を説明する属性の JWT 属性名。
ユーザーディレクトリに使用する JWT 属性	ユーザーディレクトリを説明する属性の JWT 属性名。名前の値がかっこ内にある場合、その値はコンテンツの属性値として使用されます。[例] では定数属性値「例」を提供しています。
対象オーディエンス (オーディエンス属性)	対象オーディエンスはトークンの受信者です。オーディエンス値は文字列であり、通常は https://qlik.com などのアクセスされているリソースのベースアドレスです。
SAMLシングル ログアウト	SAML シングル ログアウトのサービスプロバイダー開始フローを有効にします。有効にした場合、IdP メタデータファイルにログアウト URI が含まれていることを確認してください。また、メタデータファイルを再生成し、IdP 構成を更新する必要があります。
オプションの OIDC属性を無効化	ユーザーディレクトリコネクタを介してユーザーを同期する場合にのみ使用します。選択されている時は、ユーザーディレクトリコネクタの同期から送られてくる**名前**、**グループ**、**メール**、**画像**の属性が、OIDC からの属性で上書きされないように保護されます。

OpenID Connectメタデータ URI	OpenID Connect プロトコルを使用して ID プロバイダとやり取りする OAuth クライアントに関して、構成情報を提供するエンドポイントへの URL。
クライアント ID	ユーザ認証用に ID プロバイダーで設定されたクライアントの ID。
領域	ID プロバイダーに関連付ける名前で、マルチクラウドでの名前の一貫性に使用されます。
サブジェクト	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。 サブジェクト属性値の形式が*domainname\username*の場合、**realm**はオプションです。そうでない場合、**realm** は必須です。
名前	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。
グループ	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。
電子メール	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。
client_Id	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。
写真	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。
スコープ	アクセス トークンの発行時にアクセス権限を指定するために、OAuth 2.0 の仕様で使用されます。たとえば、ID プロバイダでユーザー グループ機能をサポートするためにグループ スコープが必要な場合は、このオプションを使用してグループ スコープを追加します。
ID	仮想プロキシの ID。
作成日時	仮想プロキシが作成された日時。
最終変更日	仮想プロキシが最後に変更された日時。
変更者	仮想プロキシを最後に変更した者。
<カスタム プロパティ>	カスタム プロパティがある場合はここに一覧表示されます。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。

	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
編集	選択した仮想プロキシを編集します。
削除	選択した仮想プロキシを削除します。
SP メタデータのダウンロード	ID プロバイダーからユーザー構成データをダウンロードします。情報は IdP メタデータとして利用できます。ユーザーはこのメタデータをダウンロードして、サービス プロバイダー (Qlik Sense) に提供できます。メタデータは QMC からアップロードして、テキスト項目 (samlMetadataIdP) としてデータベース (VirtualProxyConfig table) に保存できます。
[**新規作成**]	仮しい仮想プロキシを作成します。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

仮想プロキシ: 関連するアイテム

以下の関連アイテムは仮想プロキシで利用できます。

プロキシ

Qlik Sense Proxy Service (QPS) は、Qlik Sense の認証、セッション ハンドリング、負荷分散を管理します。

プロキシのプロパティ

プロパティ	説明
ノード	プロキシ名。
状態	次のテキストのいずれかが表示されます。 • **実行中** サービスは正常に実行中です。 • **停止** サービスは停止されました。 • **無効化** サービスは無効になっています。 *状態の詳細については、[**状態**] 列で をクリックしてください。* *Qlik Sense サービスの状態を確認する (page 375)*。
サービスの待ち受けポート HTTPS (既定)	既定のプロキシのセキュアな待ち受けポートで、Qlik Sense 通信をすべて管理します。 *ポート443 は他のソフトウェア (Web サーバーなど) によって使用されることがあるため、Qlik Sense Proxy Service (QPS) がこのポートを使用できることを確認してください。*
HTTP 許可	ステータス値:**Yes** または **No** **有効化する**: 暗号化されていない通信を許可します。これは、両方の https (セキュア通信) と (http) の暗号化されていない通信が許可されることを意味しています。 *February 2019 以降のリリースは、ユーザーが http を介してシステムにアクセスすると、セッションの Cookie ヘッダー名にサフィックス (-HTTP) が付加されます。*
サービスの待ち受けポート HTTP	非暗号化待ち受けポート、HTTP 接続が許可されている場合に使用されます。

プロパティ	説明
認証の待ち受けポート	内部認証モジュールの待ち受けポート。 *管理者権限のないユーザーとしてこのポートを編集する場合、変更を有効にするには、起動モードでレポジトリを実行する必要があります。*
Kerberos 認証	ステータス値:**Yes** または **No** **有効化する**: Kerberos 認証を有効にします。
REST API 待ち受けポート	プロキシ API の待ち受けポート。 *管理者権限のないユーザーとしてこのポートを編集する場合、変更を有効にするには、起動モードでレポジトリを実行する必要があります。*
SSL ブラウザ証明書捺印 (署名)	ブラウザからプロキシへのトラフィックの暗号化を扱う、セキュア ソケット レイヤー (SSL) 証明書の拇印。プロキシ証明書および管理者権限のないアカウントでの Qlik Sense サービス実行を編集する場合、以下のように証明書にプライベートキーのアクセス許可を設定する必要があります。
Keep-alive タイムアウト (秒)	接続が切断されるまでの 1 回の HTTP/HTTPS リクエストの最大タイムアウト時間。DoS 攻撃 (サービス拒否攻撃) に対する防御。リクエストがこの時間を超過した場合は、Qlik Sense プロキシによって接続が切断されることを意味しています。ユーザーが接続の遅さと接続の切断で困っている場合は、この値を増やしてください。
ヘッダーの最大サイズ (バイト)	ヘッダーの最大合計サイズ。
最大ヘッダー行数	最大ヘッダー行数。
監査アクティビティ ログ レベル	レベル: [**オフ**] または [**基本**] (制限的なエントリ)
監査セキュリティ ログ レベル	レベル: [**オフ**] または [**基本**] (制限的なエントリ)
サービス ログ レベル	[**エラー**] から [**デバッグ**] までの各レベルには前のレベルよりも多くの情報が含まれます。
監査ログ レベル	プロキシの呼び出しなど、より詳細なユーザーベース メッセージはこのロガーに保存されます。 [**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。

プロパティ	説明
パフォーマンス ログ レベル	パフォーマンス メッセージはすべて、このロガーに保存されます。パフォーマンス カウンター、および接続、ストリーム、セッション、チケット、ウェブ ソケットの数、負荷分散情報などです。 [**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
セキュリティ ログ レベル	証明書メッセージはすべて、このロガーに保存されます。 [**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
システム ログ レベル	標準的なプロキシ メッセージはすべて、このロガーに保存されます。 [**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
パフォーマンス ログ間隔 (分)	パフォーマンス ログの間隔。
ID	プロキシの ID。
作成日時	プロキシが作成された日時。
最終変更日	プロキシが最後に変更された日時。
変更者	プロキシを最後に変更したユーザー。
<Custom properties>	カスタム プロパティがある場合はここに一覧表示されます。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
編集	選択したプロキシを編集します。
リンクの解除	選択したプロキシからプロキシ サービスのリンクを解除します。 *仮想プロキシを機能させるためにはプロキシ サービスにリンクさせる必要があります。*
リンク	選択したプロキシにプロキシ サービスをリンクします。
アイテムをさらに表示	既定の概要では、アイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more items**] をクリックします。アイテムの並べ替えやフィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

SameSite クッキー属性

SameSite クッキー属性は、ブラウザーがファーストパーティクッキーとサードパーティクッキーの処理方法を識別するために使用します。SameSite 属性の目的は、Web ユーザーのプライバシー権を保護し、クロスサイト リクエスト フォージェリ(CSRF/XSRF) のリスクを減らすことです。CSRF は、Web サイトの悪用の一種で、Web アプリケーションが信頼しているユーザーから不正なコマンドが送信されます。

Chrome 80 リリースでは、SameSite クッキー属性が既定でオンになりました。Microsoft Edge、Firefox、Safari など他のブラウザーも SameSite クッキーに対応していますが、機能が既定で常にオンになっているわけではありません。

SameSite 属性の値

SameSite には、異なるセキュリティレベルの 3 つの値があります。

- Strict: ブラウザーは、ターゲット ドメインと同じドメイン/サイトから送信されているリクエストにのみクッキーを送信します。これによって CSRF 攻撃を阻止します。
- Lax 送信元サイトを制限しませんが、ターゲット ドメインがクッキー ドメインと同じであることを強制します。これによってクロスサイト クッキーを阻止します。
- なし: クッキーを意図的にサードパーティのコンテキストで送信することを明確に示します。

このコンテキストにおけるサイトはドメインのサフィックスで、直前のドメインの一部です。Web サイト https://help.qlik.com の場合、qlik.com がサイトと見なされます。

Chrome 80 以降では、SameSite 値が宣言されていないクッキーの既定値は SameSite=Lax に設定されます。これは、値 None を明示的に設定してオプトアウトしない限り、クッキーはファーストパーティのコンテキストでのみ自動的に送信されるということを意味します。

セキュアな接続からのアクセスである場合にのみ、`SameSite=None; Secure` 設定のクッキーを外部アクセスに利用できます。

Qlik Sense: KB 931125 のインストール後、SameSite 属性がないとChrome 80 でリクエストがブロックされるようになり、今後のブラウザーで SSL/TLS 通信の問題が発生する

スケジューラ

Qlik Sense Engine Service (QSS) はスケジュール済みのタスク(Qlik Sense アプリまたはユーザー同期化のリロード)とタスク チェーンを管理します。Qlik Sense の実装のタイプにより、QSS は、マネージャーとして、あるいはワーカーとして、あるいはその両方として、ノード上で稼働します。

[**スケジューラ**] 概要には、利用可能なスケジューラがすべて一覧表示されます。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター ( ) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

ノードのプロパティ

プロパティ	説明
ノード	スケジューラ ノードの名前。
ステータス	次のテキストのいずれかが表示されます。 • **実行中** サービスは正常に実行中です。 • **停止** サービスは停止されました。 • **無効化** サービスは無効になっています。 *状態の詳細については、[**状態**] 列で をクリックしてください。* *Qlik Sense サービスの状態を確認する (page 375)*。
タグ	スケジューラーに紐付けされているタグ。
タイプ	• [**マネージャー**]: サイト内のワーカー QSS にタスクを送信します。 • [**ワーカー**]: マネージャー QSS からタスクを受け取り、タスクを実行します。 • [**マネージャーとワーカー**]: シングル ノード サイトで、マネージャー QSS がワーカー QSS としても機能する場合。
[**同時実行リロード最大数**]	リロード最大数、スケジューラは複数のリロードを同時に実行できます。
[**エンジン タイムアウト (分)**]	[**同時実行リロード最大数**] に達する (個別のプロパティ参照) と、エンジンの新規プロセス開始要求が、稼働中のリロードプロセス数を待機しているキューに置かれて、[**同時実行リロード最大数**] を下回ります。上記が特定の時間内に起こらなかった場合、エンジンの新規プロセス開始要求はキューから削除されます。
[**監査アクティビティ ログ レベル**]	ユーザー関連アクションはこのログーに保存されます。 レベル: [**オフ**] または [**基本**] (制限的なエントリ)
[**サービス ログ レベル**]	[**エラー**] から [**デバッグ**] までの各レベルには前のレベルよりも多くの情報が含まれます。
[**アプリケーション ログ レベル**]	スケジューラ サービスのアプリケーション メッセージはすべて、このログーに保存されます。 [**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。

プロパティ	説明
[**監査ログ レベル**]	詳細な ユーザー ベース メッセージ はこのロガーに保存 されます。 [**Fatal**] から[**Debug**] までの各 レベルには前のレベルよりも多 くの情報 が含 まれます。
[**パフォーマンス ログ レベル**]	パフォーマンス メッセージはすべて、このロガーに保存 されます。 [**Fatal**] から[**Debug**] までの各 レベルには前のレベルよりも多 くの情報 が含 まれます。
[**セキュリティ ログ レベル**]	セキュリティ関連 メッセージはこのロガーに保存 されます。 [**Fatal**] から[**Debug**] までの各 レベルには前のレベルよりも多 くの情報 が含 まれます。
[**システム ログ レベル**]	標準的なスケジューラ メッセージはすべて、このロガーに保存 されます。 [**Fatal**] から[**Debug**] までの各 レベルには前のレベルよりも多 くの情報 が含 まれます。
[**タスク実行 ログ レベル**]	タスク実行 メッセージはすべて、このロガーに保存 されます。 [**Fatal**] から[**Debug**] までの各 レベルには前のレベルよりも多 くの情報 が含 まれます。
ID	スケジューラの ID。
[**作成日時**]	スケジューラが作成 された日時。
[**最終変更日**]	スケジューラが 最後に変更 された日時。
[**変更者**]	スケジューラを 最後に変更したユーザー。
[**<カスタム プロパティ>**]	カスタム プロパティがある場合はここに一覧表示 されます。
▼▲	リストを昇順 または降順で並べ替 えます。並べ替 えをサポートしない列 もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*

プロパティ	説明
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション[**Select all rows**]は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション[**Deselect all rows**]はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
[**編集**]	選択したスケジューラを編集します。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**]をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl]キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

リポジトリ

Qlik Sense Repository Service (QRS) は、Qlik Sense アプリ、ライセンス、セキュリティ、サービス構成データの持続性と同期を管理します。QRS は Qlik Sense Repository Database に付属し、Qlik Sense アプリを稼働および提供するその他すべての Qlik Sense サービスで必要です。さらに、QRS には Qlik Sense アプリの構造およびバイナリファイル (ローカル ファイル システムに保存されているアプリのデータ) へのパスが保存されています。

[**リポジトリ**] 概要では利用可能なリポジトリがすべて一覧表示されます。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター ( ) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

ノードのプロパティ

プロパティ	詳細
ノード	レポジトリ ノードの名前。
[状態]	次のテキストのいずれかが表示されます。 • 実行中 サービスは正常に実行中です。 • 停止 サービスは停止されました。 • 無効化 サービスは無効になっています。 状態の詳細については、[状態] 列で をクリックしてください。 *Qlik Sense サービスの状態を確認する (page 375)*。
[監査アクティビティ ログ レベル]	レベル: [オフ] または [基本] (制限的なエントリ)
監査セキュリティ ログ レベル	レベル: [オフ] または [基本] (制限的なエントリ)
[サービス ログ レベル]	[エラー] から [デバッグ] までの各レベルには前のレベルよりも多くの情報が含まれます。
[アプリケーション ログ レベル]	リポジトリ サービスのあらゆるアプリケーション メッセージがこのロガーに保存されます。 [Fatal] から [Debug] までの各レベルには前のレベルよりも多くの情報が含まれます。
[監査ログ レベル]	セキュリティ ルールの情報など、詳細なユーザー ベース メッセージはこのロガーに保存されます。 [Fatal] から [Debug] までの各レベルには前のレベルよりも多くの情報が含まれます。
[ライセンス ログ レベル]	ライセンス メッセージはすべて、このロガーに保存されます。トークンの使用やユーザー アクセスの割当などです。レベル: [情報] または [デバッグ]
Qlik Management Console(QMC) ログ レベル	QMC メッセージはすべて、このロガーに保存されます。 [Fatal] から [Debug] までの各レベルには前のレベルよりも多くの情報が含まれます。
[パフォーマンス ログ レベル]	リポジトリ サービスのパフォーマンス メッセージはすべて、このロガーに保存されます。 [Fatal] から [Debug] までの各レベルには前のレベルよりも多くの情報が含まれます。
[セキュリティ ログ レベル]	証明書メッセージはすべて、このロガーに保存されます。 [Fatal] から [Debug] までの各レベルには前のレベルよりも多くの情報が含まれます。
[同期 ログ レベル]	マルチノード環境の同期情報はすべて、このロガーに保存されます。 [Fatal] から [Debug] までの各レベルには前のレベルよりも多くの情報が含まれます。

プロパティ	詳細
[**システム ログ レベル**]	標準的なリポジトリ メッセージはすべて、このロガーに保存されます。 [**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
[**ユーザー管理 ログ レベル**]	ユーザー同期メッセージはすべて、このロガーに保存されます。 [**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
タグ	レポジトリに紐付けされているタグ。
[**ID**]	リポジトリの ID。
[**作成日時**]	リポジトリが作成された日時。
[**最終変更日**]	リポジトリが最後に変更された日時。
[**変更者**]	リポジトリを最後に変更したユーザー。
[**<カスタム プロパティ>**]	カスタム プロパティがある場合はここに一覧表示されます。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
[**編集**]	選択したリポジトリを編集します。

プロパティ	詳細
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

負荷分散ルール

[**負荷分散ルール**] の概要には、利用可能な負荷分散ルールがすべて列記されています。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター ( ) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

負荷分散ルール プロパティ

プロパティ	説明
名前	ルール名。生成されたルールの名前の構文は、[resource type]_[access type]_[resource name] となっています。
説明	ルールの説明。
リソース フィルター	ルールが適用されるリソースのタイプ。アスタリスク (*****) は、ルールがリソースすべてに適用されることを示します。
アクション	ルールのアクション (負荷分散)。
無効化	ステータス値:**Yes** または **No**
タイプ	Qlik Sense のインストール時には [**既定**] のタイプのルールが作成されます。ルールを編集したり新規作成したりすると、タイプは [**カスタム**] に変わります。3 番目のタイプは [**読み取り専用**] です。
タグ	負荷分散ルールに紐付けされているタグ。
条件	負荷分散ルールの条件。
ID	負荷分散ルールの ID。
作成日時	負荷分散ルールが作成された日時。
最終変更日	負荷分散ルールが最後に変更された日時。
変更者	負荷分散ルールを最後に変更したユーザー。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。

プロパティ	説明
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション [**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション [**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
編集	選択した負荷分散ルールを編集します。選択したアイテムに対する更新権限を持っていない場合、[**Edit**] は [**View**] に置き換わります。
表示	選択した負荷分散ルールを表示します。選択したアイテムに対する更新権限を持っていない場合、[**Edit**] は [**View**] に置き換わります。
削除	選択した負荷分散ルールを削除します。選択したアイテムに対する削除権限を持っていない場合、[**Delete (削除)**] は無効となります。
新規作成	新しい負荷分散ルールを作成します。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

概要でアイテムをダブルクリックすると、リソースの編集ページが開きます。複数選択するには、[Ctrl] キーを押しながら、アイテムをクリックするか、アイテムの上をドラッグします。

負荷分散ルール プロパティ

負荷分散ルールでは、次のプロパティグループが利用できます。

リソース フィルタ(詳細 ビュー)

セキュリティルールは Qlik Sense ***アプリ***に適用されます。

構文:

```
resource.resourcetype = "[プロパティ名]_*"
```

```
resource.resourcetype = "App_*"
```

条件 (詳細 ビュー)

負荷分散ルールを適用するリソースやユーザー条件を定義します。

構文

```
[resource.resourcetype = "resourcetypevalue"] [OPERATOR]
[(((resource.property = propertyvalue) [OPERATOR (resource.property =
propertyvalue)))]
```

[**基本**] ビューのドロップダウン リストからリソースおよびリソース条件を選択すると、[**詳細**] ビューの [**Conditions (条件)**] 項目には、選択したリソース タイプに対応するコードが自動的に入力されます。

条件は、プロパティ値のペアを使用して定義されます。リソースやユーザー条件を指定する必要はありません。実際、[**条件**] 項目は空欄のままにしておくことができます。

> *少なくとも 1 つの [**リソース**] 条件または [**ノード アクセス**] 条件を指定せずにルールを定義すると、このルールは条件の見出しの隣に*

条件を定義する順序は関係ありません。リソースを最初に定義してからユーザーやリソース条件を定義したり、その逆の順序で定義したりできます。ただし、リソースと条件を定義する順序は一貫させるようお勧めします。トラブルシューティングが容易になります。

引数

引数の説明

引数	説明
resource	条件がリソースに適用されることを示唆します。
resourcetype	条件が [**resourcetypevalue**] で定義されたタイプのリソースに適用されることを示唆します。 また、プロパティ値を返す条件に対してあらかじめ定義された関数を使用することもできます。

引数	説明
resourcetypevalue	利用可能な値の少なくとも 1 つのリソース タイプ値を指定する必要があります。 *リソース フィルタ(詳細 ビュー) (page 173)*
プロパティ	利用可能な名前のリソース条件のプロパティ名。 *プロパティ(page 174)*
propertyvalue	選択されたプロパティ名の値。

プロパティ

プロパティの説明

プロパティ名	説明
name	リソースの名前
owner.environment.browser	リソース所有者のブラウザ環境
owner.environment.device	リソース所有者のデバイス環境
owner.environment.ip	リソース所有者の IP 環境
owner.environment.os	リソース所有者の OS 環境
owner.environment.requesttype	リソース所有者のリクエスト タイプ 環境
owner.group	ユーザー ディレクトリから取得した所有者のグループ メンバーシップ。
owner.name	リソース所有者のユーザー名
owner.userdirectory	リソース所有者のユーザー ディレクトリ
owner.userid	リソース所有者のユーザー ID
streams.name	関連のあるストリームの名前

例と結果

例と結果

例	結果
`resource.resourcetype="App" and (resource.name like "*")`	このルールはすべてのアプリに適用されます。 *[リソース] 項目を「App*」に設定し、[条件] 項目を空にしておくだけで同じルールを定義できます。*
`resource.resourcetype="App" and (resource.name like "My*")`	このルールは、名前が「My」で始まっているすべてのアプリに適用されます。
`resource.resourcetype="App" and (resource.@Department="Test")`	このルールは カスタム プロパティ「Department」が「Test」に設定されているすべてのアプリに適用されます。

例	結果
`resource.resourcetype="App" and !(resource.@Department="Test")`	このルールはカスタム プロパティの「Department」が「Test」に設定されているノード以外のすべてのノードに適用されます。
[**リソース フィルター**]=* and Conditions field empty	このルールは、あらゆるリソースとユーザーに適用されます。

アクション (基本ビュー)

負荷分散ルール アクションは、常に [**負荷分散**] として定義されています。

クラウドの配布

クラウドの配布セクションでは、Qlik Sense Enterprise on Windows から Qlik Sense Enterprise SaaS へのアプリの配布を設定および監視します。このような展開では、Qlik Sense Enterprise on Windows のストリームに公開されたアプリを Qlik Sense Enterprise SaaS にも自動的に配布できます。アプリをクラウドに配布できるようにするには、マルチクラウドのライセンスが必要です。

マルチクラウドのライセンスを持っている場合、次のセクションを利用できます。

- **アプリの配布 ステータス**: アプリの配布を監視します。
- **配布 ポリシー**:Qlik Sense Enterprise SaaS の展開に公開アプリを配布できるかどうかを決定します。配布するには、公開アプリに接続されている配布ポリシーがあることが必要です。
- **展開の設定**:Qlik Sense Enterprise on Windows で展開を構成。

アプリの配布 ステータス

アプリの配布 ステータスの概要には、Qlik Sense Enterprise on Windows から Qlik Sense Enterprise SaaS へのアプリ配布のステータスが一覧表示されます。次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター ( ) を使用して項目を追加できます。

*[**アプリの配布 ステータス**] は [**クラウド配布**] のサブセクションであり、マルチクラウドのライセンスを持っている場合にのみ表示されます。*

アプリの配布ステータス プロパティ

プロパティ	説明
ID	アプリ配布の ID。
最終配布日時	最終配布の日時。
アプリ名	配布されたアプリの名前。
アプリ ID	配布されたアプリの ID。

プロパティ	説明
Deployment name (展開名)	アプリの配布先の展開の名前。
展開 ID	アプリの配布先の展開の ID。
ノード	アプリの配布元のノード。
ステータス	配布ステータス。値は次のとおりです:**進行中**、**キュー**、**成功**、**削除中**、**失敗**。
作成日時	アプリ配布が展開に最初に配布された日時。

配布ポリシー

アプリを Qlik Sense Enterprise on Windows から Qlik Sense Enterprise SaaS に配布するには、配布ポリシーを定義する必要があります。公開アプリを Qlik Sense Enterprise SaaS の 1 つ以上の実装環境に配布できるかどうかは、配布ポリシーにより決定されます。公開アプリが配布ポリシーの対象外である場合、その公開アプリは配布されません。

[**配布ポリシー**] の概要には、使用可能なすべての配布ポリシーが表示されています。

*[**配布ポリシー**] は [**クラウド配布**] のサブセクションであり、マルチクラウドのライセンスを持っている場合にのみ表示されます。*

次のテーブルでは、利用できる項目とボタンを示しています。既定では項目の一部のみが表示されます。列セレクター (⊞) を使用して項目を追加できます。

列幅は、ヘッダーの線をドラッグすることで調整できます。

ポリシー項目の説明

項目	説明
名前	ポリシーの名前。
説明	ルールの説明。
リソース フィルター	ルールが適用されるリソースのタイプ。アスタリスク (*****) は、ルールがリソースすべてに適用されることを示します。
アクション	ルールのアクション (Distribute)。
無効化	ステータス値:**Yes** または **No**
タイプ	Qlik Sense のインストール時には [**既定**] のタイプのルールが作成されます。ルールを編集したり新規作成したりすると、タイプは [**カスタム**] に変わります。3 番目のタイプは [**読み取り専用**] です。
タグ	配布ポリシーに接続されているタグ。

▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
アクション	フィルターと検索を消去したり、すべての行を選択または選択解除したり、折り返しを切り替えるオプション。 *オプション[**Select all rows**] は現在表示されている行に適用されています。すべての行を選択する前にフィルターが適用されている行は、選択されていても無視されます。オプション[**Deselect all rows**] はフィルターが適用された行を含むすべての行に適用されています。*
	列セレクター: 概要で表示する列を選択します。 をクリックすると既定の列にリセットされます。
	検索 - 基本とより高度な検索の両方。 *QMC での検索とフィルタリング (page 25)*
	ページを更新します。
編集	選択した配布ポリシーを編集します。選択したアイテムに対する更新権限を持っていない場合、[**Edit**] は [**View**] に置き換わります。
表示	選択した配布ポリシーを表示します。選択したアイテムに対する更新権限を持っていない場合、[**Edit**] は [**View**] に置き換わります。
削除	選択した配布ポリシーを削除します。選択したアイテムに対する削除権限を持っていない場合、[**Delete (削除)**] は無効となります。
[**新規作成**]	新しい配布ポリシーを作成します。
詳細を表示	概要では、既定のアイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more (詳細を表示)**] をクリックします。アイテムの検索や並べ替え、フィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

展開の設定

マルチクラウド セットアップを使用して、Qlik Sense Enterprise SaaS に展開できます。Qlik Sense Enterprise SaaS は、Qlik が管理するインフラストラクチャ上の展開に対応します。

セットアップの内容は、ローカル ベアラー トークン使用の有無に応じて異なります。

ローカル ベアラー トークンを使用する場合のセットアップ

ローカル ベアラー トークンを使用することで、展開のセットアップが簡略化されます。トークン エンドポイント、クライアントID、およびクライアント シークレット プロパティを使用して IdP からベアラー トークンを取得する代わりに、ベアラー トークンがローカルに生成されます。

展開のセットアップを開始する前に、Qlik が指定するテナントURL がウェルカム メールに記載されていることを確認します。

展開を設定するには、次の手順を実行します。

1. 画面左下で、[**Set up new**] (新規設定) をクリックします。
2. 展開名を入力します
3. **API エンドポイント**:Qlik から送信されたテナントURL を入力します。
4. オーディエンス: `qlik.api` を入力します。オーディエンスは、アプリ配布サービスでクラウドからAPI トークンを取得するために必要です。
5. [**Use local bearer token**] (ローカル ベアラー トークンを使用) が選択されていることを確認し、[**適用**] をクリックします。
   ローカル ベアラー トークンが生成されます。
6. 既定では、[**Qlik Cloudformat**] (書式) チェック ボックスが選択されています。次に、テキスト ボックスに IdP の定義が表示されます。
7. 使用したい書式を選択し、[**Copy to clipboard**] (クリップボードにコピー) をクリックしてテキストを保存します。テナントを構成する場合、このテキストが必要です。
8. Qlik Sense Enterprise SaaS の場合、テナント構成ページの [**ローカル ベアラー トークン**] テキストボックスに IdP の定義を貼り付けます。

IdP 統合による設定

展開の設定を開始する前に、以下を所有していることを確認します。

- クライアントID とクライアント シークレット (IdP プロバイダーから入手したもの)
- Token endpoint (トークン エンドポイント)
- テナントURL (ウェルカム メールで Qlikから提供されたもの)

展開を設定するには、次の手順を実行します。

1. 画面左下で、[**Set up new**] (新規設定) をクリックします。
2. 展開名を入力します(この名前は、アプリの配布に関する配布ポリシーで使用できます)。
3. **API エンドポイント**:Qlik から送信されたテナントURL を入力します。
4. オーディエンス: `qlik.api` を入力します。オーディエンスは、アプリ配布サービスでクラウドからAPI トークンを取得するために必要です。
5. クライアントID とクライアント シークレットを入力します。
6. トークン エンドポイントを入力します。これは *Authentication URL* (認証 URL) としても知られています。
7. [**適用**] をクリックします。

証明書

Qlik Sense は認証のために証明書を使用します。証明書により、Qlik Sense サイト内のノード間における信頼性が保たれています。証明書は、複数のノード上にあるサービス間の通信を認証するために、Qlik Sense サイト内で使用されます。

お使いの Qlik Sense インストールにサードパーティ製ツールを追加したい場合、証明書をエクスポートする必要があります。

エクスポートした証明書は、以下を行うために使用できます。

- 外部の認証モジュールを使用する。
- 新しいノードを作成したときに、QMC 機能を使う代わりに手動で証明書を移動する。

Log Collector

ログコレクタを使用すると、定義した期間のログファイルを収集およびエクスポートできます。このログは、Qlik サポートのトラブルシューティングを容易にします。

収集されたファイル

次のファイルを収集することができます。

Windows イベントログ

ログコレクタは、Windowsアプリケーションイベントログを読み取り、Qlik Sense関連するイベントだけを抽出します。これらのログから、Qlikサポートはすべてのサービスの開始と停止、警告、およびエラーの解析が可能です。

システム情報

ログコレクタは、標準の Windows Management Instrumentation (WMI) を使用して、ローカルサーバ、現在のホットフィックス、およびサービスパックに関する情報を収集します。ログコレクタは、プロキシセットアップ、実行中のサービス、証明書名、およびインターネット設定を検出するためにコマンドラインも使用します。この情報は、接続および Windows 関連する問題のトラブルシューティングに役立ちます。

Qlikフォルダの Scriptlog ファイル

ログコレクタは、アーカイブログファイルをスキャンします。現在アクティブなログファイルは、パス Universal Naming Convention (UNC) を使用して各 Qlik Sense サーバーノードからスキャンされます。

ログファイルの収集とエクスポート

次の手順を実行します。

1. 開始および終了日を手動で入力、またはカレンダーを使用して入力します: .

   指定された期間のログが含まれていないフォルダは収集されません。

2. サポート事例番号を入力します。
3. 追加で含めたいログを選択します:

- Windows イベント ログ
- システム情報
- Qlikフォルダの Scriptlog ファイル

4. **ログフォルダ フィルターを無視し、次の場合にすべてエクスポートします。**選択した場合、すべてのログが収集されます。選択されていない場合、次のフォルダのみが収集されます。
AboutService
AppDistributionService
BrokerService
CapabilityService
ConnectorRegistryProxy
ConverterService
DataProfiling
DepGraphService
DeploymentBasedWarningsService
DownloadPrepService
エンジン
HubService
HybridDeploymentService
HybridSetupConsoleBff
ライセンス
OdagService
Printing
プロキシ
Repository
ResourceDistributionService
スケジューラー
WebExtensionService

   通常、Qlik によるトラブルシューティングには、すべてのログがない既定のログ セットで十分です。

5. [**ログの収集とエクスポート**] をクリックします。

Qlikサポートに送信するための zip ファイルが生成されます。

ログコレクタの出力

以下はすべて別のファイルです:

- アプリリスト - *https://{senseApiSupport.Host}:4242/qrs/app/full*
- 通話情報 - *https://{senseApiSupport.Host}:4242/qrs/license/accesstypeinfo*
- ライセンスエージェント - *https://{senseApiSupport.Host}:4242/qrs/license*
- プロキシサービス情報 - *https://{senseApiSupport.Host}:4242/qrs/ProxyService/full*
- Qlik Sense 機械情報 - *https://{senseApiSupport.Host}:4242/qrs/servernodeconfiguration/full*
- Qlik Sense サービス情報 - *https://{senseApiSupport.Host}:4242/qrs/servicestatus/full*
- QRS 概要 - *https://{senseApiSupport.Host}:4242/qrs/about*
- サービスクラスター - *https://{senseApiSupport.Host}:4242/qrs/ServiceCluster/{_serviceClusterId}*

構成フォルダには、次のファイルがあります:

- インストールされているすべてのコネクターとその構成ファイル
- postgresql.conf
- postgresql_pg_hba.conf
- Engine_Settings.ini
- Sense_Host.cfg
- Repository.exe.config
- Repository.Core.dll.config
- Repository.Domain.dll.config
- Repository.Synchronization.dll.config
- Repository.User.dll.config
- Printing.exe.config
- Qlik.Printing.CefSharp.exe.config
- Qlik.Sense.Printing.dll.config
- Scheduler.exe.config
- Proxy.exe.config

追加ログ:

- 現在のログフォルダ:
- アーカイブログ - *https://{senseApiSupport.Host}:4242/qrs/ServiceCluster/{_serviceClusterId}*
- システム情報 - *C:\\Windows\\System32\\systeminfo.exe /S {hostName}*
- Windows ログ
- スクリプトログ

サービス証明書

プロキシとブラウザー、または 2 つの内部サービスなど、2 つのエンティティ間の安全な通信には証明書が使用されます。

Qlik Sense には、サーバー証明書およびトラストゾーン証明書の 2 種類の証明書があります。

- サーバー証明書は、Qlik Sense Proxy Service と、ブラウザーで実行されている Qlik Sense クライアントとの通信を保護するために使用します。
- トラストゾーン証明書 は、Qlik Sense内部サービス間の通信を保護するために使用します。

> *この後の説明ではトラストゾーン証明書に焦点を当てます。サーバー証明書についてはこれ以上詳細には説明しません。*

相互認証による TLS に使用される Qlik Sense トラストゾーン証明書とキー

Qlik Sense トラストゾーンは、内部サービス間の相互認証による Transport Layer Security (TLS) をベースにしています。

TLS 相互認証を確立するには、すべてのサービスで以下の 3 つの証明書および 2 つのプライベートキーが必要です。

ルート証明書

ルート証明書は、通信先とするサービスによって送信された証明書を検証するために使用します。

Windows 証明書の格納場所:*[ローカル コンピューター] > [信頼されたルート証明機関]*

サービス証明書とサービス プライベート キー

サービスがサーバーの役割を果たす場合、つまり別のサービスがお使いのサービス内で API を呼び出すときに、サーバー認証としてサービス証明書およびサービス プライベート キーが使用されます。

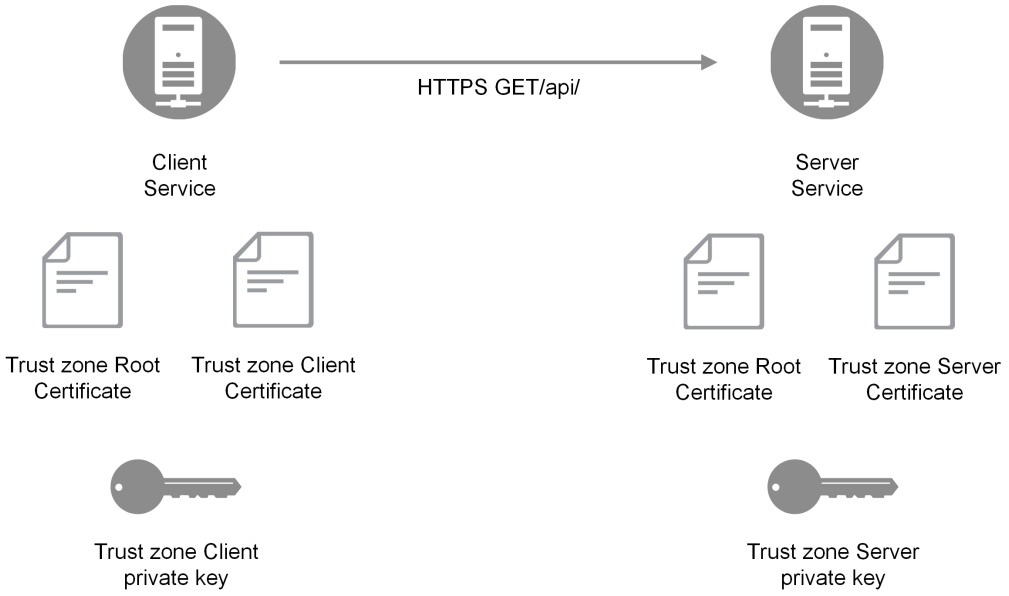
Windows 証明書の格納場所:*[ローカル コンピューター] > [個人用] > [証明書]*

クライアント証明書とクライアント プライベート キー

サービスがクライアントの役割を果たす場合、つまりお使いのサービスが別のサービスで API を呼び出すときに、クライアント認証としてクライアント証明書およびクライアント プライベート キーが使用されます。

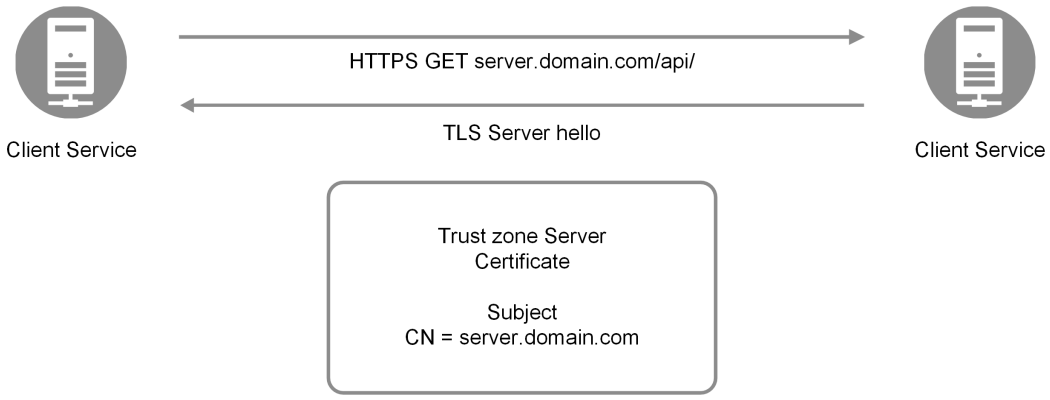
Windows 証明書の格納場所:*[ローカル サービス ユーザー] > [個人証明書]*

node.js に実装されるサービスの場合、証明書のコピーが次のフォルダー内にあります: *ProgramData%\Qlik\Sense\...\ExportedCertificates*。次の例では、サービスがサーバーの役割を果たします。



サービスがサーバーの役割を果たす例

サーバー証明書のコモン ネームにはサーバーのホスト名が含まれており、サーバーのドメイン名が証明書の情報と一致することを検証するためにクライアントが使用します。次の例では、クライアント サービスが TLS に関してサーバー *server.domain.com* とネゴシエートします。



クライアント サービスが TLS に関してサーバーとネゴシエートする例

サーバー証明書のコモン ネームは、QMC でのノード登録プロセス中に管理者が入力します。

QlikServiceCluster 証明書

QlikServiceCluster 証明書は、Qlik Sense Enterprise on Windows からマルチクラウド展開にアプリを配布するために使用します。

Windows 証明書の格納場所:*[ローカル コンピューター] > [個人用] > [証明書]*

手動構成

手動構成は、アプリ配布を使用している、または使用する予定のあるマルチノード サイトをアップグレードする場合に必要です。

2020 年 6 月 (以前) から 2020 年 9 月 (以降) にアップグレードする場合は、こちらを参照してください:「FAQ: Windows 上の Qlik Sense Enterprise からアプリを配布するための QlikServiceCluster 証明書」。

次の場合は、手動で構成する必要はありません。

- シングル ノードまたはマルチノード サイトの新規展開。
- シングル ノード サイトのアップグレード。
- アプリ配布を使用する予定のないマルチノード サイトのアップグレード。

Qlik Sense 証明書の有効期限の設定

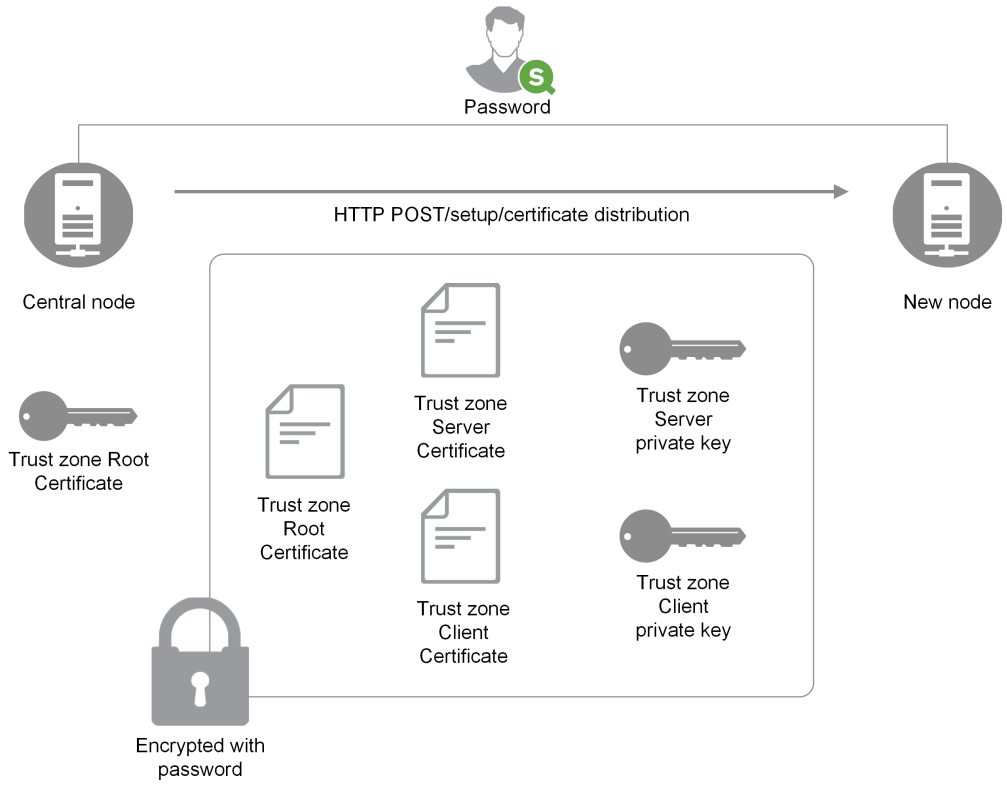
Qlik Sense は、証明書の有効期限を設定できます。既定値は 5 年 (60 か月) です。最小値は 12 か月、最大値は 60 か月です。最小値より小さい値または最大値より大きい値は無視され、それぞれ境界値である 12 か月または 60 か月に設定されます。

Qlik Sense トラストゾーンのキー管理

すべてのキーおよび証明書の作成元すべてのノード キーおよび証明書は、セントラル ノードによって作成されます。キーはランダムに生成され、対応する証明書は、トラストゾーンの Root プライベート キーによって署名されます。トラストゾーンの Root プライベート キーは、Qlik Sense が使用する第 3 のプライベート キーです。ただし、このキーは新しい証明書を発行するためにのみ使用され、相互の TLS の確立では使用されません。セントラル ノードが新しいノードの証明書およびキーを生成した場合には、ランダムに生成されたパスワードで暗号化され、新しいノードの REST エンドポイントに送信されます。

管理者は新しいノードでこのパスワードを入力して、キーおよび証明書を復号化し、新しいノードにインストールできるようにする必要があります。localhost の役割のみを果たす Web ページでパスワードを入力します。実際には、これはすべて、QMC でのノード登録ワークフローで発生します。

証明書およびキーの配布手順について、次の例で説明します。



証明書とキーの配布手順

証明書の拡張を使用して Qlik 証明書として証明書を識別し、この拡張の値で証明書のロールを「root」、「service」、または「client」のいずれかとして定義します。

データベースの暗号化

データベースの一部の項目は、アプリケーション レイヤーで Qlik Sense によって暗号化されます。これは通常、接続用パスワードなどの認証情報を含む項目です。データベースの項目は、すべての Qlik Sense ノードで使用可能にする必要のある対称キーで暗号化され、トラスト ゾーン サーバー証明書を使用してキーを保持します。

データベースの暗号化アルゴリズムおよびキーは、トラスト ゾーン サーバー証明書に拡張として格納されます。すべての拡張は 1 つのオブジェクト ID (OID) によって識別され、拡張の内容を示します。

- 1.3.6.1.5.5.7.13.1: 対称データベース キー
- 1.3.6.1.5.5.7.13.2: データベース キーのアルゴリズム

これら両方の項目は、トラスト ゾーン サーバー証明書のパブリック キーで暗号化されます。つまり、これはトラスト ゾーン サーバーのパブリック キーへのアクセス権を持つ唯一のエンティティであるため、項目を復号化できる唯一のサービスであるということです。

暗号化証明書

暗号化キーは証明書を使用することで適切に管理できます。エンジン サービスを実行しているユーザーについては、証明書を証明書ストアに保存する必要があります。

暗号化証明書は、暗号化キーを囲むシェルとして機能します。証明書の有効期限が切れていてもキーを取得できるため、有効期限が切れた暗号化証明書を更新する必要はありません。

暗号化キー

暗号化ソリューションで使用されるキーの種類は 2 つあります。

- データの暗号化キー
- キーの暗号化キー

データの暗号化キー

データ暗号化キー (DEK) は、データを AES-256 で暗号化するために自動生成されるキーです。暗号化するオブジェクトごとに新しいキーが生成されます。

キーの暗号化キー

キーの暗号化キー (KEK) は、データの暗号化キーのセキュアな非対称暗号化に使用する秘密鍵と公開鍵のペアです。公開鍵はデータの暗号化に使用され、秘密鍵は公開鍵で暗号化されたデータの復号に使用されます。

対応しているのは、RSA アルゴリズムを使用したキーのみです。

キーの暗号化に使用されるキーは、Qlik Management Console (QMC) の [*Service cluster*] (サービス クラスター) リソース内の [*Data encryption*] (データの暗号化) セクションで指定されています。*サービス クラスター (page 143)* をご確認ください。

暗号化証明書の要件:

- 証明キーは、Microsoft 社の Cryptography Next Generation (CNG) キー格納プロバイダーに保存されています。
- エンジン サービスを実行しているユーザーについては、証明書は CurrentUser の下の Windows 証明書ストアに保存されています。

データの暗号化の使用

これは、Qlik Sense においてデータの暗号化機能を使用する際の一般的なワークフローです。

1. 暗号化の証明書を作成:*Windows PowerShell を使用した暗号化証明書の作成 (page 187)*。
2. 暗号化を有効にし、キーを指定:*暗号化の有効化とキーの指定 (page 186)*。
3. マルチノードを展開、暗号化の証明書をエクスポート:*Windows PowerShell を使用した暗号化証明書のエクスポート (page 189)*。
4. マルチノードを展開、ノードすべてに暗号化の証明書をインポート:*Windows PowerShell を使用した暗号化証明書のインポート (page 192)*。

証明書を必ずバックアップしてください。証明書を紛失すると、暗号化されたアプリを開けなくなる可能性があります。必要な間、証明書のバックアップを安全に保管するのはお客様の責任です。

QlikView と共有する、QVD ファイルの暗号化

QlikView とQlik Sense Enterprise on Windows の両方で使用する QVD ファイルがある場合は、両製品で同じサムプリントが定義されていることを確認します。

暗号化の有効化とキーの指定

Qlik associative engine は、QMC の暗号化キーのサムプリントを定義することで構成されます。証明書の [*Thumbprint*] (サムプリント) フィールドの値をコピーして、QMC の [*Encryption key*] (暗号化キー) フィールドに貼り付けます。

エンジン サービスを実行しているユーザーについては、証明書を証明書ストアに保存する必要があります。

次の手順を実行します。

1. [Certificate Manager] (証明書の管理) ツール (certmgr.msc) を開きます。
2. 証明書を確認します。
3. 証明書を右クリックして [**Open**] (開く) を選択します。
4. [**Details**] (詳細) タブで [**Thumbprint**] (サムプリント) フィールドの値をコピーします。
5. QMC で、[**サービス クラスター**] > [**サムプリント**] の順に移動します。
   データ暗号化のオプションの一方、あるいは両方を有効化: [**QVF 暗号化**] と[**QVD 暗号化**]。
   サムプリントの値を [**暗号化キー**] 項目に貼り付けます。
   サービス クラスター(page 143)

Qlik Sense Enterprise on Windows は、スペースなしの 40 桁の 16 進文字列形式のSecure Hash Algorithm 1 (SHA-1) サムプリントを受け入れます。

証明書のサムプリントに **56 38 88 bb 6a ea 55 eb 0d 33 d9 d8 b9 09 e0 d2 ef 26 ff bd** のようにスペースが含まれている場合は、次のように [**暗号化キー**] 項目に入力します:

```
563888bb6aea55eb0d33d9d8b909e0d2ef26ffbd
```

組織にキー ローテーション ポリシーがある場合は、キーが変更されたときに サムプリントの定義を更新する必要があります。
すべての QVF および QVD が新しい鍵で保存されるまで、古い鍵を含む証明書をサーバーに保管してください。

暗号化証明書の管理

証明書を管理するためのツールは数多くありますが、このドキュメントでは、Windows PowerShell とMicrosoft 管理コンソールを使用した証明書の作成と配布に焦点を当てます。

他のツールを使用する場合は、次の要件を満たす必要があります。

- RSA キーが使用されている
- CNG キー格納プロバイダーにキーが保存されている
- エンジンサービスを実行しているユーザーの場合、証明書が証明書ストアに保存されている

Windows PowerShell を使用した暗号化証明書の作成

認証局 (CA) によって発行された証明書を使用する必要はありません。独自の自己署名証明書を発行して署名することもできます。作成する暗号化証明書は、エンジンサービスを実行しているユーザーの証明書ストアに保存する必要があります。

新しい暗号化証明書を作成するには、**New-SelfSignedCertificate** コマンドレットを使用して自己署名証明書を作成します。

構文: Windows Server 2016 以降

```
PS C:\Users\johndoe.ACME> New-SelfSignedCertificate -Subject <Certifcate name> -KeyAlgorithm
RSA -KeyLength <Key length, e.g.4096> -Provider "Microsoft Software Key Storage Provider" -
KeyExportPolicy ExportableEncrypted
-CertStoreLocation "cert:\CurrentUser\My"
```

構文: Windows Server 2012 R2

```
PS C:\Users\johndoe.ACME> New-SelfSignedCertificate -DnsName <Certifcate name> -
CertStoreLocation "cert:\CurrentUser\My"
```

New-SelfSignedCertificate コマンドレットパラメーター Windows Server 2016 以降

PowerShell for Windows Server 2016 以降を使用して証明書を作成する際には、少なくとも次のパラメータを定義する必要があります。

> *完全なドキュメントについては、Microsoft New-SelfSignedCertificate のドキュメントを参照してください。*

-Subject

新しい証明書のサブジェクトに表示される文字列を指定します。このコマンドレットは、等号を含まない値の前に **CN=** を付けます。複数のサブジェクト相対識別名 (RDN としても知られる) の場合は、各サブジェクト相対識別名をコンマ (,) で区切ります。相対識別名の値にコンマが含まれる場合は、各サブジェクト相対識別名をセミコロン (;) で区切ります。

```
-Subject <証明書名>
```

-KeyAlgorithm

新しい証明書に関連付けられた非対称キーを作成するアルゴリズムの名前を指定します。**RSA** でなければなりません。

```
-KeyAlgorithm RSA
```

-KeyLength
新しい証明書に関連付けられたキーの長さをビット単位で指定します。

```
-KeyLength <キーの長さ、たとえば 4096>
```

-Provider
このコマンドレットが証明書の作成に使用する KSP または CSP の名前を指定します。**Microsoft Software Key Storage Provider** である必要があります。

```
-Provider "Microsoft Software Key Storage Provider"
```

-KeyExportPolicy
証明書に関連付けられている秘密キーのエクスポートを管理するポリシーを指定します。このパラメータに指定できる値は次のとおりです:

- エクスポート可能
- ExportableEncrypted (既定)
- NonExportable

```
-KeyExportPolicy ExportableEncrypted
```

-CertStoreLocation
新しい証明書を格納する証明書ストアを指定します。現在のパスが *Cert:\CurrentUser* または *Cert:\CurrentUser\My* の場合、既定のストアは **Cert:\CurrentUser\My** です。それ以外の場合は、このパラメータに **Cert:\CurrentUser\My** を指定する必要があります。

```
-CertStoreLocation "cert:\CurrentUser\My"
```

New-SelfSignedCertificate コマンドレット パラメーター Windows Server 2012 R2

PowerShell for Windows Server 2012 R2 を使用して証明書を作成する際には、少なくとも次のパラメータを定義する必要があります。

> *完全なドキュメントについては、Microsoft New-SelfSignedCertificate のドキュメントを参照してください。*

-DnsName
証明書の件名代替名の拡張に 1 つ以上の文字列を入力するように指定します。最初の DNS 名も、件名と発行者名として保存されます。

```
-DnsName <証明書名>
```

-CertStoreLocation
新しい証明書を格納する証明書ストアを指定します。現在のパスが *Cert:\CurrentUser* または *Cert:\CurrentUser\My* の場合、既定のストアは **Cert:\CurrentUser\My** です。それ以外の場合は、このパラメータに **Cert:\CurrentUser\My** を指定する必要があります。

```
-CertStoreLocation "cert:\CurrentUser\My"
```

New-SelfSignedCertificate の既定 Windows Server 2012 R2

次の既定は、Windows Server 2012 R2 の **New-SelfSignedCertificate** コマンドレットに適用されます。

- キーのアルゴリズム: RSA
- キーの長さ: 2048
- 拡張キーの使用 (EKU): クライアント認証とサーバー認証
- キーの使用: デジタル署名、キーの暗号化 (a0)
- 有効期間: 1 年

例: PowerShell for Windows Server 2016 以降を使用したデータ暗号化の証明書の作成

この例では、test というユーザーが、サブジェクトが MyTestCert で、キーの長さが 4096 ビットの、自己署名付きのエクスポート可能な暗号化証明書を作成しています。証明書は Cert:\CurrentUser\My に保存されます。

Microsoft PowerShell で次のコマンドを入力します。

```
PS C:\Users\test> New-SelfSignedCertificate -Subject MyTestCert -KeyAlgorithm RSA -KeyLength
4096 -Provider "Microsoft Software Key Storage Provider" -KeyExportPolicy ExportableEncrypted
-CertStoreLocation "cert:\CurrentUser\My"
```

既定では、[NotAfter] パラメータが定義されていない場合、証明書は 1 年後に失効します。この例では、証明書は 3 年後に失効します:

```
PS C:\Users\test> New-SelfSignedCertificate -Subject MyTestCert -KeyAlgorithm RSA -KeyLength
4096 -Provider "Microsoft Software Key Storage Provider" -KeyExportPolicy ExportableEncrypted
-CertStoreLocation "cert:\CurrentUser\My" -NotAfter (Get-Date).AddYears(3)
```

結果:

証明書が作成されると、Microsoft PowerShell に次のように表示されます:

```
   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                                Subject
----------                                -------
563888BB6AEA55EB0D33D9D8B909E0D2EF26FFBD  CN=MyTestCert
```

Windows PowerShell を使用した暗号化証明書のエクスポート

暗号化証明書をエクスポートするには、**Export-PfxCertificate** コマンドレットを使用します。

構文:

```
PS C:\Users\johndoe.ACME> Export-PfxCertificate -cert cert:\currentuser\My\<certificate
thumbprint> -FilePath <FileName>.pfx -Password <Password or variable>
```

Export-PfxCertificate コマンドレットパラメータ

証明書をエクスポートする際には、少なくとも次のパラメータを定義する必要があります。

完全なドキュメントについては、Microsoft Export-PfxCertificate のドキュメントを参照してください。

-cert
エクスポートする証明書へのパスを指定します。

```
-cert cert:\currentuser\My\<証明書のサムプリント>
```

-FilePath
エクスポートする PFX ファイルのパスを指定します。

```
-FilePath <ファイル名>.pfx
```

-Password
エクスポートした PFX ファイルを保護するために使用するパスワードを指定します。パスワードは安全な文字列の形式にする必要があります。このパラメータを指定しないと、エラーが表示されます。

```
-Password <パスワードまたは変数>
```

例: データ暗号化証明書のエクスポート

この例では、test という名前のユーザーが、以前に作成した暗号化証明書を PFX ファイルにエクスポートします。

1. まず、テキスト形式のパスワード文字列からなる安全な文字列を作成し、`$mypwd` 変数に格納します。このために、**`ConvertTo-SecureString`** コマンドレットを使用しています。
   Microsoft PowerShell で次のコマンドを入力します。
   ```
   PS C:\Users\test> $mypwd = ConvertTo-SecureString -String "MyPassword" -Force -
   AsPlainText
   ```
2. 次に、**`Export-PfxCertificate`** コマンドレットを使用して、サムプリント `563888bb6aea55eb0d33d9d8b909e0d2ef26ffbd` で暗号化証明書の実際のエクスポートを続行します。前の手順で作成されたパスワード変数は、エクスポートされた PFX ファイルを保護するために呼び出されます。Microsoft PowerShell で次のコマンドを入力します。
   ```
   PS C:\Users\test> Export-PfxCertificate -cert
   cert:\currentuser\My\563888bb6aea55eb0d33d9d8b909e0d2ef26ffbd -Filepath MyTestCert.pfx -
   Password $mypwd
   ```

結果:

証明書がエクスポートされると、Microsoft PowerShell に次のように表示されます:

```
    Directory: C:\Users\test


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----       11/20/2019     11:21           4294 MyTestCert.pfx
```

Microsoft 管理コンソールを使用した暗号化証明書のバックアップ

証明書のバックアップは常に作成しておく必要があります。証明書がサーバーから失われた場合、またはハードディスクに障害が発生した場合は、暗号化されたアプリを開くことができない場合があります。必要な間、証明書のバックアップを安全に保持するのは、ユーザーの責任です。

証明書のバックアップ時のエクスポートと同じ手順を使用できます。*Windows PowerShell を使用した暗号化証明書のエクスポート (page 189)* を参照してください。

暗号化証明書のバックアップには、Microsoft 管理コンソールを使用する方法もあります。次の例は、Microsoft 管理コンソールを使用して、SSL 証明書を秘密キーでエクスポートまたはバックアップする方法を示しています。

次の手順を実行します。

1. SSL 証明書がインストールされている Windows サーバーで、Microsoft 管理コンソールを開きます。
   Windows の検索メニューに「mmc」と入力して開きます。
2. コンソールウィンドウで、**[ファイル] > [スナップインの追加と削除]** をクリックします。
3. [スナップインの追加と削除] ウィンドウで、左側の [利用可能なスナップイン] ペインから [**証明書**] を選択し、[**追加 >**] をクリックします。
4. ダイアログで、[**ユーザー アカウント**] を選択し、[**次へ**] をクリックします。
5. [スナップインの追加と削除] ウィンドウで、[**OK**] をクリックします。
6. コンソール ウィンドウの左側の [コンソール ルート] ペインで、[証明書 (現在のユーザー)] を展開し、エクスポートまたはバックアップする証明書を見つけます。
7. 中央のウィンドウで、エクスポートまたはバックアップする証明書を右クリックし、**[すべてのタスク] > [エクスポート]** をクリックします。
8. 証明書のエクスポート ウィザードの [証明書のエクスポート ウィザードへようこそ] ページで、[**次へ**] をクリックします。
9. [秘密キーのエクスポート] ページで、[**はい、秘密キーをエクスポートします**] を選択し、[**次へ**] をクリックします。
10. [ファイル形式のエクスポート] ページで、[**個人情報交換 - PKCS # 12 (.PFX)**] を選択し、[**可能であれば証明書パスにすべての証明書を含める**] をオンにします。

    [エクスポートが成功した場合は秘密キーを削除する] を選択しないでください。

    [**次へ**] をクリックします。
11. [セキュリティ] ページで、[**パスワード**] ボックスをチェックし、パスワードを作成して確認します。

    このパスワードは、証明書を秘密キーでインポートまたは復元するときに必要になります。

    次に、[**グループ名またはユーザー名**] ボックスをオンにします。該当する場合は、秘密キーを使用して証明書へのアクセスを割り当てる Active Directory ユーザーまたはグループ アカウントを選択します。次に [**追加**] をクリックします。
    [**次へ**] をクリックします。
12. [エクスポートするファイル] ページで、[**参照**] をクリックしてバックアップ ファイルの保存場所とファイル名を指定し、[**保存**] をクリックします。
    [エクスポートするファイル] ページに戻り、[**次へ**] をクリックします。
13. [証明書のエクスポート ウィザードの完了] ページで、設定が正しいことを確認し、[**完了**] をクリックします。
14. エクスポートが成功し、秘密キーを持つ SSL 証明書が選択した場所に保存されたことを伝えるメッセージが表示されます。

Windows PowerShell を使用した暗号化証明書のインポート

他のコンピューターなどに暗号化証明書をインポートするには、**Import-PfxCertificate** コマンドレットを使用します。

> *インポートする暗号化証明書は、エンジン サービスを実行しているユーザーの証明書ストアに保存する必要があります。*

構文:

```
PS C:\Users\johndoe.ACME> Import-PfxCertificate -CertStoreLocation cert:\currentuser\My -
FilePath <FileName>.pfx [-Exportable] -Password $mypwd
```

Import-PfxCertificate コマンドレット パラメータ

証明書をインポートする際には、少なくとも次のパラメータを定義する必要があります。

> *完全なドキュメントについては、Microsoft Import-PfxCertificate のドキュメントを参照してください。*

-CertStoreLocation

証明書のインポート先となるストアのパスを指定します。このパラメータを指定しない場合、現在のパスが保存先ストアとして使用されます。

```
-CertStoreLocation cert:\currentuser\My
```

-FilePath

PFX ファイルのパスを指定します。

```
-FilePath <ファイル名>.pfx
```

-Exportable

オプション。

インポートした秘密キーをエクスポートできるかどうかを指定します。このパラメータを指定しない場合、秘密キーはエクスポートできません。

```
-Exportable
```

-Password

インポートされた PFX ファイルのパスワードを安全な文字列の形式で指定します。

```
-Password $mypwd
```

例: データ暗号化証明書のインポート

この例では、test2 という名前のユーザーが、以前に PFX ファイルにエクスポートされたサムプリント `563888BB6AEA55EB0D33D9D8B909E0D2EF26FFBD` を使用して暗号化証明書をインポートします。

1. まず、テキスト形式のパスワード文字列からなる安全な文字列を作成し、$mypwd 変数に格納します。これには、ユーザー test2 は [**ConvertTo-SecureString**] コマンドレットを使用しています。Microsoft PowerShell で次のコマンドを入力します。
   ```
   PS C:\Users\test2>  $mypwd = ConvertTo-SecureString -String "MyPassword" -Force -AsPlainText
   ```
2. 次に、**Import-PfxCertificate** コマンドレットを使用して、PFX ファイルの実際のインポートに進みます。前の手順で作成されたパスワード変数は、PFX ファイルにアクセスするために呼び出されます。Microsoft PowerShell で次のコマンドを入力します。
   ```
   PS C:\Users\test2>  Import-PfxCertificate -CertStoreLocation cert:\currentuser\My -FilePath MyTestCert.pfx -Exportable -Password $mypwd
   ```

結果:

証明書がエクスポートされると、Microsoft PowerShell に次のように表示されます:

```
   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                                Subject
----------                                -------
563888BB6AEA55EB0D33D9D8B909E0D2EF26FFBD  CN=MyTestCert
```

Microsoft 管理コンソールを使用した暗号化証明書の復元

証明書を復元するときにインポートと同じ手順を使用できます。*Windows PowerShell を使用した暗号化証明書のインポート(page 192)* を参照してください。

Microsoft 管理コンソールを使用した暗号化証明書のバックアップ(page 190) の説明に従って Microsoft 管理コンソールを使用して証明書をバックアップした場合は、次の例に従って SSL 証明書を復元します。

> *復元する暗号化証明書は、エンジンサービスを実行しているユーザーの証明書ストアに保存する必要があります。*

次の手順を実行します。

1. SSL 証明書がインストールされている Windows サーバーで、Microsoft 管理コンソールを開きます。Windows の検索 メニューに「mmc」と入力して開きます。
2. コンソールウィンドウで、**[ファイル] > [スナップインの追加と削除]** をクリックします。
3. [スナップインの追加と削除] ウィンドウで、左側の [利用可能なスナップイン] ペインから [**証明書**] を選択し、[**追加 >**] をクリックします。
4. ダイアログで、[**ユーザー アカウント**] を選択し、[**次へ**] をクリックします。
5. [スナップインの追加と削除] ウィンドウで、[**OK**] をクリックします。
6. コンソール ウィンドウの左側の [コンソール ルート] ペインで、[証明書 (現在のユーザー)] を展開し、[個人] フォルダーを右クリックして、**[すべてのタスク] > [インポート]** を選択します。
7. [証明書のインポート ウィザードの開始] ウィンドウで、[**次へ**] をクリックします。
8. [インポートするファイル] ページで、[**参照**] をクリックしてインポートする PFX ファイルを見つけて選択し、[**次へ**] をクリックします。

> *既定では X.509 証明書 (*.cert、*.crt) ファイル タイプのみを検索するように設定されているため、ファイル エクスプローラー ウィンドウのファイル タイプ ドロップダウンですべてのファイル (*.*) を選択してください。*

9. [秘密キーの保護] ページで、SSL 証明書をエクスポートまたはバックアップしたときに作成したパスワードを入力します。
   次に、[**このキーをエクスポート可能としてマークする**] チェックボックスをオンにします。これは、必要なときに SSL 証明書をバックアップまたはエクスポートできることを意味します。
   次に、[**すべての拡張プロパティを含める**] チェックボックスもオンにします。
   [**次へ**] をクリックします。
10. [証明書ストア] ページで、[**すべての証明書を次のストアに配置する**] を選択し、[**参照**] をクリックします。
    [証明書ストアの選択] ウィンドウで、[**個人**] を選択し、[**OK**] をクリックします。
    [証明書ストア] ページに戻り、[**次へ**] をクリックします。
11. [証明書のインポートウィザードの完了] ページですべての設定が正しいことを確認し、[**完了**] をクリックします。
12. インポートが正常に完了し、秘密キーを持つ SSL 証明書が個人ストア (フォルダ) に保存されたことを示すメッセージが表示されます。

1.6 QMC リソースの管理

Qlik Sense 環境の運用には次の項目の管理と取り扱いが含まれます。

- ライセンス
- アプリ (公開、複製、リロード、インポート、削除)
- ストリーム
- データ接続および拡張機能
- ユーザー (同期、アクセス タイプ、所有、管理者ロール、非アクティブ化、削除)
- タスクとトリガー
- ノードおよびサービス
- カスタム プロパティとタグ

> *QMC での作業に有用なヒントについては、「QMC パフォーマンス – ベストプラクティス (page 449)」を参照してください。*

> *QMC リソースのトラブルシューティングについては、「トラブルシューティング - QMC リソースの管理」を参照してください。*

ライセンスの管理

ライセンス

ライセンス モデルには、シリアル番号とコントロール ナンバー、および署名付きのライセンス キーの 2 つがあります。これらのモデルで、ライセンスの契約条件およびユーザーに割り当て可能なアクセス タイプを定義します。ユーザーの割り当て、分析時間消費および製品のアクティベーションには、クラウドベースのライセンス バックエンドにアクセスするために、署名済みのライセンス キーとともにインターネット アクセス (直接またはプロキシ経由) が必要となります。

主なライセンス タイプには、アクセス タイプに基づくものと、トークンに基づくものの 2 つがあります。

- アクセス タイプのライセンスは、Professional User とAnalyzer User ライセンス (ユーザーベース) および Analyzer Capacity ライセンス (キャパシティベース) です。Professional User および Analyzer User ライセンスは、Professional アクセスおよび Analyzer アクセスを割り当てることができます。Analyzer Capacity ライセンスでは、Analyzer Capacity ライセンスを割り当てることができます。ここでは消費が時間ベース (Analyzer タイム) となっています。
- Qlik Sense Token ライセンスでは、トークンを使用してアクセス パスをユーザーに割り当てます。User アクセスおよび Login アクセスを割り当てることができます。

アクセス タイプを使うと、ユーザーは Qlik Sense Enterprise on Windows サイト内のハブとアプリにアクセスできます。

> *Qlik Sense Enterprise SaaS をセットアップする場合は、Qlik 代理店または Qlik サポートに連絡してセットアップのための有効なライセンスを入力してください。*

Qlik Sense ライセンス付与オプションの詳細については、Qlik の法的規約、製品規約、および Licensing Service リファレンスガイドを参照してください。

- Qlik Legal Terms (Qlik 法的規約)
- Qlik Product Terms (Qlik 製品規約)
- Qlik Licensing Service Reference Guide「Qlik Licensing Service リファレンスガイド」

アクセス タイプのライセンス

アクセス タイプのライセンスは、Professional とAnalyzer アクセスの既定数の割り当てを許可します。アクセス タイプの分布はライセンス モデルによって決まります。

> *ハブにアクセスすると、アクセス タイプのライセンス (Professional および Analyzer) に関するライセンス チェックが発生します。ハブにライセンスなしでアクセスし、その後 Professional またはアナライザー アクセスが割り当てられた場合は、ライセンス チェックはすでに発生しており、「アクセス パスがありません」のエラーが表示され、アプリの操作が停止されます。ログアウトし、再度ライセンスにログインして認識させます。*

Professional アクセス

識別されたユーザーに Professional アクセス権を割り当て、Qlik Sense サイト内のストリームとアプリにアクセスできるようにします。プロフェッショナル アクセスは、Qlik Sense インストールのすべての機能にアクセスする必要があるユーザーが対象です。プロフェッショナル アクセス権のあるユーザーは、シートまたはアプリを作成、編集、公開でき、Qlik Sense サイトの管理などの使用可能な機能をすべて使うことができます。

シルアル番号とコントロール ナンバーでライセンスが付与された Qlik Sense インストールでは、ユーザーから Professional アクセスの割り当てを削除すると、アクセス権が直近 7 日間で使用されていた場合、そのアクセス タイプは検疫のため隔離されます。直近 7 日間で使用されていない場合、プロフェッショナル アクセス権は直ちに解放されます。7 日以内であれば、同一のユーザーに検疫状態のプロフェッショナル アクセス権を復元することができます。

> *検疫は、署名済みライセンス キーでライセンス付与されている Qlik Sense のインストールでは強制されません。*

このアクセス パスのタイプでは、単一ユーザーが行える並列ユーザー接続の最大数は、5 回です。署名付きラインセンス キーでライセンスを使用する場合、QMC にアクセスすると、並列セッションの最大数がカウントされて追加され、5 つとなります。セッションの不必要な消費を避けるには、ルート管理者にどのタイプのアクセスも割り当てないでください。

最大数の並列ユーザー接続を持つユーザーが接続を終了する (たとえば、ログアウト) 場合、別の接続を追加する (たとえば、ログイン) には、アクセス パスが使用可能になる前に 5 分が経過する必要があります。

> *署名付きラインセンス キーでライセンスを使用する場合、QMC にアクセスすると、並列セッションの最大数がカウントされて追加され、5 つとなります。セッションの不必要な消費を避けるには、ルート管理者にどのタイプのアクセスも割り当てないでください。*

アナライザー アクセス

識別されたユーザーに割り当てられた Analyzer アクセス権によって、ハブ内のストリームとアプリにアクセスできるようにします。アナライザー アクセスは、他のユーザーによって作成されたシートとアプリを使用するユーザーが対象です。アナライザー アクセス権を持つユーザーは、シートやアプリを作成、編集、または公開することはできませんが、アプリ内のデータに基づいて、ストーリー、ブックマーク、スナップショットを作成できます。また、ユーザーは、ブックマーク、印刷オブジェクト、ストーリー、シートを作成したり、オブジェクトから Excel にデータをエクスポートしたりすることもできます。

シルアル番号とコントロール ナンバーでライセンスが付与された Qlik Sense インストールでは、ユーザーから Analyzer アクセスの割り当てを削除すると、アクセス権が直近 7 日間で使用されていた場合、そのアクセス タイプは検疫のため隔離されます。直近 7 日間で使用されていない場合、アナライザー アクセス権は直ちに解放されます。7 日以内であれば、同一のユーザーに検疫状態のアナライザー アクセス権を復元することができます。

> *検疫は、署名済みライセンス キーでライセンス付与されている Qlik Sense のインストールでは強制されません。*

このアクセス パスのタイプでは、単一ユーザーが行える並列ユーザー接続の最大数は、5 回です。最大数の並列ユーザー接続を持つユーザーが接続を終了する (たとえば、ログアウト) 場合、別の接続を追加する (たとえば、ログイン) には、アクセス パスが使用可能になる前に 5 分が経過する必要があります。

Analyzer Capacity アクセス

アナライザー キャパシティは消費ベースのライセンス タイプで、使用可能な機能に関してアナライザー アクセスに似ています。ユーザーは、ハブ内のストリームとアプリにアクセスし、他のユーザーによって作成されたシートとアプリを消費できます。Analyzer Capacity アクセスでは、アプリ内のデータに基づいてストーリー、ブックマーク、スナップショットを作成することができます。シートまたはアプリの作成、編集、または公開はできません。

アナライザー キャパシティ ライセンスにより、アナライザー時間 (毎月の定義済み分数 (カレンダー日付)) に対してサブスクライブします。これらの分時間は、ユーザー間で共有され、匿名ユーザーを含むユーザー グループの一員になっている任意のユーザーが消費可能です。消費は 6 分単位で測定されます。新しい 6 分間ごとに、1 単位が消費されます。

詳しくは「*Analyzer Capacity ライセンス (page 100)*」を参照してください。

トークンベースのライセンス

トークンを割り当てると、利用可能なトークンの数が減ります。各アクセス タイプは特定数のトークンを使用し、トークンの残数がゼロになるか不足すると、そのアクセス タイプに割り当てられなくなります。トークンの使用数を減らして、異なる方法でトークンを使用することができます。Qlik Sense サイトのトークンの数は、新しいライセンスをアクティブにすることで、増やしたり減らしたりできます。

ユーザー アクセス パス

識別されたユーザーにユーザー アクセス権を割り当て、Qlik Sense サイト内のストリームおよびアプリにアクセスできるようにします。アクセス タイプ (ユーザー アクセス) とユーザーとは、直接的に関係していますユーザーからユーザー アクセスの割り当てを解除すると、アクセス権が直近 7 日間で使用されていなければ、そのアクセス タイプは検疫のため隔離されます。直近 7 日間で使用されていないユーザー アクセス権は削除され、トークンは直ちに解放されます。7 日以内であれば、同一のユーザーに検疫状態のユーザー アクセス権を回復させることができます。その場合、ユーザーには、追加のトークンを使用せずに、再びアクセス権が付与されます。

ユーザー アクセス パスの概要:

- 指定されたユーザーに対し割り当てられる。
- コンテンツの分析や作成のために毎日アクセスすることができる。
- ストリーム、アプリ、その他のリソースに無制限にアクセス可能。
- 並列セッションの最大数は 5 つ。
- 1 トークン = 1 ユーザー アクセス パス。

ユーザー アクセス パスと、ログイン アクセス パスを消費する可能性の両方があります。アクティブ セッションが 5 つある場合は、追加のセッションを開くとログイン アクセス パスから消費されます。

ログイン アクセス パス

トークン 1 つは、事前に定義されたボリュームのログイン アクセス パスと同等です。ログイン アクセス権がある場合、ユーザーは事前に定義した時間の間、ストリームとアプリにアクセスできます。これは、単一のユーザーが同じ日に複数のログイン アクセス パスを使用できることを意味します。どのユーザーがログイン アクセス権を利用でき

るのか指定したセキュリティルールを作成します。

ログイン アクセス (グループ) 権を削除すると、ログイン アクセスに十分な数の未使用ログイン アクセス パスが含まれていれば トークンが即時 リリースされます。リリースされるトークンの数は、使用されたログイン アクセス パスの数によって決まります。使用されているログイン アクセス パスは最後の使用から28 日が経過するまでリリースされません。例: 1,000 回のログイン アクセス パスのあるトークンをグループに割り当てると、28 日間は 1,000 回を超えるログイン アクセス パスを使用できません。また、100 回のログイン アクセス パスを 1 日目に使うと、29 日目にも 100 回利用できます。使用中のアクセス パスがない場合は、ログイン アクセス インスタンスに割り当てられたすべてのトークンは、ログイン アクセス インスタンスの削除時にリリースされます。

アプリがアクティブに使用されていない場合、アプリをリロードするとセッションが延長され、アクセス パスも消費されます。アプリとともにブラウザー ページが開いている場合、アプリをリロードするとさらにアクセス パスが消費されます。

ログイン アクセス パスの概要:

- 使用頻度の低いユーザー向け。
- Qlik Senseの使用法をカスタマイズおよび制限可能。
- 時間制限はパスあたり連続 60 分。
  セッションが 20 分後に閉じられた場合、4 時間後に分析が再開され、新しいログイン アクセス パスが使用される。
- パスは 28 日ごとにリリースされる。
- 1 トークン = 10 ログイン アクセス パス。

ライセンスのアクティブ化

初めて QMC を起動すると、[**サイト ライセンス プロパティ**] ページが表示されます。すべてのフィールドが空になっており、ライセンス情報を入力する必要があります。 ライセンス情報を入力すると、Qlik Sense サイトのルート管理者 (RootAdmin) になります。

シリアル番号とコントロール ナンバーまたは署名付きのキーを使用して、Qlik Sense Enterprise のラインセンスを認証することができます。Analyzer Capacity アクセス権のライセンスを付与する場合は、署名付きキーによるライセンスを使用する必要があります。

署名付きキーによるライセンスに変更した後は、古いシリアル番号とコントロール ナンバーのライセンス モデルを再び使用することはできません。製品 ライセンスの詳細については、[Qlik 製品のライセンス] を参照してください。

次の手順を実行します。

1. シリアル番号とコントロール ナンバーを使用して Qlik Sense のライセンスを認証している場合は、必須項目を入力します。
   a. 以下を入力します。
      [**サイト ライセンス**] プロパティグループには、Qlik Sense システムのライセンスに関連するプロパティが含まれています。全項目が必須で、空欄のままにはできません。

サイト ライセンスのプロパティ

プロパティ名	説明
[所有者名]	Qlik Sense 製品所有者のユーザー名。
[所有者の組織]	Qlik Sense 製品所有者が所属する組織の名称。
[シリアル番号]	Qlik Sense ソフトウェアに割り当てられているシリアル番号。
[コントロール番号]	Qlik Sense ソフトウェアに割り当てられているコントロール番号。
LEF アクセス	Qlik Sense ソフトウェアに割り当てられる ライセンス認証 ファイル (LEF)。

b. [**LEF アクセス**] を展開し、[**LEF の取得とライセンスのレビュー**] をクリックして、Qlik Sense LEF サーバーからLEF ファイルをダウンロードします。あるいは、LEF ファイルからLEF の情報をコピーしてテキスト フィールドに貼り付けます。
[**LEF を正常に取得しました**] と表示されます。

> *シリアル番号かコントロール番号が正しくない場合には、**「サーバーからの LEF を取得することに失敗しました」**と表示されます。*

2. 署名付きのキーを使用して Qlik Sense のラインセンスを認証している場合は、専用の項目に署名付きのキーを入力します。
3. アクション バーで [**適用**] をクリックし、変更内容を保存します。
[**ライセンス認証しました**] というメッセージが表示されます。

> *署名入りのライセンス キーの場合、ライセンス キーを入力して**[適用]** で保存した後、QMC でライセンス情報を確認することができます。*

4. [**Close**] (閉じる) をクリックします。

これでライセンスが有効になります。次に、プロフェッショナル アクセスまたはユーザー アクセスを自分自身に割り当てます。

> *Qlik Sense にアクセスするために使用する消費モデルに基づいて、プロフェッショナルまたはアナライザー アクセス (ユーザーベースのライセンス) あるいはユーザー アクセスまたはログイン アクセス (トークンベースのライセンス) のアクセス タイプを管理することによって、ユーザーに Qlik Sense へのアクセス権を付与します。*

オフラインでのライセンスのアクティブ化

製品ライセンスをアクティブ化するには、インターネット経由で Qlik License Backend Server に接続する必要があります。場合によっては、インターネットにすぐにアクセスできず、オフラインライセンス認証が必要になることがあります。ライセンスに応じて、オフライン ライセンスまたは一時的な製品のアクティベーションが可能です。

製品のシリアル番号とコントロール番号をお持ちの場合は、Qlik サポートに License Enabler File (LEF) をリクエストして、[**サイト ライセンス プロパティ**] ページに貼り付けることができます。Qlik サポートからLEF を取得する方法の詳細については、[コントロール番号とLEF を要求する方法] を参照してください。

署名済みのライセンス キーをお持ちの場合は、インターネット経由でのみ製品のライセンスを取得できます。ただし、Qlik サポートに署名付きライセンス定義を要求することはできます。これにより、製品をオンラインでライセンスする前に、期間限定で製品を操作できます。詳細な手順については、[インターネットにアクセスせずに Qlik Products をアクティブ化する (April 2020 以降)] を参照してください。

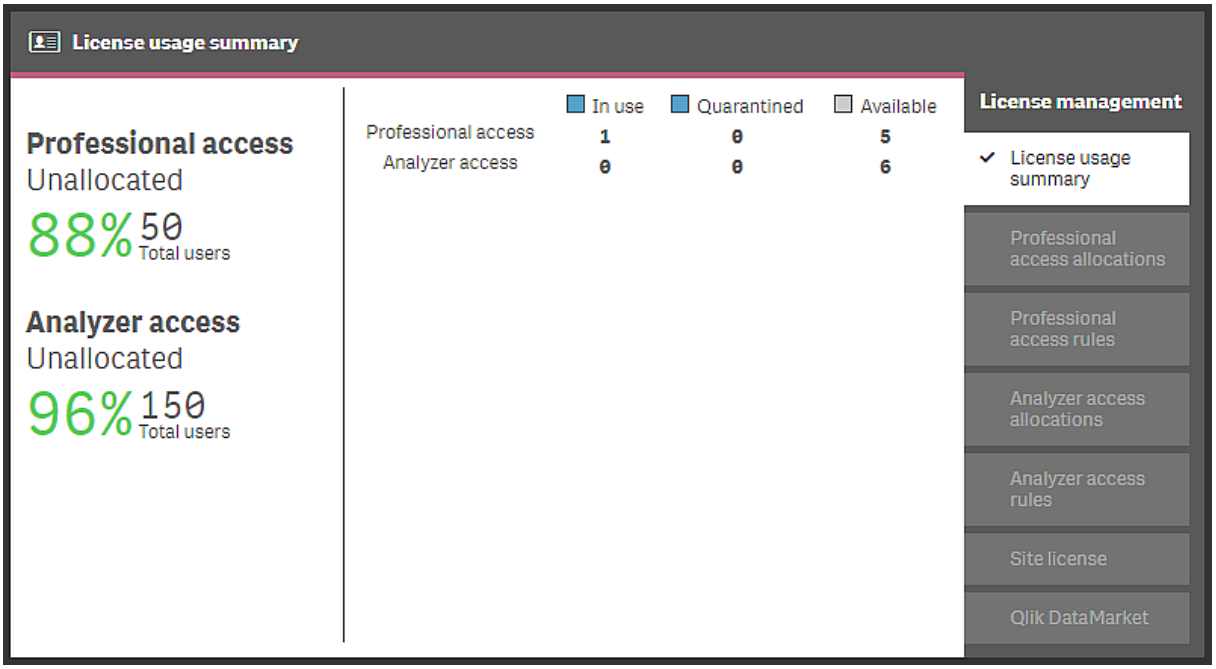
[ライセンス使用の概要] ページを理解する

[**ライセンス使用の概要**] ページの表示内容は、所有しているライセンスのタイプによって異なります。

ユーザーベースのライセンス

[**ライセンス使用の概要**] には、アクセスの利用可能性と、2 つのアクセス タイプ (プロフェッショナル アクセスとアナライザー アクセス) の分布が表示されます。このページからは、プロフェッショナル アクセスとアナライザー アクセスのユーザーの総数を調整することはできません。この総数は、Qlik Senseサイトの ライセンスによって決まります。

Analyzer Capacity は Analyzer アクセス権に類似したアクセス権で、Analyzer タイムをサブスクライブし、6 分ブロック単位で消費します。このライセンスを使用する場合は、概要に合計時間と使用時間が表示されます。Analyzer Capacity について詳しくは、*Analyzer Capacity ライセンス (page 100)* を参照してください。



左のセクションには、割り当てられていないプロフェッショナル アクセスとアナライザー アクセスの割合、およびアクセス ユーザーの総数が表示されます。

右のセクションには アクセスの分布が表示されます。

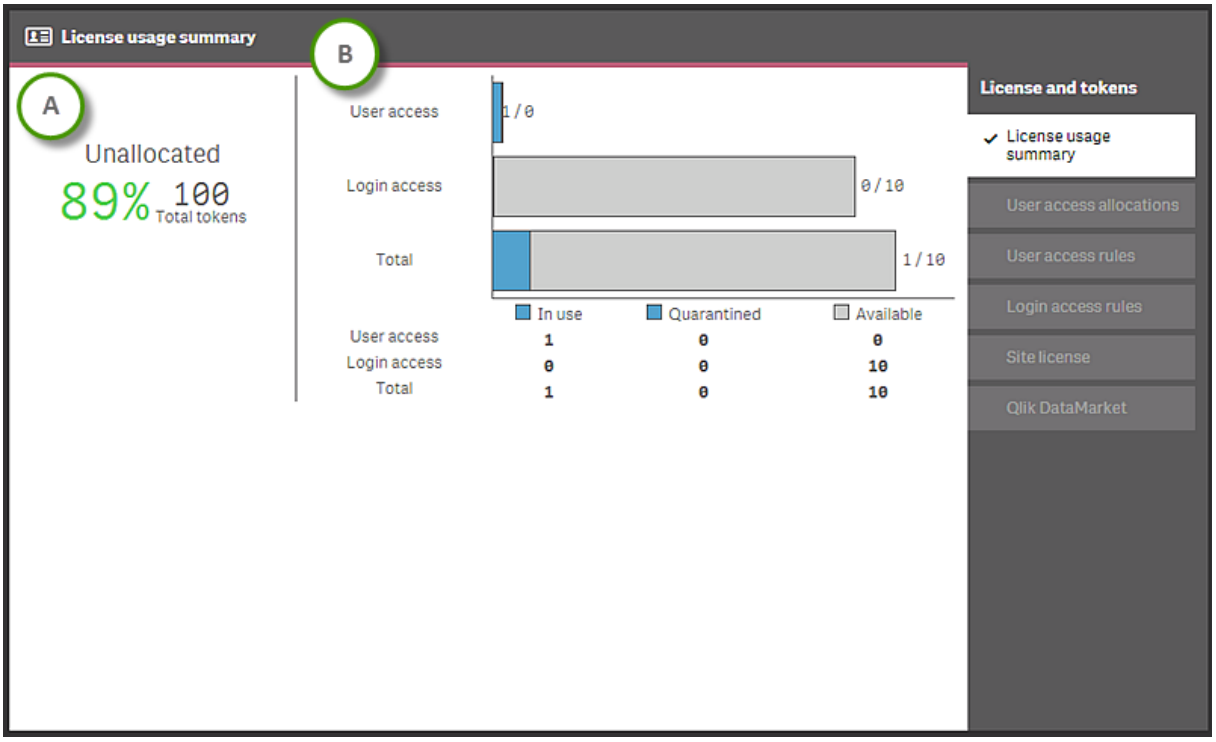
- **プロフェッショナル アクセス**: 特定のユーザーに割り当てられたプロフェッショナル アクセス数です。
- **アナライザー アクセス**: 特定のユーザーに割り当てられたアナライザー アクセス数です。

状態

- **使用中**: 現在使用中のアクセス割り当て数です。
- [**検疫済み**] (シリアル番号および管理番号を持つライセンスの場合のみ) : 検疫期間の終了後に割り当てが解除されるアクセス割り当て数です。
- **利用可能**: 現在使用されていないアクセス割り当て数です。

トークンベースのライセンス

[**ライセンス使用の概要**] 概要では、トークンの使用状況を示し、異なるアクセスタイプへのトークンの分配状況が表示されています。このページから、トークンの使用状況を調整することはできません。トークン数は、Qlik Senseサイトのライセンスによって決まります。



セクション (A) には、未割り当てのトークンの割合 (%) とトークンの合計数が表示されます。

セクション (B) には アクセスの分布が表示されます。

- **ユーザー アクセス**: 特定のユーザーに割り当てられたトークン数です。
- **ログイン アクセス**: ログイン アクセス グループに割り当て済みのトークン数です。
- **合計**: 上の 2 つの合計。

状態

- **使用中** 現在使用されている割り当て済みトークン数です。
- **検疫済み**: 検疫期間の終了後に割り当てが解除されるトークン数です。
- **利用可能**: 現在使用されていない割り当て済みトークン数です。

*ユーザー アクセス権を割り当てられたユーザーがハブに初めてログインした時点で、トークンが1 つ使用されます。ログイン アクセス パスのバッチで最初のログイン アクセス パスが使用されると、トークンが1 つ使用されます。たとえば、30 のログイン アクセス パスと11 のログイン アクセス パスの使用のために3 個のトークンを割り当てた場合、[**使用中**] は 2 個になります。ユーザー アクセスに割り当てられた検疫中のトークンは、検疫期間 (7 日間) が終了するまで、使用中になります。使用されたログイン アクセス パスの最後の使用から28 日後にリリースされます。*

ライセンスの変更

ライセンスのプロパティは、最初に設定した後、変更することができます。

LEF ライセンスの変更

LEF を更新すると、以下が変更されます。

- ユーザーベースのライセンス:Qlik Sense サイトでの Professional アクセスとAnalyzer アクセスの割り当て数が変わります。
- トークンベースのライセンス:Qlik Sense サイトのトークン数が変わります。アクセス タイプでトークンを使用して、ユーザーにハブへのアクセスを提供します。

シリアル番号とコントロール ナンバー付きのライセンスを受け入れるサイト ライセンスに加えて、署名付きライセンス キーも用意されています。Analyzer Capacity アクセス権のライセンスを付与する場合は、署名付きキーによるライセンスを使用する必要があります。署名付きキーによるライセンスに変更した後は、古いシリアル番号とコントロール ナンバーのライセンス モデルは再び使用できないことに注意してください。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、または [**スタート▼**] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
3. 右側のパネルで [**サイト ライセンス**] を選択します。
4. 項目を編集します。

   [**サイト ライセンス**] プロパティグループには、Qlik Sense システムのライセンスに関連するプロパティが含まれています。全項目が必須で、空欄のままにはできません。

   サイト ライセンスのプロパティ

プロパティ名	説明
[**所有者名**]	Qlik Sense 製品所有者のユーザー名。
[**所有者の組織**]	Qlik Sense 製品所有者が所属する組織の名称。
[**シリアル番号**]	Qlik Sense ソフトウェアに割り当てられているシリアル番号。
[**コントロール番号**]	Qlik Sense ソフトウェアに割り当てられているコントロール番号。
LEF アクセス	Qlik Sense ソフトウェアに割り当てられる ライセンス認証 ファイル (LEF)。

[**LEF アクセス**] を展開し、[**LEF の取得とライセンスのレビュー**] をクリックして、Qlik Sense LEF サーバーから LEF ファイルをダウンロードします。あるいは、LEF ファイルから LEF の情報をコピーしてテキスト フィールドに貼り付けます。

[**LEF を正常に取得しました**] と表示されます。

> *シリアル番号かコントロール番号が正しくない場合には、**「サーバーからの LEF を取得することに失敗しました」**と表示されます。*

5. アクション バーで [**適用**] をクリックし、変更内容を保存します。
[**変更内容を適用しました**] というメッセージが表示されます。

> *値が正しくなければ、**[変更内容を適用できませんでした]** というメッセージが表示されます。*

署名付きのキー ライセンスの更新

署名付きのキー ライセンスを更新すると、Professional とAnalyzer アクセスの割り当て数、および Analyzer Capacity ライセンスの保存期間 (分単位) が変更されます。

1. QMC スタート ページから、または [**スタート▼**] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
2. 右側のパネルで [**サイト ライセンス**] を選択します。
3. 新しい署名付きのキーを専用の項目に挿入します。
4. アクション バーで [**適用**] をクリックし、変更内容を保存します。
[**変更内容を適用しました**] というメッセージが表示されます。

> *値が正しくなければ、**[変更内容を適用できませんでした]** というメッセージが表示されます。*

アプリの管理

適切なアクセス権限がある場合は、Qlik Sense ハブからアプリを作成し、ストリームに公開することができます。アプリは、QMC から公開することもできます。インストールされている Qlik Sense Desktop で作成されるアプリを公開するには、まずそのアプリを QMC からインポートする必要があります。アプリ、ストリーム、ユーザーに適用されるセキュリティルールによって、コンテンツにアクセスできるユーザーおよびそのユーザーが実行できる内容が決まります。アプリは公開後ロックされます。サーバー デプロイメントの Qlik Sense ハブを介してコンテンツを公開済みのアプリに追加することは可能ですが、オリジナルのアプリで公開されたコンテンツは編集できません。アプリを Qlik Sense Enterprise SaaS に公開するには、最初に配布ポリシーを作成する必要があります。「*配布ポリシー- はじめに (page 623)*」を参照してください。

> *Qlik Sense Enterprise SaaS ではアプリの拡張機能に対応していません。拡張機能を持つアプリを Qlik Sense Enterprise SaaS 展開に公開した場合、そこでは拡張機能は使用できません。*

公開できるのは、未公開のアプリのみです

- アプリを複数のストリームに公開するには、最初にアプリの複製を作成する必要があります。
- アプリを再公開するには、公開済みアプリの複製を作成し、その複製を編集して公開します。公開済みアプリを置換するには、[**Replace existing**] オプションを使用します。エクスポートされたアプリをインポートして、既存のアプリと置き換えることもできます。

ハブからアプリを公開すると、所有者の [**作業**] フォルダー内のアプリにストリーム アイコンが取得され、公開済みであることを示します。アプリを再発行するには、まず公開済みのアプリの複製を作成する必要があります。

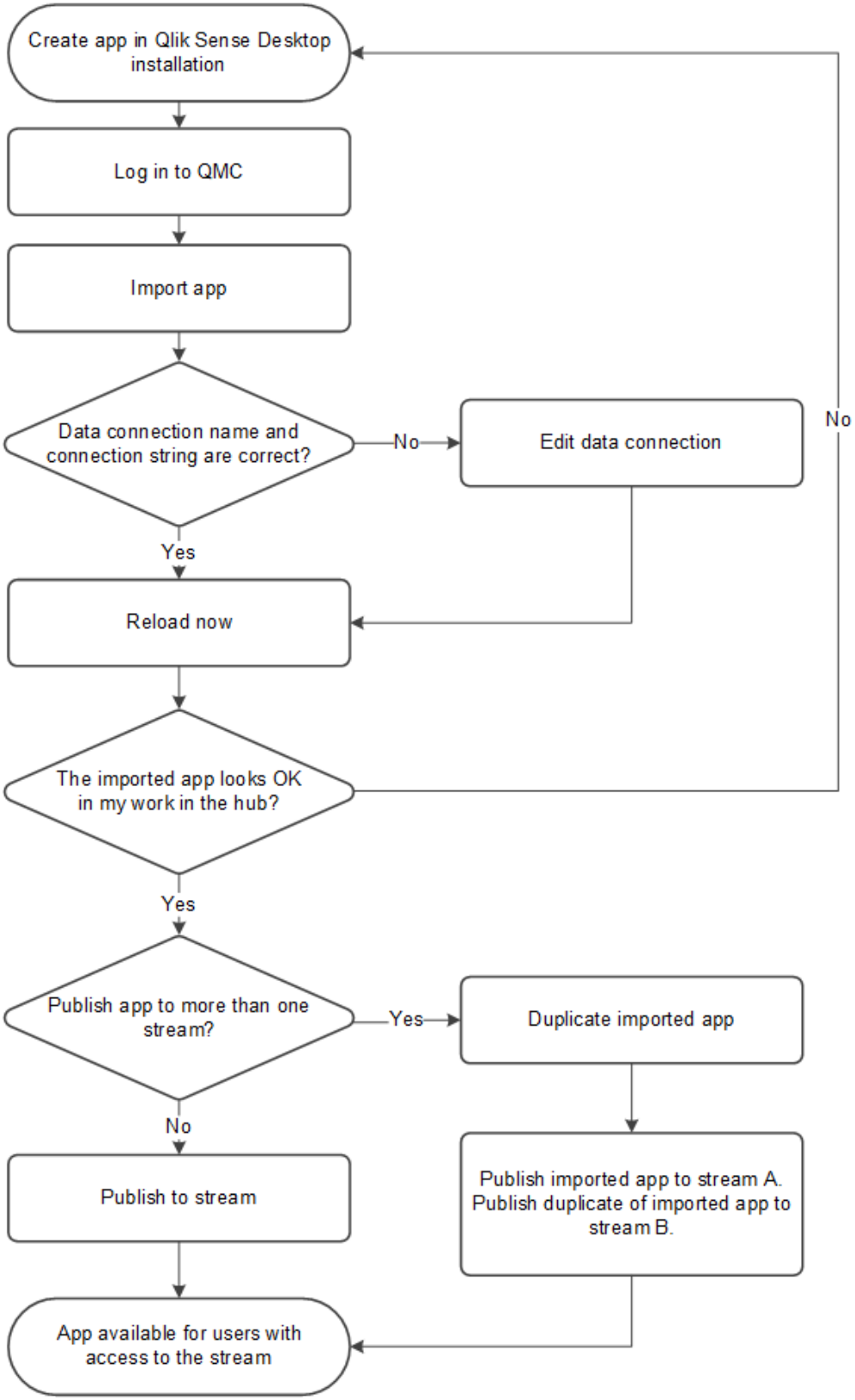
*アプリへの作成アクセス権限と読み取りアクセス権限があり、QMC の [**アプリ**] セクションへの読み取りアクセス権限がある場合、アプリを複製できます。ただし、セキュリティ上の理由で、スクリプトを複製できるのは、スクリプトの読み取り権限も持っている場合のみです。スクリプトにアクセスするとセクション アクセスを編集または削除でき、その結果、アクセスできてはならないデータをロードできます。*

Qlik Sense のローカル インストールで作成されたアプリをインポートするとき、アプリが作成された環境とサーバー環境との間でデータ接続ストレージが異なる場合があります。保存スペースが異なる場合、サーバー環境に合わせるためにデータ接続プロパティの [**名前**] および [**接続ストリング**] を更新する必要があります。アプリを公開する前に、ハブ内の自身の [**作業**] セクションでアプリを確認してください。

インポートされるアプリのデータ接続名が、既存のデータ接続の名前と同じ場合、データ接続はインポートされません。つまり、インポートされたアプリは、インポートされたアプリのデータ接続ではなく、同一名のすでに存在するデータ接続を使用します。

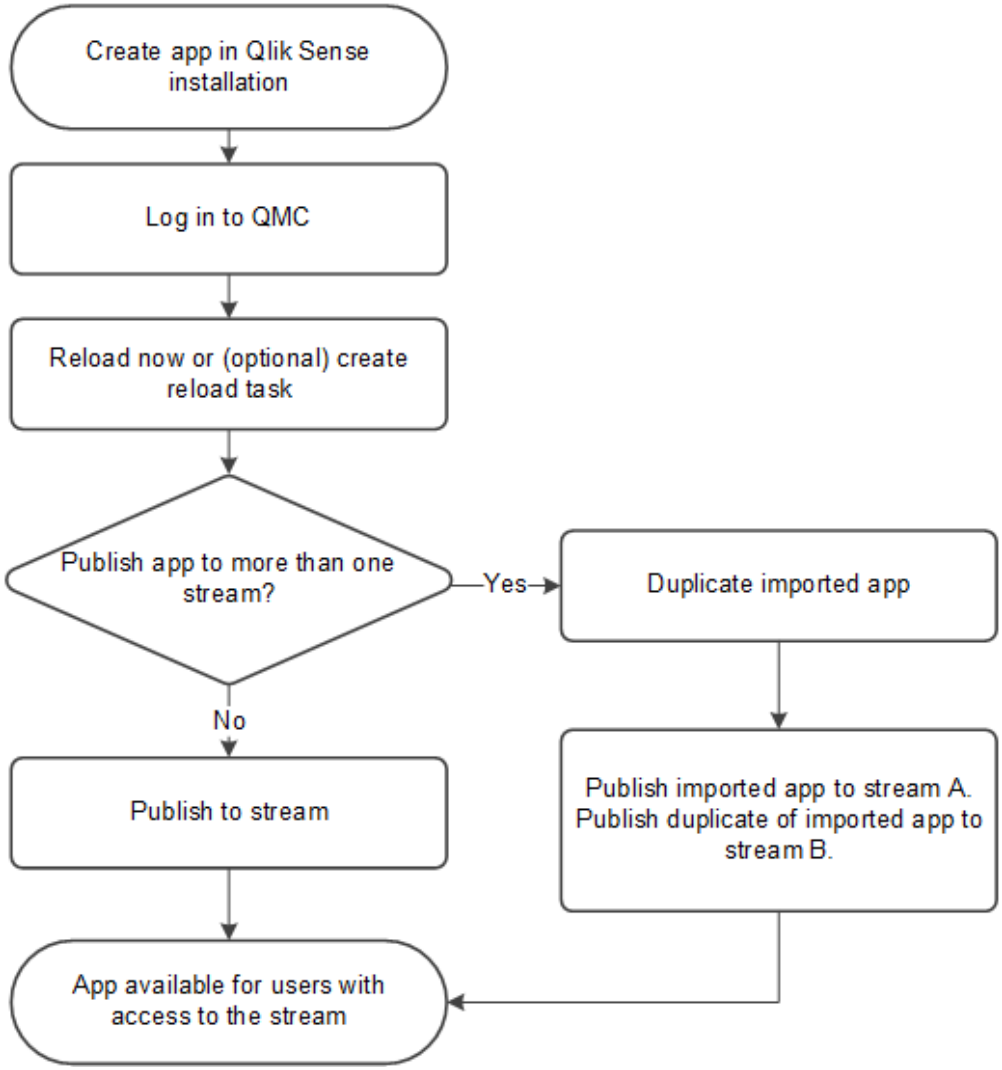
ワークフロー:Qlik Sense Desktop インストールで開発されたアプリ

以下に、Qlik Sense Desktop インストールのハブから作成されたアプリをインポートし、Qlik Sense インストールの QMC を使用してそのアプリを公開する場合のワークフローを示します。



ワークフロー: サーバー展開の Qlik Sense で開発されたアプリ

次のワークフローは、Qlik Sense のインストールで QMC からアプリを公開する場合のフローを示しています。



アプリのインポート

ブラウザが HTML5 のアップロードをサポートしている場合はアプリをインポートできます。カスタム属性などの app のプロパティは、app をアップロードするときに含まれます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**アプリ**] を選択して、概要を表示します。
3. 操作バーの ⊕[**インポート**] をクリックします。
   [**アプリのインポート**] ダイアログ ボックスが開きます。
4. インポートするファイルを選択します。
5. インポートするアプリ (*qvf ファイル*) を参照して [**開く**] をクリックします。

長いファイル名を持つ画像がアプリに含まれている場合は、画像への完全パスが260文字を超えるとインポートに失敗します。パスが長すぎる場合は、画像のファイル名を短くしてください。

参照のダイアログ ボックスが閉じ、qvfファイルの名前が [**Import app**] ダイアログ ボックスの [**アプリ名**] フィールドに表示されます。
[**アプリ名**] フィールドでアプリの名前を変更できます。[**アプリ名**] が一意でない場合は、この名前を持つアプリの数を知らせるメッセージが表示されます。

インポートされるアプリのデータ接続名が、既存のデータ接続の名前と同じ場合、データ接続はインポートされません。つまり、インポートされたアプリは、インポートされたアプリのデータ接続ではなく、同一名のすでに存在するデータ接続を使用します。

6. アプリを置き換える場合は、[**既存のアプリを置き換える**] を選択して置き換えるアプリを選択し、オプションで、データなしでのアプリのインポートを選択します。
   アプリの置き換えの詳細については、アプリの置換 (page 212) を参照してください。
7. ダイアログ ボックスで [**インポート**] をクリックします。
   [**転送中**] ダイアログが開きます。ダイアログには、自分が開始した転送がすべて表示されます。
   - ファイルのインポート中は スピナーが表示されます。
   - クリックして ⊗ インポートを取り消します。
     ⚠ [**中断**] が表示され、インポートが停止します。
   - 失敗したアイテムを削除するには、[**OK**] をクリックします。⚠.
     [**転送中**] ダイアログからこのアイテムが削除されます。

App がインポートされると、✔ が表示され、この app が [**App**] の概要に追加されます。すべての転送が正常に完了すると[**Ongoing transport**] ダイアログが閉じます。転送に失敗した場合、概要ページが最新の情報に更新されるまでダイアログが表示されます。

サーバーにアプリをインポートする場合やサーバーからアプリをエクスポートする場合は、画像などの.qvf ファイルに保存されていない関連コンテンツも移動します。関連コンテンツは、%ProgramData%\Qlik\Sense\Repository\AppContent\<App ID> フォルダに個別に保存されます。各アプリには、アプリID をフォルダ名とする独自のアプリコンテンツ フォルダがあります。

アプリを複製したりインポートした直後に開いた場合に、マルチノードサイトでのデータの同期方法が原因で、画像が含まれるアプリに破損したサムネイルやアプリ内の画像が表示される場合があります。破損した画像は、同期の完了後に復元されます。画像が復元されたことを確認するには、ブラウザ ウィンドウを更新します。

ODBC データ接続を含むアプリの移動

Qlik Sense サイトまたは Qlik Sense Desktop インストール間でアプリを移動すると、データ接続は含まれません。アプリに ODBC データ接続が含まれる場合、新たな接続を作成するか、新たなサイトにすでにある接続を使用する必要があります。また、関連の ODBC データ ソースが新たな実装に存在することも確認する必要があります。これらの ODBC データ ソースは同じ名前と構成で、同じデータベースまたはファイルを指している必要があります。

アプリの編集

更新権限を有するアプリを編集できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**アプリ**] を選択して、概要を表示します。
3. 編集するアプリを選択します。
   ストリームの関連付けからアプリを選択することも可能です。
4. アクション バーで [**編集**] をクリックします。[**Edit (編集)**] の横の数字は、選択したアイテムの中で編集できるアイテムの数を示します。
   [**アプリの編集**] ページが開きます。
5. プロパティを編集します。

ID

ID プロパティ

プロパティ	説明
[**名前**]	アプリの名前。
所有者	アプリの所有者。
[**作成日時**]	アプリが作成された日時。
[**最終変更日**]	アプリが最後に変更された日時。
[**ファイル サイズ**]	アプリのファイル サイズ。

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

> *カスタム プロパティを利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

[**適用**] をクリックして変更を保存します。必須の項目が空欄の場合、[**Apply**] は無効になります。

6. 操作バーで [**適用**] をクリックします。

ページの最下部に [**更新完了**] と表示されます。

アプリの削除

削除権限を有するアプリを削除できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**アプリ**] を選択して、概要を表示します。
3. 削除するアプリを選択します。
4. アクション バーの [**Delete**] をクリックします。[**Delete**] ダイアログが表示されます。
5. [**OK**] をクリックします。

> *アプリが削除されると、アプリ固有のフォルダ %ProgramData%\Qlik\Sense\Repository\AppContent\<App ID> のコンテンツが、アプリと共に削除されます。1 つのアプリに固有でない一般的なコンテンツ ([**コンテンツ ライブラリ**] の拡張機能、データ接続、アイテムなど) は削除されません。*

QMC からのアプリの公開

適切なアクセス権限がある場合は、Qlik Sense ハブからアプリを作成し、ストリームに公開することができます。アプリは、QMC から公開することもできます。インストールされている Qlik Sense Desktop で作成されるアプリを公開するには、まずそのアプリを QMC からインポートする必要があります。アプリ、ストリーム、ユーザーに適用されるセキュリティ ルールによって、コンテンツにアクセスできるユーザーおよびそのユーザーが実行できる内容が決まります。アプリは公開後ロックされます。サーバー デプロイメントの Qlik Sense ハブを介してコンテンツを公開済みのアプリに追加することは可能ですが、オリジナルのアプリで公開されたコンテンツは編集できません。

アプリを QMC から公開すると、所有者のアプリが [**作業**] フォルダーから [**公開済み**] フォルダーに移動され、ストリーム アイコン (≋) でマークされて、公開済みであることを示します。

- アプリを複数のストリームに公開するには、最初にアプリの複製を作成する必要があります。
- アプリを再公開するには、公開済みアプリの複製を作成し、その複製を編集して公開します。公開済みアプリを置換するには、[**Replace existing**] オプションを使用します。

アプリを Qlik Sense Enterprise SaaS に公開するには、最初に配布ポリシーを作成する必要があります。「*配布ポリシー- はじめに (page 623)*」を参照してください。

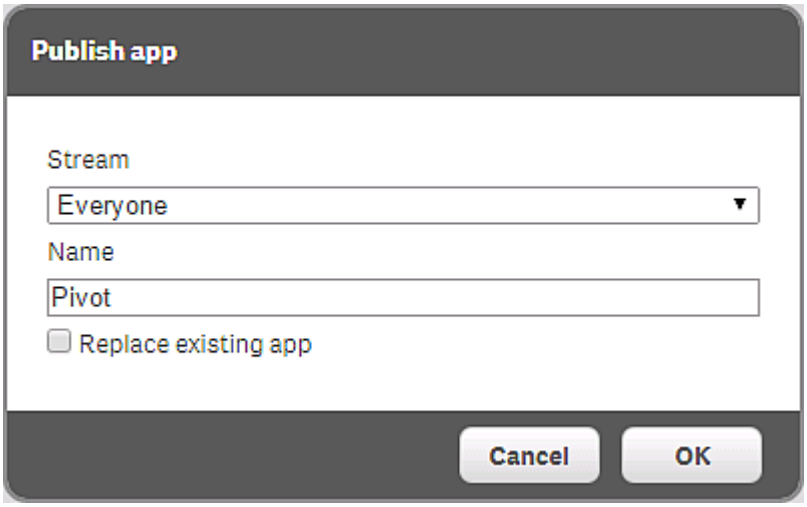
Qlik Sense Enterprise SaaS ではアプリの拡張機能に対応していません。拡張機能を持つアプリを Qlik Sense Enterprise SaaS 展開に公開した場合、そこでは拡張機能は使用できません。

次の手順を実行します。

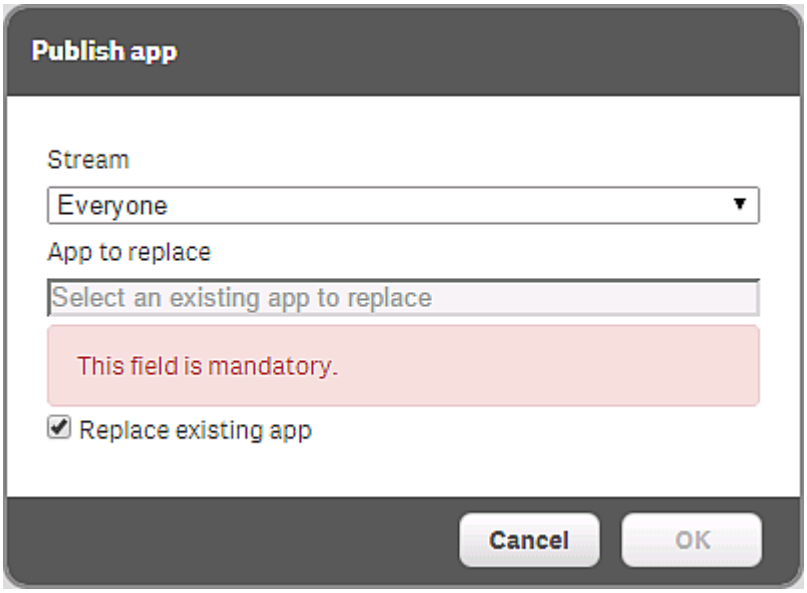
1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**アプリ**] を選択して、概要を表示します。
3. 公開するアプリを選択します。
   [**公開**] の横の数字は、選択したアプリの中で公開できるアプリの数を示します。
4. アクション バーで [**公開**] をクリックします。

   *ストリームのアクセス権がない場合は、[**公開**] ボタンは表示されません。*

   ダイアログ ウィンドウが開きます。
5. [**Publish app**] ダイアログで、以下の手順を行います。
   a. [**Select a stream**] ドロップダウン メニューを使用して、公開先のストリームを選択します。
   b. [**名前**] テキスト フィールドでは、公開するアプリの名前を変更できます。[**複数の値**] が表示された場合は、複数のアプリを公開しようとしており、アプリの名前を変更することはできません。
6. オプション: すでに公開されているアプリを置き換えることができます。これは、1 つのアプリを選択した場合のみ可能です。
   a. [**既存のアプリを置換**] を選択します。



   b. [**置き換えるアプリ**] ボックスをクリックします。



ダイアログが開きます。

c. 置き換える公開済みのアプリをダブルクリックします。
アプリが [**置き換えるアプリ**] フィールドに追加されます。

7. [**OK**] をクリックして公開します。既に公開済みのアプリを置換している場合は、表示される確認ダイアログで [**公開して置換**] をクリックします。
ダイアログが閉じ、[**s: x 選択したアプリの公開に成功しました: x**] と表示されます。ここで、x は公開されたアプリの数です。また、アプリ概要の [**ストリーム**] 列が更新され、アプリの公開先のストリームが表示されます。[**公開済み**] 列には公開日が表示されます。

アプリの再公開

QMC から公開されているアプリを再公開するには、アプリの複製を作成する必要があります。

ハブからアプリを公開すると、所有者の [**作業**] フォルダー内のアプリにストリーム アイコンが取得され、公開済みであることを示します。アプリを再発行するには、まず公開済みのアプリの複製を作成する必要があります。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**アプリ**] を選択して、概要を表示します。
3. 再公開したい公開済みのアプリを選択し、操作バーで [**複製**] をクリックします。
アプリの複製が概要に追加されます。

複製されたアプリを編集して公開できるようになります。公開済みアプリを置換するには、[**Replace existing**] オプションを使用します。

QMC のストリーム間での公開済みアプリの移動

適切なアクセス権限がある場合は、Qlik Sense ハブからストリーム間に公開済みのアプリを移動することができます。以下の権限がある場合は、QMC のストリーム間でもアプリを移動することができます。

- アプリの読み取り、更新、および公開アクセス権。
- 現在のストリームでの公開アクセス権。
- 公開先ストリームへの公開アクセス権。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMCスタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから[**アプリ**] を選択して、概要を表示します。
3. 新しいストリームに移動するアプリを選択します。
4. [**移動**] をクリックします。
5. 公開先のストリームを選択して [**OK**] をクリックします。

アプリが選択したストリームに存在するようになりました。

アプリの置換

アプリを選択して置き換えるには、アプリを再公開するか、またはアプリをインポートして置き換えます。

QMCからアプリを公開する場合には、公開済みのアプリを交換することができます。操作バーで [**公開**] をクリックすると、[**既存のアプリを置換**] オプションが [**アプリの公開**] ウィンドウで使用できます。

アプリを QMC から公開すると、所有者のアプリが [**作業**] フォルダーから[**公開済み**] フォルダーに移動され、ストリーム アイコン (≋) でマークされて、公開済みであることを示します。

アプリをインポートしてアプリを置き換える場合には、アプリ全体を置き換えることも、またはデータなしでインポートすることもできます。アプリデータなしでインポートすると、データおよびデータ モデルを除いて、アプリ内のすべてのデータが置き換えられます。アプリをインポートされたアプリと置き換えるには、次のアクセス権が必要です。

- 置き換えられるアプリ上での [**更新**]。
- アプリが公開される場合には、置き換えられるアプリでの [**公開**]、およびアプリの公開先のストリーム上での [**公開**] です。

アプリとインポートされたファイルとの置換

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMCスタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから[**アプリ**] を選択して、概要を表示します。
3. データ マネージャーでテーブルの **Import** in the action bar.
   [**アプリのインポート**] ダイアログ ボックスが開きます。
4. インポートするファイルを選択します。
5. インポートするアプリ(*qvf ファイル*) を参照して [**開く**] をクリックします。

> *長いファイル名を持つ画像がアプリに含まれている場合は、画像への完全パスが260文字を超えるとインポートに失敗します。パスが長すぎる場合は、画像のファイル名を短くしてください。*

参照のダイアログ ボックスが閉じ、qvfファイルの名前が [**Import app**] ダイアログ ボックスの [**アプリ名**] フィールドに表示されます。
[**アプリ名**] フィールドでアプリの名前を変更できます。[**アプリ名**] が一意でない場合は、この名前を持つアプリの数を知らせるメッセージが表示されます。

> *インポートされるアプリのデータ接続名が、既存のデータ接続の名前と同じ場合、データ接続はインポートされません。つまり、インポートされたアプリは、インポートされたアプリのデータ接続ではなく、同一名のすでに存在するデータ接続を使用します。*

6. [**既存のアプリを置換**] を選択します。
7. [**置き換えるアプリ**] をクリックしてアプリを選択します。
8. データなしでインポートする場合は、[**Import without data**] (データなしでインポート) を選択します。ビジュアライゼーションのみが置き換えられます。
9. ダイアログ ボックスで [**インポート**] をクリックします。
   [**転送中**] ダイアログが開きます。ダイアログには、自分が開始した転送がすべて表示されます。
   - ファイルのインポート中はスピナーが表示されます。
   - データ マネージャーでテーブルの to cancel the import.
     と[**中断**] が表示され、インポートが停止します。
   - 失敗したアイテムを削除するには、[**OK**] をクリックします。.
     [**転送中**] ダイアログからこのアイテムが削除されます。

When the app is replaced, is displayed and the app is added to the **Apps** overview. すべての転送が正常に完了すると[**Ongoing transport**] ダイアログが閉じます。転送に失敗した場合、概要ページが最新の情報に更新されるまでダイアログが表示されます。

> *サーバーにアプリをインポートする場合やサーバーからアプリをエクスポートする場合は、画像などの.qvf ファイルに保存されていない関連コンテンツも移動します。関連コンテンツは、%ProgramData%\Qlik\Sense\Repository\AppContent\<App ID> フォルダに個別に保存されます。各アプリには、アプリID をフォルダ名とする独自のアプリコンテンツ フォルダがあります。*

アプリ コンテンツ フォルダを置換する

画像などの.qvf ファイルに含まれていないアプリ コンテンツは、*%ProgramData%\Qlik\Sense\Repository\AppContent\<App ID>*フォルダに個別に保存されます。各アプリには、アプリID をフォルダ名とする独自のアプリ コンテンツ フォルダがあります。

- 既存のファイルが保存されます。
- 新しいファイルが追加されます。
- 新しいファイルが同じ名前の既存のファイルに置換されます。

アプリのエクスポート

アプリはエクスポートできます。例えば、このアプリはローカル バージョンの Qlik Sense で使用するか、別の Qlik Sense サイトにアプリをエクスポートしてください。未公開アプリの場合は、すべてのコンテンツがエクスポートされます。公開済みのアプリの場合、エクスポートには、.qvf ファイルの一部である公開済みの承認されたコンテンツのみが含まれます。エクスポートしたアプリは、お使いの Web ブラウザの既定のダウンロード フォルダに保存されます。

アプリをエクスポートするときに、オプションでデータなしでのアプリのエクスポートを選択することができます。データなしでアプリをインポートすると、データまたはデータ モデルに影響を与えずに、アプリをシートおよびストーリーと置き換えることができます。

アプリをエクスポートする場合、エクステンションはそのエクスポートに含められません。このため、Qlik Sense の異なるインスタンス間でアプリを移動すると、一部のビジュアライゼーションが描画されなくなる可能性がありますエクステンションは、インストール時に指定する共有フォルダー(\\<ドメイン>\QlikShare\StaticContent\Extensions など) から入手可能です。

QMC に表示されるアプリのファイル サイズは、ディスク上のファイル サイズとは異なります。これは、QMC でのサイズには、項目、テーブル、およびドキュメント プロパティなどのデータ オブジェクトのみが含まれており、.qvf ファイルにも含まれているビジュアライゼーション、ブックマーク、メジャーなどはこのサイズに含まれないためです。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**アプリ**] を選択して、概要を表示します。
3. エクスポートするタスクを選択します。
4. アクション バーで [**More actions**] をクリックします。
   ポップアップ メニューが開きます。
5. [**エクスポート**] をクリックします。
6. アプリをデータなしでエクスポートするには、[**Export app with data**] (データを含むアプリのエクスポート) をクリアします。
7. [**エクスポート**] をクリックします。
   [**転送中**] ダイアログが開きます。ダイアログには、自分が開始した転送がすべて表示されます。
   同時転送の最大数が設定されており、最大数に到達した場合はエラー メッセージが表示されます。
   - ファイルのエクスポート中はスピナーが表示されます。When the file export is complete, ✔ is displayed and the browser automatically starts to download the app to the default download folder of your web browser.

     エクスポートとダウンロードが完了する前に QMC を閉じたりログアウトしたりしないでください。エクスポートが完了せず、アプリ(qvf ファイル) は失われます。

- データ マネージャーでテーブルの to cancel the export.
  と[**中断**] が表示され、エクスポートが停止します。
- 失敗したアイテム を削除するには、[**OK**] をクリックします。.
  [**転送中**] ダイアログからこのアイテムが削除されます。

When the export and file download have finished, が表示されます。すべての転送が正常に完了すると[**Ongoing transport**] ダイアログが閉じます。転送に失敗した場合、概要ページが最新の情報に更新されるまでダイアログが表示されます。

サーバーにアプリをインポートする場合やサーバーからアプリをエクスポートする場合は、画像などの .qvf ファイルに保存されていない関連コンテンツも移動します。関連コンテンツは、%ProgramData%\Qlik\Sense\Repository\AppContent\<App ID> フォルダに個別に保存されます。各アプリには、アプリID をフォルダ名とする独自のアプリコンテンツ フォルダがあります。

ODBC データ接続を含むアプリの移動

Qlik Sense サイトまたは Qlik Sense Desktop インストール間でアプリを移動すると、データ接続は含まれません。アプリに ODBC データ接続が含まれる場合、新たな接続を作成するか、新たなサイトにすでにある接続を使用する必要があります。また、関連の ODBC データ ソースが新たな実装に存在することも確認する必要があります。これらの ODBC データ ソースは同じ名前と構成で、同じデータベースまたはファイルを指している必要があります。

アプリの複製

アプリを複製すると、読み取り権限のあるすべてのコンテンツが複製されます。公開済みのアプリの場合、複製には、.qvf ファイルの一部である公開済みの承認されたコンテンツのみが含まれます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**アプリ**] を選択して、概要を表示します。
3. 複製するアプリを選択します。

   アプリを複製すると、画像などの .qvf ファイルに含まれていないアプリ関連コンテンツを格納するフォルダも複製されます。このフォルダのパスは、%ProgramData%\Qlik\Sense\Repository\AppContent\<App ID> です。各アプリには、アプリ ID をフォルダ名とする独自のアプリコンテンツ フォルダがあります。
4. アクション バーで [**More actions**] をクリックし、ポップアップ メニューで [**Duplicate**] を選択します。

[**アプリが複製されました**] というメッセージが表示され、アプリの複製が [**アプリ**] 概要テーブルに追加されます。

*アプリへの作成アクセス権限と読み取りアクセス権限があり、QMC の [**アプリ**] セクションへの読み取りアクセス権限がある場合、アプリを複製できます。ただし、セキュリティ上の理由で、スクリプトを複製できるのは、スクリプトの読み取り権限も持っている場合のみです。スクリプトにアクセスするとセクションアクセスを編集または削除でき、その結果、アクセスできてはならないデータをロードできます。*

リロードタスクの作成

アプリ概要ページから、アプリ向けにリロードタスクを作成できます。

リロードタスクを新規作成する方法は複数あります。

- アプリ概要のページから
- [**App edit**] ページの [**Associated items**] タブから
- タスク概要のページから
- 適切な権限を持つユーザーによって、ハブから

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**アプリ**] を選択して、概要を表示します。
3. タスクを作成するアプリを選択し、アクション バーの右端にある [**その他のアクション**] をクリックして、ポップアップ メニューで [**リロード タスクの新規作成**] を選択します。
   別の方法:
   a. リロードタスクを作成するアプリを選択し、操作バーで [**Edit**] をクリックします。
   b. [**関連するアイテム**] の下にある [**タスク**] を選択します。
   c. タスクページの ⊕ 操作バーにある [**タスクのリロード**] をクリックします。

   どちらの方法でも [**リロード タスクの編集**] ページが表示されます。
4. プロパティを編集します。
   a. [**名前**] フィールドでタスク名を変更できます。既定で、名前は *Reload task of <App name>* (<App name> のリロードタスク) になっています。
   b. [**アプリ**] は、概要から選択したアプリを表示します。[**App**] フィールドをクリックして、タスクを作成している対象のアプリを変更できます。開いたダイアログ ボックスで、このタスクをリロードするアプリをダブルクリックします。
   c. [**実行**] プロパティを変更できます。以下の説明を参照してください。このタスクは、既定では [**有効**] ✔ になっています。選択をクリアすると、タスクが無効になります。
   d. タスクには少なくとも、自動実行するトリガーがひとつ含まれている必要があります。[**トリガー**] の表見出しにある [**アクション**] ▼ をクリックしてトリガーを管理し、次からひとつ選択します:
      - [**1 回のみのトリガーを新規作成**]、[**時間ベースのトリガーを新規作成**]、[**日単位のトリガーを新規作成**]、[**週単位のトリガーを新規作成**]、[**月単位のトリガーを新規作成**] の中から選び、新しいトリガーを作成します。これらはトリガーのショートカットで、選択したトリガーがテーブルに即座に追加されます。トリガーの開始値は、作成時から5分に設定され、トリガーが有効になります。

- [**スケジュール済みトリガーを新規作成**] または [**タスクイベントトリガーを新規作成**] を使い、選択されたタイプのトリガーを新規作成します (下記のプロパティの説明を参照)。ダイアログが開きます。トリガーを編集して [**OK**] をクリックすると、ダイアログが閉じてテーブルにトリガーが追加されます。
- 適宜、[**編集**] を使い、テーブルで選択されたトリガーの編集ダイアログを開きます。トリガーを編集し、[**OK**] をクリックしてダイアログを閉じ、変更内容を保存します。
- 適宜、[**削除**] を使い、テーブルで選択されたトリガーを削除します。

現在編集中のすべてのトリガに適用するために、↩[**トリガ**] の見出しにある元に戻す() をクリックします。

e. 任意でタグを適用します。

f. 任意で、カスタムプロパティを適用します。

ID

全項目が必須で、空欄のままにはできません。

ID プロパティ

プロパティ	説明	既定値
[**名前**]	タスクの名前。	<アプリ名> のタスクのリロード。
[**アプリ**]	タスクが作成されたアプリの名前。項目をクリックしてダイアログを開き、タスクがリロードするアプリを (ダブルクリックして) 選択します。	<App name>

実行

実行プロパティ

プロパティ	説明	既定値
[**有効化**]	選択されている場合、タスクは有効です。	選択済み
部分的なリロード	部分的なリロードでは、データモデルの既存のテーブルをすべてリロードすることなく、新しいデータを追加することができます。フル リロードでは、すべてのテーブルを削除してから、ロードスクリプトを実行します。部分的なリロードでは、新しいデータを追加するだけで、既存のテーブルは維持されます。 部分的なリロードには、完全なリロードと比較していくつかの利点があります。 • 最近変更されたデータのみをロードする必要があるため、より高速です。データセットが大きい場合、違いは大きくなります。 • ロードされるデータが少ないため、消費されるメモリも少なくなります。 • ソースデータへのクエリがより高速に実行され、ネットワークの問題のリスクが軽減されるため、信頼性が向上します。	選択されていない

プロパティ	説明	既定値
[**タスクセッション タイムアウト (分)**]	タスクが停止するまでの最大時間 タスクが開始すると、マネージャー スケジューラによってセッションが開始、ノードの 1 つによってタスクが実行されます。セッションがタイムアウトすると、マネージャー スケジューラは強制的にノードにタスクを中止させて、セッションを削除します。	1440
[**最大リトライ数**]	スケジューラが失敗したタスクの再起動を試みる最大回数。	0

トリガー (スケジュール済み)

スケジュール済みトリガーのプロパティ

プロパティ	説明
[**トリガー名**]	トリガーの名前。必須。
[**有効化**]	トリガーの状態。選択するとトリガーはアクティブになります。
[**タイムゾーン**]	オペレーティング システムのタイム ゾーンがトリガーを作成した時間になります。トリガーを保存すると設定は保持され、タイムゾーンが違う場所に行っても元の設定値のまま表示されます。タイム ゾーンやトリガーの開始時間を変更したい場合は手動で行う必要があります。 *タイム ゾーンの設定より前に作成されたトリガーについては、日時はすべてデフォルトで Coordinated Universal Time (UTC: 協定世界時) にて表示されます。*

プロパティ	説明
[**夏時間**]	夏時間を考慮する方法。 [**夏時間を使用する**]: このオプションでは夏時間 (DST) が考慮されます。選択したタイム ゾーンで DST が使われていると、実行日時はそれに応じて調整されます。 [**常に標準時**]: このオプションでは DST は考慮されません。選択したタイム ゾーンで DST が使われていても、実行日時は調整されません。 [**常に夏時間**]: このオプションでは DST が考慮されません。タイム ゾーンで DST が使われている場合は、DST の適用期間外でも実行日時は常に DST に準じます。 *DST を使用しないタイム ゾーンの場合は、常に [**永久標準時**] を選択します。* 1 月にカナダのオタワで午前 10 時に開始するイベントのトリガーを作成したとします。ここのタイム ゾーンは (GMT-0500) 東部標準時 (米国およびカナダ) で DST の期間は 3 月から 11 月です。 [**夏時間を使用する**] を選択すると、10 時に開始するよう設定されたトリガーは常に 10 時に開始します。 [**常に標準時**] を選択すると、10 時に実行するよう設定されたトリガーは冬は 10 時に実行されますが夏は 9 時に実行されます。 [**常に夏時間**] を選択すると、10 時に実行するよう設定されたトリガーは冬は 11 時に、夏は 10 時に実行されます。
[**Start**]	開始時間と開始日: • 開始時間: [**(hh:mm)**] • 開始日: **(YYYY-MM-DD)**

プロパティ	説明

[スケジュール]	トリガーの頻度。
	• [**1 回**]。
	• [**時間単位**]。トリガー実施の間隔。次の値を入力して、[**各条件の後に繰り返す**]を編集します。
	  • [**s (時間単位**] (既定 1 時間)
	  • [**s (分単位**] (既定 0 分)
	• [**日単位**]。トリガー実施の間隔。[**Every**][**s (日おき**] (既定 1 日) の値を入力します。たとえば、2 と入力すると2 日おきにトリガーが繰り返されます。
	• [**週単位**]。トリガー実施の間隔:
	  • [**Every**][**s (週おき**] (既定 1 週) の値を入力します。
	  • [**平日**] のチェックボックスを選択して (複数日可)、トリガーが繰り返される日を決めます (ユーザーが指定する週で)。たとえば、3 と入力して [**月曜日**] を選択すると、3 週おきの月曜日にトリガーが実行されます。
	• [**月単位**]。[**On these days**] のチェックボックスを選択 (複数可) すると、毎月トリガーが繰り返し実行される日を定義できます。
	  *[**Monthly**] を選択し、トリガーが毎月繰り返されるようにするには、28 日よりも前の日を選択する必要があります。*
	• ***カスタム***: [**カスタム**] を選択すると、[**フィルター**] と [**増分**] の 2 つの新しい項目が表示されます。これらのオプションは、リロードをスケジュールするときに大きな柔軟性を提供します。詳細は、「*タスク- カスタム オプション (page 228)*」を参照してください。

[**終了**]	終了時間と終了日: • 終了時間: [**(hh:mm)**] • 終了日:**(YYYY-MM-DD)** [**無期限**] を選択して、終了日のないトリガーを作成します。

トリガー (タスク イベント)

タスク イベント トリガーのプロパティ

プロパティ	説明
[**トリガー名**]	トリガーの名前。必須。

プロパティ	説明
[タイプ]	トリガーのタイプ。
[有効化]	トリガーの状態。選択するとトリガーはアクティブになります。
[時間制限]	タスクチェーンの他のタスクを完了しなければならない期間 (分単位)。トリガーがひとつのタスクだけで構成されている場合、何も起きません。 *タスクチェーンの作成 (page 355)*
[タスク]	
	次の手順を実行します。 1. ⊕ [タスクの追加] をクリックして、トリガー条件として機能するタスクを追加します。[ステータス] リストと空の [タスク] 項目が追加されます。 2. 空の項目をクリックしてタスクを追加します。 タスク選択ダイアログが開き、次の列とともにタスクの一覧が表示されます。[名前]、タスクに接続した [アプリ]、タスク名である [タグ]。 3. タスクをダブルクリックし、トリガー条件として使用します。 トリガーにタスクを追加し、ダイアログを閉じます。 4. [ステータス] リストで、トリガー条件が [**TaskSuccessful**] または [**TaskFail**] で処理されるかどうかを選択します。 *[タスク失敗] のトリガー条件を持つタスクは、先行タスクが失敗の状態で完了するときだけでなく、スキップまたはエラー (リロード前にエラーが発生する場合) の状態でも開始されます。2019 年 2 月以前の Qlik Sense バージョンでは、中止状態の先行タスクによっても「タスク失敗」トリガー条件によってもタスクが開始されました。この動作を有効にするには、すべてのスケジューラー ノードの Scheduler.exe.config で「DisableLegacyTaskEventTriggerBehavior」を「false」に設定します。* トリガーに含めたい全タスクで、上記のステップを繰り返します。タスクは一度しか追加できず、トリガーにすでに追加されている場合にはタスク選択ダイアログに表示されません。タスクの間には論理的な AND があります。

タスクを指定の順番で実行する必要はなく、[時間制限] は固定されていません。時間が制限に達した時に、1 つのタスクを除いてすべてのタスクが完了している場合、最初に完了したタスクは実行済みとはみなされず、期間の終わりを再計算します。トリガーは、再計算された期間にすべてのタスクが完了するのを待ちます。

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

カスタム プロパティ

***カスタム プロパティ**を利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

5. [**適用**] をクリックして、ルールを作成し、保存します。
ページ最下部に [**追加完了**] と表示されます。

リロード タスクの編集

更新権限を有するリロード タスクをアプリの関連付けページから編集できます。

タスク概要 ページからリロード タスクを編集することもできます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**アプリ**] を選択して、概要を表示します。
3. タスクを編集したいアプリを選択し、アクション バーで [**Edit**] をクリックします。
4. [**関連するアイテム**] の [**タスク**] を選択します。
5. 編集するタスクを選択し、操作バーで [**Edit**] をクリックします。
[**リロード タスク編集**] ページが表示されます。
6. プロパティを編集します。
    a. [**名前**] フィールドでタスク名を変更できます。
    b. [**アプリ**] は、概要から選択したアプリを表示します。[**App**] フィールドをクリックして、タスクを作成している対象のアプリを変更できます。開いたダイアログ ボックスで、このタスクをリロードするアプリをダブルクリックします。
    c. [**実行**] プロパティを変更できます。以下の説明を参照してください。
    d. タスクには少なくとも、自動実行するトリガーがひとつ含まれている必要があります。[**トリガー**] の表見出しにある [**アクション**] ▼ をクリックしてトリガーを管理し、次からひとつ選択します:
        - [**1 回のみのトリガーを新規作成**]、[**時間ベースのトリガーを新規作成**]、[**日単位のトリガーを新規作成**]、[**週単位のトリガーを新規作成**]、[**月単位のトリガーを新規作成**] の

中から選び、新しいトリガーを作成します。これらはトリガーのショートカットで、選択したトリガーがテーブルに即座に追加されます。トリガーの開始値は、作成時から5分に設定され、トリガーが有効になります。

- [**スケジュール済みトリガーを新規作成**] または [**タスクイベントトリガーを新規作成**] を使い、選択されたタイプのトリガーを新規作成します (下記のプロパティの説明を参照)。ダイアログが開きます。トリガーを編集して [**OK**] をクリックすると、ダイアログが閉じてテーブルにトリガーが追加されます。
- 適宜、[**削除**] を使い、テーブルで選択されたトリガーを削除します。
- 適宜、[**編集**] を使い、テーブルで選択されたトリガーの編集ダイアログを開きます。トリガーを編集し、[**OK**] をクリックしてダイアログを閉じ、変更内容を保存します。

e. 任意でタグを適用します。

f. 任意で、カスタムプロパティを適用します。

ID

全項目が必須で、空欄のままにはできません。

ID プロパティ

プロパティ	説明	既定値
[**名前**]	タスクの名前。	<アプリ名> のタスクのリロード。
[**アプリ**]	タスクが作成されたアプリの名前。項目をクリックしてダイアログを開き、タスクがリロードするアプリを (ダブルクリックして) 選択します。	<App name>

実行

実行プロパティ

プロパティ	説明	既定値
[**有効化**]	選択されている場合、タスクは有効です。	選択済み
部分的なリロード	部分的なリロードでは、データモデルの既存のテーブルをすべてリロードすることなく、新しいデータを追加することができます。フル リロードでは、すべてのテーブルを削除してから、ロードスクリプトを実行します。部分的なリロードでは、新しいデータを追加するだけで、既存のテーブルは維持されます。 部分的なリロードには、完全なリロードと比較していくつかの利点があります。 • 最近変更されたデータのみをロードする必要があるため、より高速です。データセットが大きい場合、違いは大きくなります。 • ロードされるデータが少ないため、消費されるメモリも少なくなります。 • ソースデータへのクエリがより高速に実行され、ネットワークの問題のリスクが軽減されるため、信頼性が向上します。	選択されていない

プロパティ	説明	既定値
[**タスクセッション タイムアウト(分)**]	タスクが停止するまでの最大時間 タスクが開始すると、マネージャー スケジューラによってセッションが開始、ノードの 1 つによってタスクが実行されます。セッションがタイムアウトすると、マネージャー スケジューラは強制的にノードにタスクを中止させて、セッションを削除します。	1440
[**最大リトライ数**]	スケジューラが失敗したタスクの再起動を試みる最大回数。	0

トリガー (スケジュール済み)

スケジュール済みトリガーのプロパティ

プロパティ	説明
[**トリガー名**]	トリガーの名前。必須。
[**有効化**]	トリガーの状態。選択するとトリガーはアクティブになります。
[**タイムゾーン**]	オペレーティング システムのタイム ゾーンがトリガーを作成した時間になります。トリガーを保存すると設定は保持され、タイムゾーンが違う場所に行っても元の設定値のまま表示されます。タイム ゾーンやトリガーの開始時間を変更したい場合は手動で行う必要があります。 *タイム ゾーンの設定より前に作成されたトリガーについては、日時はすべてデフォルトで Coordinated Universal Time (UTC: 協定世界時) にて表示されます。*

プロパティ	説明
[**夏時間**]	夏時間を考慮する方法。 [**夏時間を使用する**]: このオプションでは夏時間 (DST) が考慮されます。選択したタイム ゾーンで DST が使われていると、実行日時はそれに応じて調整されます。 [**常に標準時**]: このオプションでは DST は考慮されません。選択したタイム ゾーンで DST が使われていても、実行日時は調整されません。 [**常に夏時間**]: このオプションでは DST が考慮されません。タイム ゾーンで DST が使われている場合は、DST の適用期間外でも実行日時は常に DST に準じます。 *DST を使用しないタイム ゾーンの場合は、常に [**永久標準時**] を選択します。* 1 月にカナダのオタワで午前 10 時に開始するイベントのトリガーを作成したとします。ここのタイム ゾーンは (GMT-0500) 東部標準時 (米国およびカナダ) で DST の期間は 3 月から 11 月です。 [**夏時間を使用する**] を選択すると、10 時に開始するよう設定されたトリガーは常に 10 時に開始します。 [**常に標準時**] を選択すると、10 時に実行するよう設定されたトリガーは冬は 10 時に実行されますが夏は 9 時に実行されます。 [**常に夏時間**] を選択すると、10 時に実行するよう設定されたトリガーは冬は 11 時に、夏は 10 時に実行されます。
[**Start**]	開始時間と開始日: • 開始時間: [**(hh:mm)**] • 開始日: **(YYYY-MM-DD)**

プロパティ	説明

[スケジュール]	トリガーの頻度。
	• [**1 回**]。
	• [**時間単位**]。トリガー実施の間隔。次の値を入力して、[**各条件の後に繰り返す**]を編集します。
	  • [**s (時間単位**] (既定 1 時間)
	  • [**s (分単位**] (既定 0 分)
	• [**日単位**]。トリガー実施の間隔。[**Every**][**s (日おき**] (既定 1 日) の値を入力します。たとえば、2 と入力すると2 日おきにトリガーが繰り返されます。
	• [**週単位**]。トリガー実施の間隔:
	  • [**Every**][**s (週おき**] (既定 1 週) の値を入力します。
	  • [**平日**] のチェックボックスを選択して (複数日可)、トリガーが繰り返される日を決めます (ユーザーが指定する週で)。たとえば、3 と入力して [**月曜日**] を選択すると、3 週おきの月曜日にトリガーが実行されます。
	• [**月単位**]。[**On these days**] のチェックボックスを選択 (複数可) すると、毎月トリガーが繰り返し実行される日を定義できます。
	  *[**Monthly**] を選択し、トリガーが毎月繰り返されるようにするには、28 日よりも前の日を選択する必要があります。*
	• ***カスタム***: [**カスタム**] を選択すると、[**フィルター**] と [**増分**] の 2 つの新しい項目が表示されます。これらのオプションは、リロードをスケジュールするときに大きな柔軟性を提供します。詳細は、「*タスク- カスタム オプション (page 228)*」を参照してください。

[**終了**]	終了時間と終了日: • 終了時間: [**(hh:mm)**] • 終了日:**(YYYY-MM-DD)** [**無期限**] を選択して、終了日のないトリガーを作成します。

トリガー (タスク イベント)

タスク イベント トリガーのプロパティ

プロパティ	説明
[**トリガー名**]	トリガーの名前。必須。

プロパティ	説明
[**タイプ**]	トリガーのタイプ。
[**有効化**]	トリガーの状態。選択するとトリガーはアクティブになります。
[**時間制限**]	タスクチェーンの他のタスクを完了しなければならない期間 (分単位)。トリガーがひとつのタスクだけで構成されている場合、何も起きません。 *タスクチェーンの作成 (page 355)*
[**タスク**]	
	次の手順を実行します。 1. ⊕ [**タスクの追加**] をクリックして、トリガー条件として機能するタスクを追加します。[**ステータス**] リストと空の [**タスク**] 項目が追加されます。 2. 空の項目をクリックしてタスクを追加します。 タスク選択ダイアログが開き、次の列とともにタスクの一覧が表示されます。[**名前**]、タスクに接続した [**アプリ**]、タスク名である [**タグ**]。 3. タスクをダブルクリックし、トリガー条件として使用します。 トリガーにタスクを追加し、ダイアログを閉じます。 4. [**ステータス**] リストで、トリガー条件が [**TaskSuccessful**] または [**TaskFail**] で処理されるかどうかを選択します。 *[**タスク失敗**] のトリガー条件を持つタスクは、先行タスクが失敗の状態で完了するときだけでなく、スキップまたはエラー (リロード前にエラーが発生する場合) の状態でも開始されます。2019 年 2 月以前の Qlik Sense バージョンでは、中止状態の先行タスクによっても「タスク失敗」トリガー条件によってもタスクが開始されました。この動作を有効にするには、すべてのスケジューラー ノードの Scheduler.exe.config で「DisableLegacyTaskEventTriggerBehavior」を「false」に設定します。* トリガーに含めたい全タスクで、上記のステップを繰り返します。タスクは一度しか追加できず、トリガーにすでに追加されている場合にはタスク選択ダイアログに表示されません。タスクの間には論理的な AND があります。

*タスクを指定の順番で実行する必要はなく、[**時間制限**] は固定されていません。時間が制限に達した時に、1 つのタスクを除いてすべてのタスクが完了している場合、最初に完了したタスクは実行済みとはみなされず、期間の終わりを再計算します。トリガーは、再計算された期間にすべてのタスクが完了するのを待ちます。*

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

カスタム プロパティ

> ***カスタム プロパティ**を利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

7. アクション バーで [**適用**] をクリックし、変更内容を保存します。
ページの最下部に [**更新完了**] と表示されます。

タスク - カスタム オプション

タスクを作成する場合、[***カスタム***] オプションを使用すると、タスクのスケジュールを柔軟に設定できます。適切に機能するタスクを作成するには、それぞれの項目である [***フィルター***] と [**増分**] の構文に精通していることが重要です。このトピックでは、[***カスタム***] スケジュールを使用する場合のオプションについて詳しく説明します。

フィルター

フィルターとして設定するのは、タスクをトリガーできる場合であり、その逆ではありません。フィルターはタスクの条件を定義します。

フィルターの既定の構文は「* * - * * * * *」です。各位置の間以外に、フィルター内にスペースを入れないでください。スペース文字は位置間の区切り文字として使用され、スペース文字を挿入すると、フィルターでエラーが発生する可能性があります。

位置
左から右 (最初の位置は 0)、各位置はここで説明されています。

位置 0 - Minute

凡例: 1–60。「*」= すべて

タスクをトリガーできる時間の分数 (0〜60)。

位置 1 - Hour

凡例: 1–24。「*」= すべて

タスクをトリガーできる 1 日の時間 (1〜24)。

位置 2 - WeekDayPrefix

凡例: 1–4。「¤」= 最後。「-」= なし

WeekDayPrefix はプレフィックスを追加することで WeekDay と連携します。WeekDayPrefix を使用すると、特定の月の最後の (¤) 金曜日、または特定の月の最初の (1) 土曜日のみ、タスクをトリガーできることを指定できます。

構文: 位置 3 - WeekDay
凡例: 0–6 (日曜日は 0)

タスクをトリガーできる曜日。

位置 4 - WeeklyInterval

凡例: 整数。「*」= すべて

タスクは n: 週ごとにトリガーできます。ここで、n はこの位置に設定された数値です。

位置 5 - DayOfMonth

凡例: 1–31。「*」= すべて。「¤」= 最後

タスクをトリガーできる月の日にち。最終 (¤) を使用すると、タスクは月の最終日にトリガーされ、月 (およびうるう年) に応じて動的にチェックされます。

*Microsoft Windows ユーザー向け: 最後の記号 (¤) を追加するには、**Alt** キーを押しながらテンキーで **0164** と入力します。*

位置 6 - Month

凡例: 1–12。「*」= すべて

タスクをトリガーできる年の月。

位置 7 - MonthlyInterval

凡例: 整数。「*」= すべて

タスクをトリガーできるようになるまでに経過する必要のある月数。

Minute、Hour、WeekDay、DayOfMonth、Month の場合、ハイフン (-) を使用した構文を使用して、「From - To」を指定できます。WeekDayPrefix、WeeklyInterval、MonthlyInterval の場合、フィルターで使用する各文字を指定する必要があります。このオプションは、Minute、Hour、WeekDay、DayOfMonth、Month でも使用できます。

例: 各時間の最初の 15 分間のみタスクを許可する必要があります。最初の位置に「1–15」または「1,2,3,4,5,6,7,8,9,10,11,12,13,14,15」を入力できます。

増分

既定:「0 0 0 0」

既定の増分、つまり「0 0 0 0」が使用されている場合、タスクは 1 回だけトリガーされます。

ここでは、左から右 (最初の位置は 0) の各位置について説明します。

位置 0 - Minutes

増分する分数。

位置 1 - Hours

増分する時間数。

位置 2 - Days

増分する日数。

位置 3 - Weeks

増分する週数。

一般的なガイドライン

- 1 時間に 1 回よりも高い頻度の 1 時間ごとのタスクでは、Minutes を適切な数値に設定する必要があります。
- 1 時間に 1 回以下の頻度の 1 時間ごとのタスクでは、Hours を適切な数値に設定する必要があります。
- 毎日のタスクでは、Days が適切な数値に設定する必要があります。
- 毎週または毎月のトリガーは、毎日の評価に基づいているため (毎週木曜日と土曜日に 4 週間ごとに実行する、または毎月 5 日、10 日、15 日に実行するなど)、フィルターが存在する場合は Days を適切な数値に設定する必要があります。
- フィルターが存在しない場合、増分はタスクがトリガーされる頻度と一致する必要があります。

例

タスクを設定する方法の例をいくつか示します。

特定の時間と分

前提: タスクは 11.15 から 11.59 (任意の日) の間にのみトリガーされます。

次のフィルターでは、1 年の特定の日の 11.15 から 11.59 の間にのみタスクをトリガーできます。

フィルター:「15-59 11 - * * * * *」

説明: 位置 0 は「15-59」です。これは、それらの分の間のみトリガーされることを意味します。

位置 1 は「11」です。これは、その時間にのみトリガーされることを意味します。

このタスクの増分は、達成する内容に基づいていますが、落とし穴があります。特に、タスクをスケジュールしていて、開始時刻が 11.15～11.59 の範囲外、例えば 12.15 で、増分が一度に 1 日進むように設定されている場合、このタスクはトリガーされません。ほとんどの場合、増分は n 時間ごとまたは n 分ごとである必要があります。

WeekDayPrefix の使用
前提: タスクは、毎月第 1 月曜日にのみトリガーする必要があります。

フィルター:「* * 1 1 * * * *」

説明: 位置 2 は「1」に設定されています。これは、指定された曜日の最初の日が許可されることを意味します。位置 3 は「1」に設定されています。これは、このタスクに許可されるのは月曜日 (0 は日曜日) のみであることを意味します。

このタスクは 1 日、つまり「0 0 1 0」ずつ増加する必要があります。

月の特定の日付

ケース 1

前提: 毎月 1 日に実行します。

フィルター:「* * - * * 1 * *」

説明: 位置 5 は「1」に設定されています。これは、このタスクに許可されるのは特定の月の 1 日目のみであることを意味します。

このタスクは 1 日、つまり「0 0 1 0」ずつ増加する必要があります。

ケース 2

前提: 毎月最終日に実行します。

フィルター:「* * - * * ¤ * *」

説明: 位置 5 は「¤」に設定されています。これは、このタスクに許可されるのは特定の月の最終日のみであることを意味します。

このタスクは 1 日、つまり「0 0 1 0」ずつ増加する必要があります。

ケース 3

前提: 毎年最終日に実行します。

フィルター:「* * - * * ¤ 12 *」

説明: 位置 5 は「¤」に設定されています。これは、このタスクに許可されるのは特定の月の最終日であることを意味します。位置 6 は「12」に設定されています。これは、このタスクが許可されるのは12 か月目 (12 月) のみであることを意味します。

このタスクは 1 日、つまり「0 0 1 0」ずつ増加する必要があります。

特定の曜日
前提: 毎週月曜日と水曜日に実行します。

フィルター:「* * - 1,3 * * * *」

説明: 位置 4は「1,3」に設定されています。これは、このタスクに許可されるのは月曜日と水曜日のみであることを意味します (0 は日曜日)。

このタスクは 1 日、つまり「0 0 1 0」ずつ増加する必要があります。

WeekDayPrefix、WeekDay、Month の使用
前提: 隔月で最後の金曜日に実行します。

フィルター: 「* * ¤ 5 * * 1,3,5,7,9,11 *」

説明: 位置 3 は、位置 4 で指定された最後の曜日を意味する「¤」に設定されています。位置 4 は、このタスクに許可されるのは金曜日 (日曜日は 0) であることを意味する「5」に設定されています。合わせて「最後の金曜日」と読みます。位置 6 は「1,3,5,7,9,11」に設定されています。これは、このタスクが許可されるのはそれらの月のみであることを意味します。

このタスクは 1 日、つまり「0 0 1 0」ずつ増加する必要があります。

外部プログラム タスクの作成と編集

外部プログラムタスクを使用して、スクリプトや.exeファイルなどの外部プロセスをトリガできます。タスクチェーンに対応しており、リロードタスクと外部プログラムのタスクを組み合わせることができます。

次の手順を実行します。

1. QMCで、[**タスク**]を開きます。
2. クリック [**外部プログラムタスク**] で新しい外部プログラムタスクを作成するか、既存のタスクをダブルクリックして編集します。
3. タスク名を入力します。
4. トリガするファイルのパスを入力します。
5. トリガーするファイルの入力パラメータを入力します(ある場合) 。
6. 必要に応じて、[**EXECUTION**] セクションの設定を編集することができます。

   タスクのセッションタイムアウト: タスクが停止するまでの最大時間 タスクが開始すると、マネージャー スケジューラによってセッションが開始、ノードの 1 つによってタスクが実行されます。セッションがタイムアウトすると、マネージャー スケジューラは強制的にノードにタスクを中止させて、セッションを削除します。

7. タスクには少なくとも、自動実行するトリガーがひとつ含まれている必要があります。[**トリガー**] の表見出しにある [**アクション**] ▼ をクリックしてトリガーを管理し、次からひとつ選択します:
   - [**1 回のみのトリガーを新規作成**]、[**時間ベースのトリガーを新規作成**]、[**日単位のトリガーを新規作成**]、[**週単位のトリガーを新規作成**]、[**月単位のトリガーを新規作成**] の中から選び、新しいトリガーを作成します。これらはトリガーのショートカットで、選択したトリガーがテーブルに即座に追加されます。トリガーの開始値は、作成時から5 分に設定され、トリガーが有効になります。
   - [**スケジュール済みトリガーを新規作成**] または [**タスク イベント トリガーを新規作成**] を使い、選択されたタイプのトリガーを新規作成します (下記のプロパティの説明を参照)。ダイアログが開きます。トリガーを編集して [**OK**] をクリックすると、ダイアログが閉じてテーブルにトリガーが追加されます。

- 適宜、[**編集**] を使い、テーブルで選択されたトリガーの編集ダイアログを開きます。トリガーを編集し、[**OK**] をクリックしてダイアログを閉じ、変更内容を保存します。
- 適宜、[**削除**] を使い、テーブルで選択されたトリガーを削除します。
  現在編集中のすべてのトリガに適用するために、[**トリガ**] の見出しにある元に戻す() をクリックします。

トリガー (スケジュール済み)

スケジュール済みトリガーのプロパティ

プロパティ	説明
[**トリガー名**]	トリガーの名前。必須。
[**有効化**]	トリガーの状態。選択するとトリガーはアクティブになります。
[**タイムゾーン**]	オペレーティング システムのタイム ゾーンがトリガーを作成した時間になります。トリガーを保存すると設定は保持され、タイムゾーンが違う場所に行っても元の設定値のまま表示されます。タイム ゾーンやトリガーの開始時間を変更したい場合は手動で行う必要があります。 *タイム ゾーンの設定より前に作成されたトリガーについては、日時はすべてデフォルトで Coordinated Universal Time (UTC: 協定世界時) にて表示されます。*

プロパティ	説明
[**夏時間**]	夏時間を考慮する方法。 [**夏時間を使用する**]: このオプションでは夏時間 (DST) が考慮されます。選択したタイム ゾーンで DST が使われていると、実行日時はそれに応じて調整されます。 [**常に標準時**]: このオプションでは DST は考慮されません。選択したタイム ゾーンで DST が使われていても、実行日時は調整されません。 [**常に夏時間**]: このオプションでは DST が考慮されません。タイム ゾーンで DST が使われている場合は、DST の適用期間外でも実行日時は常に DST に準じます。 *DST を使用しないタイム ゾーンの場合は、常に [**永久標準時**] を選択します。* 1 月にカナダのオタワで午前 10 時に開始するイベントのトリガーを作成したとします。ここのタイム ゾーンは (GMT-0500) 東部標準時 (米国およびカナダ) で DST の期間は 3 月から 11 月です。 [**夏時間を使用する**] を選択すると、10 時に開始するよう設定されたトリガーは常に 10 時に開始します。 [**常に標準時**] を選択すると、10 時に実行するよう設定されたトリガーは冬は 10 時に実行されますが夏は 9 時に実行されます。 [**常に夏時間**] を選択すると、10 時に実行するよう設定されたトリガーは冬は 11 時に、夏は 10 時に実行されます。
[**Start**]	開始時間と開始日: • 開始時間: [**(hh:mm)**] • 開始日: **(YYYY-MM-DD)**

プロパティ	説明

[スケジュール]	トリガーの頻度。
	• [**1 回**]。
	• [**時間単位**]。トリガー実施の間隔。次の値を入力して、[**各条件の後に繰り返す**]を編集します。
	  • [**s (時間単位**] (既定 1 時間)
	  • [**s (分単位**] (既定 0 分)
	• [**日単位**]。トリガー実施の間隔。[**Every**][**s (日おき**] (既定 1 日) の値を入力します。たとえば、2 と入力すると2 日おきにトリガーが繰り返されます。
	• [**週単位**]。トリガー実施の間隔:
	  • [**Every**][**s (週おき**] (既定 1 週) の値を入力します。
	  • [**平日**] のチェックボックスを選択して (複数日可)、トリガーが繰り返される日を決めます (ユーザーが指定する週で)。たとえば、3 と入力して [**月曜日**] を選択すると、3 週おきの月曜日にトリガーが実行されます。
	• [**月単位**]。[**On these days**] のチェックボックスを選択 (複数可) すると、毎月トリガーが繰り返し実行される日を定義できます。
	  *[**Monthly**] を選択し、トリガーが毎月繰り返されるようにするには、28 日よりも前の日を選択する必要があります。*
	• ***カスタム***: [**カスタム**] を選択すると、[**フィルター**] と [**増分**] の 2 つの新しい項目が表示されます。これらのオプションは、リロードをスケジュールするときに大きな柔軟性を提供します。詳細は、「*タスク- カスタム オプション (page 228)*」を参照してください。

[**終了**]	終了時間と終了日: • 終了時間: [**(hh:mm)**] • 終了日:**(YYYY-MM-DD)** [**無期限**] を選択して、終了日のないトリガーを作成します。

トリガー (タスク イベント)

タスク イベント トリガーのプロパティ

プロパティ	説明
[**トリガー名**]	トリガーの名前。必須。

プロパティ	説明
[タイプ]	トリガーのタイプ。
[有効化]	トリガーの状態。選択するとトリガーはアクティブになります。
[時間制限]	タスクチェーンの他のタスクを完了しなければならない期間 (分単位)。トリガーがひとつのタスクだけで構成されている場合、何も起きません。 *タスクチェーンの作成 (page 355)*
[タスク]	
	次の手順を実行します。 1. ⊕ [タスクの追加] をクリックして、トリガー条件として機能するタスクを追加します。[ステータス] リストと空の [タスク] 項目が追加されます。 2. 空の項目をクリックしてタスクを追加します。 タスク選択ダイアログが開き、次の列とともにタスクの一覧が表示されます。[名前]、タスクに接続した [アプリ]、タスク名である [タグ]。 3. タスクをダブルクリックし、トリガー条件として使用します。 トリガーにタスクを追加し、ダイアログを閉じます。 4. [ステータス] リストで、トリガー条件が [**TaskSuccessful**] または [**TaskFail**] で処理されるかどうかを選択します。 *[タスク失敗] のトリガー条件を持つタスクは、先行タスクが失敗の状態で完了するときだけでなく、スキップまたはエラー (リロード前にエラーが発生する場合) の状態でも開始されます。2019 年 2 月以前の Qlik Sense バージョンでは、中止状態の先行タスクによっても「タスク失敗」トリガー条件によってもタスクが開始されました。この動作を有効にするには、すべてのスケジューラー ノードの Scheduler.exe.config で「DisableLegacyTaskEventTriggerBehavior」を「false」に設定します。* トリガーに含めたい全タスクで、上記のステップを繰り返します。タスクは一度しか追加できず、トリガーにすでに追加されている場合にはタスク選択ダイアログに表示されません。タスクの間には論理的な AND があります。

タスクを指定の順番で実行する必要はなく、[時間制限] は固定されていません。時間が制限に達した時に、1 つのタスクを除いてすべてのタスクが完了している場合、最初に完了したタスクは実行済みとはみなされず、期間の終わりを再計算します。トリガーは、再計算された期間にすべてのタスクが完了するのを待ちます。

8. 必要に応じて、タグとカスタムプロパティを追加します。
9. [適用] をクリックしてタスクを保存します。

配布タスク の作成および編集

配布 タスクでは、クライアントが管理する Qlik Sense から Qlik Cloud へのアプリの配布をトリガーすることができます。

次の手順を実行します。

1. QMCで、[**タスク**]を開きます。
2. 操作バーで [**配布タスク**] をクリックして新規に配布タスクを作成するか、既存のタスクをダブルクリックして編集します。
3. タスク名を入力します。
4. 配布するアプリを選択します。
5. トリガーするファイルの入力パラメータを入力します(ある場合) 。
6. 必要に応じて、[**EXECUTION**] セクションの設定を編集することができます。

   タスクのセッションタイムアウト: タスクが停止するまでの最大時間 タスクが開始すると、マネージャー スケジューラによってセッションが開始、ノードの1 つによってタスクが実行されます。セッションがタイムアウトすると、マネージャー スケジューラは強制的にノードにタスクを中止させて、セッションを削除します。

7. タスクには少なくとも、自動実行するトリガーがひとつ含まれている必要があります。[**トリガー**] の表見出しにある [**アクション**] ▼ をクリックしてトリガーを管理し、次からひとつ選択します:
   - [**1 回のみのトリガーを新規作成**]、[**時間ベースのトリガーを新規作成**]、[**日単位のトリガーを新規作成**]、[**週単位のトリガーを新規作成**]、[**月単位のトリガーを新規作成**] の中から選び、新しいトリガーを作成します。これらはトリガーのショートカットで、選択したトリガーがテーブルに即座に追加されます。トリガーの開始値は、作成時から5 分に設定され、トリガーが有効になります。
   - [**スケジュール済みトリガーを新規作成**] または [**タスク イベント トリガーを新規作成**] を使い、選択されたタイプのトリガーを新規作成します (下記のプロパティの説明を参照)。ダイアログが開きます。トリガーを編集して [**OK**] をクリックすると、ダイアログが閉じてテーブルにトリガーが追加されます。
   - 適宜、[**編集**] を使い、テーブルで選択されたトリガーの編集ダイアログを開きます。トリガーを編集し、[**OK**] をクリックしてダイアログを閉じ、変更内容を保存します。
   - 適宜、[**削除**] を使い、テーブルで選択されたトリガーを削除します。
     現在編集中のすべてのトリガに適用するために、[**トリガ**] の見出しにある元に戻す() をクリックします。

トリガー (スケジュール済み)

スケジュール済みトリガーのプロパティ

プロパティ	説明
[**トリガー名**]	トリガーの名前。必須。
[**有効化**]	トリガーの状態。選択するとトリガーはアクティブになります。
[**タイムゾーン**]	オペレーティング システムのタイム ゾーンがトリガーを作成した時間になります。トリガーを保存すると設定は保持され、タイムゾーンが違う場所に行っても元の設定値のまま表示されます。タイム ゾーンやトリガーの開始時間を変更したい場合は手動で行う必要があります。 *タイム ゾーンの設定より前に作成されたトリガーについては、日時はすべてデフォルトで Coordinated Universal Time (UTC: 協定世界時) にて表示されます。*
[**夏時間**]	夏時間を考慮する方法。 [**夏時間を使用する**]: このオプションでは夏時間 (DST) が考慮されます。選択したタイム ゾーンで DST が使われていると、実行日時はそれに応じて調整されます。 [**常に標準時**]: このオプションでは DST は考慮されません。選択したタイム ゾーンで DST が使われていても、実行日時は調整されません。 [**常に夏時間**]: このオプションでは DST が考慮されません。タイム ゾーンで DST が使われている場合は、DST の適用期間外でも実行日時は常に DST に準じます。 *DST を使用しないタイム ゾーンの場合は、常に [**永久標準時**] を選択します。* 1 月にカナダのオタワで午前 10 時に開始するイベントのトリガーを作成したとします。ここのタイム ゾーンは (GMT-0500) 東部標準時 (米国およびカナダ) で DST の期間は 3 月から 11 月です。 [**夏時間を使用する**] を選択すると、10 時に開始するよう設定されたトリガーは常に 10 時に開始します。 [**常に標準時**] を選択すると、10 時に実行するよう設定されたトリガーは冬は 10 時に実行されますが夏は 9 時に実行されます。 [**常に夏時間**] を選択すると、10 時に実行するよう設定されたトリガーは冬は 11 時に、夏は 10 時に実行されます。

プロパティ	説明
[**Start**]	開始時間と開始日: • 開始時間: [**(hh:mm)**] • 開始日: **(YYYY-MM-DD)**

[**スケジュール**]	トリガーの頻度。
	• [**1 回**]。
	• [**時間単位**]。トリガー実施の間隔。次の値を入力して、[**各条件の後に繰り返す**]を編集します。
	  • [**s (時間単位**] (既定 1 時間)
	  • [**s (分単位**] (既定 0 分)
	• [**日単位**]。トリガー実施の間隔。[**Every**][**s (日おき**] (既定 1 日) の値を入力します。たとえば、2 と入力すると2 日おきにトリガーが繰り返されます。
	• [**週単位**]。トリガー実施の間隔:
	  • [**Every**][**s (週おき**] (既定 1 週) の値を入力します。
	  • [**平日**] のチェックボックスを選択して (複数日可)、トリガーが繰り返される日を決めます (ユーザーが指定する週で)。たとえば、3 と入力して [**月曜日**] を選択すると、3 週おきの月曜日にトリガーが実行されます。
	• [**月単位**]。[**On these days**] のチェックボックスを選択 (複数可) すると、毎月トリガーが繰り返し実行される日を定義できます。
	  *[**Monthly**] を選択し、トリガーが毎月繰り返されるようにするには、28 日よりも前の日を選択する必要があります。*
	• **カスタム**: [**カスタム**] を選択すると、[**フィルター**] と [**増分**] の 2 つの新しい項目が表示されます。これらのオプションは、リロードをスケジュールするときに大きな柔軟性を提供します。詳細は、「*タスク- カスタム オプション (page 228)*」を参照してください。

[**終了**]	終了時間と終了日: • 終了時間: [**(hh:mm)**] • 終了日:**(YYYY-MM-DD)** [**無期限**] を選択して、終了日のないトリガーを作成します。

トリガー (タスク イベント)

タスク イベント トリガーのプロパティ

プロパティ	説明
[**トリガー名**]	トリガーの名前。必須。
[**タイプ**]	トリガーのタイプ。
[**有効化**]	トリガーの状態。選択するとトリガーは *アクティブ*になります。
[**時間制限**]	タスク チェーンの他のタスクを完了しなければならない期間 (分単位)。トリガーがひとつのタスクだけで構成されている場合、何も起きません。 *タスク チェーンの作成 (page 355)*
[**タスク**]	
	次の手順を実行します。 1. [**タスクの追加**] をクリックして、トリガー条件として機能するタスクを追加します。[**ステータス**] リストと空の [**タスク**] 項目が追加されます。 2. 空の項目をクリックしてタスクを追加します。 タスク選択ダイアログが開き、次の列とともにタスクの一覧が表示されます。[**名前**]、タスクに接続した [**アプリ**]、タスク名である [**タグ**]。 3. タスクをダブルクリックし、トリガー条件として使用します。 トリガーにタスクを追加し、ダイアログを閉じます。 4. [**ステータス**] リストで、トリガー条件が [**TaskSuccessful**] または [**TaskFail**] で処理されるかどうかを選択します。 *[**タスク失敗**] のトリガー条件を持つタスクは、先行タスクが失敗の状態で完了するときだけでなく、スキップまたはエラー (リロード前にエラーが発生する場合) の状態でも開始されます。2019 年 2 月以前の Qlik Sense バージョンでは、中止状態の先行タスクによっても「タスク失敗」トリガー条件によってもタスクが開始されました。この動作を有効にするには、すべてのスケジューラー ノードの Scheduler.exe.config で「DisableLegacyTaskEventTriggerBehavior」を「false」に設定します。* トリガーに含めたい全タスクで、上記のステップを繰り返します。タスクは一度しか追加できず、トリガーにすでに追加されている場合にはタスク選択ダイアログに表示されません。タスクの間には論理的な AND があります。

> *タスクを指定の順番で実行する必要はなく、[**時間制限**] は固定されていません。時間が制限に達した時に、1 つのタスクを除いてすべてのタスクが完了している場合、最初に完了したタスクは実行済みとはみなされず、期間の終わりを再計算します。トリガーは、再計算された期間にすべてのタスクが完了するのを待ちます。*

8. 必要に応じて、タグとカスタムプロパティを追加します。
9. [**適用**] をクリックしてタスクを保存します。

> *配布タスクの権限は、`ReloadTask_*` リソース フィルターによって制御できます。タスク リソース フィルターの詳細については、「タスク リソース」を参照してください。*

トリガー

タスクを実行する時点を決定するために使用するのがトリガーです。2 種類のトリガーがあります。

- スケジュール済みトリガー
- タスク イベント トリガー

スケジュール済みトリガー

スケジュール済みトリガーでは、実行予定のタスクの数と実行頻度をスケジュールできます。タスクの実行数は 1 から無限の範囲で、実行頻度は毎時間から毎月の範囲で設定できます。スケジュール済みトリガーは、リロード タスクとユーザーの同期タスクの両方に適用できます。

ユーザーの同期タスクにはスケジュール済みトリガーを作成することをお勧めします。トリガーは月ごとにアクティブになります。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Tasks (タスク)**] を選択して、概要を表示します。
3. トリガーの作成対象のユーザー同期タスクを選択し、[**編集**] をクリックします。
4. [**関連するアイテム**] で [**トリガー**] を選択します。
5. [**関連するトリガーの作成**] をクリックします。
   [**トリガー - スケジュールにより開始**] ウィンドウが表示されます。
6. トリガー名と開始の日付/時刻を入力します。
7. [**スケジュール**] で [**毎月**] を選択します。
8. トリガーの日付を選び、他の日付が選択されている場合はすべて解除します。

> *トリガーが毎月必ず繰り返されるようにするために、日付の指定は「28」より遅い日にしないでください。*

9. 必要であれば終了日と時刻を設定します。デフォルトでは終了日は設けられていません。

タスク イベント トリガー

タスク イベント トリガーでは、トリガーをアクティブにするための 1 つ以上の条件を設定します。条件を作成するには、タスクとそのステータス (タスク成功、タスク失敗) を選択します。該当の条件、および他の付加的な条件に一致する状況になると、このトリガーによってアプリのリロードが促されます。リロード タスクにのみ、タスク イベント トリガーを適用できます。

相互に関連性の高い 2 つのアプリがあり、これらのアプリの同期を確実に維持したい場合は、1 番目のアプリが「タスク成功」のステータスになった場合のみ、2 番目のアプリをリロードするようにします。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Tasks (タスク)**] を選択して、概要を表示します。
3. トリガーの作成対象のリロードタスクを選択し、[**編集**] をクリックします。
4. [**トリガー**] 見出しバーの [**アクション**] をクリックします。
   異なるトリガー オプションを提示するポップアップ画面が表示されます。
5. [**タスク イベント トリガーを新規作成**] を選択します。
   [**トリガー - タスク イベントにより開始**] ウィンドウが表示されます。
6. トリガー名と開始の時間制限を入力します。
7. [**タスクの追加**] をクリックします。
8. [**タスク**] 項目をクリックし、トリガーが依存するタスクを選択します。
9. そのタスクのステータス (この場合は [**タスク成功**]) を選択します。
   このトリガーは、該当のタスクが [**タスク成功**] のステータスになった場合のみ、アクティブになります。
10. [**OK**] をクリックします。
    新しいトリガーがトリガー リストに追加されます。
11. [**適用**] をクリックします。

> *リロード タスクまたは同期タスクのトリガーは、タスク概要ページから手動で実行することもできます。*

リロード タスクの削除

削除権限を有するタスクをアプリの関連付けページから削除できます。

> *タスク概要ページからリロード タスクを削除することもできます*

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMCスタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**アプリ**] を選択して、概要を表示します。
3. タスクを削除集したいアプリを選択し、アクション バーで [**Edit**] をクリックします。
4. [**関連するアイテム**] の [**タスク**] を選択します。
   [**関連するアイテム**] ページが [**タスクのリロード**] の概要とともに表示されます。
5. 削除するタスクを選択し、アクション バーで [**削除**] をクリックします。
   [**Delete**] ダイアログが表示されます。
6. [**OK**] をクリックします。

リロード タスクの開始

アプリの関連付けページからリロード タスクを手動で開始できます。

また、タスク概要ページからリロード タスクを開始することもできます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMCスタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**アプリ**] を選択して、概要を表示します。
3. タスクを開始したいアプリを選択し、アクション バーで [**Edit**] をクリックします。
4. [**関連するアイテム**] の [**タスク**] を選択します。
   [**App associated items**] ページが表示されます。
5. 開始するタスクを選択し、操作バーで [**スタート**] をクリックします。

トリガーでタスクを開始することも可能です。

リロード タスクの停止

アプリの関連付けページからリロード タスクを手動で停止できます。

また、タスク概要ページからリロード タスクを停止することもできます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMCスタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**アプリ**] を選択して、概要を表示します。
3. タスクを停止したいアプリを選択し、アクション バーで [**Edit**] をクリックします。
4. [**関連するアイテム**] の [**タスク**] を選択します。

[**アプリの関連付け**] ページが [**タスク**] の概要とともに表示されます。

5. 停止するタスクを選択し、操作バーで [**停止**] をクリックします。

アプリの手動リロード

アプリを手動でリロードし、アプリ内のデータをソースから完全リロードすることができます。古いデータはすべて、破棄されます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**アプリ**] を選択して、概要を表示します。
3. リロードするアプリを選択し、[**その他のアクション**] をクリックして、ポップアップ メニューで [**今すぐリロード**] を選択します。
   フィードバック メッセージが表示されます。
4. [**タスク**] 概要ページでタスクの進捗状況を確認します。[**名前**] カラムに「*Manually triggered reload of [app name] (<アプリ名> のリロードが手動でトリガーされました)*」と表示されます。When the task has finished the **Status** column displays ✔成功
5. オプション: 手動で開始したアプリのリロード タスクは 1 回だけ実行できます。このため、タスクの概要からこのタスクを削除することをお勧めします。
   a. タスクを選択して [**削除**] をクリックします。
      ダイアログが表示されます。
   b. [**OK**] をクリックして、削除を確定します。
      概要からタスクが削除されます。

コンテンツ ライブラリの作成

コンテンツ ライブラリは Qlik Sense ユーザーがアプリに共有コンテンツを追加することができるストレージです。

コンテンツ ライブラリを作成するユーザーは自動的にそのライブラリの所有者になります。ライブラリおよびライブラリ オブジェクトは、QMC で定義されたセキュリティ ルールを使用して他のユーザーと共有できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**コンテンツ ライブラリ**] を選択して、概要を表示します。
3. データ マネージャーでテーブルの ⊕**新規作成** をクリックします。
4. プロパティを編集します。

> *一番右側にあるパネルで、プロパティグループの表示/非表示を切り替えることができます。*

ID

ID プロパティ

プロパティ	説明
[**名前**]	コンテンツ ライブラリの名前。必須。
[**所有者**]	コンテンツ ライブラリの所有者。コンテンツ ライブラリが作成されるまで、このプロパティは存在しません。

タグ

タグ プロパティ

プロパティ	**説明**
[*タグ*]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

カスタム プロパティ

***カスタム プロパティ**を利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

[**適用**] をクリックして変更を保存します。必須の項目が空欄の場合、[**Apply**] は無効になります。

5. 操作バーで [**適用**] をクリックして、コンテンツ ライブラリを作成して保存します。
[**セキュリティ ルールの作成**] ダイアログが開きます。
6. コンテンツ ライブラリの管理アクセスのセキュリティ ルールを編集します:
   a. [**ID**] プロパティを編集します:

ID の項目と値

項目	値
名前	コンテンツ ライブラリの名前を入力します。必須。
[**無効化**]	ルールを無効にする場合に選択します。このルールは、既定でオンになっています。
[**説明**]	ルールについての説明を入力します。

   b. [**基本**] セクションでルールの条件を作成します。
      - ルールに適用するアクションを選択します。
      - ドロップダウン メニューを使用して、ルールが適用されるユーザーを指定する条件を作成します。

- データ マネージャーでテーブルの条件を追加します。複数の条件を使用すると、[**Group**] をクリックして 2 つの条件をグループ化できます。条件のグループ化後、[**Ungroup**] をクリックして、グループ化を解除できます。この他に、サブグループ化オプションには [**Split**] および [**Join**] があります。条件間の既定の演算子は、OR です。これは、演算子のドロップダウン リストで変更できます。AND が OR より上位になるように、条件をグループ化します。

演算子の説明

演算子	説明と例
=	この演算子では大文字と小文字は区別されません。比較対象の数式と完全に等しい場合は True を返します。 `user.name = "a*"` 名前が「a*」と完全に一致するユーザーがルールの対象になります。
like	この演算子では大文字と小文字は区別されません。比較対象の数式と等しい場合は True を返します。 `user.name = "a*"` 名前が「a」で始まるすべてのユーザーがルールによって対象になります。.
!=	この演算子では大文字と小文字の区別はされません。比較対象の数式の属性値が等しい場合は True を返します。 `user.name=resource.name` ユーザーと同じ名前を持つすべてのリソースがルールの対象になります。

ページ最下部に [**追加完了**] と表示されます。

これで新しいコンテンツ ライブラリが作成されました。

コンテンツ ライブラリの編集

コンテンツ ライブラリは Qlik Sense ユーザーがアプリに共有コンテンツを追加することができるストレージです。

コンテンツ ライブラリを作成するユーザーは自動的にそのライブラリの所有者になります。ライブラリおよびライブラリオブジェクトは、QMC で定義されたセキュリティ ルールを使用して他のユーザーと共有できます。

更新権限を有するコンテンツ ライブラリを編集できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**コンテンツ ライブラリ**] を選択して、概要を表示します。
3. 編集するライブラリを選択します。
4. アクション バーで [**編集**] をクリックします。
5. プロパティを編集します。

ID

ID プロパティ

プロパティ	**説明**
[**名前**]	コンテンツ ライブラリの名前。必須。
[**所有者**]	コンテンツ ライブラリの所有者。コンテンツ ライブラリが作成されるまで、このプロパティは存在しません。

タグ

タグ プロパティ

プロパティ	**説明**
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

カスタム プロパティ

***カスタム プロパティ**を利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

6. 操作バーで [**適用**] をクリックします。

ページの最下部に [**更新完了**] と表示されます。

コンテンツ ライブラリの削除

更新権限のあるコンテンツ ライブラリは削除できます。コンテンツ ライブラリを削除すると、すべてのライブラリ オブジェクトも削除されます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**コンテンツ ライブラリ**] を選択して、概要を表示します。

3. 削除するコンテンツ ライブラリを選択します。
4. アクション バーの [**Delete**] をクリックします。
   [**Delete**] ダイアログが表示されます。
5. [**OK**] をクリックします。

コンテンツ ライブラリにオブジェクトをアップロード

更新権限のあるコンテンツ ライブラリにオブジェクトをアップロードできます。Qlik Sense では画像ファイルのみ使用しますが、コンテンツ ライブラリの許可リストに含まれている拡張子の付いたすべての種類のファイルをアップロードできます。最大ファイル サイズは、Windows 用の Qlik Sense に関する資料で指定されています。

Qlik Sense Repository Service は、AppContent またはコンテンツ ライブラリにアップロードされた XML ファイルにあるスクリプト タグをスキャンします。

アップロードするオブジェクトは コンテンツ ライブラリ概要 ページまたは コンテンツ ライブラリの [**Associated items**] から選ぶことができます。
次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**コンテンツ ライブラリ**] を選択して、概要を表示します。

   フィルタリング オプションを使用して列にフィルターを適用できます。
3. オブジェクトをアップロードする先のコンテンツ ライブラリを選択し、[**Upload**] をクリックします。
   別の方法:
   コンテンツ ライブラリを選択して、操作 バーの [**編集**] をクリックし、[**関連するアイテム**] の [**コンテンツ**] を選択して、⊕ [**コンテンツ**] ページの操作 バーの [**アップロード**] をクリックします。
   どちらの方法でも [**静的コンテンツのアップロード**] ダイアログ ボックスが開きます。
4. [**参照**] をクリックします。
   ブラウザのウィンドウが開きます。
5. インポートしたいファイルを参照して [**開く**] をクリックします。
   ブラウザ ウィンドウが閉じて、[**静的コンテンツのアップロード**] ダイアログの [**選択されたファイル**] にファイルが追加されます。
6. [**アップロード**] をクリックします。
   [**転送中**] ダイアログが開きます。ダイアログには、自分が開始した転送がすべて表示されます。
   - ファイルのインポート中は スピナーが表示されます。[**経過時間**] に、インポート経過時間が表示されます。
   - アップロードをキャンセルしたい場合は、⊗ をクリックします。
     ⚠ と [**中止されました**] が表示され、アップロードが停止します。
   - ↻ アップロードがキューされるとが表示されます。実行中のアップロードプロセス数が 4 つを下回ると、アップロードが開始されます。
   - 失敗したアイテムを削除するには、[**削除**] をクリックします ⚠.

アイテムが削除されます。

- コンテンツ ライブラリに同一のファイル名が既に存在している場合、[**「Conflict error with existing file (既存ファイルの競合エラー)」**] が表示されます:
  - 新規ファイルで既存のファイルを置き換える場合は [**上書き**] をクリックします。
    アップロードが続行されます。
  - アップロードを停止する場合は [**キャンセル**] をクリックします。
    ダイアログからアイテムが削除され、既存のアイテムがライブラリに残ります。

ファイルがアップロードされると、✔ が 15 秒間表示され、ファイルが選択した [**コンテンツ ライブラリ**] に追加されます。すべての転送が正常に完了すると[**Ongoing transport**] ダイアログが閉じます。転送に失敗した場合、概要ページが最新の情報に更新されるまでダイアログが表示されます。

*アップロードしたファイルを表示する場合、[**「Contents (コンテンツ)」**] 概要から[**URL パス**] をクリックします。新規タブにファイルが表示されます。*

コンテンツ ライブラリからオブジェクトを削除

削除権限のあるコンテンツ ライブラリからオブジェクトを削除できます。

コンテンツ ライブラリを削除すると、ライブラリ内にあるオブジェクトもすべて削除されます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**コンテンツ ライブラリ**] を選択して、概要を表示します。
3. オブジェクトを削除したいコンテンツ ライブラリを選択して [**編集**] をクリックします。
   コンテンツ ライブラリの編集ページが開きます。
4. [**Associated items**] で [**Contents**] を選択します。
   内容の概要が表示されます。
5. 削除するファイルを選択します。
6. アクション バーの [**Delete**] をクリックします。
   [**Delete**] ダイアログが表示されます。
7. [**OK**] をクリックします。
   リポジトリからファイルが削除され、内容の概要に表示されなくなります。

コンテンツ ライブラリのアクセス権の作成

コンテンツ ライブラリは Qlik Sense ユーザーがアプリに共有コンテンツを追加することができるストレージです。

コンテンツ ライブラリを作成するユーザーは自動的にそのライブラリの所有者になります。ライブラリおよびライブラリ オブジェクトは、QMC で定義されたセキュリティ ルールを使用して他のユーザーと共有できます。

コンテンツ ライブラリへのアクセス権を付与するセキュリティ ルールを作成します。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**コンテンツ ライブラリ**] を選択して、概要を表示します。
3. ルールを作成するコンテンツ ライブラリを選択します。
4. [**編集**] をクリックします。
5. コンテンツ ライブラリの編集ページが開きます。
6. [**関連するアイテム**] の [**セキュリティルール**] を選択します。

   セキュリティルール概要が表示されます。

7. データ マネージャーでテーブルの ⊕操作バーの [**関連するルールの作成**] をクリックします。

   *[**セキュリティルールの作成**] ダイアログが開きます。*

8. コンテンツ ライブラリの管理アクセスのセキュリティルールを編集します:
   a. [**ID**] プロパティを編集します:

ID の項目と値

項目	**値**
名前	コンテンツ ライブラリの名前を入力します。必須。
[**無効化**]	ルールを無効にする場合に選択します。このルールは、既定でオンになっています。
[**説明**]	ルールについての説明を入力します。

   b. [**基本**] セクションでルールの条件を作成します。
      1. ルールに適用するアクションを選択します。
      2. ドロップダウン メニューを使用して、ルールが適用されるユーザーを指定する条件を作成します。
      3. データ マネージャーでテーブルの ⊕条件を追加します。複数の条件を使用すると、[**Group**] をクリックして 2 つの条件をグループ化できます。条件のグループ化後、[**Ungroup**] をクリックして、グループ化を解除できます。この他に、サブグループ化オプションには [**Split**] および [**Join**] があります。条件間の既定の演算子は、OR です。これは、演算子のドロップダウン リストで変更できます。AND が OR より上位になるように、条件をグループ化します。

演算子の説明

演算子	**説明と例**

=	この演算子では大文字と小文字は区別されません。比較対象の数式と完全に等しい場合は True を返します。 `user.name = "a*"` 名前が「a*」と完全に一致するユーザーがルールの対象になります。
like	この演算子では大文字と小文字は区別されません。比較対象の数式と等しい場合は True を返します。 `user.name = "a*"` 名前が「a」で始まるすべてのユーザーがルールによって対象になります。
!=	この演算子では大文字と小文字の区別はされません。比較対象の数式の属性値が等しい場合は True を返します。 `user.name=resource.name` ユーザーと同じ名前を持つすべてのリソースがルールによって対象になります。

9. [**適用**] をクリックします。

ダイアログが閉じ、セキュリティルール概要にルールが追加されます。

*[**セキュリティルール**] 概要ページに対応するセキュリティルールが表示されます。*

これで選択されたコンテンツ ライブラリに対するアクセス権が作成されました。

アプリオブジェクトの編集

更新権限を持つアプリオブジェクトを編集できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**アプリ オブジェクト**] を選択して、概要を表示します。
3. 編集したいアプリオブジェクトを選択します。
4. アクション バーで [**編集**] をクリックします。
   [**Edit (編集)**] の横の数字は、選択したアイテムの中で編集できるアイテムの数を示します。
5. プロパティを編集します。

一番右側にあるパネルで、プロパティグループの表示/非表示を切り替えることができます。

ID

ID プロパティ

プロパティ	説明
[**名前**]	アプリオブジェクトの名前。必須。
[**所有者**]	アプリオブジェクトの所有者。

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	テキスト ボックスをクリックすると、利用可能なタグが表示されます。入力を始めると、リストが少なくなります。紐付けられているタグがテキスト ボックスの下に一覧表示されます。

6. アクション バーで [**適用**] をクリックします。

ページの最下部に [**更新完了**] と表示されます。

アプリオブジェクトの削除

削除権限を有するアプリオブジェクトを削除できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**アプリ オブジェクト**] を選択して、概要を表示します。
3. 削除したいアプリオブジェクトを選択します。
4. アクション バーの [**Delete**] をクリックします。
   [**Delete**] ダイアログが表示されます。
5. [**OK**] をクリックします。

On-demand アプリの管理

On-Demand アプリは、選択アプリをテンプレート アプリに接続するナビテーション リンクから、Qlik Sense ハブに生成されます。On-Demand アプリを生成するには、On-Demand アプリ サービスを有効にする必要があります。適切なアクセス権限がある場合は、Qlik Sense ハブから選択アプリおよびテンプレート アプリを作成し、ストリームに公開することができます。選択アプリおよびテンプレート アプリは、QMC (Qlik Senseの一部) からストリームに公開することもできます。生成された On-Demand アプリは、適切なアクセス権があれば、QMC または Qlik Sense ハブから公開することも可能です。

アプリ、ストリーム、ユーザーに適用されるセキュリティルールによって、コンテンツにアクセスできるユーザーおよびそのユーザーが実行できる内容が決まります。アプリは公開後ロックされます。サーバーデプロイメントの Qlik Sense ハブを介してコンテンツを公開済みのアプリに追加することは可能ですが、オリジナルのアプリで公開されたコンテンツは編集できません。

On-Demand アプリサービスのプロパティ

選択アプリおよびテンプレートアプリは、On-demand アプリサービスを有効にしなくても作成できますが、ナビゲーション リンクを作成して On-demand アプリを生成するには、このサービスを有効にする必要があります。On-demand アプリサービスは QMC で管理します。On-Demand アプリサービスの以下のプロパティを管理できます。

プロパティの説明

プロパティ	説明
On-Demand アプリの有効化	On-Demand アプリサービスを有効化および無効化します。このサービスは、デフォルトでは無効になっています。 サービスを有効から無効に切り替えると、On-Demand アプリを生成するためにペンディング中の要求を終了することができます。ただし、いったんサービスを無効にすると、アプリを生成する新しい要求は受け入れられません。
ダイナミック ビューの有効化	ダイナミック ビューにより、チャートの更新を分析ツールの環境から実行できます。ダイナミック ビューを有効にするには、オンデマンド アプリサービスをオンにする必要があります。 ダイナミック ビューをオンにすることによって、オンデマンドのデータ ソースからロードされるチャートをアプリシートに含めることができます。 ダイナミック ビューに基づくチャートが含まれるシートがあるアプリで、[**ダイナミック ビュー**] の設定がテナントに対して無効になっている場合、アプリは次の制限付きで引き続き動作します。 • ダイナミック ビュー機能が無効になっていることを示すため、ダイナミック チャートはすべて淡色表示 (データも非表示) されます。 • ダイナミック ビュー内の情報は、シート エディターには表示されません。 ダイナミック ビューに関係のないチャートや機能はすべて正常に動作します。
ログ レベル	サービス ログ ファイルに書き込まれる詳細レベルを指定します。
一度に作成可能なアプリ数	サービスが一度に作成できるアプリの数を指定します。デフォルトは 1、最大数は 10 です。 この設定はアプリ生成の応答時間に影響しますが、一度に生成できるアプリの数を設定するときには、ロードされるデータの量も考慮する必要があります。データのロード サイズが適度である場合は、一度に生成されるアプリの数を多くすると、各アプリの応答時間が改善されます。ただし、ロード サイズが大きいと、設定数がより少ない場合よりも応答が遅くなり、アプリ生成のためにアプリがキューで待機しなければならなくなる可能性があります。 マルチ ノード環境では、一度に生成できるアプリの数に関する設定は、その環境で実行されている On-Demand アプリのすべてのインスタンスに適用されます。複数のサービスが同じ Qlik associative engine を使用している場合、その Qlik associative engine へのロードは、サービスの複数のインスタンスから一度に生成できるアプリの累積数となります。

プロパティ	説明
履歴データを解析するまでの日数	On-Demand アプリに関する特定の履歴データを削除するまでの保存日数を指定します。0 ~ 365 の値を指定できます。0 に設定するとデータは削除されません。既定値は 90 日です。 On-Demand アプリサービスでは、ナビゲーション リンクおよび要求に関するデータを保持して On-Demand アプリを生成およびリロードします。 On-Demand アプリのナビゲーション リンクが削除されると、デコミッション ステートに廃棄状態で維持されます。解析前に指定した日数に到達すると、ナビゲーション リンクに関する情報は削除されます。 On-Demand アプリサービスには、On-Demand アプリを生成およびリロードする要求に関する情報も維持されます。On-Demand アプリを削除すると、リロード要求に関する情報は解析前に指定した日数の間維持されます。
匿名ユーザーに対するアプリ生成の許可	公開された選択アプリのナビゲーション ポイントから匿名ユーザーが On-demand アプリを生成できるよう許可します。この設定は、匿名認証が設定されている Qlik Sense システム上でのみ適用されます。 *匿名の認証 (page 461)* 匿名ユーザーは、ナビゲーション リンクから自動的に公開されるアプリのみ生成できます。生成されたアプリが自動的に公開されない場合、匿名ユーザーにはそのアプリに対するアクセス権限がありません。
匿名ユーザーの代わりにアプリの生成に使用されるプロキシ ユーザー	匿名ユーザーの代わりのプロキシ ユーザーとなるユーザーを選択します。On-demand アプリリクエストを作成可能な登録ユーザーを選択します。プロキシ ユーザーには、匿名ユーザーがアクセス可能な On-demand 選択アプリに対する読み取り権限も必要です。プロキシ ユーザーとして、またはルート管理者権限を持つユーザーとして管理ユーザー (*INTERNAL\sa-xxx*) を選択しないでください。 *匿名ユーザーが使用可能な On-demand 選択アプリを含むストリームを作成する場合、On-demand アプリのプロキシ ユーザーに対して読み取りアクセスを許可するセキュリティルールを設定する必要があります。プロキシ ユーザーに読み取りアクセス権限がないと、アプリナビゲーション バーのすべてのリンクが [Invalid] (無効) として表示されます。* シングル ユーザーはすべての匿名ユーザーの代わりとなりますが、匿名ユーザーはそれぞれが On-demand アプリサービスによって特定され、識別されています。これにより、各匿名ユーザーは自身が生成したアプリにアクセスできるようになりますが、他の匿名ユーザーがそのアプリにアクセスできなくなります。各匿名ユーザーは、自身が生成したアプリにのみアクセスできます。

プロパティ	説明
匿名ユーザーが生成したアプリの保存期間	匿名ユーザーが生成したアプリが削除されるまでの保存期間を指定します。既定の設定は 60 分間です。 この時間は、最後にデータがロードされた時点から計測されます。 ナビゲーション リンクに対する保存期間の設定もあります。匿名ユーザーが生成したアプリの場合、2 種類の保存期間設定のうち短い期間が使用されます。 例えば、保存期間が 24 時間に設定されているナビゲーション リンクが匿名ユーザーに使用されていて、[**匿名ユーザーが生成したアプリの保存期間**] の設定が 60分間の場合、アプリは最後のデータ ロードから60 分後に削除されます。ただし、ナビゲーション リンクの保存期間の設定が 30 分であれば、匿名ユーザーが生成したアプリは最後のデータ ロードから30 分後に削除されます。 *[**匿名ユーザーが生成したアプリの保存期間**] がゼロ(0) に設定されている場合、アプリはできるだけ長く、すなわち365 日間保存されます。*

On-Demand アプリ サービスのシャットダウン

On-Demand アプリ サービスは、Qlik Sense がシャットダウンされている場合にのみオフになります。要求のペンディング中にサービスをオフにすることを避けるには、サービスのユーザーにオフになることを通知する必要があります。間違ってアプリ要求を中断しないようにするには、サービスを無効にして、ペンディング中の要求が終了するまで数秒間待機してから、シャットダウンする必要があります。

ペンディング中の要求が存在するかどうかを調べるため、RootAdmin 権限を持つユーザーは、Web ブラウザーの URL 項目に次の URL を入力することができます。

https://yourhost.yourdomain.com/api/odag/v1/requests?state=qvhl&createdOnOrAfter=YYYY-MM-DDTHH:MI:SS.sssZ

ここで

yourhost.yourdomain.com は、お使いの Qlik Sense プロキシの URL です。

また、

YYY-MM-DDTHH:MI:SS.sssZ は、最新の On-Demand アプリ サービスのログ ファイルで最初のレコードの日付と時刻であり、サービスが最後に開始された時刻です。

これによって、On-Demand アプリを JSON 形式で生成する配列が返されます。これらは、最後に On-Demand アプリ サービスが開始された時点以降に開始され、まだ完了していない要求です。ペンディング中の要求がない場合は、ブラウザーでの応答は、次のように開き角括弧と閉じ角括弧として表示されます。

[ ]

シャットダウン後にサービスを再起動すると、シャットダウン発生時のステートで起動されます。サービスをシャットダウン前に無効にした場合は、サービスの再起動後に再度有効にする必要があります。

On-Demand アプリサービスが強制的にシャットダウンされたためにペンディング中の要求がキャンセルされた場合、これらの要求は失われ、回復することはできません。サービスを再起動して有効にしたときに、これらの要求を手動で再入力する必要があります。

On-Demand アプリの保存期間

ナビゲーション リンクを作成したときに、On-Demand アプリの保存期間を設定できます。

保存期間は時間数または日数で指定でき、無期限に設定することも可能です。ナビゲーション リンクから生成されたすべての On-Demand アプリが、この設定に従って保持されます。生成された On-demand アプリの存在期間は、現在の時間および最後のデータロードの時間の差に相当します。On-demand アプリの存在期間のこの計算は、公開アプリと未公開アプリで同じです。On-demand アプリを生成してから手動で公開した場合、存在期間の計算は同じです。生成されたアプリの最後のデータロードに基づきます。

*匿名ユーザーが生成したアプリの保存期間は On-demand アプリサービスで設定します。この設定は、On-demand アプリのナビゲーション リンクで設定されている保存期間よりも優先します。上記の On-demand アプリサービスのプロパティの**匿名ユーザープロパティが生成したアプリの保存期間**を参照してください。*

On-Demand アプリサービスは 10 分ごとにスイープを実行して、保存期間の切れた On-Demand アプリを削除します。スイープは 10 分ごとに実行されるので、On-Demand アプリはその保存設定よりも最大で 10 分間長くアクティブなままにできます。例えば、アプリの保存設定が 1 時間の場合、スイープの実行後間もなく保存期間が終了し、次のスイープまではアクティブなままになります。

保存期間はナビゲーション リンクの設定に基づきますが、アプリの生成後も保存期間は変わりません。ナビゲーション リンクの所有者が保存期間を変更した場合、この変更は、すでに生成されている On-Demand アプリには反映されません。

On-Demand アプリの所有権

On-Demand アプリの所有者は、アプリを生成したユーザーです。アプリの生成が完了するまではそのユーザーは所有者にはなりません。On-Demand アプリがデータのロードの処理中である間は、所有者は *INTERNAL\sa_api* です。この理由は、ユーザーが通常、テンプレート アプリで使用されるデータ接続にアクセスできないためです。これは、ユーザーがテンプレート アプリへのアクセス権を持っていない場合、ロード スクリプトとすべての添付ファイル (画像を除く) が、生成されたアプリケーションから削除されることを意味します。そのデータ接続へのアクセスは、セキュリティ上の理由で制限されます。

On-Demand アプリの生成を完了できなかった場合、QMC にはアプリの所有者が *INTERNAL\sa_api* として表示されます。

生成されたアプリの所有権は、公開時に変更されます。生成されたアプリが公開されると、アプリの所有者はナビゲーション リンクの所有者となります。

匿名ユーザーが生成したアプリはすべて公開する必要があるため、匿名ユーザーは生成されたアプリを所有しません。匿名ユーザーは、未公開アプリにはアクセスできません。ただし、匿名ユーザーが生成したアプリは、そのアプリを生成した匿名ユーザーに関連付けられた識別子によってタグ付けされます。それにより、ある匿名ユーザーは別の匿名ユーザーが生成したアプリを使用できなくなります。

On-Demand アプリの自動公開

ナビゲーション リンクには、リンクから生成されたアプリが自動的に公開されるストリームを、リンク作成者が指定できるようにするプロパティがあります。ナビゲーション リンクを作成するユーザーは、対象のストリームに公開する権限を持っている必要があり、アプリを生成するユーザーは、ストリーム上での読み取り権限を持っている必要があります。いずれの権限も見つからない場合、On-demand アプリは生成されません。

匿名ユーザーが使用できるのは公開されたアプリのみであり、匿名ユーザーが自らアプリを公開することはできません。そのため、匿名ユーザーは、アプリを自動的に公開するナビゲーション リンクからのみアプリを生成できます。

ストリームに公開された On-demand アプリを生成したユーザーは、アプリを削除することはできません。ナビゲーション リンクの所有者のみが、ストリームから On-demand アプリを削除することができます。

マルチノード環境におけるリロードの制御

管理者は、マルチノード環境において On-demand アプリをリロードする場所を制御できます。負荷分散ルールは、個々のノード上のカスタム プロパティで設定します。アプリが特定のリロード サーバーを使用するよう、カスタム プロパティをアプリに設定することができます。

On-demand アプリの生成は 3 ステップのプロセスです。

1. 現在の選択条件に基づいて、テンプレート アプリのスクリプトが生成され、検証されます。
2. テンプレート アプリが複製されます。
3. 新規生成されたアプリにスクリプトを適用することによって、アプリがリロードされます。
   アプリの複製では、アプリを作成および複製する環境内に開発ノードが必要です。開発ノードの [**ノードの目的**] を [**開発**] または [**両方**] に設定することで、これを実現できます。

既定では、On-demand アプリは、環境の負荷分散ルールで設定されたリロード ノード上でロードされます。ただし、テンプレート アプリに対してカスタム プロパティを設定し、そのテンプレート アプリにリンクされているアプリがロードされる場所を制御することができます。

生成されたアプリにカスタム プロパティを適用し、特定のリロード ノードにそれらアプリが送られるようにすることもできます。生成されたアプリに設定したカスタム プロパティにより、生成元のノードとは異なる、テンプレート アプリに指定されたノードからアプリをリロードするよう指示することができます。カスタム プロパティは、生成された後の On-demand アプリに対して設定します。

ストリームの管理

ストリームを利用すると、ユーザーはアプリ、シート、ストーリーを読み取ったり公開したりできます。ストリームへの公開アクセス権があるユーザーは、その特定のストリームのコンテンツを作成できます。Qlik Senseサイトでのストリーム アクセス パターンは、各ストリームのセキュリティ ルールによって決まります。既定で、Qlik Sense には次の 2

つのストリームが含まれます。**Everyone** および **Monitoring apps** 。

1 つのアプリは、1 つのストリームにしか公開できません。ただし、アプリを複製してコピーを作成する場合は、コピーを別のストリームに公開することができます。アプリはストリーム間で移動できます。

ハブでは、アプリを持たないストリーム (空のストリームまたはユーザーの既存のセキュリティ規則によりアプリが表示されないストリーム) は表示されません。アプリを公開、別のストリームから移動、または削除すると、ストリームのリストが動的に更新され、アプリが 1 つ以上あるか否かによって、ストリームはハブから表示または非表示になります。QMC など、ハブ外での変更は、ハブ内のストリームのリストの更新をトリガーしません。

*すべての認証ユーザーには [**Everyone**] ストリームの読み取りと公開権限があり、すべての匿名ユーザーには読み取り専用権限があります。あらかじめ定義された管理者のロールの 3 つ (RootAdmin、ContentAdmin、SecurityAdmin) には、Monitoring apps ストリームの読み取り権限と公開権限があります。*

ユーザーがストリーム内の公開されたアプリを編集できるようなルールを作成することは推奨されません。

ストリームの作成

ストリームを作成して、アプリ、シートおよびストーリーをユーザーが読んだり公開したりできるようにします。ストリームのセキュリティルールによって、ストリーム内でユーザーに付与される特権が決まります。ストリームがハブに表示されるには、少なくとも 1 つのアプリが必要です。空のストリームまたはユーザーの既存のセキュリティ規則によりアプリが表示されないストリームは表示されません。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Streams (ストリーム)**] を選択して、概要を表示します。
3. 操作バーで ⊕ **新規作成** をクリックします。
4. プロパティを編集します。

ID

ID プロパティ

プロパティ	説明
[**名前**]	ストリームの名前。
[**所有者**]	ストリームの所有者。ストリームが作成されるまで、このプロパティは存在しません。

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

カスタム プロパティ

> ***カスタム プロパティ**を利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

5. 操作バーで [**適用**] をクリックし、ストリームを作成して保存します。
   [**セキュリティ ルールの作成**] ダイアログが開きます。
6. ストリームのセキュリティ ルールを作成し、[**適用**] をクリックします。

> *ストリームを削除すると、すべての関連するセキュリティ ルールも同時に削除されます。関連するセキュリティ ルールは、**[関連するアイテム]** で確認できます。*

ストリームの編集

更新権限を有するストリームを編集できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Streams (ストリーム)**] を選択して、概要を表示します。
   編集するストリームを選択します。
3. アクション バーで [**編集**] をクリックします。
4. プロパティを編集します。

ID

ID プロパティ

プロパティ	説明
[**名前**]	ストリームの名前。
[**所有者**]	ストリームの所有者。ストリームが作成されるまで、このプロパティは存在しません。

タグ

タグ プロパティ

プロパティ	説明
[タグ]	利用可能なタグがない場合、このプロパティグループは空となります。 紐付けられているタグがテキスト ボックスの下に表示されます。

カスタム プロパティ

カスタム プロパティを利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。

5. 操作バーで [**適用**] をクリックし、変更を適用して保存します。

ページの最下部に [**更新完了**] と表示されます。

ストリームの削除

削除権限を有するストーリーを削除できます。

*[**Monitoring apps**] ストリームは削除しないでください。ストリームを削除すると、取り消すことができません。(RootAdmins、ContentAdmins、SecurityAdmins はストリームを削除できます。)*

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Streams (ストリーム)**] を選択して、概要を表示します。
3. 削除するストリームを選択します。
4. アクション バーの [**Delete**] をクリックします。
   [**Delete**] ダイアログが表示されます。
5. [**OK**] をクリックします。

ストリームのアクセス権の作成

ストリームへのアクセス権を付与するセキュリティ ルールを作成します。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Streams (ストリーム)**] を選択して、概要を表示します。

3. ルールを作成するストリームを選択して [**編集**] をクリックします。
   [Stream edit (ストリームの編集)] ページが開きます。
4. [**関連するアイテム**] の [**セキュリティルール**] を選択します。
   システム ルール概要が表示されます。
5. データ マネージャーでテーブルの ➕操作バーの [**関連するルールの作成**] をクリックします。
   [**セキュリティルールの作成**] ダイアログが開きます。
6. ストリームの管理アクセスのセキュリティルールを編集します。
   a. [**ID**] プロパティを編集します:

ID プロパティ

項目	**値**
名前	ストリームの名前を入力します。必須。
[**無効化**]	ルールを無効にする場合に選択します。このルールは、既定でオンになっています。
[**説明**]	ルールについての説明を入力します。

   b. [**基本**] プロパティを編集します。

演算子の説明

項目	**値**
演算子	**説明と例**
=	この演算子では大文字と小文字は区別されません。比較対象の数式と完全に等しい場合は True を返します。 `user.name = ”a*”` 名前が「a*」と完全に一致するユーザーがルールの対象になります。
like	この演算子では大文字と小文字は区別されません。比較対象の数式と等しい場合は True を返します。 `user.name like ”a*”` 名前が「a」で始まるすべてのユーザーがルールによって対象になります。.
!=	この演算子では大文字と小文字は区別されません。比較対象の数式の値が等しくない場合に True を返します。 `user.name != resource.name` ユーザーと同じ名前ではないすべてのリソースがルールによって対象になります。

7. オプションとして、[**詳細設定**] プロパティを編集し、ルールの [**条件**] を作成します。
    1. 条件を追加します。
    2. [**コンテキスト**] リストを使用し、ルールの適用対象を指定します。
8. [**適用**] をクリックします。
   ダイアログが閉じ、ストリームのセキュリティルール概要にルールが追加されます。

*セキュリティルールは、[**セキュリティルール**] 概要ページにも表示されます。*

*ストリームを削除すると、すべての関連するセキュリティルールも同時に削除されます。関連するセキュリティルールは、[**関連するアイテム**] で確認できます。*

データ接続および拡張機能の管理

データ接続

データ接続により、データソースからデータを選択およびロードすることができます。すべてのデータ接続は、QMC から集中的に管理されています。データ接続は、Qlik Sense データロードエディタで作成されますデータ接続を作成したユーザーは自動的に、その接続の所有者となり、既定ではそのデータ接続にアクセスできる唯一のユーザーです。データ接続は、QMC で定義されたセキュリティルールを使用して他のユーザーと共有できます。

Qlik Sense Desktop で開発されたアプリをインポートすると、既存のデータ接続が QMC にインポートされます。サーバーからアプリをエクスポートすると、既存のデータ接続はそのアプリとともにはエクスポートされません。

インポートされるアプリのデータ接続名が、既存のデータ接続の名前と同じ場合、データ接続はインポートされません。つまり、インポートされたアプリは、インポートされたアプリのデータ接続ではなく、同一名のすでに存在するデータ接続を使用します。

既定のセキュリティルール

データフォルダの接続は、QMC の既定のルールによって制限されています。このセキュリティルールは、データフォルダ接続の作成を RootAdmin、ContentAdmin、SecurityAdmin ユーザーに制限します。特定のユーザーにデータフォルダ接続を作成する権限を与える場合は、その特定のユーザーに新しいルールを作成します。既定のセキュリティルールを変更しないでください。 セキュリティの脆弱性が発生し、ユーザーがフォルダ構造を参照できるようになる可能性があります。

データ接続のアクセス権の作成 (page 264)

分析接続

分析接続を使用すると、外部分析をビジネスディスカバリと統合することができます。分析接続は、外部計算エンジンの呼び出し (このとき外部計算エンジンはサーバーサイド拡張 (SSE) として動作) によって、ロードスクリプトおよびチャートで使用可能な数式を拡張します。たとえば、R への分析接続を作成し、データのロード時に統計数式を使用できます。

拡張機能

拡張機能には、ウィジェット ライブラリ、カスタム テーマ、またはビジュアライゼーション エクステンションなどさまざまなものがあり、これらを使用して、たとえば、多様な地域を選択できるインタラクティブ マップで、データを可視化します。

データ接続の編集

データ接続は、Qlik Sense のデータ ロード エディタで作成するか、[**データの追加**] オプションを使用して作成します。データ接続を作成したユーザーは自動的に、その接続の所有者となり、既定ではそのデータ接続にアクセスできる唯一のユーザーです。

更新権限を有するデータ接続を編集できます。次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Data connections (データ接続)**] を選択して、概要を表示します。
3. 編集したいデータ接続を選択します。

   複数のデータ接続を選択すると、セキュリティ ルールの表示、編集、追加ができなくなります。

4. アクション バーで [**編集**] をクリックします。
5. プロパティを編集します。
   一番右側にあるパネルで、プロパティ グループの表示/非表示を切り替えることができます。

ID

ID プロパティ

プロパティ	説明
[**名前**]	データ接続名。
[**所有者**]	データ接続所有者のユーザー名。
[**接続文字列**]	データ接続の接続文字列。通常はデータ ソースやドライバー、パスの名前が含まれています。
[**タイプ**]	データ接続のタイプ。ODBC、OLEDB およびフォルダーなど標準的なデータ接続。
[**ユーザー ID**]	接続文字列で使用されているユーザー ID。
[**パスワード**]	接続文字列で使用されているユーザー ID と関連付けられているパスワード。 *パスワードは暗号化されて保存されます。*

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

カスタム プロパティ

***カスタム プロパティ**を利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

[**適用**] をクリックして変更を保存します。必須の項目が空欄の場合、[**Apply**] は無効になります。

6. 操作バーで [**適用**] をクリックします。

「**データ接続が更新されました**」というメッセージがページの最下部に表示されます。

データ接続の削除

削除権限を有するデータ接続を削除できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Data connections (データ接続)**] を選択して、概要を表示します。
3. 削除するデータ接続を選択します。
4. アクション バーの [**Delete**] をクリックします。
   [**Delete**] ダイアログが表示されます。
5. [**OK**] をクリックします。

データ接続のアクセス権の作成

データ接続へのアクセス権を付与するセキュリティ ルールを作成します。次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Data connections (データ接続)**] を選択して、概要を表示します。
3. ルールを作成するデータ接続を選択して、[**編集**] をクリックします。
   データ接続の編集ページが開きます。
4. [**関連するアイテム**] の [**セキュリティ ルール**] を選択します。
5. データ マネージャーでテーブルの ➕ 操作バーの [**関連するルールの作成**] をクリックします。

[**セキュリティルールの作成**] ダイアログが開きます。

6. データ接続の管理アクセスのセキュリティルールを編集します:
   a. [**ID**] プロパティを編集します:

ID の項目と値

項目	値
名前	データ接続名を入力します。必須。
[**無効化**]	ルールを無効にする場合に選択します。このルールは、既定でオンになっています。
[**説明**]	ルールについての説明を入力します。

   b. [**詳細**] セクションのドロップダウンを使用して、ルールを適用するコンテキストを指定します。
   c. [**基本**] セクションで、次の演算子で使用するルールの条件を選択します。

演算子の説明

演算子	説明と例
=	この演算子では大文字と小文字は区別されません。比較対象の数式と完全に等しい場合は True を返します。 `user.name = "a*"` 名前が「a*」と完全に一致するユーザーがルールの対象になります。
like	この演算子では大文字と小文字は区別されません。比較対象の数式と等しい場合は True を返します。 `user.name like "a*"` 名前が「a」で始まるすべてのユーザーがルールによって対象になります。
!=	この演算子では大文字と小文字は区別されません。比較対象の数式の値が等しくない場合に True を返します。 `user.name != resource.name` ユーザーと同じ名前ではないすべてのリソースがルールによって対象になります。

7. [**適用**] をクリックします。
   ダイアログが閉じ、セキュリティルール概要にルールが追加されます。

> *[**セキュリティルール**] 概要ページに対応するセキュリティルールが表示されます。*

これで、選択されたデータ接続に対するアクセス権が作成されました。

インポート拡張機能

デフォルトでは、RootAdmin ユーザーのみに拡張機能をインポートするアクセス権が付与されています。拡張機能のインポートを有効にするには、セキュリティルールを定義する必要があります。既定では、すべての Qlik Sense ユーザーが追加したすべての拡張機能にアクセスできます。アクセスを制限したい場合は、*Extension* というセキュリティルールを見直します。

> *QMC にすでに存在する拡張子をインポートする場合は、プロンプトが表示されたら、[**Replace**] (置き換え) をクリックして既存のファイルを新しいファイルに置き換えるか、[✕] をクリックしてキャンセルします。*

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**Start**] ▼ ドロップダウン メニューから [**Extensions**] を選択して、概要を表示します。
3. 操作バーの ⊕ [**インポート**] をクリックします。
4. [**拡張ファイルのインポート**] ダイアログが開きます。インポートする zip ファイルを選択します。
   パスワードで保護されている場合は zip ファイルのパスワードを入力してください。
5. ファイル エクスプローラ ウィンドウで [**開く**] をクリックします。
6. [**インポート**] をクリックします。

> *拡張機能は、\\QlikShare\StaticContent\Extensions に保存されます。ファイルの最大サイズは、次のトピックの「制限事項」で指定されています。「データ ファイルの添付とデータのアプリへの追加」拡張機能のインポートに失敗した場合は、%ProgramData%Qlik/Sense/Log/Repository/System にあるログ ファイルを確認してください。*

拡張機能名

QMC に既に拡張機能が存在する場合、インポート時に新しい拡張機能と置き換えることができます。既存の拡張機能を置き換える場合、古いファイルは新しいファイルで上書きされますが、拡張機能の GUID および関連する項目 (カスタム セキュリティ ルールなど) は影響を受けません。拡張機能を置き換えない場合は、最低限 .zip ファイル内の .qext ファイルの名前を変更することによって、新しい拡張機能の名前を変更できます。ただし、後々の名前の重複を避けるため、.zip ファイル、.qext ファイル、および .zip ファイル内の関連する .js ファイルはすべて同じファイル名を使用することをお勧めします。

既定では、インポートされた拡張機能は [**拡張機能**] の概要に表示されます。拡張機能名は .qext ファイル名と同じになります。ただし Qlik Sense ハブでは、拡張機能は .qext ファイルの [Name] フィールドで編集して変更できる通常のファイル名で表示されます。

[**Extensions**] の概要でファイル名のみを表示する場合は、拡張機能の zip ファイルにある .js ファイルと .qext ファイルから *com-qliktech-* の部分を削除する必要があります。

> *ユーザーは Dev Hub にインポートされた拡張機能の名前のみ変更できます。*

ライブラリID とウィジェットID との間に重複がないかどうかのチェックが行われないため、QMC からウィジェット ライブラリをインポートすることは避けます。代わりに、自動的にチェックが実行される Dev Hub からインポートしてください。

拡張機能の編集

更新権限を有する拡張機能を編集できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start**] ▼ ドロップダウン メニューから [**Extensions**] を選択して、概要を表示します。
3. 編集する拡張機能を選択します。
4. アクション バーで [**編集**] をクリックします。
5. プロパティを編集します。

ID

ID プロパティ

プロパティ	説明
[**名前**]	拡張機能名はアップロードされた圧縮ファイルの拡張機能定義ファイル (*.qext*) のファイル名から名付けられます。
[**所有者**]	拡張の所有者のユーザー名。 *このプロパティは、拡張の編集時にのみ表示されます。*

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

カスタム プロパティ

> *カスタム プロパティを利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

[**適用**] をクリックして変更を保存します。必須の項目が空欄の場合、[**Apply**] は無効になります。

6. このフィールドは [**Associated items**] でも編集できます。

関連するアイテム

関連するアイテムのプロパティ

プロパティ	説明
[**ユーザー アクセス**]	プレビューには、ターゲット リソースと選択したアイテムにアクセスできるソース ユーザーが表示されます。
[**セキュリティ ルール**]	拡張機能のセキュリティ ルールが表示されます。

7. アクション バーで [**適用**] をクリックします。

ページの最下部に [**更新完了**] と表示されます。

> *Web ブラウザでは拡張機能が 6 時間までキャッシュされます。手動でキャッシュを消去すれば、新しいバージョンの拡張機能を利用することができます。*

拡張機能の削除

削除権限を有する拡張機能を削除できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start**] ▼ ドロップダウン メニューから [**Extensions**] を選択して、概要を表示します。
3. 削除する拡張機能を選択します。
4. アクション バーの [**Delete**] をクリックします。
   [**Delete**] ダイアログが表示されます。
5. [**OK**] をクリックします。

分析接続の作成

分析接続を使用すると、外部分析をビジネス ディスカバリと統合することができます。分析接続は、外部計算エンジンの呼び出し (このとき外部計算エンジンはサーバーサイド拡張 (SSE) として動作) によって、ロード スクリプトおよびチャートで使用可能な数式を拡張します。たとえば、R への分析接続を作成し、データのロード時に統計数式を使用できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
   複数のサーバーがある場合は、中央サーバーを使用します。
2. QMC スタートページから、あるいは [**開始**] から [**分析接続**] を選択します。▼ 選択して、概要を表示します。
3. データマネージャーでテーブルの **新規作成** をクリックします。
4. プロパティを編集します。

ID

ID プロパティ

プロパティ	説明
[**名前**]	分析接続の名前。一意である必要があり、数字で始まってはなりません。プラグイン関数 (例えば、Python プラグインの場合の SSEPython または R プラグインの場合の R) により、アプリの数式内から使用されるプラグインへのマッピング/エイリアス。
ホスト	分析接続のホストは、例えば同じマシン上では *localhost*、別のマシン上にある場合は *mymachinename.qlik.com* です。
ポート	接続時に使用するポート。
証明書ファイルのパス	証明書へのフルパス:*C:\ProgramData\Qlik\Sense\Repository\Exported Certificates\<サーバー名>*。このパスは、クライアントおよびサーバーの両方の証明書とキーを含むフォルダーを指し示す必要があります。このパスは、証明書が配置されているフォルダーを指し示しているだけです。証明書が実際にこのフォルダーにコピーされていることを確認する必要があります。3 つの証明書の名前は、*root_cert.pem*、*sse_client_cert.pem*、*sse_client_key.pem* とする必要があります。許可されているのは相互認証のみです (サーバーとクライアント間の認証)。 *証明書のファイルパスの設定は任意ですが、パスがないと接続は安全ではありません。*
再接続タイムアウト (秒)	既定値: 20
要求タイムアウト (秒)	既定値: 0

カスタム プロパティ

> *カスタム プロパティを利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

5. 操作バーで [**適用**] をクリックし、分析接続を作成して保存します。

> *ページ最下部に [**追加完了**] と表示されます。*

> *QMC での設定に対する変更は、Settings.ini ファイルでの設定より優先されます。*

分析接続の編集

分析接続を使用すると、外部分析をビジネスディスカバリと統合することができます。分析接続は、外部計算エンジンの呼び出し (このとき外部計算エンジンはサーバーサイド拡張 (SSE) として動作) によって、ロード スクリプトおよびチャートで使用可能な数式を拡張します。たとえば、R への分析接続を作成し、データのロード時に統計数式を使用できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**開始**] から [**分析接続**] を選択します。▼選択して、概要を表示します。
3. 編集する分析接続を選択し、操作バーで [**編集**] をクリックします。
4. プロパティを編集します。

ID プロパティ

プロパティ	説明
[**名前**]	分析接続の名前。一意である必要があり、数字で始まってはなりません。プラグイン関数 (例えば、Python プラグインの場合の SSEPython または R プラグインの場合の R) により、アプリの数式内から使用されるプラグインへのマッピング/エイリアス。
ホスト	分析接続のホストは、例えば同じマシン上では *localhost*、別のマシン上にある場合は *mymachinename.qlik.com* です。
ポート	接続時に使用するポート。

プロパティ	説明
証明書ファイルのパス	証明書へのフル パス:*C:\ProgramData\Qlik\Sense\Repository\Exported Certificates\<サーバー名>*。このパスは、クライアントおよびサーバーの両方の証明書とキーを含むフォルダーを指し示す必要があります。このパスは、証明書が配置されているフォルダーを指し示しているだけです。証明書が実際にこのフォルダーにコピーされていることを確認する必要があります。3 つの証明書の名前は、*root_cert.pem*、*sse_client_cert.pem*、*sse_client_key.pem* とする必要があります。許可されているのは相互認証のみです (サーバーとクライアント間の認証)。 *証明書のファイル パスの設定は任意ですが、パスがないと接続は安全ではありません。*
再接続タイムアウト (秒)	既定値: 20
要求タイムアウト (秒)	既定値: 0

カスタム プロパティ

***カスタム プロパティ**を利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

5. 操作バーで [**適用**] をクリックし、分析接続を保存します。

ページの最下部に [**更新完了**] と表示されます。

QMC での設定に対する変更は、Settings.ini ファイルでの設定より優先されます。

分析接続のセキュリティ

分析接続を使用する場合は、Qlik Sense 環境のセキュリティを強化するため以下のベストプラクティスを検討してください。

- 管理者権限が付与されていない、分離された環境にサーバーサイド拡張 (SSE) プラグインをインストールし、実行します。悪意あるスクリプトからの害を最小限に抑えるため、プラグインを開始しているユーザーアカウントおよびそのユーザーがマシンとドメインについて保有しているアクセス権について注意します。

- セキュリティ強化のため、EvaluateScript 機能は、SSE プラグイン構成ファイルで構成パラメーター `allowScript` を false に設定することで無効化することができます。これにより任意のスクリプトを実行することができなくなり、SSE プラグインは事前に定義された関数のみを実行できます。
- Qlik Sense アプリを作成するアプリケーション開発者には、SSE 式で使用される変数の形式を制限して設定することをお勧めします。例えば、変数の形式を数値のみに制限することができます。

ユーザーの管理

ユーザー データはすべて、Qlik Sense Repository Service (QRS) データベースに保存されます。QMCでユーザーディレクトリコネクタを作成し、構成されているディレクトリサービスからユーザー データを同期および取得できるようにします。ユーザーがQlik SenseまたはQMCにログインすると、ユーザー データが自動的に取得されます。

Qlik Senseでのユーザーの管理には以下が含まれます。

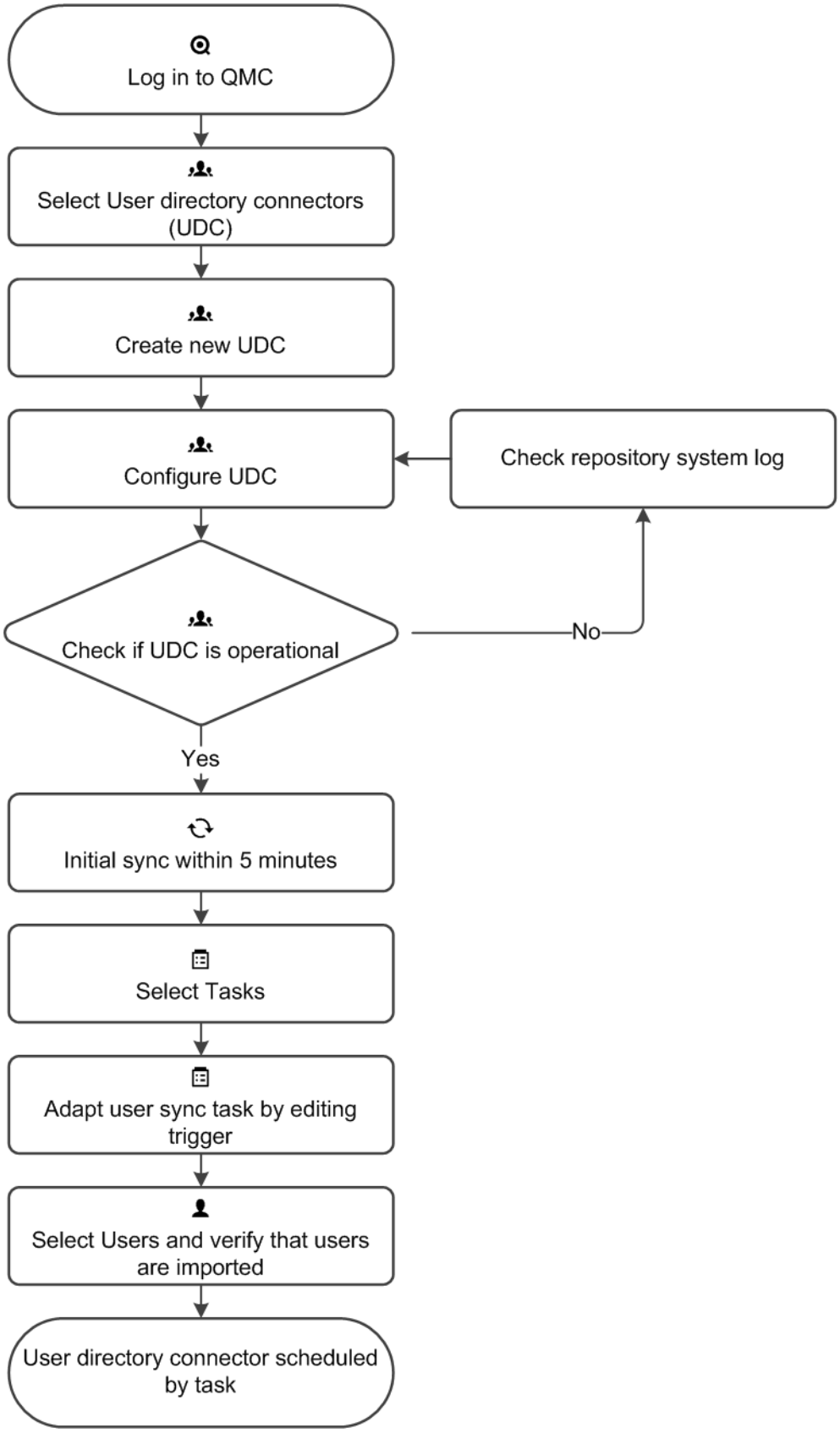
- 新規ユーザー ディレクトリコネクタの作成
- ユーザー ディレクトリの同期
- アクセス タイプの管理
- リソース所有者の変更
- ユーザーが所有するリソースの削除
- ユーザーへの管理者 ロールの関連付け
- ユーザーの非アクティブ化
- ユーザーの削除

タスク別にユーザー ディレクトリコネクタとスケジュールを設定

ユーザー ディレクトリコネクタ (UDC) の新規インスタンスを作成すると、スケジュールされたユーザー同期タスクがデフォルトで作成され、最初の同期が 5 分以内に実行されます。ユーザー ディレクトリコネクタは 機能するように構成して操作を可能にしなくてはなりません。

必要に応じて、ユーザー同期タスクのデフォルトのトリガーを変更し、さらにトリガーを追加できます。ユーザー データはユーザー ディレクトリコネクタの概要から手動で同期できます。

次のワークフローは、新しいユーザー ディレクトリコネクタの設定について説明したものです。


Log in to QMC
Select User directory connectors (UDC)
Create new UDC
Configure UDC
Check repository system log
Check if UDC is operational
No
Yes
Initial sync within 5 minutes
Select Tasks
Adapt user sync task by editing trigger
Select Users and verify that users are imported
User directory connector scheduled by task

ODBC の例

各データソースには異なる構成があります。以下に、ODBC ユーザーディレクトリコネクタを追加する 2 つの例 (csv と SQL) を示します。

ODBC の例 (csv)

次の手順を実行します。

1. Microsoft Access Text Driver がインストールされていることを確認します。
2. サーバーで ODBC ソースを設定します。以下の場所に、2 つの別個の csv ファイルのデータを保存する必要があります。*%ProgramData%\Qlik\Sense\temp*。

   > *既定のインストールには、一時フォルダは含まれません。QMC 管理者が作成していなかった場合は、一時フォルダーを作成する必要があります。*

   Table1.csv にはユーザー、*Table2.csv* にはユーザー属性が含まれます。csv ファイルの値は、カンマ区切りです。

   Table1.csv のコンテンツ:
   ```
   userid,name
   JoD,John Doe
   ```

   Table2.csv のコンテンツ:
   ```
   userid,type,value
   JoD,email,jod@gmail.com
   ```
3. QMC を開く: *https://<QPS サーバー名>/qmc*
4. QMC スタートページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**User directory connectors (ユーザー ディレクトリ コネクタ)**] を選択して、概要を表示します。新規ユーザーディレクトリコネクタ (ODBC) を作成し、プロパティを編集します。

   [**ID**]
   全項目が必須で、空欄のままにはできません。

   ID プロパティ

プロパティ	説明
名前	QMC で定義された UDC プロパティの名前です。
タイプ	UDC タイプです。

   ユーザー同期設定

ユーザー同期プロパティの説明と値

プロパティ	説明	既定値
[**既存のユーザーのユーザーデータの同期**]	• 選択されている場合は、既存のユーザーのみが同期されます。既存のユーザーは、にログインしているユーザーや、構成済みディレクトリサービスから同期されたことのあるユーザーです。Qlik Sense • 選択されていない場合は、UDC のプロパティで定義されているすべてのユーザーが構成済みのディレクトリサービスから同期されます。 *ユーザー属性は、ユーザーがハブにログインするときにのみ同期されます。QMC でユーザーを削除しても、削除されたユーザーに対してアクティブなセッションは引き続き有効です。ハブの更新のみが行われた場合、ユーザーはデータベースに追加されますが、いかなる属性も持ちません。*	選択値

接続

プロパティ	説明	既定値
ユーザーディレクトリ名	ユーザーディレクトリの名前。ユーザーディレクトリは一意でなければなりません。一意でないと、コネクタは構成されません。この名前にスペースを含んではいけません。	-
ユーザーテーブル名	ユーザーが一覧表示されているテーブルの名前。テーブル名にファイル拡張子を含めます。例:*Table.csv*.	-
属性テーブル名	ユーザー属性を含むテーブルの名前。テーブル名にファイル拡張子を含めます。例:*Table.csv*.	-

プロパティ	説明	既定値
表示されている接続文字列	データソースへの接続に使われる接続文字列関数の表示可能な部分。以下のいずれかを指定します。 • 完全な接続文字列。例:*Driver={Microsoft Access Text Driver (*.txt, *.csv)};Extensions=asc,csv,tab,txt;Dbq=%ProgramData%\Qlik\Sense\temp* ◦ *Driver*は現在コンピュータにあるドライバを指定する必要があります。[**ODBC データ ソース アドミニストレータ**] で、指定するドライバーを確認してください。「データ ソース」を検索して、アプリケーションを見つけます。 ◦ *Dbq*: csv ファイルが保存されているフォルダへのパス。 • 確立されたシステム DNS へのポインタ。例えば、*dsn=MyDSN;* *データベースに接続する場合、2 つの接続文字列関数は単一の接続文字列関数に連結されます。*	-
暗号化された接続文字列	データソースへの接続に使われる接続文字列関数の暗号化された部分。通常、この文字列にはユーザー名とパスワードが含まれます。 *データベースに接続する場合、2 つの接続文字列関数は単一の接続文字列関数に連結されます。*	-
同期タイムアウト (秒)	データソースからのデータ読み取りのタイムアウト。	240

ユーザー テーブル名:*Table1.csv*
属性テーブル名:*Table2.csv*
表示されている接続文字列: *Driver={Microsoft Access Text Driver (*.txt, *.csv)};Extensions=asc,csv,tab,txt;Dbq=%ProgramData%\Qlik\Sense\temp*

5. [**適用**] をクリックして変更を適用します。
6. [**ユーザー ディレクトリ コネクタ**] の概要に進み、ユーザー ディレクトリが [**構成済み**] で [**操作可能**] として表示されているかチェックします。

ユーザー ディレクトリ名が一意でなければ、コネクタは構成されません。操作可能でない場合は、リポジトリシステムのログインを確認します: %ProgramData%\Qlik\Sense\Log\Repository\Trace。

ODBC データ ソースが追加され、5 分以内に最初の同期が実行されます (既定)。

ODBC の例 (SQL)

次の手順を実行します。

1. ユーザーを含めた SQL データベースを作成します。データベースには 2 つのテーブルを含め、1 つのテーブルにはユーザーを、もう1 つのテーブルにはユーザーの属性を含めます。

   Table1: SQL ユーザー

   SQL ユーザー

Index	**値**
1	ID,userid,name
2	1,JoD,John Doe

   Table2: SQL 属性

   SQL 属性

Index	**値**
1	userid,type,value
2	JoD,email,jod@gmail.com

   ユーザーID が一意である場合、ID 列は冗長になります。

2. サーバー (SQL Server Native Client 11.0 など) に SQL ドライバーをインストールします。
3. QMC を開く: *https://<QPS サーバー名>/qmc*
4. QMC スタートページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**User directory connectors (ユーザー ディレクトリ コネクタ)**] を選択して、概要を表示します。新規ユーザー ディレクトリ コネクタ (ODBC) を作成し、プロパティを編集します。

   [**ID**]
   全項目が必須で、空欄のままにはできません。

   ID プロパティ

プロパティ	**説明**
名前	QMC で定義された UDC プロパティの名前です。
タイプ	UDC タイプです。

   ユーザー同期設定

ユーザー同期プロパティ、説明、既定値

プロパティ	説明	既定値
[**既存のユーザーのユーザーデータの同期**]	• 選択されている場合は、既存のユーザーのみが同期されます。既存のユーザーは、にログインしているユーザーや、構成済みディレクトリサービスから同期されたことのあるユーザーです。Qlik Sense • 選択されていない場合は、UDC のプロパティで定義されているすべてのユーザーが構成済みのディレクトリサービスから同期されます。 *ユーザー属性は、ユーザーがハブにログインするときにのみ同期されます。QMC でユーザーを削除しても、削除されたユーザーに対してアクティブなセッションは引き続き有効です。ハブの更新のみが行われた場合、ユーザーはデータベースに追加されますが、いかなる属性も持ちません。*	選択値

接続

接続プロパティ、説明、既定値

プロパティ	説明	既定値
ユーザー ディレクトリ名	ユーザー ディレクトリの名前。ユーザー ディレクトリは一意でなければなりません。一意でないと、コネクタは構成されません。この名前にスペースを含んではいけません。	-
ユーザー テーブル名	*UsersTable* など、ユーザーが含まれているテーブルの名前。 *Oracle ODBC ユーザー ディレクトリコネクターを設定する場合、**ユーザー テーブル名** および **属性 テーブル名** の前に、それらのテーブルの所有者を付ける必要があります。例: ただの USERS でなく OWNER.USERS。*	-

プロパティ	説明	既定値
属性テーブル名	*AttributesTable* など、ユーザー属性が含まれているテーブルの名前。 *Oracle ODBC ユーザーディレクトリコネクターを設定する場合、**ユーザーテーブル名**および**属性テーブル名**の前に、それらのテーブルの所有者を付ける必要があります。例: ただの USERS でなく OWNER.USERS。*	-
表示されている接続文字列	データソースへの接続に使われる接続文字列関数の表示可能な部分。以下のいずれかを指定します。 • 完全な接続文字列。例: *Driver={SQL Server Native Client 11.0};Server=localhost;Database=Users;Trusted_Connection=yes;* 1. *Driver*は現在コンピュータにあるドライバを指定する必要があります。[**ODBC データ ソース アドミニストレータ**] で、指定するドライバーを確認してください。「データ ソース」を検索して、アプリケーションを見つけます。 2. *Server* は接続するサーバーを指定する必要があります。 3. *Database* はテーブルがあるデータベースを指定する必要があります。 4. *Trusted_Connection=yes* は設定によって必要になる場合があります。この例では、必要です。 • 確立されたシステム DNS へのポインタ。例えば、*dsn=MyDSN;* *データベースに接続する場合、2 つの接続文字列関数は単一の接続文字列関数に連結されます。*	-

プロパティ	説明	既定値
暗号化された接続文字列	データソースへの接続に使われる接続文字列関数の暗号化された部分。通常、この文字列にはユーザー名とパスワードが含まれます。 *データベースに接続する場合、2 つの接続文字列関数は単一の接続文字列関数に連結されます。*	-
同期タイムアウト(秒)	データソースからのデータ読み取りのタイムアウト。	240

ユーザー テーブル名:*UsersTable*

属性テーブル名:*AttributesTable*

表示されている接続文字列: *Driver={SQL Server Native Client 11.0};Server=localhost;Database=Users;Trusted_Connection=yes;*

5. [**適用**] をクリックして変更を適用します。
6. [**ユーザー ディレクトリ コネクタ**] の概要に進み、ユーザー ディレクトリが [**構成済み**] で [**操作可能**] として表示されているかチェックします。

ユーザー ディレクトリ名が一意でなければ、コネクタは構成されません。操作可能でない場合は、リポジトリシステムのログインを確認します: %ProgramData%\Qlik\Sense\Log\Repository\Trace。

ODBC データソースが追加され、5 分以内に最初の同期が実行されます (既定)。

ODBC の例 (Access)

各データソースには異なる構成があり、以下は ODBC ユーザー ディレクトリ コネクタを追加する例 (txt) です。

Microsoft Access Text Driver (.txt, *.csv) を使用して .txt ファイルをロードする場合、コネクター タイプは [**ODBC**]. ではなく [**Access (ODBC 経由)**] を使用する必要があります。*

txt ファイルおよび csv ファイルに対する Access の使用 (ODBC 経由)

次の手順を実行します。

1. Microsoft Access Text Driver がインストールされていることを確認します。
2. サーバーで ODBC ソースを設定します。以下の場所に、2 つの別個の txt ファイルのデータを保存する必要があります。*%ProgramData%\Qlik\Sense\Temp*。

   > *既定のインストールには、一時フォルダーは含まれません。QMC 管理者が作成していなかった場合は、一時フォルダーを作成する必要があります。*

   Users.txt にはユーザー、*Attributes.txt* にはユーザー属性が含まれます。

   Users.txt に含まれるもの:
   ```
   userid,name
   JoD,John Doe
   ```

   Attributes.txt に含まれるもの:
   ```
   userid,type,value
   JoD,email,jod@gmail.com
   ```

3. QMC を開く: *https://<QPS サーバー名>/qmc*
4. QMC スタートページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**User directory connectors (ユーザー ディレクトリ コネクタ)**] を選択して、概要を表示します。新しいユーザー ディレクトリ コネクタ: [**Access (ODBC 経由)**] を作成し、プロパティを編集します。

   ID
   全項目が必須で、空欄のままにはできません。

   ID プロパティ

プロパティ	説明
名前	QMC で定義された UDC プロパティの名前です。
タイプ	UDC タイプです。

   ユーザー同期設定

ユーザー同期プロパティの説明と値

プロパティ	説明	既定値
[**既存のユーザーのユーザーデータの同期**]	• 選択されている場合は、既存のユーザーのみが同期されます。既存のユーザーは、にログインしているユーザーや、構成済みディレクトリサービスから同期されたことのあるユーザーです。Qlik Sense • 選択されていない場合は、UDC のプロパティで定義されているすべてのユーザーが構成済みのディレクトリサービスから同期されます。 *ユーザー属性は、ユーザーがハブにログインするときにのみ同期されます。QMC でユーザーを削除しても、削除されたユーザーに対してアクティブなセッションは引き続き有効です。ハブの更新のみが行われた場合、ユーザーはデータベースに追加されますが、いかなる属性も持ちません。*	選択値

接続

接続プロパティの説明と値

プロパティ	説明	既定値
ユーザーディレクトリ名	ユーザー ディレクトリの名前。ユーザー ディレクトリは一意でなければなりません。一意でないと、コネクタは構成されません。この名前にスペースを含んではいけません。	-
[**ユーザーテーブル名**]	このテキスト ファイルにはユーザーが含まれます。テーブル名にファイル拡張子を含めます。例:*File.txt/File.csv*.	-
[**属性テーブル名**]	このテキスト ファイルにはユーザー属性が含まれます。テーブル名にファイル拡張子を含めます。例:*File.txt/File.csv*.	-

プロパティ	説明	既定値
表示されている接続文字列	データソースへの接続に使われる接続文字列関数の表示可能な部分。以下のいずれかを指定します。 • 完全な接続文字列。例:*Driver={Microsoft Access Text Driver (*.txt, *.csv)};Extensions=asc,csv,tab,txt;Dbq=C:\ProgramData\Qlik\Sense\Temp* *既定の**表示されている接続文字列**:Driver={Microsoft Access Driver (*.mdb, *.accdb)};DBQ=C:\Database.accdb で、ドライバーの名前を Driver={Microsoft Access Text Driver (*.txt, *.csv)};DBQ=C:\ProgramData\Qlik\Sense\Temp と置き換えて、txt および csv ファイルを使用可能にする必要があります。* ◦ 「*Driver*」は現在コンピューターにあるドライバーを指定する必要があります。[**ODBC データ ソース アドミニストレータ**] で、指定するドライバーを確認してください。「データ ソース」を検索して、アプリケーションを見つけます。 ◦ *DBQ*: txt ファイルが保存されているフォルダーへのパス。 • 確立されたシステム DSN へのポインター。例えば、*dsn=MyDSN;* *データベースに接続する場合、2 つの接続文字列関数は単一の接続文字列関数に連結されます。*	-
暗号化された接続文字列	データソースへの接続に使われる接続文字列関数の暗号化された部分。通常、この文字列にはユーザー名とパスワードが含まれます。 *データベースに接続する場合、2 つの接続文字列関数は単一の接続文字列関数に連結されます。*	-
同期タイムアウト(秒)	データソースからのデータ読み取りのタイムアウト。	240

ユーザー テーブル名:*Users.txt*
属性 テーブル名:*Attributes.txt*
表示されている接続文字列: *Driver={Microsoft Access Text Driver (*.txt, *.csv)};Extensions=asc,csv,tab,txt;DBQ=C:\ProgramData\Qlik\Sense\Temp*

5. [**適用**] をクリックして変更を適用します。
6. [**ユーザー ディレクトリ コネクタ**] の概要に進み、ユーザー ディレクトリが [**構成済み**] で [**操作可能**] として表示されているかチェックします。

> *ユーザーディレクトリ名が一意でなければ、コネクタは構成されません。操作可能でない場合は、リポジトリシステムのログインを確認します: %ProgramData%\Qlik\Sense\Log\Repository\Trace。*

ODBC データソースが追加され、5 分以内に最初の同期が実行されます (既定)。

LDAP 追加フィルタを使用して、特定のユーザー情報を取得する

ユーザーディレクトリコネクタを作成して、ユーザーディレクトリと同期する時に、特定のユーザーの情報を取得できます。その情報を取得するには、汎用 LDAP または Active Directory のユーザーディレクトリコネクタの新規作成時に [**LDAP 追加フィルター**] プロパティを使用します。

[**詳細設定**] プロパティグループにある [**LDAP 追加フィルタ**] テキスト項目にクエリを入力します。例えば、以下をインポートしたい場合:

- John という名前のすべてのユーザー: *&(objectClass=user)(name=John*)*
- 特定のユーザー: *&(objectClass=user)(sAMAccountName=userid)*
- 特定の複数ユーザー: *(&(objectCategory=person)(objectClass=user)(|(sAMAccountName=userid)(sAMAccountName=userid)))*

ユーザーディレクトリコネクタの作成

ユーザーディレクトリコネクタ (UDC) を新規作成できます。

> *ユーザーディレクトリのユーザーおよび帰属の合計数は、1,000,000 (百万) 未満でなければなりません。大規模なユーザーディレクトリの場合は、[**ユーザー同期設定**] プロパティグループの [**既存ユーザーのユーザーデータを同期**] を常に選択することをお勧めします。大量のユーザーおよびユーザー属性を追加すると、監視アプリのリロードに失敗することがあります。*

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**User directory connectors (ユーザーディレクトリコネクタ)**] を選択して、概要を表示します。
3. データマネージャーでテーブルの **新規作成** をクリックします。
   利用可能なユーザーディレクトリコネクタのタイプを示すダイアログが表示されます。
4. 新しいユーザーディレクトリコネクタのタイプやそのソースを選択します。以下のタイプを利用できます。
   - 汎用 LDAP
   - 高度な LDAP
   - アクティブディレクトリ
   - ApacheDS
   - ODBC

- Access (ODBC 経由)
- Excel (ODBC 経由)
- SQL (ODBC 経由)
- Teradata (ODBC 経由)

ローカル ユーザーが Qlik Sense にログオンする場合、UDC は不要です。ただし、ローカル ユーザーがアプリにアクセスできるようにするには、アクセスを割り当てる必要があります。ユーザーベースのライセンスでは、プロフェッショナルまたはアナライザーのアクセス ルールを使用できます。トークンベースのライセンスでは、ユーザーまたはログイン アクセス ルールを使用してアクセスを割り当てることができます。あるいは、まずローカル ユーザーがログオンしてユーザーとして認識され、それからトークンが割り当てられるようにすることもできます。

5. プロパティを編集します。

ID

全項目が必須で、空欄のままにはできません。

ID プロパティ

プロパティ	説明
名前	QMC で定義された UDC プロパティの名前です。
タイプ	UDC タイプです。

ユーザー同期設定

ユーザー同期プロパティ

プロパティ	説明	既定値
[**既存のユーザーのユーザー データの同期**]	• 選択されている場合は、既存のユーザーのみが同期されます。既存のユーザーは、Qlik Sense にログインしているユーザーや、構成済みディレクトリサービスから同期されたことのあるユーザーです。 • 選択されていない場合は、UDC のプロパティで定義されているすべてのユーザーが構成済みのディレクトリサービスから同期されます。選択したユーザーのみを同期する場合は、[**Active Directory**]、[**ApacheDS**]、[**汎用 LDAP**] または [**Advanced LDAP**] でフィルターを作成できます。 *ユーザー属性は、ユーザーがハブにログインするときにのみ同期されます。QMC でユーザーを削除しても、削除されたユーザーに対してアクティブなセッションは引き続き有効です。ハブの更新のみが行われた場合、ユーザーはデータベースに追加されますが、いかなる属性も持ちません。*	選択値

*[**ユーザー同期設定**] プロパティグループの [**既存ユーザーのユーザー データを同期**] を選択するか、選択をクリアして、同期の実行方法を決定します。*

接続 (汎用 LDAP、高度な LDAP、Active Directory、ApacheDS)

接続プロパティ

プロパティ	説明	既定値
ユーザー ディレクトリ名	ユーザー ディレクトリは一意でなければなりません。一意でないと、コネクタは構成されません。UDC インスタンスの名前 (Active Directory のドメイン名に喩えられる)。ユーザー アカウント名と共に、この名前はユーザーを固有のものにします。 *Active Directory には手動で入力できません。*	-
パス	ディレクトリサーバーへの接続に使用する URI。SSL をサポートするため、プロトコルを LDAPS として指定します。 *カスタム ポートには対応していません。*	ldap://company.domain.com
[**ユーザー名**]	ディレクトリサーバーへの接続に使用する、オプションのユーザー ID。空の場合、Qlik Sense リポジトリを実行するユーザーを使用して、ディレクトリサーバーにログインします。	-
[**パスワード**]	ユーザー向けのオプションのパスワード。	-

ユーザーが Active Directory コネクターを作成する場合、Qlik Sense サービスを実行しているユーザーがディレクトリサーバーへのアクセスを許可されている場合のみ、そのコネクターは動作します。Qlik Sense サービスを実行しているユーザーがディレクトリサーバーへのアクセスを許可されていない場合、ディレクトリサーバーにアクセス可能なユーザー名とパスワードを入力する必要があります。

接続 (ODBC) と(ODBC 経由)

Microsoft Access Text Driver (.txt, *.csv) を使用して .txt ファイルをロードする場合、コネクタータイプは [**ODBC**]. ではなく [**Access (ODBC 経由)**] を使用する必要があります。*

接続プロパティ

プロパティ	説明	既定値
ユーザーディレクトリ名	ユーザーディレクトリの名前。ユーザーディレクトリは一意でなければなりません。一意でないと、コネクタは構成されません。この名前にスペースを含んではいけません。	-
ユーザーテーブル名	ユーザーが一覧表示されているテーブルの名前。テーブル名にファイル拡張子を含めます。例:*Table.csv*. *Oracle ODBC ユーザーディレクトリコネクターを設定する場合、**ユーザー テーブル名** および **属性 テーブル名** の前に、それらのテーブルの所有者を付ける必要があります。例: ただの USERS でなく OWNER.USERS。*	-
属性テーブル名	ユーザー属性を含むテーブルの名前。テーブル名にファイル拡張子を含めます。例:*Table.csv*. *Oracle ODBC ユーザーディレクトリコネクターを設定する場合、**ユーザー テーブル名** および **属性 テーブル名** の前に、それらのテーブルの所有者を付ける必要があります。例: ただの USERS でなく OWNER.USERS。*	-

プロパティ	説明	既定値
表示されている接続文字列	データソースへの接続に使われる接続文字列関数の表示可能な部分。以下のいずれかを指定します。 • 完全な接続文字列。例: *Driver={SQL Server Native Client 11.0};Server=localhost;Database=Users;Trusted_Connection=yes;* 1. *Driver*は現在コンピュータにあるドライバを指定する必要があります。[**ODBC データ ソース アドミニストレータ**] で、指定するドライバーを確認してください。「データ ソース」を検索して、アプリケーションを見つけます。 2. *Server* は接続するサーバーを指定する必要があります。 3. *Database* はテーブルがあるデータベースを指定する必要があります。 4. *Trusted_Connection=yes* は設定によって必要になる場合があります。この例では、必要です。 • 確立されたシステム DNS へのポインタ。例えば、*dsn=MyDSN;* *データベースに接続する場合、2 つの接続文字列関数は単一の接続文字列関数に連結されます。*	-
暗号化された接続文字列	データソースへの接続に使われる接続文字列関数の暗号化された部分。通常、この文字列にはユーザー名とパスワードが含まれます。 次の接続文字列があると見なされます: *Driver={Microsoft Access Driver (.mdb)};Dbq=C:\mydatabase.mdb;Uid=Admin;Pwd=verySecretAdminPassword;* この接続文字列は、そのままデータベースに保存すると秘密のパスワードが表示されてしまうため注意が必要です。パスワードを保護するため以下の手順に従ってください。 最初の部分 (*Driver={Microsoft Access Driver (.mdb)};Dbq=C:\mydatabase.mdb;*) を [**表示されている接続文字列**] 項目に保存し、二番目の部分 *(Uid=Admin;Pwd=verySecretAdminPassword;)* を [**暗号化された接続文字列**] 項目に保存します。このようにすれば二番目の部分がデータベースに暗号化されて保存されるため、後に編集のため UDC で開いても表示されません。 *データベースに接続する場合、2 つの接続文字列関数は単一の接続文字列関数に連結されます。*	-

プロパティ	説明	既定値
同期タイムアウト(秒)	データソースからのデータ読み取りのタイムアウト。	240

詳細設定 (汎用 LDAP、Active Directory、ApacheDS)
[**詳細設定**] プロパティグループには、Qlik Sense システムの詳細な LDAP コネクタプロパティが含まれています。

詳細設定プロパティ

プロパティ	説明	デフォルト値
[**LDAP 追加フィルター**]	LDAP クエリとして使用し、ディレクトリでユーザーを再取得します。	-
同期タイムアウト(秒)	データソースからのデータ読み取りのタイムアウト。	240
[**検索のページサイズ**]	データソースからデータを読み取るときに取得する投稿数を指定します。指定した数の投稿が検出されると検索が停止し、結果が返されます。検索を再開すると、停止した位置から検索が続行されます。 *ユーザーの同期に失敗した場合は、設定値を「0」(ゼロ) にし、ページ指定検索を行わないのと同じ設定にします。*	2000 (ApacheDS の場合: 1000)
[**最適化されたクエリを使用**]	このプロパティにより、Qlik Sense は、再取得されたユーザーの数に比例する多くのグループを含むディレクトリのクエリを最適化できます。 *最適化を使用できるようにするには、グループでユーザーを参照するようディレクトリを設定する必要があります。ディレクトリが正しく設定されていない場合、最適化されたクエリは、ユーザーに関連付けられたすべてのグループを検索しません。* このプロパティは、汎用 LDAP およびアクティブなディレクトリ検索でのみ表示されます (Active Directory は常に最適化を使用します)。	選択されていない

プロパティ	説明	デフォルト値
認証の種類	*オプション*。LDAP に接続するための認証タイプ。 複数の値はカンマで区切ることができます。 [値]:*Secure*、*Encryption*、*SecureSocketsLayer*、*ReadonlyServer*、*FastBind*、*Signing*、*Sealing*、*Delegation*、*ServerBind*。 *「Active Directory および汎用 LDAP UDC での LDAP チャネルバインディングと LDAP 署名」をサポートするには、次の認証タイプの値を使用します。Secure,Signing。*	資格情報の設定に基づいて、*FastBind* または *Anonymous*。

*[**詳細設定**] プロパティグループで、[**LDAP 追加フィルタ**] を使用して、ユーザーの選択のみを取得するフィルタを適用します。*

詳細設定 (高度な LDAP)

[**詳細設定**] プロパティグループには、Qlik Sense システムの詳細な LDAP コネクタプロパティが含まれています。

LDAP の詳細なプロパティ

プロパティ	説明	既定値
ページ サイズ	データソースからデータを読み取るときに取得する投稿数を指定します。指定した数の投稿が検出されると検索が停止し、結果が返されます。検索を再開すると、停止した位置から検索が続行されます。 *ユーザーの同期に失敗した場合は、設定値を「0」(ゼロ) にし、ページ指定検索を行わないのと同じ設定にします。*	2000 (ApacheDS の場合: 1000)

プロパティ	説明	既定値
[**最適化されたクエリを使用**]	このプロパティにより、Qlik Sense は、再取得されたユーザーの数に比例する多くのグループを含むディレクトリのクエリを最適化できます。 *最適化を使用できるようにするには、グループでユーザーを参照するようディレクトリを設定する必要があります。ディレクトリが正しく設定されていない場合、最適化されたクエリは、ユーザーに関連付けられたすべてのグループを検索しません。* このプロパティは、汎用 LDAP、高度な LDAP およびアクティブなディレクトリ検索でのみ表示されます (Active Directory は常に最適化を使用します)。	選択されていない
タイムアウト (秒)	データソースからのデータ読み取りのタイムアウト。	400
認証の種類	LDAP に接続するための認証タイプ。 *オプション:匿名、基本、ネゴシエート、NTLM、ダイジェスト、Sicily、DPA、MSN、外部、Kerberos*。	-

プロパティ	説明	既定値
フラグ	LDAP 接続セッション設定について言及するフラグ。複数の値をカンマ区切りで指定できます。 *Tcpkeepalive*: TCP keep-alive を有効にします。 *Autoreconnect*: Autoreconnect を有効にします。 *Rootdsecache*: 内部 RootDSE キャッシュを有効にします。 *封印*: Kerberos 暗号化を有効にします。 *セキュア ソケット レイヤーまたは SSL*: 接続でセキュア ソケット レイヤーを有効にします。 *署名*: Kerberos 暗号化を有効にします。 *コネクションレス*: 接続が UDP かどうかを指定します。 *No_fqdn*: [**ホスト**] 項目のホストが IP アドレスとして指定されている場合は、このフラグを使用します。 *noclientcert*: SSL 接続がの確立されたときにクライアント証明書の指定に使用されるデフォルトのコールバック関数をスキップします。 *NoCertVerify*: SSL 接続が確立されたときにサーバー証明書の検証をスキップします。 *NoCertVerify とCertdebug を一緒に使用しないでください。* *Certdebug*: デバッグのために、特定のサーバー証明書検証エラーがあれば取得します。 *AllProps*: LDAP オブジェクトのすべての属性を取得します。	-

プロパティ	説明	既定値
ロケーター フラグ	DC ロケーターのロケーター フラグ。複数の値をカンマ区切りで指定できます。 *なし* *ForceRediscovery* *DirectoryServiceRequired* *DirectoryServicePreferred* *GCRequired* *PdcRequired* *IPRequired* *KdcRequired* *TimeServerRequired* *WriteableRequired* *GoodTimeServerPreferred* *AvoidSelf* *OnlyLdapNeeded* *IsFlatName* *IsDnsName* *ReturnDnsName* *ReturnFlatName*	-
LDAP フィルターの検索	オプションの LDAP フィルター クエリ。	-
プロトコル バージョン	使用する LDAP プロトコルのバージョン。	3
Simple Authentication and Security Layer (SASL) メソッド	SASL バインディング方式: *gssapi* *外部* *gss-spnego* *digest-md5*	-
証明書のパス	認証のために送信するクライアント証明書のパス。	-

*[**詳細設定**] プロパティグループで、[**LDAP 追加フィルタ**] を使用して、ユーザーの選択のみを取得するフィルタを適用します。*

ディレクトリエントリ属性 (汎用 LDAP と高度な LDAP)

ディレクトリエントリ属性は、大文字と小文字を区別します。

ディレクトリエントリ属性のプロパティ

プロパティ	説明	デフォルト値
[**タイプ**]	ディレクトリエントリのタイプを特定する属性名 (ユーザーとグループのみを LDAP UDC で使用)。	objectClass
[**ユーザー ID**]	ユーザーを識別するディレクトリエントリの属性値。	inetOrgPerson
[**グループ ID**]	グループを識別するディレクトリエントリの属性値。	group
[**アカウント名**]	ユーザーがログインに使用する (UDC 内の) 一意のユーザー名。	sAMAccountName
[**電子メール**]	ディレクトリエントリの電子メールを含む属性名 (ユーザー)。	mail
[**表示名**]	ユーザーまたはグループ ディレクトリエントリのフルネーム。	名前
[**グループ メンバーシップ**]	この属性は、ディレクトリエントリがメンバーの直属のグループを示します。ユーザー同期化の間に、間接的なグループ メンバーシップは解消されます。 この設定または下記の設定である [**ディレクトリエントリのメンバー**] は、空欄のままにできます。つまり、グループ メンバーシップは、2 つの設定のうちのどちらか 1 つの設定のみを使用して解消されます。	memberOf
[**ディレクトリエントリのメンバー**]	このディレクトリエントリの直接メンバーへの参照が入っている属性の名前。 上記の [**グループ メンバーシップ**] の設定も参照してください。	member
カスタム属性 (高度な LDAP のみ)	取得する追加の LDAP オブジェクト属性。	-

ディレクトリエントリ属性 (ApacheDS)

ディレクトリエントリ属性は、大文字と小文字を区別します。

エントリのプロパティ

プロパティ	説明	デフォルト値
[**タイプ**]	ディレクトリエントリのタイプを特定する属性名 (ユーザーとグループのみを ApacheDS UDC で使用)。	objectClass

プロパティ	説明	デフォルト値
[**ユーザー ID**]	ユーザーを識別するディレクトリエントリの属性値。	inetOrgPerson
[**グループ ID**]	グループを識別するディレクトリエントリの属性値。	groupOfNames
[**アカウント名**]	ユーザーがログインに使用する (UDC 内の) 一意のユーザー名。	uid
[**電子メール**]	ディレクトリエントリの電子メールを含む属性名 (ユーザー)。	mail
[**表示名**]	ユーザーまたはグループ ディレクトリエントリのフルネーム。	cn
[**グループ メンバーシップ**]	ディレクトリエントリが直属のグループを示す属性の名前。ユーザー同期化の間に、間接的なグループ メンバーシップは解消されます。この設定または下記の設定である [**ディレクトリ エントリのメンバー**] は、空欄のままにできます。つまり、グループ メンバーシップは、2 つの設定のうちのどちらか 1 つの設定のみを使用して解消されます。	-
[**ディレクトリ エントリのメンバー**]	このディレクトリエントリの直接メンバーへの参照が入っている属性の名前。 上記の [**グループ メンバーシップ**] の設定も参照してください。	member

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

[**適用**] をクリックして変更を保存します。必須の項目が空欄の場合、[**Apply**] は無効になります。

6. 操作バーで [**適用**] をクリックして、ユーザー ディレクトリ コネクターを作成および保存します。
ページ最下部に [**追加完了**] と表示されます。

これで、ユーザー ディレクトリ コネクタを新規作成できました。ユーザー ディレクトリ コネクタの新規の*ユーザー同期 タスク*は、デフォルトで作成されます。

コネクタのプロパティの設定が、ユーザー ディレクトリとの通信を有効にしていない場合は、[**The User Directory Connector (UDC) is not operational**] と表示されます。この場所で *UserManagement_Repository* ログを確認します: *%ProgramData%\Qlik\Sense\Log\Repository\Trace*

[**ユーザー ディレクトリ名**] がすでに使用されていたり、項目が空欄の場合は、[**The User Directory Connector (UDC) is not configured**] と表示されます。

ユーザー ディレクトリ コネクタの編集

ユーザー ディレクトリ コネクタを編集できます。複数のユーザー ディレクトリ コネクターを、一度に編集することはできません。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**User directory connectors (ユーザー ディレクトリ コネクタ)**] を選択して、概要を表示します。
3. 編集したいユーザー ディレクトリ コネクタを選択して、操作 バーで [**編集**] をクリックします。
   編集ページが開きます。
4. プロパティを編集します。

   ID
   全項目が必須で、空欄のままにはできません。

   ID プロパティ

プロパティ	説明
名前	QMC で定義された UDC プロパティの名前です。
タイプ	UDC タイプです。

   ユーザー同期設定

   ユーザー同期プロパティ

プロパティ	説明	既定値
[**既存のユーザーのユーザー データの同期**]	• 選択されている場合は、既存のユーザーのみが同期されます。既存のユーザーは、Qlik Sense にログインしているユーザーや、構成済みディレクトリ サービスから同期されたことのあるユーザーです。 • 選択されていない場合は、UDC のプロパティで定義されているすべてのユーザーが構成済みのディレクトリ サービスから同期されます。選択したユーザーのみを同期する場合は、[**Active Directory**]、[**ApacheDS**]、[**汎用 LDAP**] または [**Advanced LDAP**] でフィルターを作成できます。 *ユーザー属性は、ユーザーがハブにログインするときにのみ同期されます。QMC でユーザーを削除しても、削除されたユーザーに対してアクティブなセッションは引き続き有効です。ハブの更新のみが行われた場合、ユーザーはデータベースに追加されますが、いかなる属性も持ちません。*	選択値

   *[**ユーザー同期設定**] プロパティ グループの [**既存ユーザーのユーザー データを同期**] を選択するか、選択をクリアして、同期の実行方法を決定します。*

接続 (汎用 LDAP、高度な LDAP、Active Directory、ApacheDS

接続プロパティ

プロパティ	説明	既定値
ユーザーディレクトリ名	ユーザー ディレクトリは一意でなければなりません。一意でないと、コネクタは構成されません。UDC インスタンスの名前 (Active Directory のドメイン名に喩えられる)。ユーザー アカウント名と共に、この名前はユーザーを固有のものにします。 *Active Directory には手動で入力できません。*	-
パス	ディレクトリサーバーへの接続に使用する URI。SSL をサポートするため、プロトコルを LDAPS として指定します。 *カスタム ポートには対応していません。*	ldap://company.domain.com
[**ユーザー名**]	ディレクトリサーバーへの接続に使用する、オプションのユーザー ID。空の場合、Qlik Sense リポジトリを実行するユーザーを使用して、ディレクトリサーバーにログインします。	-
[**パスワード**]	ユーザー向けのオプションのパスワード。	-

ユーザーが Active Directory コネクターを作成する場合、Qlik Sense サービスを実行しているユーザーがディレクトリサーバーへのアクセスを許可されている場合のみ、そのコネクターは動作します。Qlik Sense サービスを実行しているユーザーがディレクトリサーバーへのアクセスを許可されていない場合、ディレクトリサーバーにアクセス可能なユーザー名とパスワードを入力する必要があります。

接続 (ODBC) と(ODBC 経由)

Microsoft Access Text Driver (.txt, *.csv) を使用して .txt ファイルをロードする場合、コネクター タイプは [**ODBC**]. ではなく[**Access (ODBC 経由)**] を使用する必要があります。*

接続プロパティ

プロパティ	説明	既定値
ユーザーディレクトリ名	ユーザーディレクトリの名前。ユーザーディレクトリは一意でなければなりません。一意でないと、コネクタは構成されません。この名前にスペースを含んではいけません。	-
ユーザーテーブル名	ユーザーが一覧表示されているテーブルの名前。テーブル名にファイル拡張子を含めます。例:*Table.csv*. *Oracle ODBC ユーザーディレクトリコネクターを設定する場合、**ユーザー テーブル名** および **属性 テーブル名** の前に、それらのテーブルの所有者を付ける必要があります。例: ただの USERS でなく OWNER.USERS*。	-
属性テーブル名	ユーザー属性を含むテーブルの名前。テーブル名にファイル拡張子を含めます。例:*Table.csv*. *Oracle ODBC ユーザーディレクトリコネクターを設定する場合、**ユーザー テーブル名** および **属性 テーブル名** の前に、それらのテーブルの所有者を付ける必要があります。例: ただの USERS でなく OWNER.USERS*。	-

プロパティ	説明	既定値
表示されている接続文字列	データソースへの接続に使われる接続文字列関数の表示可能な部分。以下のいずれかを指定します。 • 完全な接続文字列。例: *Driver={SQL Server Native Client 11.0};Server=localhost;Database=Users;Trusted_Connection=yes;* 1. *Driver*は現在コンピュータにあるドライバを指定する必要があります。[**ODBC データ ソース アドミニストレータ**] で、指定するドライバーを確認してください。「データ ソース」を検索して、アプリケーションを見つけます。 2. *Server* は接続するサーバーを指定する必要があります。 3. *Database* はテーブルがあるデータベースを指定する必要があります。 4. *Trusted_Connection=yes* は設定によって必要になる場合があります。この例では、必要です。 • 確立されたシステム DNS へのポインタ。例えば、*dsn=MyDSN;* *データベースに接続する場合、2 つの接続文字列関数は単一の接続文字列関数に連結されます。*	-
暗号化された接続文字列	データソースへの接続に使われる接続文字列関数の暗号化された部分。通常、この文字列にはユーザー名とパスワードが含まれます。 次の接続文字列があると見なされます: *Driver={Microsoft Access Driver (.mdb)};Dbq=C:\mydatabase.mdb;Uid=Admin;Pwd=verySecretAdminPassword;* この接続文字列は、そのままデータベースに保存すると秘密のパスワードが表示されてしまうため注意が必要です。パスワードを保護するため以下の手順に従ってください。 最初の部分 (*Driver={Microsoft Access Driver (.mdb)};Dbq=C:\mydatabase.mdb;*) を [**表示されている接続文字列**] 項目に保存し、二番目の部分 *(Uid=Admin;Pwd=verySecretAdminPassword;)* を [**暗号化された接続文字列**] 項目に保存します。このようにすれば二番目の部分がデータベースに暗号化されて保存されるため、後に編集のため UDC で開いても表示されません。 *データベースに接続する場合、2 つの接続文字列関数は単一の接続文字列関数に連結されます。*	-

プロパティ	説明	既定値
同期タイムアウト(秒)	データソースからのデータ読み取りのタイムアウト。	240

詳細設定 (汎用 LDAP、Active Directory、ApacheDS)
[**詳細設定**] プロパティグループには、Qlik Sense システムの詳細な LDAP コネクタプロパティが含まれています。

詳細設定プロパティ

プロパティ	説明	デフォルト値
[**LDAP 追加フィルター**]	LDAP クエリとして使用し、ディレクトリでユーザーを再取得します。	-
同期タイムアウト(秒)	データソースからのデータ読み取りのタイムアウト。	240
[**検索のページサイズ**]	データソースからデータを読み取るときに取得する投稿数を指定します。指定した数の投稿が検出されると検索が停止し、結果が返されます。検索を再開すると、停止した位置から検索が続行されます。 *ユーザーの同期に失敗した場合は、設定値を「0」(ゼロ) にし、ページ指定検索を行わないのと同じ設定にします。*	2000 (ApacheDS の場合: 1000)
[**最適化されたクエリを使用**]	このプロパティにより、Qlik Sense は、再取得されたユーザーの数に比例する多くのグループを含むディレクトリのクエリを最適化できます。 *最適化を使用できるようにするには、グループでユーザーを参照するようディレクトリを設定する必要があります。ディレクトリが正しく設定されていない場合、最適化されたクエリは、ユーザーに関連付けられたすべてのグループを検索しません。* このプロパティは、汎用 LDAP およびアクティブなディレクトリ検索でのみ表示されます (Active Directory は常に最適化を使用します)。	選択されていない

プロパティ	説明	デフォルト値
認証の種類	*オプション*。LDAP に接続するための認証タイプ。 複数の値はカンマで区切ることができます。 [値]:*Secure*、*Encryption*、*SecureSocketsLayer*、*ReadonlyServer*、*FastBind*、*Signing*、*Sealing*、*Delegation*、*ServerBind*。 *「Active Directory および汎用 LDAP UDC での LDAP チャネルバインディングと LDAP 署名」をサポートするには、次の認証タイプの値を使用します。Secure,Signing。*	資格情報の設定に基づいて、*FastBind* または *Anonymous*。

*[**詳細設定**] プロパティグループで、[**LDAP 追加フィルター**] を使用して、ユーザーの選択のみを取得するフィルターを適用します (LDAP およびアクティブディレクトリに該当する場合のみ)。*

詳細設定 (高度な LDAP)
[**詳細設定**] プロパティグループには、Qlik Sense システムの詳細な LDAP コネクタプロパティが含まれています。

LDAP の詳細なプロパティ

プロパティ	説明	既定値
ページ サイズ	データソースからデータを読み取るときに取得する投稿数を指定します。指定した数の投稿が検出されると検索が停止し、結果が返されます。検索を再開すると、停止した位置から検索が続行されます。 *ユーザーの同期に失敗した場合は、設定値を「0」(ゼロ) にし、ページ指定検索を行わないのと同じ設定にします。*	2000 (ApacheDS の場合: 1000)

プロパティ	説明	既定値
[**最適化されたクエリを使用**]	このプロパティにより、Qlik Sense は、再取得されたユーザーの数に比例する多くのグループを含むディレクトリのクエリを最適化できます。 *最適化を使用できるようにするには、グループでユーザーを参照するようディレクトリを設定する必要があります。ディレクトリが正しく設定されていない場合、最適化されたクエリは、ユーザーに関連付けられたすべてのグループを検索しません。* このプロパティは、汎用 LDAP、高度な LDAP およびアクティブなディレクトリ検索でのみ表示されます (Active Directory は常に最適化を使用します)。	選択されていない
タイムアウト (秒)	データソースからのデータ読み取りのタイムアウト。	400
認証の種類	LDAP に接続するための認証タイプ。 *オプション:匿名、基本、ネゴシエート、NTLM、ダイジェスト、Sicily、DPA、MSN、外部、Kerberos*。	-

プロパティ	説明	既定値
フラグ	LDAP 接続セッション設定について言及するフラグ。複数の値をカンマ区切りで指定できます。 *Tcpkeepalive*: TCP keep-alive を有効にします。 *Autoreconnect*: Autoreconnect を有効にします。 *Rootdsecache*: 内部 RootDSE キャッシュを有効にします。 *封印*: Kerberos 暗号化を有効にします。 *セキュア ソケット レイヤーまたは SSL*: 接続でセキュア ソケット レイヤーを有効にします。 *署名*: Kerberos 暗号化を有効にします。 *コネクションレス*: 接続が UDP かどうかを指定します。 *No_fqdn*: [**ホスト**] 項目のホストが IP アドレスとして指定されている場合は、このフラグを使用します。 *noclientcert*: SSL 接続がの確立されたときにクライアント証明書の指定に使用されるデフォルトのコールバック関数をスキップします。 *NoCertVerify*: SSL 接続が確立されたときにサーバー証明書の検証をスキップします。 *NoCertVerify とCertdebug を一緒に使用しないでください。* *Certdebug*: デバッグのために、特定のサーバー証明書検証エラーがあれば取得します。 *AllProps*: LDAP オブジェクトのすべての属性を取得します。	-

プロパティ	説明	既定値
ロケーター フラグ	DC ロケーターのロケーター フラグ。複数の値をカンマ区切りで指定できます。 *なし* *ForceRediscovery* *DirectoryServiceRequired* *DirectoryServicePreferred* *GCRequired* *PdcRequired* *IPRequired* *KdcRequired* *TimeServerRequired* *WriteableRequired* *GoodTimeServerPreferred* *AvoidSelf* *OnlyLdapNeeded* *IsFlatName* *IsDnsName* *ReturnDnsName* *ReturnFlatName*	-
LDAP フィルターの検索	オプションの LDAP フィルター クエリ。	-
プロトコル バージョン	使用する LDAP プロトコルのバージョン。	3
Simple Authentication and Security Layer (SASL) メソッド	SASL バインディング方式: *gssapi* *外部* *gss-spnego* *digest-md5*	-
証明書のパス	認証のために送信するクライアント証明書のパス。	-

*[**詳細設定**] プロパティグループで、[**LDAP 追加フィルタ**] を使用して、ユーザーの選択のみを取得するフィルタを適用します。*

ディレクトリエントリ属性 (汎用 LDAP と高度な LDAP

ディレクトリエントリ属性は、大文字と小文字を区別します。

ディレクトリエントリ属性のプロパティ

プロパティ	説明	デフォルト値
[**タイプ**]	ディレクトリエントリのタイプを特定する属性名 (ユーザーとグループのみを LDAP UDC で使用)。	objectClass
[**ユーザー ID**]	ユーザーを識別するディレクトリエントリの属性値。	inetOrgPerson
[**グループ ID**]	グループを識別するディレクトリエントリの属性値。	group
[**アカウント名**]	ユーザーがログインに使用する (UDC 内の) 一意のユーザー名。	sAMAccountName
[**電子メール**]	ディレクトリエントリの電子メールを含む属性名 (ユーザー)。	mail
[**表示名**]	ユーザーまたはグループ ディレクトリエントリのフルネーム。	名前
[**グループ メンバーシップ**]	この属性は、ディレクトリエントリがメンバーの直属のグループを示します。ユーザー同期化の間に、間接的なグループ メンバーシップは解消されます。 この設定または下記の設定である [**ディレクトリエントリのメンバー**] は、空欄のままにできます。つまり、グループ メンバーシップは、2 つの設定のうちのどちらか 1 つの設定のみを使用して解消されます。	memberOf
[**ディレクトリエントリのメンバー**]	このディレクトリエントリの直接メンバーへの参照が入っている属性の名前。 上記の [**グループ メンバーシップ**] の設定も参照してください。	member
カスタム属性 (高度な LDAP のみ)	取得する追加の LDAP オブジェクト属性。	-

ディレクトリエントリ属性 (ApacheDS)

ディレクトリエントリ属性は、大文字と小文字を区別します。

エントリのプロパティ

プロパティ	説明	デフォルト値
[**タイプ**]	ディレクトリエントリのタイプを特定する属性名 (ユーザーとグループのみを ApacheDS UDC で使用)。	objectClass

プロパティ	説明	デフォルト値
[**ユーザー ID**]	ユーザーを識別するディレクトリエントリの属性値。	inetOrgPerson
[**グループ ID**]	グループを識別するディレクトリエントリの属性値。	groupOfNames
[**アカウント名**]	ユーザーがログインに使用する (UDC 内の) 一意のユーザー名。	uid
[**電子メール**]	ディレクトリエントリの電子メールを含む属性名 (ユーザー)。	mail
[**表示名**]	ユーザーまたはグループ ディレクトリエントリのフルネーム。	cn
[**グループ メンバーシップ**]	ディレクトリエントリが直属のグループを示す属性の名前。ユーザー同期化の間に、間接的なグループ メンバーシップは解消されます。この設定または下記の設定である [**ディレクトリ エントリのメンバー**] は、空欄のままにできます。つまり、グループ メンバーシップは、2 つの設定のうちのどちらか 1 つの設定のみを使用して解消されます。	-
[**ディレクトリ エントリのメンバー**]	このディレクトリエントリの直接メンバーへの参照が入っている属性の名前。 上記の [**グループ メンバーシップ**] の設定も参照してください。	member

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

[**適用**] をクリックして変更を保存します。必須の項目が空欄の場合、[**Apply**] は無効になります。

5. 操作バーで [**適用**] をクリックして、ユーザー ディレクトリ コネクターを作成および保存します。
ページ最下部に [**追加完了**] と表示されます。

これでユーザー ディレクトリ コネクターの編集は完了です。

コネクタのプロパティの設定が、ユーザー ディレクトリとの通信を有効にしていない場合は、[**The User Directory Connector (UDC) is not operational**] と表示されます。この場所で *UserManagement_Repository* ログを確認します: *%ProgramData%\Qlik\Sense\Log\Repository\Trace*

[**ユーザー ディレクトリ名**] がすでに使用されていたり、項目が空欄の場合は、[**The User Directory Connector (UDC) is not configured**] と表示されます。

ユーザー ディレクトリタイプの更新

利用できるユーザー ディレクトリのタイプを変更できます。この場合、ユーザー ディレクトリコネクタを新規作成する前に、ソース ファイルを更新する必要があります。

ユーザー ディレクトリコネクタの基になっているソース ファイルを削除すると、機能しません。

次の手順を実行します。

1. 次にソース ファイルが存在する、ユーザー ディレクトリのタイプを追加または削除します: *%ProgramFiles%\Qlik\Sense\Repository\UserDirectoryConnectors*.
2. QMC を開く: *https://<QPS サーバー名>/qmc*
3. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**User directory connectors (ユーザー ディレクトリ コネクタ)**] を選択して、概要を表示します。
4. ページ最下部にあるアクション バーで [**ユーザー ディレクトリ タイプの更新**] をクリックします。
   ページの最下部に [**ソースからユーザー ディレクトリの更新完了**] と表示されます。

これで、このユーザー ディレクトリタイプをユーザー ディレクトリコネクタで利用できるようになりました。

ユーザー ディレクトリ コネクターとユーザーの削除

削除権限を有するユーザー ディレクトリコネクタを削除できます。

削除オプションは 2 つあります。

- ユーザー ディレクトリコネクタのみを削除
- ユーザー ディレクトリコネクタと、ユーザー ディレクトリからインポートされたユーザーすべてを削除

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**User directory connectors (ユーザー ディレクトリ コネクタ)**] を選択して、概要を表示します。

   2 つ以上のユーザー ディレクトリコネクタを、一度に削除することはできません。
3. 削除するユーザー ディレクトリコネクタを選択します。
4. アクション バーの [**Delete**] をクリックします。
   [**Delete**] ダイアログが表示されます。
5. [**Delete all users imported from this user directory**] を任意で選択します。

   ユーザーの削除は元に戻せません。

   ユーザーを削除すると、所有リソースの所有権がサービス アカウント (sa_repository ユーザー) に移ります。
6. [**OK**] をクリックします。

ユーザー ディレクトリの同期

ユーザー ディレクトリからユーザー データを同期できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**User directory connectors (ユーザー ディレクトリ コネクタ)**] を選択して、概要を表示します。
3. ユーザー ディレクトリ コネクタが [**設定**] されていて、[**稼働**] していることを確認します。

   > *ユーザー ディレクトリ コネクタが [**設定**] されていないか、[**稼働**] していない場合は、同期を実行できません。[**ユーザー ディレクトリ**] の値は一意でなければなりません。一意でなければ、コネクタは設定できません。この場所で UserManagement_Repository ログを確認します: %ProgramData%\Qlik\Sense\Log\Repository\Trace*

4. 同期を開始する前に、同期するのはすべてのユーザーか、あるいは既存のユーザーのみか確認します。ユーザー ディレクトリ コネクタを選択し、[**編集**] をクリックして [**ユーザー同期設定**] の下の [**既存ユーザーのユーザー データを同期**] 設定を確認します。
   - 選択されている場合は、既存のユーザーのみが同期されます。既存のユーザーは、Qlik Sense にログインしているユーザーや、構成済みディレクトリ サービスから同期されたことのあるユーザーです。
   - 選択されていない場合は、UDC のプロパティで定義されているすべてのユーザーが構成済みのディレクトリ サービスから同期されます。選択したユーザーのみを同期する場合は、[**Active Directory**]、[**ApacheDS**]、[**汎用 LDAP**] または [**Advanced LDAP**] でフィルターを作成できます。

   > *ユーザー属性は、ユーザーがハブにログインするときにのみ同期されます。QMC でユーザーを削除しても、削除されたユーザーに対してアクティブなセッションは引き続き有効です。ハブの更新のみが行われた場合、ユーザーはデータベースに追加されますが、いかなる属性も持ちません。*

5. 左上の [**ユーザー ディレクトリ コネクタ**] をクリックして概要に戻ります。
6. 同期したいユーザー ディレクトリを選択します。
7. 操作バーの にある [**同期**] をクリックします。[**選択したユーザー ディレクトリをすべて同期**] というメッセージがページの最下部に表示されます。同期中に [**状態**] の列が表示されます。
   a. [**外部フェッチ**]
   b. [**データベース保管**]
   c. [**アイドル**]
8. [**アイドル**] が表示されたら、[**最後に完了した同期**] の日時が更新されていることを確認します。

   > *状態が [**アイドル**] と表示され、[**最後に開始された同期**] が [**最後に完了した同期**] よりも後になっている場合は、同期に失敗したということです。*

選択したユーザー ディレクトリからユーザー データを同期できました。スタート ページから[**ユーザー**] を選択して、更新されたユーザーの表を表示します。

Professional アクセスの管理

指定されたユーザーにプロフェッショナル アクセスを割り当て、そのユーザーが、Qlik Sense サイト内の ストリーム、アプリ、その他のリソースに無制限にアクセスできるようにします。

他の場所で使用するためにライセンスを解放する場合は、プロフェッショナル アクセスを割り当て解除できます。アクセス タイプが過去 7 日以内に使用されていた場合、そのアクセス タイプは隔離されます。直近 7 日間で使用されていない場合、プロフェッショナル アクセス権が削除され、直ちにライセンスが解放されます。

7 日以内であれば、同一のユーザーに検疫状態のプロフェッショナル アクセス権を復元することができます。

> *検疫は、署名済みライセンス キーでライセンス付与されている Qlik Sense のインストールでは強制されません。*

Professional アクセスの割り当て

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、または [**スタート**▼] ドロップダウン メニューから[**ライセンスの管理**] を選択して、概要を表示します。
3. パネル右側の [**プロフェッショナル アクセスの割り当て**] を選択します。
4. データ マネージャーでテーブルの ⊕[**割り当て**] をクリックします。
   [**ユーザー**] ダイアログが開きます。
5. リストからユーザーを選択し、[**割り当て**] をクリックします。

   > *割り当て可能なライセンス数が選択したユーザー数を下回る場合は、[**割り当て**] が無効になります。*

   ダイアログが閉じ、ユーザーは [**プロフェッショナル アクセスの割り当て**] の概要表に追加されます。

プロフェッショナル アクセスの割り当て解除

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、または [**スタート**▼] ドロップダウン メニューから[**ライセンスの管理**] を選択して、概要を表示します。
3. パネル右側の [**プロフェッショナル アクセスの割り当て**] を選択します。
4. 割り当てを解除するユーザーを選択し、操作 バーで [**割当て解除**] をクリックします。
   確認のダイアログが表示されます。.
5. [**OK**] をクリックします。
   - [**ステータス**] は、ユーザーが過去 7 日以内にログインしている場合には、[**検疫済み**] に変更されます。

- 過去 7 日以内にユーザーがログインしていなければ、ユーザーは 概要から削除されて、ライセンスが解放されます。

プロフェッショナル アクセスの回復

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、または [**スタート▼**] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
3. パネル右側の [**プロフェッショナル アクセスの割り当て**] を選択します。
4. ステータスが [**検疫済み**] のユーザーを選択し、操作バーで [**回復**] をクリックします。
これでステータスは [**割り当て済み**] に変更されます。

プロフェッショナル アクセス ルールの作成

プロフェッショナル アクセス ルールは、ストリームとアプリへのプロフェッショナル アクセス権をどのユーザーに付与するのかを定義します。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、または [**スタート▼**] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
3. パネル右側の [**プロフェッショナル アクセス ルール**] を選択します。
4. データ マネージャーでテーブルの **新規作成** をクリックします。
5. プロパティを編集します。

ID

ID プロパティ

プロパティ名	説明
無効化	ルールを無効にする場合に選択します。既定では、ルールが有効になっています。
名前	ルール名。
説明	ルールの説明。

基本

基本プロパティ

プロパティ名	説明
リソース フィルター	ルールを評価するリソース タイプの定義。
アクション	ルールによって許可されるアクション。

詳細設定

詳細設定プロパティ

プロパティ名	説明
条件	ルールを適用する上で一致しなければならないリソース条件、ユーザー条件、複合条件 。
ルールの検証	クリックすると、ルールの構文が検証されます。

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

6. [**適用**] をクリックして、ユーザー アクセス ルールを作成し、保存します。

ページ最下部に [**追加完了**] と表示されます。

プロフェッショナル アクセス ルールの編集

プロフェッショナル アクセス ルールは、ストリームとアプリへのプロフェッショナル アクセス権をどのユーザーに付与するのかを定義します。既存のルールを編集できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、または [**スタート▼**] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
3. パネル右側の [**プロフェッショナル アクセス ルール**] を選択します。
4. 編集したいルールを選択します。
5. アクション バーで [**編集**] をクリックします。
6. プロパティを編集します。

ID

ID プロパティ

プロパティ名	説明
無効化	ルールを無効にする場合に選択します。既定では、ルールが有効になっています。
名前	ルール名。
説明	ルールの説明。

基本

基本プロパティ

プロパティ名	説明
リソース フィルター	ルールを評価するリソース タイプの定義。
アクション	ルールによって許可されるアクション。

演算子の説明と例

演算子	説明と例
=	この演算子では大文字と小文字は区別されません。比較対象の数式と完全に等しい場合は True を返します。 `user.name = "a*"` 名前が「a*」と完全に一致するユーザーがルールの対象になります。
like	この演算子では大文字と小文字は区別されません。比較対象の数式と等しい場合は True を返します。 `user.name like "a*"` 名前が「a」で始まるすべてのユーザーがルールによって対象になります。.
!=	この演算子では大文字と小文字は区別されません。比較対象の数式の値が等しくない場合に True を返します。 `user.name != resource.name` ユーザーと同じ名前ではないすべてのリソースがルールによって対象になります。

複数の条件を使用すると、[**Group**] をクリックして 2 つの条件をグループ化できます。条件のグループ化後、[**Ungroup**] をクリックして、グループ化を解除できます。この他に、サブグループ化オプションには [**Split**] および [**Join**] があります。条件間の既定の演算子は、OR です。これは、演算子のドロップダウンリストで変更できます。AND が OR より上位になるように、条件をグループ化します。

詳細設定

詳細設定プロパティ

プロパティ名	プロパティ
条件	ルールを適用する上で一致しなければならないリソース条件、ユーザー条件、複合条件 。

ルールの検証	クリックすると、ルールの構文が検証されます。ルールを適用する上で一致しなければならないリソース条件、ユーザー条件、複合条件 。

タグ

タグ プロパティ

プロパティ	説明
[タグ]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

ユーザー

ユーザーのプロパティ

プロパティ名	説明
名前	ユーザーの氏名。
許可されている操作	ユーザーが実行を許可されているアクション。

7. [**適用**] をクリックし、更新内容を保存します。

ページ最下部に [**追加完了**] と表示されます。

アナライザー アクセスの管理

指定されたユーザーにアナライザー アクセスを割り当て、そのユーザーが、Qlik Sense サイト内のストリーム、アプリ、その他のリソースにアクセスできるようにします。

他の場所で使用するためにライセンスを解放する場合は、アナライザー アクセスを割り当て解除できます。アクセス タイプが過去 7 日以内に使用されていた場合、そのアクセス タイプは隔離されます。過去 7 日以内に使用されていない場合には、アナライザー アクセス権が削除され、ライセンスは直ちに解放されます。

7 日以内であれば、同一のユーザーに検疫状態のアナライザー アクセス権を復元することができます。

検疫は、署名済みライセンス キーでライセンス付与されている Qlik Sense のインストールでは強制されません。

アナライザー アクセスの割り当て

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、または [**スタート▼**] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
3. パネル右側の [**アナライザー アクセスの割り当て**] を選択します。

4. 操作バーで[**割り当て**] をクリックします。
   [**ユーザー**] ダイアログが開きます。
5. リストからユーザーを選択し、[**割り当て**] をクリックします。

   > *指定されたユーザー数に対し、割り当て可能なライセンス数が不十分な場合には、[**割り当て**] が無効になります。*

   ダイアログが閉じ、ユーザーは [**アナライザー アクセスの割り当て**] の概要表に追加されます。

アナライザー アクセスの割り当て解除

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、または [**スタート**▼] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
3. パネル右側の [**アナライザー アクセスの割り当て**] を選択します。
4. 割り当てを解除するユーザーを選択し、操作バーで [**割当て解除**] をクリックします。
   確認のダイアログが表示されます。.
5. [**OK**] をクリックします。
   - [**ステータス**] は、ユーザーが過去 7 日以内にログインしている場合には、[**検疫済み**] に変更されます。
   - 過去 7 日以内にユーザーがログインしていなければ、ユーザーは 概要から削除されて、ライセンスが解放されます。

アナライザー アクセスの回復

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、または [**スタート**▼] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
3. パネル右側の [**アナライザー アクセスの割り当て**] を選択します。
4. ステータスが [**検疫済み**] のユーザーを選択し、操作バーで [**回復**] をクリックします。
   これでステータスは [**割り当て済み**] に変更されます。

アナライザー アクセス ルールの作成

アナライザー アクセス ルールは、ストリームとアプリへのアナライザー アクセス権をどのユーザーに付与するのかを定義します。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、または [**スタート**▼] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
3. パネル右側の [**Analyzer access rules**] (アナライザー アクセス ルール) を選択します。

4. データ マネージャーでテーブルの **新規作成** をクリックします。
5. プロパティを編集します。

ID

ID プロパティ

プロパティ名	説明
無効化	ルールを無効にする場合に選択します。既定では、ルールが有効になっています。
名前	ルール名。
説明	ルールの説明。

基本

基本プロパティ

プロパティ名	説明
リソース フィルター	ルールを評価するリソース タイプの定義。
アクション	ルールによって許可されるアクション。

詳細設定

詳細設定プロパティ

プロパティ	説明
条件	ルールを適用する上で一致しなければならないリソース条件、ユーザー条件、複合条件 。
ルールの検証	クリックすると、ルールの構文が検証されます。

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

6. [**適用**] をクリックして、ユーザー アクセス ルールを作成し、保存します。
ページ最下部に [**追加完了**] と表示されます。

アナライザー アクセス ルールの編集

アナライザー アクセス ルールは、ストリームとアプリへのアナライザー アクセス権をどのユーザーに付与するのかを定義します。既存のルールを編集できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、または [**スタート▼**] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
3. パネル右側の [**Analyzer access rules**] (アナライザー アクセス ルール) を選択します。
4. 編集したいルールを選択します。
5. アクション バーで [**編集**] をクリックします。
6. プロパティを編集します。

ID

ID プロパティ

プロパティ名	説明
無効化	ルールを無効にする場合に選択します。既定では、ルールが有効になっています。
名前	ルール名。
説明	ルールの説明。

基本

基本プロパティ

プロパティ名	説明
リソース フィルター	ルールを評価するリソース タイプの定義。
アクション	ルールによって許可されるアクション。

演算子の説明

演算子	説明と例
=	この演算子では大文字と小文字は区別されません。比較対象の数式と完全に等しい場合は True を返します。 `user.name = "a*"` 名前が「a*」と完全に一致するユーザーがルールの対象になります。
like	この演算子では大文字と小文字は区別されません。比較対象の数式と等しい場合は True を返します。 `user.name like "a*"` 名前が「a」で始まるすべてのユーザーがルールによって対象になります。.

!=	この演算子では大文字と小文字は区別されません。比較対象の数式の値が等しくない場合に True を返します。 `user.name != resource.name` ユーザーと同じ名前ではないすべてのリソースがルールによって対象になります。

複数の条件を使用すると、[**Group**] をクリックして 2 つの条件をグループ化できます。条件のグループ化後、[**Ungroup**] をクリックして、グループ化を解除できます。この他に、サブグループ化オプションには [**Split**] および [**Join**] があります。条件間の既定の演算子は、OR です。これは、演算子のドロップダウンリストで変更できます。AND が OR より上位になるように、条件をグループ化します。

詳細設定

詳細設定プロパティ

プロパティ名	**プロパティ**
条件	ルールを適用する上で一致しなければならないリソース条件、ユーザー条件、複合条件 。
ルールの検証	クリックすると、ルールの構文が検証されます。ルールを適用する上で一致しなければならないリソース条件、ユーザー条件、複合条件 。

タグ

タグ プロパティ

プロパティ	**説明**
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキストボックスの下に表示されます。

ユーザー

ユーザーのプロパティ

プロパティ名	**説明**
名前	ユーザーの氏名。
許可されている操作	ユーザーが実行を許可されているアクション。

7. [**適用**] をクリックし、更新内容を保存します。

ページ最下部に [**追加完了**] と表示されます。

Analyzer Capacity ルールの作成と編集

Analyzer Capacity ルールは、ストリームとアプリへの Analyzer Capacity アクセス権をどのユーザーに付与するのかを定義します。

次の手順を実行します。

1. QMC スタートページから、または [**スタート▼**] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
2. パネル右側の [**Analyzer Capacity ルール**] を選択します。
3. 以下のいずれかを行います。
   - データ マネージャーでテーブルの **新規作成** をクリックします。
   - ルールを選択し、[**編集**] をクリックします。
4. プロパティを編集します。

ID

既定では、ルールが有効になっています。

基本

基本プロパティ

プロパティ名	説明
リソース フィルター	ルールを評価するリソース タイプの定義。
アクション	ルールによって許可されるアクション。

詳細設定

詳細設定プロパティ

項目	値
条件	ルールを適用する上で一致しなければならないリソース条件、ユーザー条件、複合条件 。
ルールの検証	クリックすると、ルールの構文が検証されます。

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

5. [**適用**] をクリックして、Analyzer Capacity ルールを保存します。

ユーザー アクセスの管理

指定されたユーザーにユーザー アクセスを割り当て、そのユーザーが、サイト内のストリーム、アプリ、その他のリソースに無制限にアクセスできるようにします。Qlik Sense

他の場所で使用するためにトークンをリリースする場合は、ユーザー アクセスを割り当て解除できます。アクセス タイプが過去 7 日以内に使用されていた場合、そのアクセス タイプは隔離されます。直近 7 日間で使用されていないユーザー アクセス権は削除され、トークンは直ちに解放されます。

7 日以内であれば、同一のユーザーに検疫状態のユーザー アクセス権を回復させることができます。その場合、ユーザーには、追加のトークンを使用せずに、再びアクセス権が付与されます。

ユーザー アクセスの割り当て

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、または [**スタート**▼] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
3. パネル右側の [**ユーザー アクセス権の割り当て**] を選択します。
4. データ マネージャーでテーブルの **Allocate** in the action bar.
   [**ユーザー**] ダイアログが開きます。
5. リストからユーザーを選択し、[**割り当て**] をクリックします。

   > *選択したユーザー数に対して、割り当てることができるトークン数が十分でない場合は、[**割り当て**] が無効になります。*

   ダイアログが閉じ、ユーザーは [**ユーザー アクセスの割り当て**] の概要表に追加されます。

ユーザー アクセスの割り当て解除

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、または [**スタート**▼] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
3. パネル右側の [**ユーザー アクセス権の割り当て**] を選択します。
4. 割り当てを解除するユーザーを選択し、操作バーで [**割当て解除**] をクリックします。
   確認のダイアログが表示されます。.
5. [**OK**] をクリックします。
   - [**ステータス**] は、ユーザーが過去 7 日以内にログインしている場合には、[**検疫済み**] に変更されます。
   - 過去 7 日以内にユーザーがログインしていなければ、ユーザーは概要から削除されて、トークンが解放されます。

   また、[**トークン**] ページで情報が更新されます。

ユーザー アクセスの回復

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、または [**スタート**▼] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
3. パネル右側の [**ユーザー アクセス権の割り当て**] を選択します。
4. ステータスが [**検疫済み**] のユーザーを選択し、操作バーで [**回復**] をクリックします。
これでステータスは [**割り当て済み**] に変更されます。また、[**トークン**] ページで情報が更新されます。

アナライザー アクセス ルールの作成

アナライザー アクセス ルールは、ストリームとアプリへのアナライザー アクセス権をどのユーザーに付与するのかを定義します。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、または [**スタート**▼] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
3. パネル右側の [**Analyzer access rules**] (アナライザー アクセス ルール) を選択します。
4. データ マネージャーでテーブルの ⊕**新規作成** をクリックします。
5. プロパティを編集します。

ID

ID プロパティ

プロパティ名	説明
無効化	ルールを無効にする場合に選択します。既定では、ルールが有効になっています。
名前	ルール名。
説明	ルールの説明。

基本

基本プロパティ

プロパティ名	説明
リソース フィルター	ルールを評価するリソース タイプの定義。
アクション	ルールによって許可されるアクション。

詳細設定

詳細設定プロパティ

プロパティ	説明
条件	ルールを適用する上で一致しなければならないリソース条件、ユーザー条件、複合条件 。
ルールの検証	クリックすると、ルールの構文が検証されます。

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

6. [**適用**] をクリックして、ユーザー アクセス ルールを作成し、保存します。
   ページ最下部に [**追加完了**] と表示されます。

ユーザー アクセス ルールの作成

ユーザー アクセス ルールでは、利用可能なトークンへのアクセス権を持つユーザーを定義できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、または [**スタート▼**] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
3. パネル右側の [**ユーザー アクセス ルール**] を選択します。
4. データ マネージャーでテーブルの **新規作成** をクリックします。
5. プロパティを編集します。

ID

ID プロパティ

プロパティ名	説明
無効化	ルールを無効にする場合に選択します。既定では、ルールが有効になっています。
名前	ルール名。
説明	ルールの説明。

基本

ID プロパティ

プロパティ名	説明
リソース フィルター	ルールを評価するリソース タイプの定義。
アクション	ルールによって許可されるアクション。

詳細設定

詳細設定プロパティ

プロパティ名	説明
条件	ルールを適用する上で一致しなければならないリソース条件、ユーザー条件、複合条件 。
ルールの検証	クリックすると、ルールの構文が検証されます。

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

6. [**適用**] をクリックして、ユーザー アクセス ルールを作成し、保存します。
ページ最下部に [**追加完了**] と表示されます。

ユーザー アクセス ルールが削除され、削除時に、削除されたルールでトークンを割り当てられていたユーザーがいる場合、それらのトークンの割り当てが自動で解除されることはありません。トークンの割り当ては手動で解除する必要があります。

ルールに記載されているユーザーは、アクセス トークンがある限り、アプリケーションへのアクセスが付与されています。

ユーザー アクセス ルールの編集

ユーザー アクセス ルールでは、利用可能なトークンへのアクセス権を持つユーザーを定義できます。既存のルールを編集できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、または [**スタート▼**] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。

3. パネル右側の [**ユーザー アクセス ルール**] を選択します。
4. 編集したいルールを選択します。
5. アクション バーで [**編集**] をクリックします。
6. プロパティを編集します。

ID

ID プロパティ

プロパティ名	**説明**
無効化	ルールを無効にする場合に選択します。既定では、ルールが有効になっています。
名前	ルール名。
説明	ルールの説明。

基本

基本プロパティ

プロパティ名	**説明**
リソース フィルター	ルールを評価するリソース タイプの定義。
アクション	ルールによって許可されるアクション。

演算子の説明

演算子	**説明と例**
=	この演算子では大文字と小文字は区別されません。比較対象の数式と完全に等しい場合は True を返します。 `user.name = ”a*”` 名前が「a*」と完全に一致するユーザーがルールの対象になります。
like	この演算子では大文字と小文字は区別されません。比較対象の数式と等しい場合は True を返します。 `user.name like ”a*”` 名前が「a」で始まるすべてのユーザーがルールによって対象になります。.

!=	この演算子では大文字と小文字は区別されません。比較対象の数式の値が等しくない場合に True を返します。 `user.name != resource.name` ユーザーと同じ名前ではないすべてのリソースがルールによって対象になります。
複数の条件を使用すると、[**Group**] をクリックして 2 つの条件をグループ化できます。条件のグループ化後、[**Ungroup**] をクリックして、グループ化を解除できます。この他に、サブグループ化オプションには [**Split**] および [**Join**] があります。条件間の既定の演算子は、OR です。これは、演算子のドロップダウン リストで変更できます。AND が OR より上位になるように、条件をグループ化します。	

詳細設定

詳細設定プロパティ

プロパティ名	プロパティ
条件	ルールを適用する上で一致しなければならないリソース条件、ユーザー条件、複合条件 。
ルールの検証	クリックすると、ルールの構文が検証されます。ルールを適用する上で一致しなければならないリソース条件、ユーザー条件、複合条件 。

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

ユーザー

ユーザーのプロパティ

プロパティ名	説明
名前	ユーザーの氏名。
許可されている操作	ユーザーが実行を許可されているアクション。

7. [**適用**] をクリックし、更新内容を保存します。
ページ最下部に [**追加完了**] と表示されます。

ユーザー アクセス ルールでトークンを割り当てられていたユーザーが存在する状態でそのルールが削除された場合、それらのトークンの割り当ては自動的には解除されません。トークンの割り当ては手動で解除する必要があります。

ルールに記載されているユーザーは、アクセス トークンがある限り、アプリケーションへのアクセスが付与されています。

ユーザー アクセス ルールの削除

削除権限を有するユーザー アクセス ルールは、削除できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. Select **License management** on the QMC start page or from the **Start** ドロップダウン メニューからリソースを選択します。
3. パネル右側の [**ユーザー アクセス ルール**] を選択します。
4. 削除するルールを選択します。
5. アクション バーの [**Delete**] をクリックします。
   [**Delete**] ダイアログが表示されます。
6. [**OK**] をクリックします。

ログイン アクセス ルールの作成

ログイン アクセス パスでは、指定されたユーザーあるいは匿名ユーザーが、28 日間につき最大 60 分間続けてハブにアクセスできます。ユーザーが 60 分の制限を超えても、ユーザー接続はタイムアウトしません。その代わり、別のログイン アクセス パスが使用されます。利用できるログイン アクセス パスがこれ以上ない場合、セッションは終了します。

新規ログイン アクセス ルールを作成すると、次が設定されます。

- 多くのログイン アクセス パス向けに割り当てたいトークン数
- どのユーザーがログイン アクセス ルールを使用できるかを指定したライセンス ルール。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、または [**スタート**] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
3. パネル右側の [**ログイン アクセス ルール**] を選択します。
4. データ マネージャーでテーブルの **新規作成** をクリックします。
5. プロパティを編集します。

ID

[**名前**] はログイン アクセス グループの名前です。

トークン

[**割り当てられたトークン**] は、ログイン アクセス グループが使用できるトークンの数を表します。

6. [**適用**] をクリックして変更を保存します。必須の項目が空欄の場合、[**Apply**] は無効になります。

> *[ライセンス ルールの作成] ダイアログが開きます。詳細については、「ライセンス ルールの作成 (page 331)」を参照してください。*

利用できるトークンの数が十分でなければ、エラー ダイアログが表示されます。[**トークン数**] を減らして [**適用**] を再度クリックしてください。

ログイン アクセス ルールの編集

更新権限のあるログイン アクセス ルールを編集して、次を変更することができます。

- ログイン アクセス パス用に割り当て済みトークン数
- どのユーザーがログイン アクセス ルールを使用できるかを指定したライセンス ルール。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、または [**スタート▼**] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
3. パネル右側の [**ログイン アクセス ルール**] を選択します。
4. 編集するログイン アクセス ルールを選択し、操作バーで [**編集**] をクリックします。
5. プロパティを編集します。

   ID

   [**名前**] はログイン アクセス グループの名前です。
   ログイン アクセスの名前を変更できます。

   トークン

   [**割り当てられたトークン**] は、ログイン アクセス グループが使用できるトークンの数を表します。
   割り当てたいトークンの数を変更できます。項目の下のメッセージには、[**適用**] のクリック後にトークン数によって決まるログイン アクセス パスの数が表示されます。
   [**適用**] をクリックして変更を保存します。必須の項目が空欄の場合、[**Apply**] は無効になります。
6. 以下の項目は [**関連するアイテム**] でも編集できます。
   ユーザー アクセス
   [**ユーザー アクセス**] は、リソースを編集する際に [**関連するアイテム**] から利用できます。
   プレビューには、ターゲット リソースと選択したアイテムにアクセスできるソース ユーザーが表示されます。
   権限に応じて、ユーザーやリソース、関連するルールを編集したり、表示することができます。
   ライセンス ルール
   ライセンス ルールの編集 (page 333)
7. [**適用**] をクリックします。
8. 利用できるトークンの数が十分でなければ、エラー ダイアログが表示されます。[**トークン数**] を減らして [**適用**] を再度クリックしてください。

ログイン アクセス ルールの削除

トークンを解放するために、削除権限のあるログイン アクセス ルールを削除できます。実行すると、ログイン アクセス グループに所属するユーザーの、ストリームやアプリへのアクセス権が削除されます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. Select **License management** on the QMC start page or from the **Start** ドロップダウン メニューからリソースを選択します。
3. 右側のパネルで [**ログイン アクセス ルール**] を選択して概要を表示します。
4. 削除するログイン アクセス ルールを選択します。
5. アクション バーの [**Delete**] をクリックします。[**Delete**] ダイアログが表示されます。
6. [**OK**] をクリックします。
    - ログイン アクセスに十分な数の未使用ログイン アクセス パスが含まれている場合はトークンがすみやかにリリースされます。
    - 使用されているログイン アクセス パスは最後の使用から28 日が経過するまでリリースされません。

    3 つのトークンを割り当て、30 のログイン アクセス パスを提供しました。また、11 のログイン アクセス パスが使用されました。ログイン アクセスを削除すると、1 つのトークンがすぐにリリースされ、2 つのトークンは最後の使用から28 日が経過するまでリリースされません。つまり、2 番目のトークンは 10 番目のログイン アクセス パスの最後の使用から28 日後にリリースされ、3 番目のトークンは 11 番目のログイン アクセス パスの最後の使用から28 日後にリリースされます。
    また、[**トークン**] ページで情報が更新されます。

ログイン アクセス: トークン使用数の例

トークンベースの Qlik Sense ライセンスによって、トークンを購入し、トークンの割り当てや再割り当てを行って、時間の経過とともに変化する使用ニーズに適合させることができます。トークンは、システムへの頻繁なアクセスが必要な、特定の個人に対して、またはシステムの使用頻度が頻繁ではないユーザー グループに対して割り当てます。

トークンの割り当て

トークンの割り当てには、ユーザー アクセスとログイン アクセスの 2 種類があります。

トークンの割り当ての説明

トークンの割り当て	アクセス パスの説明

1 トークン= 1 ユーザー アクセス パス 	組織のセキュリティポリシーとルールによる認証に基づくの使用制限がない、一意の、識別された特定のユーザーに対して割り当てられます。Qlik Sense
1 トークン= 10 ログイン アクセス パス 	アクセスが頻繁ではない場合、または匿名アクセスに使用します。ログイン アクセス パスは、へのフル アクセスが提供されますが、時間に制限があります。Qlik Sense

ログイン アクセス パス

ユーザー アクセス パスは、その言葉が表すように、専用のユーザーに対してトークンを使用します。ログイン アクセス パスは異なるユーザーどうしで共有することができます。そのため、より多くのシナリオが考えられ、説明が必要な場合があります。次の例は、ログインアクセス パスの使用および新規使用のためプールへの返却がどのように行われるかを示しています。

ログイン アクセス パスの説明

# 日目	ログイン アクセス パスの使用	説明
0 日目		1 個のトークンを 1 つのグループに割り当てると仮定します。グループは、10 のログイン アクセス パスが利用可能となります。
1 日目		そのグループに割り当てられたユーザーが Qlik Sense にログインします。直ちに 1 個のログイン アクセス パスが使用されます。

1 日目		ユーザーのアクティブな状態が 60 分間続き、2 個目のログイン アクセス パスが使用されました。この 1 時間単位のプロセスはセッションの終了まで続きます。セッションは次の 3 つのいずれかで終了します。 • ユーザーがログアウトする。 • ユーザーが (タブではなく) ブラウザーを閉じる。 • QMC で、ユーザーの非アクティブ状態がタイムアウト時間以上続いている。(仮想プロキシ設定 [**タイムアウトまでのセッション アイドル時間 (分)**]、既定値は 30分間。)
15 日目		2 週間後、同じユーザーが再びログイン。今回は、1 時間に満たない時間 を使用し、プレゼンテーション スクリーンに接続されたタブレットとラップトップの両方を使用してプレゼンテーションを実施しました。Qlik Sense このユーザーは指定されたユーザー、つまり匿名ではないため、今回のログインでは 1 個のログイン アクセス パスのみを使用しています。実際、指定されたユーザーは、追加のログイン アクセス パスを使用しなくてもセッション時に最大 5 台のデバイスで にアクセスできます。Qlik Sense これは、その性質上匿名ユーザーの場合には当てはまらず、セッションをリンクさせることはできません。

25 日目		さらに 1 週間後、同じユーザーがログインし、4 個目のパスを使用します。ただし、同じユーザーは今回、ログインしてから 30 分経過後ログアウトし、数分後再びログインして、何らかの情報を確認してすぐにログアウトしています。サーバーへの接続は同じ 1 時間以内に発生しているため、1 個のログイン アクセス パスのみが使用されています。

この例では、このユーザーにとってユーザー アクセスではなく、ログイン アクセスが適していることは明らかです。約 1 か月が経過し、4 個のログイン アクセス パスのみが使用されました。そのため、このプロファイルの 2 人のユーザーを、トークン 1 個というコストでサポートできます。

セッション プールへのログイン アクセス パスの返却

このセクションでは、ログイン アクセス パスをプールに返却する方法を説明します。各ログイン アクセス パスは、最初に使用されてから 28 日後に再び利用可能になります。

ログイン パスの使用の説明

# 日目	ログイン アクセス パスの使用	説明
29 日目		このシナリオの開始から 28 日が経過し、最初の 2 つのログイン アクセス パスが再び使用できる状態になりました。
43 日目		上記ユーザーの 2 度目のログインから 28 日が経過し、その時のログイン アクセス パスが再び使用できる状態になりました。
54 日目		最後のログインから 28 日が経過し、すべてのログイン アクセス パスが使用できるようになりました。

必要なトークン数の予測

適切なトークン数を予測するには、さまざまなユーザーのニーズを特定する必要があります。フロントラインマネージャー、ビジネスアナリスト、管理職、データエンジニア、そして一般の知識労働者それぞれに異なるニーズが存在します。

話をわかりやすくするため、この例のユーザーは、1 か月あたり平均で 4 個のログインアクセスパスを使用すると仮定します。さらに、ユーザーが実際に毎月ログインする正確な回数がわからないため、バッファが必要です。この例では、バッファは 20% です。

前述したように、1 トークンは 10 ログインアクセスパスです。必要なトークン数は次のように計算することができます。

*[ユーザー数] * [1 人あたりのログインアクセスパスの予測数] * [バッファ] /10 = 必要なトークン数*

ユーザー数は 103 人と仮定します。計算は次のようになります。

*103 * 4 * 1,2 /10 = 49.4*

トークンを部分的に購入することはできないため、繰り上げて 50 個のトークンが必要と計算されます。

ライセンスルールの作成

ライセンスルールを作成すると、ログインアクセスルールを使用できるユーザーの指定が可能になります。ライセンスルールがなくてもログインアクセスルールは設定できますが、システム全体にログインアクセスルールが適用されてしまうため、お勧めできません。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、または [**スタート▼**] ドロップダウンメニューから [**ライセンスの管理**] を選択して、概要を表示します。
3. パネル右側の [**ログインアクセスルール**] を選択します。
4. ログインアクセスルールを選択し、[**編集**] をクリックします。

   ログインアクセスルールを新規作成します (「」を参照)。ログインアクセスルールの作成 (page 325)。

5. [**関連するアイテム**] で [**ライセンスルール**] を選択します。
6. [**関連付けルールの作成**] をクリックします。
7. 必要に応じてライセンスルールを編集します。

a. **ID**

ログイン アクセス ID のルール

ルール	説明
無効化	ルールを切り替えます。(既定では無効化)
名前	ログイン アクセス ルールの名前です。(必須)
説明	ルールの説明。

b. **基本**

リソース フィルターを変更すると、ルールが意図通りに動作しないことがあります。

[**アクセスの許可**] オプションが自動で選択されます。

演算子の説明

演算子	説明と例
=	この演算子では大文字と小文字は区別されません。比較対象の数式と完全に等しい場合は True を返します。 `user.name = "a*"` 名前が「a*」と完全に一致するユーザーがルールの対象になります。
like	この演算子では大文字と小文字は区別されません。比較対象の数式と等しい場合は True を返します。 `user.name like "a*"` 名前が a で始まるすべてのユーザーがルールの対象になります。
!=	この演算子では大文字と小文字は区別されません。比較対象の数式の値が等しくない場合に True を返します。 `user.name != resource.name` ユーザーと同じ名前ではないすべてのリソースがルールによって対象になります。

c. **詳細設定**

ルールを適用すべきリソース**条件**やユーザー条件、複合条件を定義します。

8. オプションとして、[**詳細設定**] プロパティを編集し、ルールの [**条件**] を作成します。
9. [**適用**] をクリックして、ライセンス ルールを作成し、保存します。
[**ライセンス ルールは関連するアイテムに正常に追加されました**] というメッセージがページの最下部に表示されます。

ライセンス ルールの編集

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、または [**スタート▼**] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
3. パネル右側の [**ログイン アクセス ルール**] を選択します。
4. ログイン アクセス ルールを選択し、[**編集**] をクリックします。
5. [**関連するアイテム**] で [**ライセンス ルール**] を選択します。
6. ライセンス ルールを選択し、[**編集**] をクリックします。
   必要に応じてライセンス ルールを編集します。

   a. **ID**

   ログイン アクセス ID のルール

ルール	説明
無効化	ルールを切り替えます。(既定では無効化)
名前	ログイン アクセス ルールの名前です。(必須)
説明	ルールの説明。

   b. **基本**
   リソース フィルターを変更すると、ルールが意図通りに動作しないことがあります。

   *[**アクセスの許可**] オプションが自動で選択されます。*

   演算子の説明と例

演算子	説明と例
=	この演算子では大文字と小文字は区別されません。比較対象の数式と完全に等しい場合は True を返します。 `user.name = "a*"` 名前が「a*」と完全に一致するユーザーがルールの対象になります。

like	この演算子では大文字と小文字は区別されません。比較対象の数式と等しい場合は True を返します。 `user.name like "a*"` 名前が a で始まるすべてのユーザーがルールの対象になります。
!=	この演算子では大文字と小文字は区別されません。比較対象の数式の値が等しくない場合に True を返します。 `user.name != resource.name` ユーザーと同じ名前ではないすべてのリソースがルールによって対象になります。

c. **詳細設定**
[**条件**] で、ルールを適用すべきリソース**条件**やユーザー条件、複合条件を定義することができます。

7. オプションとして、[**詳細設定**] プロパティを編集し、ルールの [**条件**] を作成します。
8. [**適用**] をクリックして、ライセンス ルールを作成し、保存します。

「**ライセンス ルールが更新されました**」というメッセージがページの最下部に表示されます。

ユーザー同期タスクの開始

ユーザー ディレクトリ コネクタの関連付けページからユーザー同期タスクを手動で開始できます。

タスク概要ページから、またはスケジュールされたトリガーによってユーザー同期タスクを開始することもできます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**User directory connectors (ユーザー ディレクトリ コネクタ)**] を選択して、概要を表示します。
3. タスクを編集したいユーザー ディレクトリ コネクタを選択し、アクション バーで [**編集**] をクリックします。

   一番左側のパネルには、選択が一覧表示されています。

4. [**関連するアイテム**] の [**タスク**] を選択します。
[**User synchronization tasks**] の概要が表示されます。
5. 開始するタスクを選択し、操作バーで [**スタート**] をクリックします。
ページの最下部に [**x 件のアイテムの内 x 件の開始を指示しました**] と表示されます。

ユーザー同期タスクの編集

ユーザー ディレクトリコネクタの関連付けページからユーザー同期タスクを編集できます。

タスク概要ページからユーザー同期タスクを編集することもできます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**User directory connectors (ユーザー ディレクトリ コネクタ)**] を選択して、概要を表示します。
3. タスクを編集したいユーザー ディレクトリコネクタを選択し、アクション バーで [**編集**] をクリックします。
4. [**関連するアイテム**] で [**タスク**] を選択し、編集するタスクを選択して操作バーで [**編集**] をクリックします。[**User synchronization task edit**] ページが表示されます。
5. プロパティを編集します。

ID

全項目が必須で、空欄のままにはできません。

ID プロパティ

プロパティ	説明	既定値
[**名前**]	タスクの名前。	ユーザー ディレクトリコネクタを新規作成すると、ユーザー ディレクトリコネクタ名から自動生成されます。
有効化	選択されている場合、タスクは有効です。	有効化

[**有効化**] チェックボックスを選択または選択解除して、タスクを有効または無効にします。

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

6. アクション バーで [**適用**] をクリックし、変更内容を保存します。
ページの最下部に [**更新完了**] と表示されます。

*タスクのトリガーは [**Associated items**] に表示されます。またここでは新しいトリガーを作成できます。*

ユーザー同期タスクのトリガーの作成 - スケジュール済み

タスクのために予定されたトリガー (複数可) を作成できます。トリガーはタスクを一回実行、あるいは開始と終了を指定期間ほどタスクを繰り返したり、無期限でタスクを繰り返したりします。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Tasks (タスク)**] を選択して、概要を表示します。
3. トリガーを追加したいタスクを選択し、ページの最下部にあるアクション バーで [**編集**] をクリックします。
4. [**Associated items**] で [**Triggers**] を選択します。
   [**トリガー**] の概要が表示されます。
5. データ マネージャーでテーブルの **Create associated trigger** in the action bar.
   [**トリガー - スケジュールにより開始**] ダイアログが表示されます。
6. ダイアログの項目を編集して、トリガーの条件を設定します。

スケジュール済みトリガーのプロパティ

プロパティ	説明
[**トリガー名**]	トリガーの名前。必須。
[**有効化**]	トリガーの状態。選択するとトリガーはアクティブになります。
[**タイムゾーン**]	オペレーティング システムのタイム ゾーンがトリガーを作成した時間になります。トリガーを保存すると設定は保持され、タイムゾーンが違う場所に行っても元の設定値のまま表示されます。タイム ゾーンやトリガーの開始時間を変更したい場合は手動で行う必要があります。 *タイム ゾーンの設定より前に作成されたトリガーについては、日時はすべてデフォルトで Coordinated Universal Time (UTC: 協定世界時) にて表示されます。*

プロパティ	説明
[**夏時間**]	夏時間を考慮する方法。 [**夏時間を使用する**]: このオプションでは夏時間 (DST) が考慮されます。選択したタイム ゾーンで DST が使われていると、実行日時はそれに応じて調整されます。 [**常に標準時**]: このオプションでは DST は考慮されません。選択したタイム ゾーンで DST が使われていても、実行日時は調整されません。 [**常に夏時間**]: このオプションでは DST が考慮されません。タイム ゾーンで DST が使われている場合は、DST の適用期間外でも実行日時は常に DST に準じます。 *DST を使用しないタイム ゾーンの場合は、常に [**永久標準時**] を選択します。* 1 月にカナダのオタワで午前 10 時に開始するイベントのトリガーを作成したとします。ここのタイム ゾーンは (GMT-0500) 東部標準時 (米国およびカナダ) で DST の期間は 3 月から 11 月です。 [**夏時間を使用する**] を選択すると、10 時に開始するよう設定されたトリガーは常に 10 時に開始します。 [**常に標準時**] を選択すると、10 時に実行するよう設定されたトリガーは冬は 10 時に実行されますが夏は 9 時に実行されます。 [**常に夏時間**] を選択すると、10 時に実行するよう設定されたトリガーは冬は 11 時に、夏は 10 時に実行されます。
[**Start**]	開始時間と開始日: • 開始時間: [**(hh:mm)**] • 開始日: **(YYYY-MM-DD)**

プロパティ	説明

[スケジュール]	トリガーの頻度。
	• [**1 回**]。
	• [**時間単位**]。トリガー実施の間隔。次の値を入力して、[**各条件の後に繰り返す**]を編集します。
	  • [**s (時間単位**] (既定 1 時間)
	  • [**s (分単位**] (既定 0 分)
	• [**日単位**]。トリガー実施の間隔。[**Every**][**s (日おき**] (既定 1 日) の値を入力します。たとえば、2 と入力すると2 日おきにトリガーが繰り返されます。
	• [**週単位**]。トリガー実施の間隔:
	  • [**Every**][**s (週おき**] (既定 1 週) の値を入力します。
	  • [**平日**] のチェックボックスを選択して (複数日可)、トリガーが繰り返される日を決めます (ユーザーが指定する週で)。たとえば、3 と入力して [**月曜日**] を選択すると、3 週おきの月曜日にトリガーが実行されます。
	• [**月単位**]。[**On these days**] のチェックボックスを選択 (複数可) すると、毎月トリガーが繰り返し実行される日を定義できます。
	  *[**Monthly**] を選択し、トリガーが毎月繰り返されるようにするには、28 日よりも前の日を選択する必要があります。*
	• ***カスタム***: [**カスタム**] を選択すると、[**フィルター**] と [**増分**] の 2 つの新しい項目が表示されます。これらのオプションは、リロードをスケジュールするときに大きな柔軟性を提供します。詳細は、「*タスク- カスタム オプション (page 228)*」を参照してください。

[**終了**]	終了時間と終了日: • 終了時間: [**(hh:mm)**] • 終了日:**(YYYY-MM-DD)** [**無期限**] を選択して、終了日のないトリガーを作成します。

7. [**適用**] をクリックして、トリガーを作成および保存します。
   ダイアログが閉じて、[**Successfully added**] と表示されます。そして [**Associated items**] の概要に、新しいトリガーがリストされます。

ユーザー同期タスクのトリガー編集

ユーザー同期タスクのトリガーを編集できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. Select **Tasks** on the QMC start page or from the **Start** ドロップダウン メニューからリソースを選択します。
3. トリガーを編集したいタスクを選択し、ページの最下部にあるアクション バーで [**編集**] をクリックします。

4. [**関連するアイテム**] で [**トリガー**] を選択します。
   [**トリガー**] の概要が表示されます。
5. 編集したいタスクを選択し、ページの最下部にあるアクション バーで [**編集**] をクリックします。
   [**トリガー - スケジュールにより開始**] ダイアログが表示されます。
6. ダイアログの項目を編集して、トリガーの条件を変更します。

スケジュール済みトリガーのプロパティ

プロパティ	**説明**
[**トリガー名**]	トリガーの名前。必須。
[**有効化**]	トリガーの状態。選択するとトリガーはアクティブになります。
[**タイムゾーン**]	オペレーティング システムのタイム ゾーンがトリガーを作成した時間になります。トリガーを保存すると設定は保持され、タイムゾーンが違う場所に行っても元の設定値のまま表示されます。タイム ゾーンやトリガーの開始時間を変更したい場合は手動で行う必要があります。 *タイム ゾーンの設定より前に作成されたトリガーについては、日時はすべてデフォルトで Coordinated Universal Time (UTC: 協定世界時) にて表示されます。*

プロパティ	説明
[**夏時間**]	夏時間を考慮する方法。 [**夏時間を使用する**]: このオプションでは夏時間 (DST) が考慮されます。選択したタイム ゾーンで DST が使われていると、実行日時はそれに応じて調整されます。 [**常に標準時**]: このオプションでは DST は考慮されません。選択したタイム ゾーンで DST が使われていても、実行日時は調整されません。 [**常に夏時間**]: このオプションでは DST が考慮されません。タイム ゾーンで DST が使われている場合は、DST の適用期間外でも実行日時は常に DST に準じます。 *DST を使用しないタイム ゾーンの場合は、常に [**永久標準時**] を選択します。* 1 月にカナダのオタワで午前 10 時に開始するイベントのトリガーを作成したとします。ここのタイム ゾーンは (GMT-0500) 東部標準時 (米国およびカナダ) で DST の期間は 3 月から 11 月です。 [**夏時間を使用する**] を選択すると、10 時に開始するよう設定されたトリガーは常に 10 時に開始します。 [**常に標準時**] を選択すると、10 時に実行するよう設定されたトリガーは冬は 10 時に実行されますが夏は 9 時に実行されます。 [**常に夏時間**] を選択すると、10 時に実行するよう設定されたトリガーは冬は 11 時に、夏は 10 時に実行されます。
[**Start**]	開始時間と開始日: • 開始時間: [**(hh:mm)**] • 開始日: **(YYYY-MM-DD)**

プロパティ	説明

[スケジュール]	トリガーの頻度。
	• [**1 回**]。
	• [**時間単位**]。トリガー実施の間隔。次の値を入力して、[**各条件の後に繰り返す**] を編集します。
	  • [**s (時間単位**] (既定 1 時間)
	  • [**s (分単位**] (既定 0 分)
	• [**日単位**]。トリガー実施の間隔。[**Every**][**s (日おき**] (既定 1 日) の値を入力します。たとえば、2 と入力すると2 日おきにトリガーが繰り返されます。
	• [**週単位**]。トリガー実施の間隔:
	  • [**Every**][**s (週おき**] (既定 1 週) の値を入力します。
	  • [**平日**] のチェックボックスを選択して (複数日可)、トリガーが繰り返される日を決めます (ユーザーが指定する週で)。たとえば、3 と入力して [**月曜日**] を選択すると、3 週おきの月曜日にトリガーが実行されます。
	• [**月単位**]。[**On these days**] のチェックボックスを選択 (複数可) すると、毎月トリガーが繰り返し実行される日を定義できます。
	  *[**Monthly**] を選択し、トリガーが毎月繰り返されるようにするには、28 日よりも前の日を選択する必要があります。*
	• **カスタム**: [**カスタム**] を選択すると、[**フィルター**] と [**増分**] の 2 つの新しい項目が表示されます。これらのオプションは、リロードをスケジュールするときに大きな柔軟性を提供します。詳細は、「*タスク- カスタム オプション (page 228)*」を参照してください。

[**終了**]	終了時間と終了日: • 終了時間: [**(hh:mm)**] • 終了日:**(YYYY-MM-DD)** [**無期限**] を選択して、終了日のないトリガーを作成します。

7. ページの最下部にあるアクション バーで [**適用**] をクリックして、変更内容を保存します。

ダイアログを閉じると、[**更新完了**] と表示されます。

ユーザー同期タスクの停止

ユーザー ディレクトリ コネクタの関連付けページからユーザー同期タスクを停止できます。

タスク概要ページからユーザー同期タスクを停止することもできます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**User directory connectors (ユーザー ディレクトリ コネクタ)**] を選択して、概要を表示します。
3. 開始したいユーザー ディレクトリ コネクタを選択して、アクション バーで [**編集**] をクリックします。
4. [**関連するアイテム**] の [**タスク**] を選択します。
   [**User synchronization tasks**] の概要が表示されます。
5. 停止するタスクを選択し、操作バーで [**停止**] をクリックします。
   ページの最下部に [**x 件のアイテムの内 x 件の停止を指示しました**] と表示されます。

ユーザー同期タスクの削除

ユーザー同期タスクは、ユーザー ディレクトリ コネクター (UDC) を削除すると、同時に削除されます。ユーザー同期タスクを個別に削除することはできません。

ユーザー ディレクトリ コネクターとユーザーの削除 (page 307)

ユーザーの編集

更新権限を有するユーザーを編集できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**ユーザー**] を選択して、概要を表示します。

   フィルタリング オプションを使用して列にフィルターを適用できます。
3. 編集するユーザーを選択します。
4. アクション バーで [**編集**] をクリックします。
5. プロパティを編集します。

ID

ID プロパティ

プロパティ	**説明**
名前	ユーザーの氏名。
ユーザー ディレクトリ	ユーザーと関連のあるユーザー ディレクトリ。
[**ユーザー ID**]	ユーザーに関連付けられているユーザー ID。
[**ブロック**]	ユーザーをブロック (非アクティブ化) します。デフォルトでは、選択されていない状態です。

プロパティ	説明
[**削除禁止**]	管理者ロール RootAdmin を持つユーザーの削除や非アクティブ化を禁止 デフォルトでは、選択されていない状態です。
[**管理者ロール**]	ユーザーに関連付けられている QMC 管理者ロール。テキストボックスをクリックすると、利用可能な管理者ロールが表示されます。 *新規の存在しない管理者ロールを追加できますが、適切に定義するまでは有効になりません。*

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキストボックスの下に表示されます。

カスタム プロパティ

リソースのカスタム プロパティがアクティブになると、リストからカスタム プロパティの値を選択できます。

カスタム プロパティ

プロパティ	説明
[**カスタム プロパティ**]	利用できるカスタム プロパティがない場合、このプロパティグループは表示されません (もしくは空欄で表示されます)。ここに表示させる前にこのリソースタイプで利用できるカスタム プロパティを作成する必要があります。

6. [**適用**] をクリックして変更を保存します。必須の項目が空欄の場合、[**Apply**] は無効になります。

ページの最下部に [**更新完了**] と表示されます。

ユーザーの非アクティブ化

ユーザーをブロック (非アクティブ化) することができます。ブロックすると、[**ユーザー**] 概要ページに [**ブロック**] とマークされます。Qlik Sense と接続しているディレクトリから削除されたユーザーは、Qlik Sense によって自動的に非アクティブ化されます。ブロックすると、[**Users**] 概要ページに [**Removed externally**] とマークされます。

非アクティブ ユーザーが作成したオブジェクトの所有者あるいは所有者として割り当てられた場合の所有者は、そのままその非アクティブ ユーザーとなります。該当する非アクティブ ユーザーは、彼らに割り当てられたカスタム プロパティを保持します。

非アクティブ化されたユーザーが Qlik Sense システムにログインを試みると、システム管理者に問い合わせるよう通知されます。

*[**削除が禁止**] されているRootAdmin ユーザーを非アクティブ化 (ブロックまたは外部から削除) することはできません。RootAdmin ユーザーを非アクティブ化するには、まず最初に [**削除禁止**] 設定をクリアする必要があります。*

ユーザーが削除されると、そのユーザーが所有するオブジェクトの所有権は、sa_repository ユーザーに委譲されます。カスタム プロパティなどユーザーに関する情報はすべて、ユーザーと共に削除されます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**ユーザー**] を選択して、概要を表示します。
3. 非アクティブ化するユーザーを選択します。
4. アクション バーで [**編集**] をクリックします。
   [**User edit**] プロパティ ページが開きます。
5. [**Blocked**] を選択します。
6. アクション バーで [**適用**] をクリックし、変更内容を保存します。

ユーザーの削除

必要な削除権限がある場合は、Qlik Sense システムからユーザーを削除できます。ユーザーを削除すると:

- ユーザーは、Qlik Sense システムの一部ではなくなります。
- セキュリティの観点から、ユーザーにはアクセス権が付与されません。
- ユーザーのオブジェクトの所有権は *sa_repository* ユーザーに譲渡されます。カスタム プロパティなどユーザーに関する情報はすべて、ユーザーと共に削除されます。

Qlik Sense と接続しているディレクトリ サービスから削除されたユーザーは自動的に、QMC で非アクティブとなります。

ユーザー ディレクトリ コネクタを削除する際は、そのユーザー ディレクトリからインポートされたユーザーをすべて削除するか選択できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**ユーザー**] を選択して、概要を表示します。
3. 削除するユーザーを選択します。

フィルタリング オプションを使用して列にフィルターを適用できます。

4. アクション バーの [**Delete**] をクリックします。
   [**Delete**] ダイアログが表示されます。
5. [**OK**] をクリックします。

ルート管理者ユーザーの作成

QMCにアクセスしてサーバー ライセンスを追加する最初のユーザーは、Qlik Senseシステムのルート管理者 (RootAdmin) ロールを取得します。このユーザーは、サイトのあらゆるリソース (セキュリティルール、ストリーム、ノードなど) への完全なアクセス権があります。追加ユーザーを RootAdmin に割り当てることや、異なる管理権限を持つ他の管理者ロールに割り当てることもできます。

*ルート管理者は、Qlik Senseシステムで作成されたセキュリティルールを変更または削除することはできません。このようなセキュリティルールは [**セキュリティルール**] 概要ページに一覧表示され、[**タイプ**] は [**既定**] に設定されます。*

ユーザーの管理者ロールの管理

Qlik Sense ユーザープロパティはユーザー ディレクトリから取得され、QMC では編集できません。しかし、ユーザーに対し管理者ロールの割り当て、削除、変更を行うことができます。

QMCは、ユーザー ロール定義での変更を 20 秒ごとに探します。

*[**ストリーム**] の概要からストリームにアクセス権を持つユーザーを編集できます。ストリームを選択し、プロパティグループから [**ユーザー**] をクリックして、ユーザー (複数可) を選択して、[**編集**] をクリックします。*

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**ユーザー**] を選択して、概要を表示します。
3. 管理者ロールを停止または変更したいユーザーを選択します。
4. アクション バーで [**編集**] をクリックします。
   [**User edit**] プロパティページが開きます。
5. [**Properties**] で [**Identification**] を選択します。
6. データ マネージャーでテーブルの ⊕in the **Admin roles** attribute and type the name of the admin role that you want to connect to in the text box that appears, or click ⊕in the text box of the role that you want to disconnect.
   [**Admin roles**] テキスト フィールドは、大文字と小文字の区別をします。QMC は、入力内容に沿ってロールを提案します。ロールの 1 つを選択します。

Qlik Senseの場合と同様、ユーザーは、QMCのリソースへのアクセス権を持っていない場合には、QMCインターフェースからそのリソースにアクセスすることができません。たとえば、ユーザーのロールをRootAdmin からDeploymentAdmin に変更すると、そのユーザーはQMCのアプリやシート、ストリーム、データ接続ページなどにアクセス不能になります。

*[**削除が禁止**] されているRootAdmin ユーザーの管理者ロールを変更することはできません。ロールを変更するには、まず最初に[**削除禁止**] 設定をクリアする必要があります。*

7. アクション バーで [**適用**] をクリックし、変更内容を保存します。

*QMC で利用可能なリソースの中には、機密情報が非特権ユーザーに開示されるのを防ぐために、追加のセキュリティが設定されているものもあります。QMC にカスタム管理者ロールを定義する場合、管理者は、これらのロールに割り当てられたユーザーに適切なセキュリティルールが設定されていることを確認する必要があります。例:QMCの**監査**セクションにアクセスするには、`UserDirectory_*` リソースへの読み取りアクセスが必要です。*

リソース所有者の変更

リソースの作成者は、デフォルトで所有者となります。所有権は、リソースの編集時に変更することができます。

必要な管理権限を持つ管理者のみが、リソースの所有権を変更できます。

次の手順を実行します。

1. リソース概要で、所有者を変更するリソースを選択して、[**編集**] をクリックします。
2. [**所有者**] フィールドに入力し始めます。
   基準を満たすユーザーが表示されます。
3. 新規所有者として割り当てたいユーザーを選択します。所有権は、Qlik Senseシステムに存在するユーザーに対してのみ割り当てることができます。
4. [**適用**] をクリックします。
   [**更新されました**] と表示されます。

ユーザーが所有するアイテムの管理

ユーザーが所有するリソースは [**User edit**] ページの [**Associated items**] にある [**Owned items**] から管理できます。

所有者のいるアイテムの表示

ユーザーが所有するアイテムを表示できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**ユーザー**] を選択して、概要を表示します。

   フィルタリング オプションを使用して列にフィルターを適用できます。
3. 表示するアイテムを所有するユーザーを選択します。
4. アクション バーで [**編集**] をクリックします。
   [**User edit**] プロパティページが開きます。
5. [**Associated items**] で [**Owned items**] をクリックします。
   [**Owned items**] の概要が開きます。

ユーザーの所有するアイテムの編集

ユーザーが所有するアイテムを編集できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**ユーザー**] を選択して、概要を表示します。

   フィルタリング オプションを使用して列にフィルターを適用できます。
3. 編集するアイテムを所有するユーザーを選択します。
4. アクション バーで [**編集**] をクリックします。
   [**User edit**] プロパティページが開きます。
5. [**Associated items**] で [**Owned items**] をクリックします。
   [**User associated items**] の概要が開きます。
6. 編集するアイテムを選択します。
7. アクション バーで [**編集**] をクリックします。
   選択したアイテム タイプの編集ページが開きます。
8. プロパティを編集します。
9. [**適用**] をクリックして変更を保存します。必須の項目が空欄の場合、[**Apply**] は無効になります。

ページの最下部に [**更新完了**] と表示されます。

ユーザーが所有するアイテムの削除

削除権限を有する特定のユーザーが所有するアイテムを削除できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**ユーザー**] を選択して、概要を表示します。

3. 表示するアイテムを所有するユーザーを選択します。
4. アクション バーの [**Delete**] をクリックします。
   [**User edit**] プロパティページが開きます。
5. [**Associated items**] で [**Owned items**] をクリックします。
   [**User associated items**] の概要が開きます。
6. 削除するアイテムを選択します。
7. [**削除**] をクリックします。
   [**Delete**] ダイアログが表示されます。リソースが削除されると、そのリソースに関連付けられている負荷分散ルールとセキュリティルールはすべて自動的に削除されます。
8. [**OK**] をクリックします。

QMC でカスタマイズされたロールを定義する

Qlik Sense のベストプラクティスは、ユーザー グループのセキュリティルールを定義することです。そのひとつの方法が、管理者 ロールを定義するために QMC 内蔵機能を使用して、ロールをユーザーに割り当てることです。

もうひとつの方法は、ディレクトリサービスから提供されたプロパティかカスタム プロパティのいずれかを使用してユーザーをタイプごとにまとめることです。

いずれの方法についても次のトピックで説明します。

ロールを使用して管理者にアクセス権を提供

Qlik Sense には、管理者向けにあらかじめ定義された (既定) ルールが含まれています。このようなルールは、管理者 ロールと呼ばれます。

凡例 (page 458)

管理者 ロールはセキュリティルールを使用して定義されます。既存の管理者 (admin) ロールを編集するか、セキュリティルール エディタを使用して新しいロールを定義して追加することができます。

セキュリティルールの例: カスタム管理者 ロールの作成 (page 601)

ユーザー タイプを使用してユーザーにアクセス権を提供する

管理者 ロールはQMCへのアクセス権を定義するために使用されますが、Qlik Senseのユーザーのユーザー タイプを定義できます。ユーザー タイプは、次のいずれか、または両方のプロパティ値の条件と一緒にセキュリティルール エディタを使用して定義します。

- ユーザーのプロパティ
- カスタム プロパティ

ロールを作成したいユーザー タイプに完全に対応する既存の Active Directory (AD) グループがある場合は、そのグループの条件を定義して、セキュリティルールに適切な名前を付けることができます。たとえば、*開発者* と呼ばれる AD グループがあれば、適切なセキュリティルールを提供する「*開発者*」と呼ばれるセキュリティルールを作成できます。また、*ユーザー ロール* と呼ばれるカスタム プロパティを作成して、*開発者*や*テスト担当者*、*貢献者*、*消費者* といった値を与えることもできます。その後、カスタム プロパティをユーザーに適用してから、適切なセキュリティルールをカスタム プロパティ値に適用します。

セキュリティルールの例: ユーザー タイプ別 Qlik Sense アクセス権の適用 (page 606)

タスクとトリガーの管理

タスク

タスクは幅広い作業を行うために使用され、任意のパターンでの連動が可能です。タスクは、Qlik Sense Engine Service (QSS) によって処理されます。4 種類のタスクがあります。

- リロード
- ユーザー同期化
- 外部プログラム
- 配布

このリロード タスクは、アプリ内のデータをソースから完全リロードします。古いデータはすべて、破棄されます。新しいリロード タスクを作成できます。

ユーザー同期タスクは、ユーザー ディレクトリからユーザーおよびユーザー情報をインポートします。ユーザー ディレクトリ コネクタ (UDC) のインスタンスを新規作成すると、スケジュールされたトリガーを含む同期化タスクがシステムによって作成されます。

外部プログラムのタスクによって、サード パーティのプログラムがトリガーされます。外部プログラムのタスクを編集することはできず、タスク変更に使用することもできません。

トリガー

タスク概要のページから、トリガーまたは手動で、タスク実行を開始します。タスクを実行する追加のトリガーを作成できます。トリガーには以下の 2 種類があります。

- スケジュールによるもの
- タスク イベント

リロード タスクおよびユーザー同期タスクの両方に、スケジュールされたトリガーを適用できます。リロード タスクにのみ、タスク イベント トリガーを適用できます。

リロード タスクのトリガーは、[**タスク編集**] ページから直接利用できます。

ユーザー同期タスクのトリガーは、[**タスク編集**] ページの [**関連付け**] タブからアクセスできます。タスク編集ページでは [**トリガー**] 概要に、選択したタスキをトリガーするために利用できるトリガーがすべて一覧表示されています。

タスクからのリロード タスクの作成

タスク概要ページから、アプリ向けにリロード タスクを作成できます。

リロード タスクを新規作成する方法は複数あります。

- アプリ概要のページから
- [**App edit**] ページの [**Associated items**] タブから
- タスク概要のページから
- 適切な権限を持つユーザーによって、ハブから

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Tasks (タスク)**] を選択して、概要を表示します。
3. データ マネージャーでテーブルの ⊕**新規作成** をクリックします。
   [**リロード タスク編集**] ページが表示されます。
4. プロパティを編集します。
   a. [**名前**] 項目にリロード タスクの名前を入力します。
   b. [**アプリ名**] 項目で [**アプリ選択**] をクリックします。
   ダイアログが開きます。ダイアログで、このタスクによりリロードしたいアプリをダブルクリックします。
   ダイアログが閉じると、[**アプリ名**] 項目に選択したアプリが表示されます。
   c. [**実行**] プロパティを変更できます。以下の説明を参照してください。このタスクは、既定では [**有効**] ✔ になっています。選択をクリアすると、タスクが無効になります。
   d. タスクには少なくとも、自動実行するトリガーがひとつ含まれている必要があります。[**トリガー**] の表見出しにある [**アクション**] ▼ をクリックしてトリガーを管理し、次からひとつ選択します:
      - [**1 回のみのトリガーを新規作成**]、[**時間ベースのトリガーを新規作成**]、[**日単位のトリガーを新規作成**]、[**週単位のトリガーを新規作成**]、[**月単位のトリガーを新規作成**] の中から選び、新しいトリガーを作成します。これらはトリガーのショートカットで、選択したトリガーがテーブルに即座に追加されます。トリガーの開始値は、作成時から5 分に設定され、トリガーが有効になります。
      - [**スケジュール済みトリガーを新規作成**] または [**タスク イベント トリガーを新規作成**] を使い、選択されたタイプのトリガーを新規作成します (下記のプロパティの説明を参照)。ダイアログが開きます。トリガーを編集して [**OK**] をクリックすると、ダイアログが閉じてテーブルにトリガーが追加されます。
      - 適宜、[**削除**] を使い、テーブルで選択されたトリガーを削除します。
      - 適宜、[**編集**] を使い、テーブルで選択されたトリガーの編集ダイアログを開きます。トリガーを編集し、[**OK**] をクリックしてダイアログを閉じ、変更内容を保存します。
   e. 任意でタグを適用します。
   f. 任意で、カスタム プロパティを適用します。

ID

全項目が必須で、空欄のままにはできません。

ID プロパティ

プロパティ	説明	既定値
[**名前**]	タスクの名前。	<アプリ名> のタスクのリロード。
[**アプリ**]	タスクが作成されたアプリの名前。項目をクリックしてダイアログを開き、タスクがリロードするアプリを (ダブルクリックして) 選択します。	<App name>

実行

実行プロパティ

プロパティ	説明	既定値
[**有効化**]	選択されている場合、タスクは有効です。	選択済み
部分的なリロード	部分的なリロードでは、データモデルの既存のテーブルをすべてリロードすることなく、新しいデータを追加することができます。フル リロードでは、すべてのテーブルを削除してから、ロード スクリプトを実行します。部分的なリロードでは、新しいデータを追加するだけで、既存のテーブルは維持されます。 部分的なリロードには、完全なリロードと比較していくつかの利点があります。 • 最近変更されたデータのみをロードする必要があるため、より高速です。データセットが大きい場合、違いは大きくなります。 • ロードされるデータが少ないため、消費されるメモリも少なくなります。 • ソース データへのクエリがより高速に実行され、ネットワークの問題のリスクが軽減されるため、信頼性が向上します。	選択されていない
[**タスク セッション タイムアウト(分)**]	タスクが停止するまでの最大時間 タスクが開始すると、マネージャー スケジューラによってセッションが開始、ノードの 1 つによってタスクが実行されます。セッションがタイムアウトすると、マネージャー スケジューラは強制的にノードにタスクを中止させて、セッションを削除します。	1440
[**最大リトライ数**]	スケジューラが失敗したタスクの再起動を試みる最大回数。	0

トリガー (スケジュール済み)

スケジュール済みトリガーのプロパティ

プロパティ	説明
[**トリガー名**]	トリガーの名前。必須。
[**有効化**]	トリガーの状態。選択するとトリガーはアクティブになります。

プロパティ	説明
[**タイムゾーン**]	オペレーティング システムのタイム ゾーンがトリガーを作成した時間になります。トリガーを保存すると設定は保持され、タイムゾーンが違う場所に行っても元の設定値のまま表示されます。タイム ゾーンやトリガーの開始時間を変更したい場合は手動で行う必要があります。 *タイム ゾーンの設定より前に作成されたトリガーについては、日時はすべてデフォルトで Coordinated Universal Time (UTC: 協定世界時) にて表示されます。*
[**夏時間**]	夏時間を考慮する方法。 [**夏時間を使用する**]: このオプションでは夏時間 (DST) が考慮されます。選択したタイム ゾーンで DST が使われていると、実行日時はそれに応じて調整されます。 [**常に標準時**]: このオプションでは DST は考慮されません。選択したタイム ゾーンで DST が使われていても、実行日時は調整されません。 [**常に夏時間**]: このオプションでは DST が考慮されません。タイム ゾーンで DST が使われている場合は、DST の適用期間外でも実行日時は常に DST に準じます。 *DST を使用しないタイム ゾーンの場合は、常に [**永久標準時**] を選択します。* 1 月にカナダのオタワで午前 10 時に開始するイベントのトリガーを作成したとします。ここのタイム ゾーンは (GMT-0500) 東部標準時 (米国およびカナダ) で DST の期間は 3 月から 11 月です。 [**夏時間を使用する**] を選択すると、10 時に開始するよう設定されたトリガーは常に 10 時に開始します。 [**常に標準時**] を選択すると、10 時に実行するよう設定されたトリガーは冬は 10 時に実行されますが夏は 9 時に実行されます。 [**常に夏時間**] を選択すると、10 時に実行するよう設定されたトリガーは冬は 11 時に、夏は 10 時に実行されます。
[**Start**]	開始時間と開始日: • 開始時間: [**(hh:mm)**] • 開始日: **(YYYY-MM-DD)**

プロパティ	説明

[スケジュール]	トリガーの頻度。
	• [**1 回**]。
	• [**時間単位**]。トリガー実施の間隔。次の値を入力して、[**各条件の後に繰り返す**]を編集します。
	  • [**s (時間単位**] (既定 1 時間)
	  • [**s (分単位**] (既定 0 分)
	• [**日単位**]。トリガー実施の間隔。[**Every**][**s (日おき**] (既定 1 日) の値を入力します。たとえば、2 と入力すると2 日おきにトリガーが繰り返されます。
	• [**週単位**]。トリガー実施の間隔:
	  • [**Every**][**s (週おき**] (既定 1 週) の値を入力します。
	  • [**平日**] のチェックボックスを選択して (複数日可)、トリガーが繰り返される日を決めます (ユーザーが指定する週で)。たとえば、3 と入力して [**月曜日**] を選択すると、3 週おきの月曜日にトリガーが実行されます。
	• [**月単位**]。[**On these days**] のチェックボックスを選択 (複数可) すると、毎月トリガーが繰り返し実行される日を定義できます。
	  *[**Monthly**] を選択し、トリガーが毎月繰り返されるようにするには、28 日よりも前の日を選択する必要があります。*
	• ***カスタム***: [**カスタム**] を選択すると、[**フィルター**] と [**増分**] の 2 つの新しい項目が表示されます。これらのオプションは、リロードをスケジュールするときに大きな柔軟性を提供します。詳細は、「*タスク- カスタム オプション (page 228)*」を参照してください。

[**終了**]	終了時間と終了日: • 終了時間: [**(hh:mm)**] • 終了日:**(YYYY-MM-DD)** [**無期限**] を選択して、終了日のないトリガーを作成します。

トリガー (タスク イベント)

タスク イベント トリガーのプロパティ

プロパティ	説明
[**トリガー名**]	トリガーの名前。必須。

プロパティ	説明
[**タイプ**]	トリガーのタイプ。
[**有効化**]	トリガーの状態。選択するとトリガーはアクティブになります。
[**時間制限**]	タスクチェーンの他のタスクを完了しなければならない期間 (分単位)。トリガーがひとつのタスクだけで構成されている場合、何も起きません。 *タスクチェーンの作成 (page 355)*
[**タスク**]	
	次の手順を実行します。 1. ⊕ [**タスクの追加**] をクリックして、トリガー条件として機能するタスクを追加します。[**ステータス**] リストと空の [**タスク**] 項目が追加されます。 2. 空の項目をクリックしてタスクを追加します。 タスク選択ダイアログが開き、次の列とともにタスクの一覧が表示されます。[**名前**]、タスクに接続した [**アプリ**]、タスク名である [**タグ**]。 3. タスクをダブルクリックし、トリガー条件として使用します。 トリガーにタスクを追加し、ダイアログを閉じます。 4. [**ステータス**] リストで、トリガー条件が [**TaskSuccessful**] または [**TaskFail**] で処理されるかどうかを選択します。 *[**タスク失敗**] のトリガー条件を持つタスクは、先行タスクが失敗の状態で完了するときだけでなく、スキップまたはエラー (リロード前にエラーが発生する場合) の状態でも開始されます。2019 年 2 月以前の Qlik Sense バージョンでは、中止状態の先行タスクによっても「タスク失敗」トリガー条件によってもタスクが開始されました。この動作を有効にするには、すべてのスケジューラー ノードの Scheduler.exe.config で「DisableLegacyTaskEventTriggerBehavior」を「false」に設定します。* トリガーに含めたい全タスクで、上記のステップを繰り返します。タスクは一度しか追加できず、トリガーにすでに追加されている場合にはタスク選択ダイアログに表示されません。タスクの間には論理的な AND があります。

*タスクを指定の順番で実行する必要はなく、[**時間制限**] は固定されていません。時間が制限に達した時に、1 つのタスクを除いてすべてのタスクが完了している場合、最初に完了したタスクは実行済みとはみなされず、期間の終わりを再計算します。トリガーは、再計算された期間にすべてのタスクが完了するのを待ちます。*

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

カスタム プロパティ

> ***カスタム プロパティ**を利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

アクション バーで [**適用**] をクリックし、変更内容を保存します。

5. ページ最下部に [**追加完了**] と表示されます。

タスク チェーンの作成

タスクは任意のパターンで連動できます。この例では、3 つの異なるアプリでデータを再読み込みするタスクチェーンを作成する方法について説明しますが、タスクチェーンは外部プログラム タスクと配布タスクにも使用できます。

- タスク 1 はアプリ A を毎時間リロードします。
- タスク 2 はアプリ B を毎日リロードします。
- タスク 3 はタスク 1 とタスク 2 が 120 分以内に実行されている場合、アプリ C をリロードします。

次の手順を実行します。

1. アプリ A の新規リロード タスクを作成します。
   a. QMC を開く: *https://<QPS サーバー名>/qmc*
   b. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Tasks (タスク)**] を選択して、概要を表示します。
   c. データ マネージャーでテーブルの ⊕ **新規作成** をクリックします。
   [**リロード タスク編集**] ページが表示されます。
   d. [**名前**] 項目に *「Task 1」* と入力します。
   e. [**アプリ名**] 項目で [**アプリ選択**] をクリックします。開くダイアログでアプリ A をダブルクリックします。ダイアログが閉じ、[**アプリ名**] 項目にアプリ A が表示されます。
   f. [**実行**] プロパティはそのままにします。
   g. [**アクション**] を ▼ [**トリガー**] 表見出しでクリックして [**毎時間 トリガーを新規作成**] を選択します。トリガーが [**トリガー**] 表に追加されます。トリガーの開始値は作成時には 5 分に設定されます。
   h. [**適用**] をクリックします。

   [**追加されました**] と表示されます。
2. 次のステップでは アプリ B のリロード タスクを作成します。

a. 左側の選択パネルで[**タスク**] をクリックします。
[**タスク**] の概要が表示されます。

b. データマネージャーでテーブルの**新規作成** をクリックします。
[**リロードタスク編集**] ページが表示されます。

c. [**名前**] 項目に*「Task 2」*と入力します。

d. [**アプリ名**] 項目で [**アプリ選択**] をクリックします。開くダイアログでアプリB をダブルクリックします。
ダイアログが閉じ、[**アプリ名**] 項目にアプリB が表示されます。

e. [**実行**] プロパティはそのままにします。

f. [**アクション**] を▼ [**トリガー**] 表見出しでクリックして [**毎日トリガーを新規作成**] を選択します。

g. トリガーをダブルクリックし、[**開始時間**] を*「12:00」*に設定して [**OK**] をクリックします。
ダイアログが閉じます。

h. [**適用**] をクリックします。

[**追加されました**] と表示されます。

3. 次のステップでは アプリC のリロードタスクを作成します。

a. 左側の選択パネルで[**タスク**] をクリックします。
[**タスク**] の概要が表示されます。

b. アクションバーで**新規作成** をクリックします。
[**リロードタスク編集**] ページが表示されます。

c. [**名前**] 項目に*「Task 3」*と入力します。

d. [**アプリ名**] 項目で [**アプリ選択**] をクリックします。開くダイアログでアプリC をダブルクリックします。
ダイアログが閉じ、[**アプリ名**] 項目にアプリC が表示されます。

e. [**実行**] プロパティはそのままにします。

f. [**アクション**] を▼ [**トリガー**] 表見出しでクリックして [**タスクイベントトリガーを新規作成**] を選択します。
[**他のタスクの開始によりトリガー**] ダイアログが表示されます。

g. [**トリガー名**] 項目で、たとえば*「My trigger」*と入力します。

h. このトリガーは、既定では [**有効**] になっています。

i. [**時間制約**] を*120* 分に設定します。

j. [**タスクの追加**] をクリックします。表示される空の項目をクリックしてから、開いたダイアログでタスク 1 をダブルクリックし、ドロップダウンは [**タスク成功**] のままにします。

k. [**タスクの追加**] をクリックします。表示される空の項目をクリックしてから、開いたダイアログでタスク 2 をダブルクリックし、ドロップダウンは [**タスク成功**] のままにします。

l. [**OK**] をクリックします。
トリガーダイアログが閉じます。

m. [**適用**] をクリックします。

[**追加されました**] と表示されます。

これでタスクチェーンが作成され、タスクがタスクの概要に追加されました。ここをクリックすると タスクチェーンを表示できます。

循環タスクチェーンの作成

それ自体をトリガーするリロードタスク(循環タスクチェーン) を作成できます。この例では単純なタスクチェーンの作成方法について説明しています。タスクは任意のパターンで連動できます。

次の手順を実行します。

1. 循環タスクチェーンを作成したいアプリにタスクが適用されていない場合、アプリの新規リロードタスクの作成から始めます。
    a. 選択 **Create new** from **Tasks** overview.

    > *Alternatively, select* ***Create new*** *from* ***Apps*** *overview* > ***Edit*** > ***Associated items*** > ***Tasks***.

    a. タスクを作成します。
    b. [**適用**] をクリックします。
    [**追加されました**] と表示されます。
2. タスクの編集を続けて循環タスクチェーンを作成します。
    a. [**Triggers**] > [**Actions**] > [**Create new task event trigger**] と選択します。
    b. [**トリガー名**] を入力します。
    c. データマネージャーでテーブルの **Add task event**.
    [**トリガー**] ダイアログが開きます。
    d. [**タスク成功**] の右側の空の項目をクリックして開くダイアログで現在編集中のタスクと同じタスクをダブルクリックします。
    タスクが [**トリガー**] ダイアログに追加されます。
    e. ドロップダウンリストから、[**タスク成功**] あるいは [**タスク失敗**] のいずれかのトリガー条件を選択します。
    f. [**OK**] をクリックします。
    ダイアログが閉じます。
    g. [**適用**] をクリックします。

    [**更新されました**] と表示されます。

これで循環タスクチェーンが作成され、タスクがタスク概要に追加されました。From the overview you can click to view the task chain.

タスクチェーンの表示

リロードタスクおよびアプリのトリガーを作成することにより、さまざまなパターンでタスクチェーンを作成できます。タスク概要ページからタスクチェーンダイアログボックスにアクセスし、選択されたタスクのリロードをトリガーするタスクについての情報を取得することができます。

> *タスクは 循環タスクチェーンでそれ自体をトリガーできます。*

次の手順を実行します。fmaster

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Tasks (タスク)**] を選択して、概要を表示します。

   フィルタリング オプションを使用して列にフィルターを適用できます。

3. 選択したタスク上で🔗をクリックします。
   [**タスク チェーン**] ダイアログが開きます。選択されたタスクは強調表示され、ダイアログの左側の矢印がタスク概要ページの選択されたタスクを指し示します。ダイアログ ボックスにはタスク チェーンに関する情報が表示されます。タスクを管理するために実施できるアクションは次のとおりです。
   - [**Preceding tasks**] には、完了した際に選択したタスクを開始するタスクが表示されます。これは 1 つのタスクにすることもできますが、一定時間内にすべて完了させる複数のタスクにすることもできます。をクリックしてリストを展開し、▶をクリックして折りたたみます▼.
   - [**後続タスク**] には選択されたタスクが完了した際に開始されるタスクが表示されます。選択されたタスクはそれ自体が別のタスクをトリガーすることもできますが、別のタスクと連動してトリガーすることもできます。をクリックしてリストを展開し、▶をクリックして折りたたみます▼.

     以下の2 種類のレベルのタスクが表示されます。

   - 各タスクの左側に表示されるタスクの状態を更新したい場合は、ダイアログ見出しの🔄をクリックします:
     •••未開始: タスクは開始されていません。
     🔄 トリガー: タスクを実行する要求がスケジューラに送信されました。
     🔄 開始: タスクが開始されました。
     ⧗ キュー: タスクはキューに入れられ、先行するタスクが処理されると開始されます。キューイングは、**最大同時リロード**の値によって制御されます。*スケジューラの編集 (page 422)* を参照してください。
     🔄 中止の開始: マネージャー スケジューラは中止要求を受け取りましたが、処理を開始していません。
     🔄 中止中: マネージャー スケジューラが中止要求の処理を開始しました。
     ☒ 中止: タスクは中止されました。
     ✔成功: タスクの実行は成功しました。
     ✘失敗: タスクは実行のためにワーカー スケジューラに送信されましたが、完了できませんでした。例えば、データ接続に対する読み取り権限がないか、リロード スクリプトにエラーがあるため、リロードが失敗する可能性があります。
     •••スキップ: タスクの開始が要求されましたが、何らかの理由でタスクの実行が開始されていません。例えば、タスクが有効になっていない可能性があります。
     🔄 再試行中: タスクの開始に失敗し、新しい試行が開始されました。
     ✘エラー: タスクは実行のためにワーカー スケジューラに正常に送信されず、エラーが返されました。例えば、タスクを実行するために使用できるワーカー スケジューラがない場合、またはアプリケーションが別のタスクによってすでに更新されている場合に、エラーが発生する可能性があります。

••• リセット: 現在のステータスが非ターミナルの場合、つまり実行がまだ終了していないトリガー、起動、キューなどの状態の場合に、マネージャー スケジューラが起動時にタスクに設定する状態。

- タスクを手動で開始するには、タスクのとなりの [**開始**] をクリックします。
- タスクを手動で停止するには、タスクのとなりの [**停止**] をクリックします。
- ダイアログを閉じたい場合は、ダイアログの外側をクリックします。
- ダイアログ内でタスクをダブルクリックします。
  タスク概要ページが表示され、ダブルクリックしたタスクが選択されます。を🔗クリックするとタスクに適用されたタスクチェーンが表示されます。

これで、タスクのタスクチェーン概要が表示されます。

タスクの編集

更新権限を有するタスクを編集できます。タスクの概要ページからタスクを編集する方法を以下に説明します。

> *[**アプリ**] と[**ユーザーディレクトリコネクタ**] のアプリやユーザーディレクトリと関連するタスクを編集できます。該当する概要でアプリやユーザーディレクトリコネクタを選択して、[**Tasks**] タブをクリックしてタスクを選択し、[**Edit**] をクリックします。*

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Tasks (タスク)**] を選択して、概要を表示します。
3. 編集するタスクを選択します。
4. ページの最下部にあるアクション バーで [**編集**] をクリックします。
5. プロパティを編集します。
   [**有効化**] チェックボックスを選択または選択解除して、タスクを有効または無効にします。

   > *[**タスク**] 概要のページから、一度に複数のタスクを有効または無効にできます。*

   ID
   全項目が必須で、空欄のままにはできません。

ID プロパティ

プロパティ	説明	既定値
[**名前**]	タスクの名前。	<アプリ名> のタスクのリロード。
[**アプリ**]	タスクが作成されたアプリの名前。項目をクリックしてダイアログを開き、タスクがリロードするアプリを (ダブルクリックして) 選択します。	<App name>

実行

実行プロパティ

プロパティ	説明	既定値
[有効化]	選択されている場合、タスクは有効です。	選択済み
部分的なリロード	部分的なリロードでは、データモデルの既存のテーブルをすべてリロードすることなく、新しいデータを追加することができます。フル リロードでは、すべてのテーブルを削除してから、ロード スクリプトを実行します。部分的なリロードでは、新しいデータを追加するだけで、既存のテーブルは維持されます。 部分的なリロードには、完全なリロードと比較していくつかの利点があります。 • 最近変更されたデータのみをロードする必要があるため、より高速です。データセットが大きい場合、違いは大きくなります。 • ロードされるデータが少ないため、消費されるメモリも少なくなります。 • ソース データへのクエリがより高速に実行され、ネットワークの問題のリスクが軽減されるため、信頼性が向上します。	選択されていない
[タスク セッション タイムアウト (分)]	タスクが停止するまでの最大時間 タスクが開始すると、マネージャー スケジューラによってセッションが開始、ノードの 1 つによってタスクが実行されます。セッションがタイムアウトすると、マネージャー スケジューラは強制的にノードにタスクを中止させて、セッションを削除します。	1440
[最大リトライ数]	スケジューラが失敗したタスクの再起動を試みる最大回数。	0

トリガー (スケジュール済み)

スケジュール済みトリガーのプロパティ

プロパティ	説明
[トリガー名]	トリガーの名前。必須。
[有効化]	トリガーの状態。選択するとトリガーはアクティブになります。

プロパティ	説明
[**タイムゾーン**]	オペレーティング システムのタイム ゾーンがトリガーを作成した時間になります。トリガーを保存すると設定は保持され、タイムゾーンが違う場所に行っても元の設定値のまま表示されます。タイム ゾーンやトリガーの開始時間を変更したい場合は手動で行う必要があります。 *タイム ゾーンの設定より前に作成されたトリガーについては、日時はすべてデフォルトで Coordinated Universal Time (UTC: 協定世界時) にて表示されます。*
[**夏時間**]	夏時間を考慮する方法。 [**夏時間を使用する**]: このオプションでは夏時間 (DST) が考慮されます。選択したタイム ゾーンで DST が使われていると、実行日時はそれに応じて調整されます。 [**常に標準時**]: このオプションでは DST は考慮されません。選択したタイム ゾーンで DST が使われていても、実行日時は調整されません。 [**常に夏時間**]: このオプションでは DST が考慮されません。タイム ゾーンで DST が使われている場合は、DST の適用期間外でも実行日時は常に DST に準じます。 *DST を使用しないタイム ゾーンの場合は、常に [**永久標準時**] を選択します。* 1 月にカナダのオタワで午前 10 時に開始するイベントのトリガーを作成したとします。ここのタイム ゾーンは (GMT-0500) 東部標準時 (米国およびカナダ) で DST の期間は 3 月から 11 月です。 [**夏時間を使用する**] を選択すると、10 時に開始するよう設定されたトリガーは常に 10 時に開始します。 [**常に標準時**] を選択すると、10 時に実行するよう設定されたトリガーは冬は 10 時に実行されますが夏は 9 時に実行されます。 [**常に夏時間**] を選択すると、10 時に実行するよう設定されたトリガーは冬は 11 時に、夏は 10 時に実行されます。
[**Start**]	開始時間と開始日: • 開始時間: [**(hh:mm)**] • 開始日: **(YYYY-MM-DD)**

プロパティ	説明

[スケジュール]	トリガーの頻度。
	• [**1 回**]。
	• [**時間単位**]。トリガー実施の間隔。次の値を入力して、[**各条件の後に繰り返す**]を編集します。
	  • [**s (時間単位**] (既定 1 時間)
	  • [**s (分単位**] (既定 0 分)
	• [**日単位**]。トリガー実施の間隔。[**Every**][**s (日おき**] (既定 1 日) の値を入力します。たとえば、2 と入力すると2 日おきにトリガーが繰り返されます。
	• [**週単位**]。トリガー実施の間隔:
	  • [**Every**][**s (週おき**] (既定 1 週) の値を入力します。
	  • [**平日**] のチェックボックスを選択して (複数日可)、トリガーが繰り返される日を決めます (ユーザーが指定する週で)。たとえば、3 と入力して [**月曜日**] を選択すると、3 週おきの月曜日にトリガーが実行されます。
	• [**月単位**]。[**On these days**] のチェックボックスを選択 (複数可) すると、毎月トリガーが繰り返し実行される日を定義できます。
	  *[**Monthly**] を選択し、トリガーが毎月繰り返されるようにするには、28 日よりも前の日を選択する必要があります。*
	• ***カスタム***: [**カスタム**] を選択すると、[**フィルター**] と [**増分**] の 2 つの新しい項目が表示されます。これらのオプションは、リロードをスケジュールするときに大きな柔軟性を提供します。詳細は、「*タスク- カスタム オプション (page 228)*」を参照してください。

[**終了**]	終了時間と終了日: • 終了時間: [**(hh:mm)**] • 終了日:**(YYYY-MM-DD)** [**無期限**] を選択して、終了日のないトリガーを作成します。

トリガー (タスク イベント)

タスク イベント トリガーのプロパティ

プロパティ	説明
[トリガー名]	トリガーの名前。必須。

プロパティ	説明
[**タイプ**]	トリガーのタイプ。
[**有効化**]	トリガーの状態。選択するとトリガーはアクティブになります。
[**時間制限**]	タスクチェーンの他のタスクを完了しなければならない期間 (分単位)。トリガーがひとつのタスクだけで構成されている場合、何も起きません。 *タスクチェーンの作成 (page 355)*
[**タスク**]	
	次の手順を実行します。 1. ⊕ [**タスクの追加**] をクリックして、トリガー条件として機能するタスクを追加します。[**ステータス**] リストと空の [**タスク**] 項目が追加されます。 2. 空の項目をクリックしてタスクを追加します。 タスク選択ダイアログが開き、次の列とともにタスクの一覧が表示されます。[**名前**]、タスクに接続した [**アプリ**]、タスク名である [**タグ**]。 3. タスクをダブルクリックし、トリガー条件として使用します。 トリガーにタスクを追加し、ダイアログを閉じます。 4. [**ステータス**] リストで、トリガー条件が [**TaskSuccessful**] または [**TaskFail**] で処理されるかどうかを選択します。 *[**タスク失敗**] のトリガー条件を持つタスクは、先行タスクが失敗の状態で完了するときだけでなく、スキップまたはエラー (リロード前にエラーが発生する場合) の状態でも開始されます。2019 年 2 月以前の Qlik Sense バージョンでは、中止状態の先行タスクによっても「タスク失敗」トリガー条件によってもタスクが開始されました。この動作を有効にするには、すべてのスケジューラー ノードの Scheduler.exe.config で「DisableLegacyTaskEventTriggerBehavior」を「false」に設定します。* トリガーに含めたい全タスクで、上記のステップを繰り返します。タスクは一度しか追加できず、トリガーにすでに追加されている場合にはタスク選択ダイアログに表示されません。タスクの間には論理的な AND があります。

*タスクを指定の順番で実行する必要はなく、[**時間制限**] は固定されていません。時間が制限に達した時に、1 つのタスクを除いてすべてのタスクが完了している場合、最初に完了したタスクは実行済みとはみなされず、期間の終わりを再計算します。トリガーは、再計算された期間にすべてのタスクが完了するのを待ちます。*

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

カスタム プロパティ

***カスタム プロパティ**を利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

ユーザー同期化タスクのプロパティ

全項目が必須で、空欄のままにはできません。

ID プロパティ

プロパティ	説明	既定値
名前	タスクの名前	ユーザー ディレクトリ コネクタを新規作成すると、ユーザー ディレクトリ コネクタ名から自動生成されます。
有効化	選択されている場合、タスクは有効です。	有効化

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

***カスタム プロパティ**を利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

6. アクション バーで [**適用**] をクリックし、変更内容を保存します。

ページの最下部に [**更新完了**] と表示されます。

タスクの削除

削除権限を有するタスクを削除できます。

*[**アプリ**] と[**ユーザー ディレクトリ コネクタ**] のアプリやユーザー ディレクトリと関連するタスクを削除できます。*

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMCスタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Tasks (タスク)**] を選択して、概要を表示します。
3. 削除するタスクを選択します。

   フィルタリング オプションを使用して列にフィルターを適用できます。
4. アクション バーの [**Delete**] をクリックします。
   [**Delete**] ダイアログが表示されます。
5. [**OK**] をクリックします。

アプリやユーザー ディレクトリ コネクタを編集できる関連ページからでも、タスクを削除できます。

タスクの有効化

タスク編集ページまたはタスク概要ページからタスクを有効にすることができます。タスク概要ページからタスクを有効にする方法を以下に説明します。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMCスタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Tasks (タスク)**] を選択して、概要を表示します。
3. 有効にするタスクを選択します。
4. アクション バーで [**More actions**] をクリックします。
   ポップアップ メニューが開きます。[**Enable**] の横の数字は、有効化できるアイテムの数を示します。
5. [**Enable**] をクリックします。
   タスク概要の [**有効**] 列に が表示されます。✔.

これでタスクが有効になりました。

*タスクを編集する際のプロパティ[**Execution**] でもタスクを有効にできます。*

タスクの無効化

タスク編集ページまたはタスク概要ページからタスクを無効にすることができます。タスクの概要ページからタスクを無効にする方法を以下に説明します。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMCスタートページから、あるいは [**Start (スタート)**] ▼ドロップダウン メニューから [**Tasks (タスク)**] を選択して、概要を表示します。
3. 有効にするタスクを選択します。
4. アクション バーで [**More actions**] をクリックします。
   ポップアップ メニューが開きます。[**Disable**] の横の数字は、無効化できるアイテムの数を示します。
5. [**Disable**] をクリックします。

タスク概要の [**有効**] 列が空になります。

タスクを編集する際にプロパティタブからでもタスクを無効にできます。

タスクの開始

手動でタスクを開始できます。タスクの概要ページからタスクを開始する方法を以下に説明します。

*[**アプリ**] と [**ユーザー ディレクトリ コネクタ**] のアプリやユーザー ディレクトリと関連するタスクを開始できます。該当する概要でアプリやユーザー ディレクトリ コネクタを選択して、[**Tasks**] をクリックしてタスクを選択し、[**Start**] をクリックします。*

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMCスタートページから、あるいは [**Start (スタート)**] ▼ドロップダウン メニューから [**Tasks (タスク)**] を選択して、概要を表示します。

   フィルタリング オプションを使用して列にフィルターを適用できます。
3. 開始するタスクを選択します。ページ最下部のアクション バーの [**開始**] の横の数字は、選択したアイテムの中で開始できるアイテムの数を示します。
4. [**開始**] をクリックします。
   ページの最下部に [**x 件のアイテムの開始を指示しました**] と表示されます。

トリガーでタスクを開始することも可能です。

タスクの停止

手動でタスクを停止できます。タスクの概要ページからタスクを開始する方法を以下に説明します。

*[**アプリ**] と [**ユーザー ディレクトリ コネクタ**] のアプリやユーザー ディレクトリと関連するタスクを停止できます。該当する概要でアプリやユーザー ディレクトリ コネクタを選択して、[**Tasks**] をクリックしてタスクを選択し、[**Stop**] をクリックします。*

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Tasks (タスク)**] を選択して、概要を表示します。

   フィルタリング オプションを使用して列にフィルターを適用できます。

3. 停止するタスクを選択します。[**Stop**] の横の数字は、停止できるアイテムの数を示します。
4. ページの最下部にあるアクション バーで [**Stop**] をクリックします。
   ページの最下部に [**<number> items were successfully instructed to stop**] と表示されます。

システム通知の管理

システム通知によって、モバイル デバイス上の Qlik Sense Mobile Client Managed アプリへの通知を作成して送信することができます。管理者として通知を作成し、選択されたユーザーまたはユーザーのグループに対して、モバイル デバイス上の Qlik Sense Mobile Client Managed アプリを介した配布をトリガーします。システム通知は自由形式のテキストであり、ユーザーがアクセス権を持つ Qlik Sense アプリケーションに関する有益な情報を、ユーザーに通知することができます。

システム通知は、展開時にすべてのノードに自動インストールされている Qlik の通知サービスおよび Qlik の Mobility Registrar によって実行されます。Qlik の通知サービスは、Qlik Sense Enterprise 環境の外部に対して通知を行います。ファイアウォールがアウトバウンド トラフィックをブロックした場合、外部に通知することはできません。

システム通知はシステム通知ポリシーによって定義されます。
参照先: *システム通知ポリシーの管理 (page 370)*。

システム通知およびシステム通知ポリシーの機能は、署名付きキーでライセンスが付与された Qlik Sense Enterprise on Windows インストールでのみ使用できます。ライセンスの詳細については、Qlik Sense ライセンスの資料。

システム通知の作成

システム通知の概要ページから、システム通知を作成することができます。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. スタート ページから、または [**スタート**QMC] ドロップダウン メニューから [**システム通知**] を選択し、概要を表示します。▼ ドロップダウン メニューからリソースを選択します。
3. データ マネージャーでテーブルの **新規作成** をクリックします。
   [**Edit system notification**] (システム通知の編集) ページが表示されます。
4. [**ID**] セクションで、以下のプロパティを編集します。

ID プロパティ

プロパティ	説明
タイトル	システム通知の名前。
メッセージ	システム通知によってモバイル デバイス上に表示されるメッセージ。以前に配布されています。
Application link (アプリケーション リンク)	*qliksenselink://<link to the sense application>* の形式での Qlik Sense アプリケーションへのリンク。

5. [**ユーザー**] セクションを編集して、システム通知を受け取るユーザーを選択します。
   a. 選択 [ユーザーの追加 を選択してユーザーを追加します。
      A dedicated **Users** window is displayed.
   b. Select a user from the list or search for a user by clicking the search icon.
   c. [**追加**] を選択して、選択したユーザーの追加を確定します。

   > *To remove all listed users, select* ***Remove all users****.*

6. [**User groups**] (ユーザー グループ) セクションを編集して、システム通知を受け取るユーザー グループを選択するか、新しいユーザー グループを作成します。
   a. 選択 **Add group** to add a user group.
   b. 空の項目に、追加するユーザー グループの名前を入力します。
   c.

   > *To remove a user group, select the remove icon.*

   [***カスタム プロパティ***] セクションに、このリソースに使用可能なカスタム プロパティが表示されます。利用可能なカスタム プロパティがない場合、このプロパティ グループは空になっています。ここに表示されるようにするには、このリソース タイプに使用可能なカスタム プロパティを作成する必要があります。
7. 操作バーで [**適用**] をクリックし、システム通知を作成して保存します。

システム通知の編集

システム通知の概要ページから、システム通知を編集することができます。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. スタート ページから、または [**スタート**QMC] ドロップダウン メニューから [**システム通知**] を選択し、概要を表示します。▼ドロップダウン メニューからリソースを選択します。
3. 編集するシステム通知を選択します。
4. 操作バーで [**編集**] をクリックします。
   [**Edit system notification**] (システム通知の編集) ページが表示されます。
5. [**ID**] セクションで、以下のプロパティを編集します。

ID プロパティ

プロパティ	説明
タイトル	システム通知の名前。
メッセージ	システム通知によってモバイル デバイス上に表示されるメッセージ。以前に配布されています。
Application link (アプリケーション リンク)	*qliksenselink://<link to the sense application>* の形式での Qlik Sense アプリケーションへのリンク。

6. [**ユーザー**] セクションを編集して、システム通知を受け取るユーザーを選択します。
   a. 選択 [ユーザーの追加 を選択してユーザーを追加します。
      A dedicated **Users** window is displayed.
   b. Select a user from the list or search for a user by clicking the search icon.
   c. [**追加**] を選択して、選択したユーザーの追加を確定します。

   > *To remove all listed users, select **Remove all users**.*

7. [**User groups**] (ユーザー グループ) セクションを編集して、システム通知を受け取るユーザー グループを選択するか、新しいユーザー グループを作成します。
   a. 選択 **Add group** to add a user group.
   b. 空の項目に、追加するユーザー グループの名前を入力します。
   c.

   > *To remove a user group, select the remove icon.*

8. [**カスタム プロパティ**] セクションに、このリソースに使用可能なカスタム プロパティが表示されます。利用可能なカスタム プロパティがない場合、このプロパティグループは空になっています。ここに表示されるようにするには、このリソース タイプに使用可能なカスタム プロパティを作成する必要があります。
9. 操作バーで [**適用**] をクリックし、システム通知を作成して保存します。

システム通知の削除

システム通知の概要ページから、システム通知を削除することができます。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. スタート ページから、または [**スタート**QMC] ドロップダウン メニューから [**システム通知**] を選択し、概要を表示します。▼ドロップダウン メニューからリソースを選択します。
3. 削除するシステム通知を選択します。
4. アクション バーの [**Delete**] をクリックします。

   > *[**Delete**] ダイアログが表示されます。*

5. [**OK**] を選択して、システム通知を削除します。

システム通知ポリシーの管理

システム通知ポリシーを作成して、システム通知の配布対象とするユーザーを指定することができます。システム通知ポリシーの作成によって、モバイル デバイス上で通知を受信するユーザーのプールまたはユーザーのグループをカスタマイズすることができます。

既定では、システム通知ポリシーによって、システム通知設定の [**ユーザー**] および [**User groups**] (ユーザー グループ) 項目に従って、通知の受信者を確立します。受信者のリストをさらにカスタマイズするには、カスタム プロパティを使用します。

システム通知およびシステム通知ポリシーの機能は、署名付きキーでライセンスが付与された Qlik Sense Enterprise on Windows インストールでのみ使用できます。ライセンスの詳細については、Qlik Sense ライセンスの資料。

カスタム プロパティを使用したシステム通知ポリシーのカスタマイズ

カスタム プロパティを作成し、これを使用してシステム通知ポリシーをカスタマイズすることができます。

カスタム プロパティをシステム通知ポリシーに使用するには、以下を実行する必要があります。

1. カスタム プロパティを作成し、以下のリソースに割り当てます:**ユーザー、システム通知**。
2. 通知の配布先とするユーザーにカスタム プロパティを割り当てます。
3. システム通知にカスタム プロパティを割り当てます。
4. 新しいシステム通知ポリシーを作成し、カスタム プロパティに従って通知を配布するように設定します。

次の例では、カスタム プロパティを使用してシステム通知の配布グループを作成する方法について説明しています。

例: カスタム プロパティを使用した配布グループの作成

管理者として、ユーザー グループ リストに含まれていない「品質向上仮想チーム」に通知を送信する必要があるとします。ユーザー グループ リストが社員名簿によって定義され、Qlik Sense にインポートされます。社員名簿に新しい品質向上仮想チーム グループを作成するよう要求する代わりに、新しいカスタム プロパティを作成して、システム通知ポリシーと組み合わせて使用し、品質向上仮想チームのユーザー パートを定義します。

カスタム プロパティの新規作成

次の手順を実行します。

1. QMC で、[**カスタム プロパティ**] に移動します。
2. 選択 新規作成
3. カスタム プロパティに *virtual_team* という名前を付けます。
4. [**リソース タイプ**] で、[**システム通知**] と [**ユーザー**] を選択します。
5. Under **Values**, select 新規作成
6. 次の値を入力します: *quality_improvement*。
7. [**適用**] を選択します。

選択したユーザーへのカスタム プロパティの割り当て

次の手順を実行します。

1. QMC で、[**ユーザー**] に移動します。
2. Select the users part of the Quality improvement virtual team from the list or search for users by clicking the search icon.
3. [**編集**] をクリックして、選択したユーザーを編集します。
4. [**カスタム プロパティ**] で *virtual_team* プロパティを割り当てて、*quality_improvement* の値を設定します。
5. [**適用**] を選択します。

システム通知へのカスタム プロパティの割り当て

次の手順を実行します。

1. QMC で、[**システム通知**] に移動します。
2. カスタム プロパティを割り当てるシステム通知を選択します。別の方法としては、新しいシステム通知を作成します。
3. [**編集**] をクリックして、選択したユーザーを編集します。
4. [**カスタム プロパティ**] で *virtual_team* プロパティを割り当てて、*quality_improvement* の値を設定します。
5. [**適用**] を選択します。

システム通知ポリシーの配布ルールとしてカスタム プロパティを設定

次の手順を実行します。

1. QMC で、[**System notification policies**] (システム通知ポリシー) に移動します。
2. 選択 新規作成
3. [**Conditions**] (条件) ボックスの [**Advance**] (詳細設定) セクションには、次の構文が自動入力されます。
   `((subject.targetGroups=resource.group))`
   ここで、
   - [subject] とは、システム通知を指します。
   - [targetGroups] は、システム通知のプロパティで、通知を受け取るユーザー グループを定義します。
   - [resource] は、リソース フィルターによって定義され、システム通知ポリシーで次のように定義されます。User_*
     したがって、[resource.group] はユーザーが所属するグループを定義します。
4. 自動入力された構文を必須のカスタム プロパティを指定する次の文字列に置き換えます。
   `((subject.@virtual_team=resource.@virtual_team))`
5. [**Validate rule**] (ルールの検証) をクリックします。ルールの構文がチェックされ、有効な場合は「確認」のメッセージが表示されます。
6. [**適用**] を選択します。

システム通知ポリシーの作成

システム通知ポリシーの概要ページから、システム通知ポリシーを作成することができます。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、または [**スタート**] ドロップダウン メニューから [**システム通知 ポリシー**] を選択し、概要を表示します。▼選択して、概要を表示します。
3. データ マネージャーでテーブルの **新規作成** をクリックします。
   [**Edit system notification policies**] (システム通知ポリシーの編集) ページが表示されます。
4. プロパティを編集します。

ID

ID プロパティ

プロパティ	説明	既定値
テンプレートからルールを作成	システム通知ポリシーのテンプレートを選択します。	**不特定**
Disable (無効化)	ルールをアクティブにしない場合、ルールを無効化することを選択します。	選択されていない
名前	ポリシーの名前	空
説明	ポリシーの説明	空

基本

基本プロパティ

プロパティ	説明	既定値
リソース フィルター	このリストで、ルールを適用するリソースを選択します。	**User_***
[**アクション**]	ルールのアクションを選択します。	**Notify** (通知する)

詳細設定

詳細設定プロパティ

プロパティ	説明	既定値
条件	このテキスト ボックスは、前述のポリシー エディターで行われた変更を反映します。テキスト ボックスに入力して、条件を定義できます。	((subject.targetGroups=resource.group))

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

5. 操作バーで [**適用**] をクリックし、変更内容を保存します。
   ページ最下部に [**追加完了**] と表示されます。

システム通知ポリシーの編集

システム通知ポリシーの概要ページから、システム通知ポリシーを編集することができます。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMCスタートページから、または [**スタート**] ドロップダウン メニューから [**システム通知ポリシー**] を選択し、概要を表示します。▼選択して、概要を表示します。
3. 編集するシステム通知ポリシーを選択します。
4. 操作バーで [**編集**] をクリックします。
   [**Edit system notification policies**] (システム通知ポリシーの編集) ページが表示されます。
5. プロパティを編集します。

ID

ID プロパティ

プロパティ	説明	既定値
テンプレートからルールを作成	システム通知ポリシーのテンプレートを選択します。	**不特定**
Disable (無効化)	ルールをアクティブにしない場合、ルールを無効化することを選択します。	選択されていない
名前	ポリシーの名前	空
説明	ポリシーの説明	空

基本

基本プロパティ

プロパティ	説明	既定値
リソース フィルター	このリストで、ルールを適用するリソースを選択します。	**User_***
[**アクション**]	ルールのアクションを選択します。	**Notify** (通知する)

詳細設定

詳細設定プロパティ

プロパティ	説明	既定値
条件	このテキストボックスは、前述のポリシー エディターで行われた変更を反映します。テキストボックスに入力して、条件を定義できます。	((subject.targetGroups=resource.group))

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキストボックスの下に表示されます。

6. 操作バーで [**適用**] をクリックし、変更内容を保存します。

ページの最下部に [**更新完了**] と表示されます。

システム通知ポリシーの削除

システム通知ポリシーの概要ページから、システム通知ポリシーを削除することができます。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. Select **System notification policies** in the QMC start page or from the **Start** ドロップダウン メニューからリソースを選択します。
3. 削除するシステム通知ポリシーを選択します。
4. アクション バーの [**Delete**] をクリックします。

[**Delete**] ダイアログが表示されます。

5. [**OK**] を選択して、システム通知を削除します。

ノードおよびサービスの管理

地理的に分散したマルチノードの Qlik Sense インストールの場合でも、QMC を使うと1 か所からノードを管理しサービスを運用できます:

Qlik Sense サービスの状態を確認する

Qlik Sense システムでは、ノードのエンジン、リポジトリ、プロキシ、スケジューラ サービスの状態をチェックできます。

QMC の状態の表示は、20 秒ごとに変更されます。

1 つ以上のサービスが停止している場合、停止しているサービスの数がスタート ページに表示されます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Nodes (ノード)**] を選択して、概要を表示します。
   概要の [**状態**] カラムに各 ノードのサービスの状態が表示されます。状態のテキストに関する情報については、*状態 (page 375)*をご覧ください。

   また、エンジンなど、サービスの状態をチェックしたいノードの種類をクリックすると、概要を表示できます。

3. サービスの ⓘ をクリックすると、日付と時刻などの状態に関する詳細な情報が表示されます。
   [**サービスの状態**] ウィンドウが開きます。
4. [**Service status**] ウィンドウで [**Manage node**] をクリックしてサービスを実行中のノードを編集するか、[**Cancel**] をクリックして概要に戻ります。

これでサービスの状態がチェックされました。

状態

[**状態**] 属性リストには、サービスの状態が表示されます。

属性

属性の状態

属性名	説明
実行中	サービスは正常に実行中です。
停止	サービスは停止されました。
無効化	サービスは無効になっています。サービスを有効にするには、[**スタート**] > [**ノード**] > [ノード名] > [**編集**] を選択します。

属性名	説明
(x)/(y) 件のサービスが実行中	有効なサービス (y) 件に比べて、(x) 件のサービスが実行中であることを示します。
(x)/(y) 件のサービスが停止	有効なサービス (y) 件に比べて、(x) 件のサービスが停止されていることを示します。
(z) が停止	停止したサービス (z) の名前です (1 つのサービスのみが停止した場合)。

Qlik Sense ポートの管理

本セクションは、マルチノードサイトにのみ該当します。

サイトにノードを追加する前に、通信できるポートを管理する必要があります。

ポートに関連する情報については、Qlik Sense の計画と展開 を参照してください。

次の手順を実行します。

1. セントラル ノードの Windows ファイアウォールをオフにするか、追加予定の他のサーバー (ノード) から必要な Qlik Sense ポートに接続できるように設定します。
2. 新しいノードの Windows ファイアウォールをオフにするか、または、必要な Qlik Sense ポートによるセントラル ノードや追加予定の他のサーバー (ノード) からの接続を可能にします。

参照先:

Qlik Senseのインストールとアップグレードの既定の Qlik Sense インストールのポート

ノードの設定

このセクションは、マルチノードサイトにのみ該当します。

新しいノードに Qlik Sense をインストール後、セントラル ノード上の QMC にノードを追加する必要があります。

次の手順を実行します。

1. セントラル ノード上の QMC を開く: *https://<QPS サーバー名>/qmc*
2. [**Start**] ページから [**Nodes**] を選択し、概要を表示します。
3. データ マネージャーでテーブルの **新規作成** をクリックします。
   [**Node edit**] ページが表示されます。
4. [**ID**] セクションで、ノードの [**Name**] を入力し、追加予定のサーバーの [**Host name**] (アドレス) を入力します。ホスト名は保存したら変更することはできません。ホスト名を変更するには、新しいノードを作成する必要があります。

*サーバー アドレスは、完全修飾ドメイン名形式 (node2.domain.com) にするか、マシン名形式 (node2) にする必要があります。完全修飾ドメイン名 (FQDN) を使用することをお勧めします。ホスト名としてマシン名のみを使用する場合は、仮想プロキシの [**ホスト許可リスト**] に FQDN を手動で追加する必要があります。*

5. [**Node purpose**] セクションでドロップ ダウン リストからノードの使用目的を[**Production**]、[**Development**]、[**Both**] から選択します。
6. [**Services activation**] セクションで、追加するノードにインストールするサービスをすべて選択します。
リポジトリ サービスは常に含まれます。アクティブ化しようとしたときにサービスがインストールされていなければ、インストールの完了時にプロパティが適用されます。

一番右側にあるパネルで、プロパティグループの表示/非表示を切り替えることができます。プロパティを編集するときは、プロパティ名の横に矢印 (↩) が表示されて、プロパティ値が変更されることを示します。をクリックすると、↩その特定のプロパティ値がリセットされます。

7. [**適用**] をクリックして、ノードを作成および保存します。
プロセスを追加するノードが起動します。セントラル ノードのセキュア証明書はパッケージされパスワード保護されて新しいノードに送信されます。
完了すると、ページの最下部に [**Successfully added**] というメッセージが表示され、承認パスワードを示すダイアログが表示されます。

*[**ホスト名**] の入力を間違えると、[**ノードを登録できませんでした**] というエラー メッセージが表示されます。ホスト名は保存後に変更できないため、正しいホスト名で新しいノードを作成する必要があります。*

*必須項目が空欄の場合は、[**Apply**] をクリックできません。[**適用**] をクリックしないで編集ページから移動しようとすると、未保存の変更があることを示すダイアログが表示されます。[**キャンセル**] をクリックすると、編集を続けることができます。QRS との通信に失敗するとエラー メッセージが表示されます。その後、編集を続行するか、再度 [**Apply**] をクリックします。*

8. URL と承認パスワードをメモしてください。

ノードの証明書を認証

このセクションは、マルチノード サイトにのみ該当します。

セントラル ノードにノードを新規に設定して、証明書認証の URL およびパスワードを受け取った後、ホスト名のマシンで証明書を認証する必要があります。

インストールした各ノードで、この手順を実行する必要があります。

次の手順を実行します。

1. リモートデスクトップ経由で新しいノードと接続します。

   *セントラル ノード上で新しいノードを設定していない場合は、[**Certificate setup**] ダイアログが表示され、サービスがロックされ、(QMC) にマシンを追加する必要があることを示します。*

2. 新しいノードで Web ブラウザを開き、ノードの設定時にセントラル ノードで取得した URL を入力します。
   ノードの設定 (page 376)
   パスワードの入力を求められます。
3. 承認パスワードを入力し、[**送信**] をクリックします。
   新しいノードがセントラル ノードに接続され、[**証明書の設定**] ダイアログにサービスのロックが無事に解除されたことが示されます。

   [証明書の設定] ダイアログに Qlik Sense 証明書パッケージのインストールに失敗したことを知らせるメッセージが表示される場合は、QMC を使用してノードを再配置します。問題が解決しない場合は、ログ ファイルで詳細を確認します。

これでノードが追加され、稼働できるようになりました。

リポジトリの編集

更新権限のあるリポジトリは、編集できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. Select **Repositories** on the QMC start page or from the **Start** ドロップダウン メニューからリソースを選択します。
3. 編集するリポジトリを選択します。
4. アクション バーで [**編集**] をクリックします。
   複数のスケジューラが選択され、特定の項目の値と異なる場合は、項目名に [**複数の値**] と表示されます。
5. プロパティを編集します。

   ID
   全項目が必須で、空欄のままにはできません。

   ID プロパティ

プロパティ	説明	デフォルト値
[ノード]	リポジトリ名。	ノード名を継承します。

   ログ
   [**ログ**] プロパティグループには、Qlik Sense システムの Qlik Sense Repository Service (QRS) のログ プロパティとトレース プロパティが含まれています。

リポジトリログのプロパティ

プロパティ	説明	デフォルト値
[**監査アクティビティログ レベル**]	ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**Basic (基本)**]: 限定的なエントリのセット	基本
[**監査セキュリティログ レベル**]	ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**Basic (基本)**]: 限定的なエントリのセット	基本
[**サービス ログ レベル**]	ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**エラー**]: エラーのエントリのみ • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる	Info

[**トレース**]

トレース設定情報

設定	説明	値
[**アプリケーション ログ レベル**]	リポジトリサービスのあらゆるアプリケーション メッセージがこのロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info

[**監査 ログ レベル**]	セキュリティルールの情報など、詳細なユーザー ベース メッセージはこのロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info
[**ライセンス ログ レベル**]	ライセンス メッセージはすべて、このロガーに保存されます。トークンの使用やユーザー アクセスの割当などです。 ドロップダウンから、ロガーの冗長性を設定します。 • [**情報**]: 致命的なエラー、警告、情報エントリ • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info
Qlik Management Console(QMC) ログ レベル	QMC メッセージはすべて、このロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info
[**パフォーマンス ログ レベル**]	リポジトリサービスのパフォーマンス メッセージはすべて、このロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info

[**セキュリティ ログ レベル**]	証明書メッセージはすべて、このロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info
[**同期 ログ レベル**]	マルチノード環境の同期情報はすべて、このロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info
[**システム ログ レベル**]	標準的なリポジトリメッセージはすべて、このロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info

[**ユーザー管理 ログ レベル**]	ユーザー同期 メッセージはすべて、このロガーに保存 されます。 エラー: ユーザー インポートの失敗、またはユーザー ディレクトリ コネクタの設定が不適正な理由。 警告: データ ソースでの潜在的なエラー (アクティブ ディレクトリ グループでの循環依存など)。 情報: エンジンの開始と進捗状況、またはユーザー インポートの開始およびユーザー インポートの結果 (ユーザーおよびユーザー グループの数など)。 デバッグ: アクティブ ディレクター/LDAP サーバーへのユーザー リクエスト文字列、または ODBC ソースへの SQL ユーザー クエリ。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info

Qlik Sense ログ フォルダへの既定のパスは、%ProgramData%\Qlik\Sense\Log\<サービス> です。

タグ

タグ プロパティ

プロパティ	**説明**
[***タグ***]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

カスタム プロパティ

***カスタム プロパティ**を利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

6. [**適用**] をクリックして変更を保存します。

ページの最下部に [**更新完了**] と表示されます。

ノードの作成

1 つ以上のノードを作成して、マルチノードサイトで使用できます。展開内で各ノードに特定のロールを割り当てて、リソースの計画をサポートします。たとえば、ノードにより予定のリロードを実行するか、またはユーザーにコンテンツを表示するかを指定します。

ノードを作成すると、関連のあるサービスも作成され、ノード名、レポジトリ、エンジン、印刷、プロキシ、スケジューラーが継承されます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Nodes (ノード)**] を選択して、概要を表示します。
3. データ マネージャーでテーブルの **新規作成** をクリックします。
4. プロパティの項目を入力します。

ID

全項目が必須で、空欄のままにはできません。

ID プロパティの説明

プロパティ	説明
[**名前**]	ノード名。
[**ホスト名**]	ホスト名。ノードを作成したら、ホスト名は編集できません。サーバー アドレスは、完全修飾ドメイン名形式 (`node2.domain.com`) にするか、マシン名形式 (`node2`) にする必要があります。 *完全修飾ドメイン名 (FQDN) を使用することをお勧めします。ホスト名としてマシン名のみを使用する場合は、仮想プロキシの [**ホスト許可リスト**] に FQDN を手動で追加する必要があります。* *IPv6 アドレスをホスト名として使用する方法もサポートされています。*

ノードの目的

ドロップダウン リストからノードの使用目的を選択します。[**実稼働環境**]、[**開発環境**]、または [**両方**]。この設定は、追加される各ノードの QMC で定義されます。選択するノードの目的に応じて、異なるプロパティがノードに適用されます。適用されるプロパティは、負荷分散ルールに使用したり、アクセスを制御するセキュリティルールに使用したりすることができます。
異なるオプションを選択する場合、以下の影響があります。

- **実稼働環境**: このサーバーは、ユーザーがアプリにアクセスするのをサポートすることを目的としていますが、アプリを作成することはできません。ユーザーがこのノードに接続するとき、ハブの [**アプリの新規作成**] ボタンはユーザーに表示されません。ハブの [**Work (ワーク)**] セクションを非表示にするには、そのアプリケーション所有者にアクセス権を付与するセキュリティルールを無効にする必要があります。ユーザーがこのノードに接続するとき、アプリおよび [**Work**] (ワーク) セクションを作成するためのハブのボタンはユーザーに表示されません。実稼働環境のノード上でアプリを編集することはできません。
- **開発環境**: このサーバーは、ユーザーがアプリを作成できるようにすることを目的としていますが、公開済みのアプリを消費するための通常のユーザー トラフィックは処理されません。機能の作成と編集は有効化されています。
- **両方**: この設定では、ノードで両方のアクティビティを実行できます。つまり、通常のユーザー トラフィックが処理され、ユーザーはアプリを作成することもできます。

ノード構成

このセクションは Shared Persistence インストールをお持ちの場合にのみ利用可能です。

マルチノード環境の場合、1 つ以上のノードを**フェールオーバー候補**に選択できます。フェールオーバーのシナリオの場合、セントラル ノードが動作を停止すると、1 つの**フェールオーバー候補**がセントラル ノードのロールを担います。この解決策によって、単一障害点であるセントラル ノードに関わるリスクがなくなります。
フェールオーバー候補の要件は、リポジトリ、エンジン、プロキシ、スケジューラーといったサービスがアクティブであることです。これらのサービスすべてがアクティブになっていないノードは、フェールオーバー候補になれません。

*新しいノードを作成するときにだけ、**フェールオーバー候補**に指定できます。ノードの作成後、そのノードを**フェールオーバー候補**にすることはできず、**フェールオーバー候補**の選択を取り消すこともできません。*

ノード ロール
フェールオーバー ノードにデフォルトで割り当てられるロールです。

ノード ロール

ロール	説明
スケジューラー マスター	Qlik Sense サイト内のスケジュール済みリロード タスクとユーザーの同期タスクを実行します。
ライセンス保守管理者	Qlik Sense サイト内のライセンスとトークンの保守を行います。
ユーザー シンクロナイザー	Qlik Sense サイト内のユーザーの同期を行います。
ノード レジスター	Qlik Sense サイト内のノードの登録と削除を行います。
アプリ マネージャー	Qlik Sense サイト内のアプリの管理を行います。

ロール	説明
データベース クリーナー	Qlik Sense サイト内のデータベースのクリーニングを行います。

サービスのアクティブ化

含めるサービスを選択します。アクティブ化しようとしたときにサービスがインストールされていなければ、インストールの完了時にプロパティが適用されます。

サービスの説明

プロパティ	説明
[リポジトリ]	Qlik Sense Repository Service (QRS) が必ず含まれています。
[エンジン]	Qlik Sense Engine Service (QES)。
[印刷]	Qlik Sense Printing Service (QPR)。
[プロキシ]	Qlik Sense Proxy Service (QPS)。
[スケジューラ]	Qlik Sense Engine Service (QSS)。

タグ

タグ プロパティ

プロパティ	説明
[タグ]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

カスタム プロパティ

***カスタム プロパティ**を利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

[**適用**] をクリックして変更を保存します。必須の項目が空欄の場合、[**Apply**] は無効になります。

5. アクション バーで [**適用**] をクリックし、ノードを作成して保存します。
ページの最下部に [**追加されました**] というメッセージが表示され、[**承認パスワード**] のあるダイアログが表示されます。
[**ホスト名]** の入力を間違えると、[**ノードを登録できませんでした**] というメッセージが表示されます。

ノードを作成したら、ホスト名は編集できません。新しいノードを作成して正しいホスト名を入力します。

6. 承認パスワードをコピーして、ダイアログの指示に従い、ホスト名 コンピュータで証明書を承認します。

成功すると、[**証明書の設定**] ダイアログに [**サービスのロックが解除されました**] と表示されます。

7. 新しいノードでインストールしたサービスを再起動します。

これで新しいノードが作成され、ノードを機能させるための証明書が承認されました。

負荷分散

負荷分散を使用すると、異なるノード間のワークロードをさらに均等に分散できます。セントラル ノードでは、負荷分散は仮想プロキシに自動的に追加されますが、その他のノードでは負荷分散を使用して仮想プロキシを主導で構成する必要があります。新しい仮想プロキシを作成する場合、負荷分散を追加して、仮想プロキシが作業を転送するノードを選択して構成する必要があります。

ノードの編集

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Nodes (ノード)**] を選択して、概要を表示します。
3. 編集するノードを選択します。
4. アクション バーで [**編集**] をクリックします。
5. プロパティを編集します。

ID

全項目が必須で、空欄のままにはできません。

ID プロパティの説明

プロパティ	説明
[**名前**]	ノード名。
[**ホスト名**]	ホスト名。ノードを作成したら、ホスト名は編集できません。サーバー アドレスは、完全修飾ドメイン名形式 (`node2.domain.com`) にするか、マシン名形式 (`node2`) にする必要があります。 *完全修飾ドメイン名 (FQDN) を使用することをお勧めします。ホスト名としてマシン名のみを使用する場合は、仮想プロキシの [**ホスト許可リスト**] に FQDN を手動で追加する必要があります。* *IPv6 アドレスをホスト名として使用する方法もサポートされています。*

ノードの目的

ドロップダウン リストからノードの使用目的を選択します。[**実稼働環境**]、[**開発環境**]、または [**両方**]。

この設定は、追加される各ノードの QMC で定義されます。選択するノードの目的に応じて、異なるプロパティがノードに適用されます。適用されるプロパティは、負荷分散ルールに使用したり、アクセスを制御するセキュリティルールに使用したりすることができます。
異なるオプションを選択する場合、以下の影響があります。

- **実稼働環境**: このサーバーは、ユーザーがアプリにアクセスするのをサポートすることを目的としていますが、アプリを作成することはできません。ユーザーがこのノードに接続するとき、ハブの [**アプリの新規作成**] ボタンはユーザーに表示されません。ハブの [**Work (ワーク)**] セクションを非表示にするには、そのアプリケーション所有者にアクセス権を付与するセキュリティルールを無効にする必要があります。ユーザーがこのノードに接続するとき、アプリおよび [**Work**] (ワーク) セクションを作成するためのハブのボタンはユーザーに表示されません。実稼働環境のノード上でアプリを編集することはできません。
- **開発環境**: このサーバーは、ユーザーがアプリを作成できるようにすることを目的としていますが、公開済みのアプリを消費するための通常のユーザー トラフィックは処理されません。機能の作成と編集は有効化されています。
- **両方**: この設定では、ノードで両方のアクティビティを実行できます。つまり、通常のユーザー トラフィックが処理され、ユーザーはアプリを作成することもできます。

ノード構成

このセクションは Shared Persistence インストールをお持ちの場合にのみ利用可能です。

マルチノード環境の場合、1 つ以上のノードを**フェールオーバー候補**に選択できます。フェールオーバーのシナリオの場合、セントラル ノードが動作を停止すると、1 つの**フェールオーバー候補**がセントラル ノードのロールを担います。この解決策によって、単一障害点であるセントラル ノードに関わるリスクがなくなります。
フェールオーバー候補の要件は、リポジトリ、エンジン、プロキシ、スケジューラーといったサービスがアクティブであることです。これらのサービスすべてがアクティブになっていないノードは、フェールオーバー候補になれません。

*新しいノードを作成するときにだけ、**フェールオーバー候補**に指定できます。ノードの作成後、そのノードを**フェールオーバー候補**にすることはできず、**フェールオーバー候補**の選択を取り消すこともできません。*

ノード ロール
フェールオーバー ノードにデフォルトで割り当てられるロールです。

ノード ロール

ロール	説明
スケジューラー マスター	Qlik Sense サイト内のスケジュール済みリロード タスクとユーザーの同期タスクを実行します。
ライセンス保守管理者	Qlik Sense サイト内のライセンスとトークンの保守を行います。

ロール	説明
ユーザー シンクロナイザー	Qlik Sense サイト内のユーザーの同期を行います。
ノード レジスター	Qlik Sense サイト内のノードの登録と削除を行います。
アプリ マネージャー	Qlik Sense サイト内のアプリの管理を行います。
データベース クリーナー	Qlik Sense サイト内のデータベースのクリーニングを行います。

サービスのアクティブ化

含めるサービスを選択します。アクティブ化しようとしたときにサービスがインストールされていなければ、インストールの完了時にプロパティが適用されます。

サービスの説明

プロパティ	説明
[リポジトリ]	Qlik Sense Repository Service (QRS) が必ず含まれています。
[エンジン]	Qlik Sense Engine Service (QES)。
[印刷]	Qlik Sense Printing Service (QPR)。
[プロキシ]	Qlik Sense Proxy Service (QPS)。
[スケジューラ]	Qlik Sense Engine Service (QSS)。

タグ

タグ プロパティ

プロパティ	説明
[タグ]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

カスタム プロパティ

***カスタム プロパティ**を利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

6. 操作バーで [**適用**] をクリックします。

ページの最下部に [**更新完了**] と表示されます。

証明書の再配布

適切な証明書を受け取っていないノードは再登録する必要があります。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Nodes (ノード)**] を選択して、概要を表示します。
3. [**状態**] カラムで [**インストールされていない証明書**] とともに表示されている、再配置するノードを選択します。
   アクション バーの [**再配布**] ボタンがアクティブになります。
4. [**再配布**] をクリックします。
   終了すると、[**承認パスワード**] のあるダイアログが表示されます。
5. 承認パスワードをコピーして、ダイアログの指示に従い、ホスト名 コンピュータで証明書を承認します。
   成功すると、[**証明書の設定**] ダイアログに [**サービスのロックが解除されました**] と表示されます。

これでノードを機能させるための証明書が再配布され、承認されました。

ノードの削除

削除権限を有するノードを削除できます。

> *ノードを削除すると、ノードに属するサービス (プロキシ、エンジン、スケジューラ) も削除されます。セントラル データベース内にある関連するエンティティによっては、ノードの削除に時間がかかる場合があります。そのため、削除したノードがしばらく表示されることがあるのでご注意ください。セントラル ノードは削除できません。*

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Nodes (ノード)**] を選択して、概要を表示します。
3. 削除するノードを選択します。
4. アクション バーの [**Delete**] をクリックします。
   [**Delete**] ダイアログが表示されます。
5. [**OK**] をクリックします。

> *削除したノードをクラスターに追加できるようにするには、ノードから証明書を削除して Qlik Sense を再インストールする必要があります。Qlik Sense をアンインストールする場合は、[**Qlik Sense 証明書とデータ フォルダーの削除**] オプションを選択します。また、手動で C:\ProgramData\Qlik フォルダーを削除できます。*

プロキシの編集

更新権限を有するプロキシを編集できます。

> *セキュリティ上の理由で、既定の仮想プロキシの一部の設定は編集できません。*

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMCスタートページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Proxies (プロキシ)**] を選択して、概要を表示します。
3. 編集するプロキシを選択します。
4. アクション バーで [**編集**] をクリックします。
5. プロパティを編集します。

ID

全項目が必須で、空欄のままにはできません。

ID プロパティ

プロパティ	説明	デフォルト値
[ノード]	プロキシ名。	ノード名を継承します。

ポート

ポートプロパティ

プロパティ	説明	既定値
サービスの待ち受けポート HTTPS (既定)	既定のプロキシのセキュアな待ち受けポートで、Qlik Sense 通信をすべて管理します。 *ポート443 は他のソフトウェア(Web サーバーなど) によって使用されることがあるため、Qlik Sense Proxy Service (QPS) がこのポートを使用できることを確認してください。* *既定の受け入れポート443 または 80 をQMC で変更すると、QMC またはハブに移動できるよう、URL で新たなポート番号を使用する必要があります。その後、QMC アドレスは https://<QPS サーバー名>:Service listen port HTTP/qmc となります。*	443
認証の待ち受けポート	内部認証モジュールの待ち受けポート。 *管理者権限のないユーザーとしてこのポートを編集する場合、変更を有効にするには、起動モードでレポジトリを実行する必要があります。*	4244
Kerberos 認証	選択するとKerberos 認証を有効にします。 *Kerberos 認証のセットアップの構成に誤りがあると、自分をQMC からロックアウトしてしまう危険性があります。*	選択されていない

プロパティ	説明	既定値
REST API 待ち受けポート	プロキシ API の待ち受けポート。 *管理者権限のないユーザーとしてこのポートを編集する場合、変更を有効にするには、起動モードでレポジトリを実行する必要があります。*	4243
HTTP 許可	プロキシのプロパティ[**Allow HTTP**] を選択する場合、暗号化されていない通信が許可されます。つまり、https (セキュアな通信) とhttp (暗号化されていない通信) の両方が許可されます。その後、QMC アドレスは *https://<QPS server name>:Service listen port HTTP/qmc* になります(ここで、*https* は *http* で置換できます)。QMC の既定のアドレスは、*https://<QPS サーバー名>/qmc*です. *プロパティ[**HTTP 許可**] を変更すると、(Qlik Sense ユーザーまたは、QMC 管理ユーザーが作成した) Web ブラウザーのすべてのブックマークが無効になります。* *[**HTTP 許可**] をチェックすると、[**サービスの待ち受けポートHTTP**] の設定が必要です。* *ユーザーは複数の異なるプロトコルを使って、複数のエンジンセッションを持つことはできません。*	False (不許可)
サービスの待ち受けポート HTTP	非暗号化待ち受けポート、HTTP 接続が許可されている場合に使用されます。	80

詳細設定

詳細設定プロパティ

プロパティ	説明	デフォルト値
[**最大ヘッダー行数**]	最大ヘッダー行数。	100

プロパティ	説明	デフォルト値
[**ヘッダーの最大サイズ (バイト)**]	ヘッダーの最大合計サイズ。	16384 バイト
[**Keep-alive タイムアウト (秒)**]	接続が切断されるまでの 1 回の HTTP/HTTPS リクエストの最大タイムアウト時間。DoS 攻撃 (サービス拒否攻撃) に対する防御。リクエストがこの時間を超過した場合は、Qlik Sense プロキシによって接続が切断されることを意味しています。ユーザーが接続の遅さと接続の切断で困っている場合は、この値を増やしてください。	10 秒

ログ

[**ログ**] プロパティグループには、Qlik Sense システムのプロキシ ログ プロパティとトレース プロパティが含まれています。

ログ プロパティ

プロパティ	説明	デフォルト値
[**監査アクティビティ ログ レベル**]	ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**Basic (基本)**]: 限定的なエントリのセット	基本
[**監査セキュリティ ログ レベル**]	ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**Basic (基本)**]: 限定的なエントリのセット	基本
[**サービス ログ レベル**]	ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**エラー**]: エラーのエントリのみ • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる	Info

[**トレース**]

トレース設定情報

設定	説明	値

パフォーマンス ログ間隔 (分)	パフォーマンス ログの間隔。	5 分間
[**監査 ログ レベル**]	プロキシの呼び出しなど、より詳細なユーザー ベース メッセージはこのロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info
[**パフォーマンス ログ レベル**]	パフォーマンス メッセージはすべて、このロガーに保存されます。パフォーマンス カウンタ、および接続、ストリーム、セッション、チケット、ウェブ ソケットの数、負荷分散情報などです。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info
[**セキュリティ ログ レベル**]	証明書メッセージはすべて、このロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info
[**システム ログ レベル**]	標準的なプロキシ メッセージはすべて、このロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info

Qlik Sense ログ フォルダへの既定のパスは、%ProgramData%\Qlik\Sense\Log\<サービス> です。

セキュリティ

セキュリティプロパティ

プロパティ	説明
[**SSL ブラウザ証明書捺印 (署名)**]	ブラウザからプロキシへのトラフィックの暗号化を扱う、セキュア ソケット レイヤー (SSL) 証明書の捺印。プロキシ証明書および管理者権限のないアカウントでの Qlik Sense サービス実行を編集する場合、以下のように証明書にプライベートキーのアクセス許可を設定する必要があります。 *有効にするには、証明書が秘密キーを含む必要があります。証明書は、Qlik Sense Proxy Service を実行するために使用されるユーザー アカウントのローカル コンピューター/コンピューター アカウント> MMC の個人部分にインストールされている必要があります。* *サードパーティの証明書を使用する場合、その証明書が Windows で信頼されること、その証明書を使って秘密キーが Windows 証明書ストアに保存されていることが必要です。証明書は、Qlik Sense Proxy Service を実行するために使用されるユーザー アカウントのローカル コンピューター/コンピューター アカウント> MMC の個人部分にインストールされている必要があります。* *Qlik Sense は SHA-1 や SHA-256 に基づいた署名アルゴリズムを使用して作成される証明書をサポートします。*

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

カスタム プロパティ

> *カスタム プロパティを利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

[**適用**] をクリックして変更を保存します。必須の項目が空欄の場合、[**Apply**] は無効になります。

6. [**Associated items**] でフィールドを編集します。

仮想プロキシ

仮想プロキシのプロパティ

プロパティ	説明
[**説明**]	仮想プロキシの名前。
プレフィックス	各追加パスを定義するプロキシの URI のパス名。
[**セッション クッキー ヘッダー名**]	セッション クッキーのために使用される HTTP ヘッダー名。
[**既定の仮想プロキシ**]	ステータス値:**Yes** または **No**

7. アクション バーで [**適用**] をクリックし、変更内容を保存します。

> *ほとんどの場合、変更内容を適用するときにプロキシを再起動する必要があります。このプロキシでハンドルされているセッションが終了し、ユーザーはログアウトされます。次のリソースを変更すると、プロキシは自動的に再起動しません。タグ、カスタム プロパティ、ログ (監査アクティビティ ログ レベル、監査セキュリティ ログ レベル、サービス ログ レベル)、トレース (監査ログ レベル、パフォーマンス ログ レベル、セキュリティ ログ レベル、システム ログ レベル)。*

ページの最下部に [**更新完了**] と表示されます。

負荷分散の追加

複数のエンジンと仮想プロキシをインストールする場合、新しいノードと下層プロキシに負荷分散を追加する必要があります。負荷分散が自動的に追加されるのは、セントラル ノードのみです。仮想プロキシを構成せずにノードを作成すると、ノードは実際に使用されることはありません。新しい仮想プロキシを作成する場合、負荷分散を追加して、仮想プロキシが作業を転送するノードを選択して構成する必要があります。

負荷分散で使用される既定のアルゴリズムはラウンドロビンで、マルチノード サイト上の利用可能なノード間で均等に負荷が分散されます。ただし、同じユーザー/クライアントからの後続セッションは、ラウンド ロビンに従わず、現在のエンジン ノードで開かれます。

同じユーザー/クライアント セッションは、次のリクエスト ヘッダーに含まれる情報によって決定されます:

- X-Qlik-ProxySession ヘッダー
- X-Qlik-Security ヘッダー
- X-Qlik-User ヘッダー

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**仮想プロキシ**] を選択して、概要を表示します。
3. 負荷分散を追加したい仮想プロキシを選択します。
4. [**編集**] をクリックします。
   仮想プロキシのプロパティが表示されます。
5. [**負荷分散**] プロパティで、[⊕ **新しいサーバー ノードの追加**] をクリックして、負荷分散を追加するサーバー ノードを選択します。
   ダイアログが開きます。
6. リストからノードを選択します。
7. [**追加**] をクリックします。
   ダイアログが閉じ、ノードが仮想プロキシ編集ページの [**負荷分散ノード**] リストに追加されます。
   確認のダイアログが表示されます。
8. [**OK**] をクリックします。
   ページの最下部に [**更新完了**] と表示されます。

開発ノードを分離するため負荷分散を設定

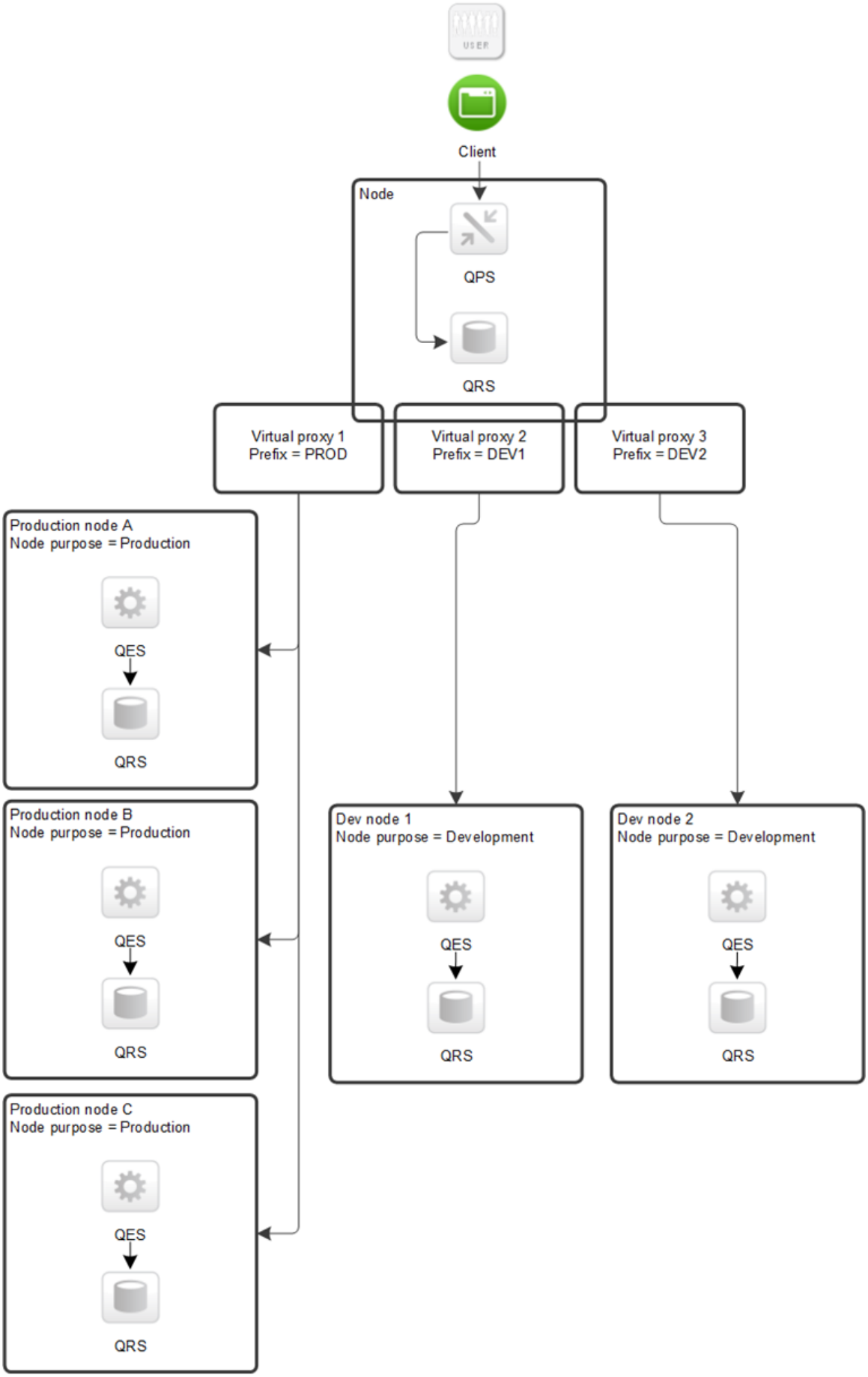
複数のエンジンと仮想プロキシをインストールする場合、新しいノードと下層プロキシに負荷分散を追加する必要があります。負荷分散が自動的に追加されるのは、セントラル ノードのみです。プロキシがローカル エンジンまたは特定のエンジンまたはエンジンのサブセットとのみ通信するように変更できます。これにより多数の実装オプションに対応でき、さまざまなシナリオをサポートできます。

アプリの負荷分散を選択的に実行するときは個別の開発ノードを使用することをお勧めします。

スクリプト作成およびリロード実行などの開発作業では、多くの場合大量のシステム リソースが必要とされます。そのため、開発作業は通常のユーザー アクティビティから離した特定のノードで行うことが有益です。

この実装シナリオでは、Qlik Sense サイトは以下のノードで構成されています。

- 実稼働ノードA
- 実稼働ノードB
- 実稼働ノードC
- 開発ノード1
- 開発ノード2
- 3 つの仮想プロキシを持つプロキシ ノードこのノードは上記のノードのうちどこでも常駐できます。


USER
Client
Node
QPS
QRS
Virtual proxy 1
Prefix = PROD
Virtual proxy 2
Prefix = DEV1
Virtual proxy 3
Prefix = DEV2
Production node A
Node purpose = Production
QES
QRS
Production node B
Node purpose = Production
QES
QRS
Production node C
Node purpose = Production
QES
QRS
Dev node 1
Node purpose = Development
QES
QRS
Dev node 2
Node purpose = Development
QES
QRS

別個の実環境 ノードと開発 ノードのあるマルチノードサイト

負荷分散の設定方法については、Qlik Community を参照してください。

負荷分散の削除

仮想プロキシから負荷分散を削除できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**仮想プロキシ**] を選択して、概要を表示します。
3. 編集する仮想プロキシを選択します。
4. [**編集**] をクリックします。
   仮想プロキシのプロパティが表示されます。
5. In the **Load balancing** property, click ⊗ next to the node you want to delete load balancing from.
6. 操作バーで [**適用**] をクリックし、変更内容を保存します。
   確認のダイアログが表示されます。.
7. [**OK**] をクリックします。

仮想プロキシの作成

仮想プロキシを使用して、認証、セッションの取り扱い、同じ物理サーバーの負荷分散の複数の設定を処理できます。1 つの構成を持つ代わりに、仮想プロキシを使用して必要に応じてサーバー数を減らすことができます。

仮想プロキシは、使用する前にプロキシ サービスにリンクしておく必要があります。リンクせずに仮想プロキシを作成することもできますが、リンクするまで仮想プロキシは使用できません。参照先: 仮想プロキシのプロキシへのリンク(page 422)

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**仮想プロキシ**] を選択して、概要を表示します。
3. [**新規作成**] をクリックします。仮想プロキシを複数のプロキシに同時に追加することはできません。
4. [**仮想プロキシの編集**] ウィンドウでプロパティを編集します。

   ID
   全項目が必須で、空欄のままにはできません。

ID プロパティ

プロパティ	説明	デフォルト値
[**説明**]	仮想プロキシの名前。	空
[**プレフィックス**]	各追加パスを定義するプロキシの URI のパス名。例: *https://[node]/[prefix]/* 次の点に注意してください。 • プレフィックスでは小文字のみを使用できます。Qlik Sense 3.0 へのアップグレード後、既存の仮想プロキシに含まれるすべての大文字は、自動的に小文字で置き換えられます。 • 使用可能な文字は、次の予約されていない文字のみです。(a-z, 0-9, "-", ".", "_" , "~"。詳細については、次のドキュメントの「非予約文字」のセクションを参照してください: Uniform Resource Identifier (URI): 一般的な構文	空
[**タイムアウトまでのセッションアイドル時間 (分)**]	タイムアウトするまでのアイドル状態の最大時間。この時間が経過すると、セッションは無効となり、ユーザーはシステムからログアウトされます。	30 分間
[**セッション クッキー ヘッダー名**]	セッション クッキーのために使用される HTTP ヘッダー名。既定ではこの値は空欄なので、値を入力する必要があります。 *February 2019 以降のリリースは、ユーザーが http を介してシステムにアクセスすると、セッションの Cookie ヘッダー名にサフィックス (-HTTP) が付加されます。* *クッキー名のサフィックスとして、上記の [**プレフィックス**] プロパティの値が含まれていると、役に立ちます。*	空

認証

認証プロパティ

プロパティ	説明	既定値
[**匿名アクセス モード**]	• **匿名ユーザーを拒否**: ユーザは、ユーザ ID と資格情報を指定する必要があります。 • **匿名ユーザーを許可**: ユーザは匿名で入力しますが、ユーザアカウントで切り替えてログインすることができます。 • **常に匿名ユーザー**: ユーザーは常に匿名です。	匿名ユーザーなし

プロパティ	説明	既定値
[**認証方法**]	• [**Ticket**]: チケットは認証に使用されます。 • [**ヘッダー認証静的ユーザーディレクトリ**]: 静的ヘッダー認証を許可します。QMC でユーザーディレクトリを設定します。 • [**ヘッダー認証動的ユーザーディレクトリ**]: 動的ヘッダー認証を許可します。ヘッダーからユーザーディレクトリの情報を取得します。 • SAML:SAML2 は認証に使用されます。 • JWT:JSON Web Token は認証に使用されます。 • OIDC:OpenID Connect は認証に使用されます。	チケット
[**ヘッダー認証ヘッダー名**]	ヘッダー認証が許可される場合、ユーザーを識別する HTTP ヘッダー名. ([**Authentication method**] プロパティに [**Header authentication static user directory**] または [**Header authentication dynamic user directory**] のいずれかを選択して) ヘッダー認証を許可する場合、必須です。 *ヘッダー認証は US-ASCII のみをサポートしています (UTF-8 はサポートしていません)。*	空
[**ヘッダー認証静的ユーザーディレクトリ**]	ヘッダー認証を受けたユーザーの追加情報を取得できるユーザーディレクトリ名。([**Authentication method**] プロパティに [**Header authentication static user directory**] を選択して) 静的ヘッダー認証を許可する場合は必須です。	空
[**ヘッダー認証動的ユーザーディレクトリ**]	([**Authentication method**] プロパティに [**Header authentication dynamic user directory**] を選択して) 動的ヘッダー認証を許可する場合、必須です。入力するパターンには '$ud' や '$id' が含まれ、これらを分離する方法も含まれている必要があります。 **ヘッダーの設定および一致の例** `$ud\\$id` – USERDIRECTORY\userid と一致させます (\を追加して、バックラッシュをエスケープする必要があります) `$id@$ud` – userid@USERDIRECTORY と一致させます ($id と$ud の順番は関係ありません) `$ud:::$id` – USERDIRECTORY:::userid と一致させます	空
[**Windows 認証パターン**]	ログイン用に選択された認証パターン。User-Agent ヘッダーに Windows 認証パターン文字列が含まれている場合、Windows 認証が使用されます。一致する文字列がない場合は、フォーム認証が使用されます。	Windows

プロパティ	説明	既定値
[**認証モジュールは URI をリダイレクトします**]	外部の認証モジュールを使用する場合、クライアントは認証のため、この URI へリダイレクトされます。	空欄 (既定モジュール: Windows 認証の Kerberos/NTLM)
SAML シングル ログアウト	SAML シングル ログアウト用にサービス プロバイダーが開始するフローを有効にする場合は、このチェック ボックスをオンにします。オンにした場合、仮想プロキシ用に生成されたメタデータ ファイルに、POST およびリダイレクト バインディング用のシングル ログアウトの場所が含められます。	空
SAML ホスト URI	クライアントに表示されるサーバー名。この名前は、クライアントが QMC などの Qlik サービスにアクセスする際に使用されます。 サーバー名はコンピュータ名と同一である必要はありませんが、ほとんどの場合、同じ名前が使用されます。 URI には http:// または https:// のいずれかを使用できます。http:// を使用するには、仮想プロキシがリンクされているプロキシの編集ページで [**Allow HTTP (HTTP を許可)**] を選択する必要があります。 ([**Authentication method**] プロパティで **SAML** を選択することにより) SAML 認証を許可する場合は必須になります。	空
SAML エンティティ ID	サービス プロバイダーを識別する ID。ID は一意にする必要があります。 ([**Authentication method**] プロパティで **SAML** を選択することにより) SAML 認証を許可する場合は必須になります。	空
[**SAML IdP メタデータ**]	IdP からのメタデータはサービス プロバイダーの構成に使用され、SAML 認証が正常に動作するために必要です。メタデータの一般的な入手方法は、IdP Web サイトからのダウンロードです。 [参照] ボタンをクリックしてアップロード用に IdP metadata .xml ファイルを開きます。エラーを回避するには、[**View content (コンテンツを表示)**] をクリックしてファイルのコンテンツと形式が正しいことを確認します。 メタデータがないと構成は未完了になります。	-
SAML ユーザー ID に使用する属性	ユーザー ID を説明する属性の SAML 属性名。名前やフレンドリな名前を使用して属性を識別できます。 *必須の SAML 属性名が分からない (page 641)*	空

プロパティ	説明	既定値
SAML ユーザーディレクトリに使用する属性	ユーザーディレクトリを説明する属性の SAML 属性名。名前やフレンドリな名前を使用して属性を識別できます。名前の値がかっこ内にある場合、その値はコンテンツの属性値として使用されます。[例] では定数属性値「例」を提供しています。 *必須の SAML 属性名が分からない (page 641)*	空
SAML 署名アルゴリズム	署名 SAML 要求に使用されるハッシュアルゴリズム。SHA-256 を使用するには、関連する秘密キーのプロバイダーが「Microsoft Enhanced RSA and AES Cryptographic Provider」である第三者機関の証明書が必要となります。	-
[**SAML 属性マッピング**]	[**新しい属性の追加**] をクリックして SAML 属性を Qlik Sense 属性にマッピングして、[**必須**] を選択することでこれらを必須とするかどうかを定義します。名前やフレンドリな名前を使用して属性を識別できます。名前の値がかっこ内にある場合、その値はコンテンツの属性値として使用されます。[例] では定数属性値「例」を提供しています。 *SAML 応答ベースの属性は、製品監査を実行するときに考慮に入れられます。*	-

プロパティ	説明	既定値
JWT 証明書	JWT .X509 パブリック キー証明書を PEM 形式で追加します。パブリック キー証明書の例は次の通りです。 -----BEGIN CERTIFICATE----- MIIDYTCCAkmgAwIBAgIJAM/oG48ciCGeMA0GCSqGSIb3DQEBCwUAMEcxEDAOBgNV BAoMB0NvbXBhbnkxEzARBgNVBAMMCkpvaG4gRG9ubmUxHjAcBgkqhkiG9w0BCQEW D2pkZUBjb21wYW55LmNvbTAeFw0xNzAzMjAxMjMxNDhaFw0yNzAzMTgxMjMxNDha MEcxEDAOBgNVBAoMB0NvbXBhbnkxEzARBgNVBAMMCkpvaG4gRG9ubmUxHjAcBgkq hkiG9w0BCQEWD2pkZUBjb21wYW55LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP ADCCAQoCggEBALIaab/y0u/kVIZnUsRVJ9vaZ2coiB3dVl/PCa40fyZdOIK5CvbA d0mJhuM7m/L4PldKmWh7nsPVC6SHAwgVwXASPHZQ6qha9ENChI2NfvqY4hXTH//Y FYaGLuKHD7pE7Jqt7Bhdh1zbBjrzsr1eU4Owwv9W9DxM4tVx3Xx8AUCNRoEWgObz Oqw9CfYY7/AWB8Hnr8G22X/l0/i4uJhiIKDVEisZ55hiNTEyqwW/ew0ilI7EAngw L8OD7WXpC2tCCe2V3fgUjQM4Q+0jEZGiARhzRhtaceuTBnnKq3+DnHmW4HzBuhZB CLMuWaJowkKaSfCQMel6u0/Evxc8i8FkPeMCAwEAAaNQME4wHQYDVR0OBBYEFNQ9 M2Y5WlRCyftHlD2oIk12YHyBMB8GA1UdIwQYMBaAFNQ9M2Y5WlRCyftHlD2oIk12 YHyBMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAHO46YLxtcMcanol PUC5nGdyYchZVHkd4F5MIe82mypwFszXGvpxKQXyAIPMkTIGb1wnE/wbCfB7moxX oFo+NoASER6wtt6FPHNcCiCXHm3B+2at16nOeMLfDefhQq03Q7qjfoa+7woAYole C9fTHGAl4TMIPThGSluiVLOLgHFUHpZryI6DdiEutXiH4afXaw0mScG36Z1uvHIq dPtjb/vDm1b9jvLITe8mZ8c2is1aBCLOdFvNupARxK7U3UD6HzGIh4x7eqo6Q9CK m[illegible]pCuIBY9Cu2l1Xeq4QW5E AqFLKKE=	空

プロパティ	説明	既定値
JWT ユーザー ID に使用する属性	ユーザー ID を説明する属性の JWT 属性名。	空
JWT ユーザーディレクトリに使用する属性	ユーザーディレクトリを説明する属性の JWT 属性名。名前の値がかっこ内にある場合、その値はコンテンツの属性値として使用されます。[例] では定数属性値「例」を提供しています。	-
[**JWT 属性マッピング**]	[**新しい属性の追加**] をクリックして JWT 属性を Qlik Sense 属性にマッピングします。名前の値がかっこ内にある場合、その値はコンテンツの属性値として使用されます。[例] では定数属性値「例」を提供しています。	空
オプションのOIDC属性を無効化	ユーザーディレクトリコネクタを介してユーザーを同期する場合にのみ使用します。選択されている時は、ユーザーディレクトリコネクタの同期から送られてくる**名前**、**グループ**、**メール**、**画像**の属性が、OIDC からの属性で上書きされないように保護されます。	
OpenID Connect メタデータ URI	OpenID Connect プロトコルを使用して ID プロバイダとやり取りする OAuth クライアントに関して、構成情報を提供するエンドポイントへの URL。	
クライアント ID	ユーザ認証用に ID プロバイダーで設定されたクライアントの ID。	
クライアントシークレット	ID プロバイダで構成されているクライアントのシークレット。	
領域	ID プロバイダーに関連付ける名前で、マルチクラウドでの名前の一貫性に使用されます。 サブジェクト属性値の形式が*domainname**username*の場合、**realm** はオプションです。そうでない場合、**realm** は必須です。	
サブジェクト	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。 必須。	
名前	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。 必須。	

プロパティ	説明	既定値
グループ	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。	
電子メール	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。 必須。	
client_id:	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。	
写真	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。	
スコープ:	アクセス トークンの発行時にアクセス権限を指定するために、OAuth 2.0 の仕様で使用されます。たとえば、ID プロバイダでユーザー グループ機能をサポートするためにグループ スコープが必要な場合は、このオプションを使用してグループ スコープを追加します。	
OIDC 属性マッピング	[**新しい属性の追加**] をクリックして OIDC 属性を Qlik Sense 属性にマッピングして、[**必須**] を選択することでこれらを必須とするかどうかを定義します。名前やフレンドリな名前を使用して属性を識別できます。	

負荷分散

負荷分散プロパティ

プロパティ	説明	既定値
[**負荷分散ノード**]	ノードに負荷分散を追加するには、[**Add new server node (新しいサーバーノードの追加)**] をクリックします。	空

詳細設定

詳細設定プロパティ

プロパティ	説明	デフォルト値
[**拡張セキュリティ環境**]	この設定を有効にすると、クライアントの環境についての情報(OS、デバイス、ブラウザー、IP) は、セキュリティヘッダーで送信されます。 選択されていない場合、ユーザーは、同じエンジンセッションを複数のデバイスで同時に実行できます。	空
[**セッション Cookie ドメイン**]	既定では、プロキシがインストールされたマシンに対してのみ、セッション Cookie が有効です。この (オプションの) プロパティであれば、より大きいドメインへの有効性を高められます。例: `company.com`	空欄 (既定マシン)
[**Secure 属性あり (https)**]	Secure 属性を持ち、https を使用するセッション クッキー用のオプション。	選択値
[**SameSite 属性 (https)**]	https 用の SameSite 属性値: **属性なし**、**None**、**Lax**、**Strict** 詳しくは「*SameSite クッキー属性 (page 165)*」を参照してください。	Lax
[**Secure 属性あり (http)**]	Secure 属性を持ち、http を使用するセッション クッキー用のオプション。	空
[**SameSite 属性 (http)**]	http 用の SameSite 属性値: **属性なし**、**None**、**Lax**、**Strict** 詳しくは「*SameSite クッキー属性 (page 165)*」を参照してください。	属性なし

追加の応答ヘッダー	クライアントに返す HTTP 応答すべてに付加されるヘッダー。例:
	`Header1: value1`
	`Header2: value2`
		空

プロパティ	説明	デフォルト値
[**ホスト許可リスト**]	Websocket オリジン ホワイト リストに追加されたすべての値は、ボトム レベルから検証されます。たとえば、「*domain.com*」が追加された場合、「*domain.com*」で終わるすべての値が承認されます。 「*subdomain.domain.com*」が追加された場合は、「*subdomain.domain.com*」で終わるすべての値が承認されます。 Cross-Origin Resource Sharing (CORS) の使用時にスイッチング スキーマに対応するには、CORS ポリシーによって要求がブロックされないようにするスキーマが、ホストのホワイト リストに含まれている必要があります。 安全でない Web サイト (*http://subdomain.domain.com*) および安全な Web サイト *(https://qlik.sense...*) を実行する Qlik Sense からマッシュアップをロードしている場合、このスキーマ (*http://subdomain.domain.com*) がホストの許可リストに記載されている必要があります。 *許可リストが空の場合でも、Qlik Sense がインストールされたマシンの名前は、表示されませんが許可リストの一部とみなされます。*	空

統合

統合プロパティ

プロパティ	説明	デフォルト値
[**セッション モジュール ベース URI**]	存在する場合、外部セッション モジュールへのアドレス。	空欄 (既定モジュール: インメモリ)
[**負荷分散モジュール ベース URI**]	存在する場合、ユーザーのセッションのために使用する Qlik Sense エンジンを選択する外部の負荷分散モジュールへのアドレス。	空欄 (既定モジュール: ラウンドロビン)

クライアント認証 リンク

クライアント認証 リンクは、Qlik Sense サーバーに対してクライアントの認証を要求するために使用されます。

クライアント認証 リンクは、QMC 内の任意の仮想プロキシから生成可能です。ただし、クライアント認証 リンクをハブから取得する場合は、中央ノードの既定の仮想プロキシからリンクを生成する必要があります。

クライアント認証 リンクのプロパティ

プロパティ	説明	デフォルト値
クライアント認証 リンク ホスト URI	クライアント認証 リンクの一部となる Qlik Sense URI。	空
クライアント認証 リンク フレンドリ名	ユーザーがホストを識別するために役立つ名前。フレンドリ名は、クライアント認証 リンクの一部となります。	空
クライアント認証 リンクの生成	ボタンをクリックすると、コピーしてユーザーに配布できるリンクが生成されます。	-

クライアント認証の構成 (page 501)

タグ

利用可能な QMC タグがない場合、このプロパティグループは表示されません。

テキスト ボックスをクリックすると、利用可能なタグが一覧表示されます。入力を始めると、リストが少なくなります。紐付けられているタグがテキスト ボックスの下に表示されます。

カスタム プロパティ

***カスタム プロパティ**を利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

5. [**適用**] をクリックして変更を保存します。必須の項目が空欄の場合、[**Apply**] は無効になります。
6. 操作バーで [**適用**] をクリックし、変更内容を保存します。

ページの最下部に [**更新完了**] と表示されます。

仮想プロキシの編集

既存の仮想プロキシを編集できます。

仮想プロキシは、使用する前にプロキシ サービスにリンクしておく必要があります。リンクせずに仮想プロキシを作成することもできますが、リンクするまで仮想プロキシは使用できません。参照先: 仮想プロキシのプロキシへのリンク(page 422)

セキュリティ上の理由で、既定の仮想プロキシの一部の設定は編集できません。誤って設定すると、システムが動作不能になることがあります。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**仮想プロキシ**] を選択して、概要を表示します。
3. 編集する仮想プロキシを選択し、操作バーで [**編集**] をクリックします。1 度に 1 つのプロキシに対する仮想プロキシしか編集できません。
4. [**仮想プロキシの編集**] ウィンドウでプロパティを編集します。

ID

全項目が必須で、空欄のままにはできません。

ID プロパティ

プロパティ	**説明**	**デフォルト値**
[**説明**]	仮想プロキシの名前。	空
[**プレフィックス**]	各追加パスを定義するプロキシの URI のパス名。例: *https://[node]/[prefix]/* 次の点に注意してください。 • プレフィックスでは小文字のみを使用できます。Qlik Sense 3.0 へのアップグレード後、既存の仮想プロキシに含まれるすべての大文字は、自動的に小文字で置き換えられます。 • 使用可能な文字は、次の予約されていない文字のみです。(a-z, 0-9, "-", ".", "_" , "~"。詳細については、次のドキュメントの「非予約文字」のセクションを参照してください: Uniform Resource Identifier (URI): 一般的な構文	空
[**タイムアウトまでのセッション アイドル時間 (分)**]	タイムアウトするまでのアイドル状態の最大時間。この時間が経過すると、セッションは無効となり、ユーザーはシステムからログアウトされます。	30 分間
[**セッション クッキー ヘッダー名**]	セッション クッキーのために使用される HTTP ヘッダー名。既定ではこの値は空欄なので、値を入力する必要があります。 *February 2019 以降のリリースは、ユーザーが http を介してシステムにアクセスすると、セッションの Cookie ヘッダー名にサフィックス (-HTTP) が付加されます。* *クッキー名のサフィックスとして、上記の [**プレフィックス**] プロパティの値が含まれていると、役に立ちます。*	空

認証

認証プロパティ

プロパティ	説明	既定値
[**匿名アクセス モード**]	• **匿名ユーザーを拒否**: ユーザは、ユーザ ID と資格情報を指定する必要があります。 • **匿名ユーザーを許可**: ユーザは匿名で入力しますが、ユーザアカウントで切り替えてログインすることができます。 • **常に匿名ユーザー**: ユーザーは常に匿名です。	匿名ユーザーなし
[**認証方法**]	• [**Ticket**]: チケットは認証に使用されます。 • [**ヘッダー認証静的ユーザー ディレクトリ**]: 静的ヘッダー認証を許可します。QMC でユーザー ディレクトリを設定します。 • [**ヘッダー認証動的ユーザー ディレクトリ**]: 動的ヘッダー認証を許可します。ヘッダーからユーザー ディレクトリの情報を取得します。 • SAML:SAML2 は認証に使用されます。 • JWT:JSON Web Token は認証に使用されます。 • OIDC:OpenID Connect は認証に使用されます。	チケット
[**ヘッダー認証ヘッダー名**]	ヘッダー認証が許可される場合、ユーザーを識別する HTTP ヘッダー名. ([**Authentication method**] プロパティに [**Header authentication static user directory**] または [**Header authentication dynamic user directory**] のいずれかを選択して) ヘッダー認証を許可する場合、必須です。 *ヘッダー認証は US-ASCII のみをサポートしています (UTF-8 はサポートしていません)。*	空
[**ヘッダー認証静的ユーザー ディレクトリ**]	ヘッダー認証を受けたユーザーの追加情報を取得できるユーザー ディレクトリ名。([**Authentication method**] プロパティに [**Header authentication static user directory**] を選択して) 静的ヘッダー認証を許可する場合は必須です。	空

プロパティ	説明	既定値
[**ヘッダー認証動的ユーザーディレクトリ**]	([**Authentication method**] プロパティに [**Header authentication dynamic user directory**] を選択して) 動的ヘッダー認証を許可する場合、必須です。入力するパターンには '$ud' や '$id' が含まれ、これらを分離する方法も含まれている必要があります。 **ヘッダーの設定および一致の例** `$ud\\$id` – USERDIRECTORY\userid と一致させます (\を追加して、バックラッシュをエスケープする必要があります) `$id@$ud` – userid@USERDIRECTORY と一致させます ($id と$ud の順番は関係ありません) `$ud:::$id` – USERDIRECTORY:::userid と一致させます	空
[**Windows 認証パターン**]	ログイン用に選択された認証パターン。User-Agent ヘッダーに Windows 認証パターン文字列が含まれている場合、Windows 認証が使用されます。一致する文字列がない場合は、フォーム認証が使用されます。	Windows
[**認証モジュールは URI をリダイレクトします**]	外部の認証モジュールを使用する場合、クライアントは認証のため、この URI へリダイレクトされます。	空欄 (既定モジュール: Windows 認証の Kerberos/NTLM)
SAML シングル ログアウト	SAML シングル ログアウト用にサービス プロバイダーが開始するフローを有効にする場合は、このチェック ボックスをオンにします。オンにした場合、仮想プロキシ用に生成されたメタデータ ファイルに、POST およびリダイレクト バインディング用のシングル ログアウトの場所が含められます。	空
SAML ホスト URI	クライアントに表示されるサーバー名。この名前は、クライアントが QMC などの Qlik サービスにアクセスする際に使用されます。 サーバー名はコンピュータ名と同一である必要はありませんが、ほとんどの場合、同じ名前が使用されます。 URI には http:// または https:// のいずれかを使用できます。http:// を使用するには、仮想プロキシがリンクされているプロキシの編集ページで [**Allow HTTP (HTTP を許可)**] を選択する必要があります。 ([**Authentication method**] プロパティで **SAML** を選択することにより) SAML 認証を許可する場合は必須になります。	空
SAML エンティティ ID	サービス プロバイダーを識別する ID。ID は一意にする必要があります。 ([**Authentication method**] プロパティで **SAML** を選択することにより) SAML 認証を許可する場合は必須になります。	空

プロパティ	説明	既定値
[**SAML IdP メタデータ**]	IdP からのメタデータはサービスプロバイダーの構成に使用され、SAML 認証が正常に動作するために必要です。メタデータの一般的な入手方法は、IdP Web サイトからのダウンロードです。 [参照] ボタンをクリックしてアップロード用に IdP metadata .xml ファイルを開きます。エラーを回避するには、[**View content (コンテンツを表示)**] をクリックしてファイルのコンテンツと形式が正しいことを確認します。 メタデータがないと構成は未完了になります。	-
SAML ユーザー ID に使用する属性	ユーザー ID を説明する属性の SAML 属性名。名前やフレンドリな名前を使用して属性を識別できます。 *必須の SAML 属性名が分からない (page 641)*	空
SAML ユーザーディレクトリに使用する属性	ユーザーディレクトリを説明する属性の SAML 属性名。名前やフレンドリな名前を使用して属性を識別できます。名前の値がかっこ内にある場合、その値はコンテンツの属性値として使用されます。[例] では定数属性値「例」を提供しています。 *必須の SAML 属性名が分からない (page 641)*	空
SAML 署名アルゴリズム	署名 SAML 要求に使用されるハッシュアルゴリズム。SHA-256 を使用するには、関連する秘密キーのプロバイダーが「Microsoft Enhanced RSA and AES Cryptographic Provider」である第三者機関の証明書が必要となります。	-
[**SAML 属性マッピング**]	[**新しい属性の追加**] をクリックして SAML 属性を Qlik Sense 属性にマッピングして、[**必須**] を選択することでこれらを必須とするかどうかを定義します。名前やフレンドリな名前を使用して属性を識別できます。名前の値がかっこ内にある場合、その値はコンテンツの属性値として使用されます。[例] では定数属性値「例」を提供しています。 *SAML 応答ベースの属性は、製品監査を実行するときに考慮に入れられます。*	-

プロパティ	説明	既定値
JWT 証明書	JWT .X509 パブリック キー証明書をPEM 形式で追加します。パブリック キー証明書の例は次の通りです。 -----BEGIN CERTIFICATE----- MIIDYTCCAkmgAwIBAgIJAM/oG48ciCGeMA0GCSqGSIb3DQEBCwUAMEcxED AOBgNV BAoMB0NvbXBhbnkxEzARBgNVBAMMCkpvaG4gRG9ubmUxHjAcBgkqhkiG9w 0BCQEW D2pkZUBjb21wYW55LmNvbTAeFw0xNzAzMjAxMjMxNDhaFw0yNzAzMTgxMj MxNDha MEcxEDAOBgNVBAoMB0NvbXBhbnkxEzARBgNVBAMMCkpvaG4gRG9ubmUxHj AcBgkq hkiG9w0BCQEWD2pkZUBjb21wYW55LmNvbTCCASIwDQYJKoZIhvcNAQEBBQ ADggEP ADCCAQoCggEBALIaab/y0u/kVIZnUsRVJ9vaZ2coiB3dVl/PCa40fyZdOI K5CvbA d0mJhuM7m/L4PldKmWh7nsPVC6SHAwgVwXASPHZQ6qha9ENChI2NfvqY4h XTH//Y FYaGLuKHD7pE7Jqt7Bhdh1zbBjrzsr1eU4Owwv9W9DxM4tVx3Xx8AUCNRo EWgObz Oqw9CfYY7/AWB8Hnr8G22X/l0/i4uJhiIKDVEisZ55hiNTEyqwW/ew0ilI 7EAngw L8OD7WXpC2tCCe2V3fgUjQM4Q+0jEZGiARhzRhtaceuTBnnKq3+DnHmW4H zBuhZB CLMuWaJowkKaSfCQMel6u0/Evxc8i8FkPeMCAwEAAaNQME4wHQYDVR0OBB YEFNQ9 M2Y5WlRCyftHlD2oIk12YHyBMB8GA1UdIwQYMBaAFNQ9M2Y5WlRCyftHlD 2oIk12 YHyBMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAHO46YLxtc Mcanol PUC5nGdyYchZVHkd4F5MIe82mypwFszXGvpxKQXyAIPMkTIGb1wnE/wbCf B7moxX oFo+NoASER6wtt6FPHNcCiCXHm3B+2at16nOeMLfDefhQq03Q7qjfoa+7w oAYole C9fTHGAl4TMIPThGSluiVLOLgHFUHpZryI6DdiEutXiH4afXaw0mScG36Z 1uvHIq dPtjb/vDm1b9jvLITe8mZ8c2is1aBCLOdFvNupARxK7U3UD6HzGIh4x7eq o6Q9CK mKEz3SFHtKTpyiSn/0ESAl[illegible]pCuIBY9Cu2l1Xe q4QW5E AqFLKKE=	空

プロパティ	説明	既定値
JWT ユーザー ID に使用する属性	ユーザー ID を説明する属性の JWT 属性名。	空
JWT ユーザーディレクトリに使用する属性	ユーザーディレクトリを説明する属性の JWT 属性名。名前の値がかっこ内にある場合、その値はコンテンツの属性値として使用されます。[例] では定数属性値「例」を提供しています。	-
[**JWT 属性マッピング**]	[**新しい属性の追加**] をクリックして JWT 属性を Qlik Sense 属性にマッピングします。名前の値がかっこ内にある場合、その値はコンテンツの属性値として使用されます。[例] では定数属性値「例」を提供しています。	空
オプションのOIDC属性を無効化	ユーザーディレクトリコネクタを介してユーザーを同期する場合にのみ使用します。選択されている時は、ユーザーディレクトリコネクタの同期から送られてくる**名前**、**グループ**、**メール**、**画像**の属性が、OIDC からの属性で上書きされないように保護されます。	
OpenID Connect メタデータ URI	OpenID Connect プロトコルを使用して ID プロバイダとやり取りする OAuth クライアントに関して、構成情報を提供するエンドポイントへの URL。	
クライアント ID	ユーザ認証用に ID プロバイダーで設定されたクライアントの ID。	
クライアントシークレット	ID プロバイダで構成されているクライアントのシークレット。	
領域	ID プロバイダーに関連付ける名前で、マルチクラウドでの名前の一貫性に使用されます。 サブジェクト属性値の形式が*domainname**username*の場合、**realm** はオプションです。そうでない場合、**realm** は必須です。	
サブジェクト	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。 必須。	
名前	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。 必須。	

プロパティ	説明	既定値
グループ	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。	
電子メール	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。 必須。	
client_id:	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。	
写真	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。	
スコープ:	アクセス トークンの発行時にアクセス権限を指定するために、OAuth 2.0 の仕様で使用されます。たとえば、ID プロバイダでユーザー グループ機能をサポートするためにグループ スコープが必要な場合は、このオプションを使用してグループ スコープを追加します。	
OIDC 属性マッピング	[**新しい属性の追加**] をクリックして OIDC 属性を Qlik Sense 属性にマッピングして、[**必須**] を選択することでこれらを必須とするかどうかを定義します。名前やフレンドリな名前を使用して属性を識別できます。	

負荷分散

負荷分散プロパティ

プロパティ	説明	既定値
[**負荷分散ノード**]	ノードに負荷分散を追加するには、[**Add new server node (新しいサーバー ノードの追加)**] をクリックします。	空

詳細設定

詳細設定プロパティ

プロパティ	説明	デフォルト値
[**拡張セキュリティ環境**]	この設定を有効にすると、クライアントの環境についての情報(OS、デバイス、ブラウザー、IP) は、セキュリティヘッダーで送信されます。 選択されていない場合、ユーザーは、同じエンジンセッションを複数のデバイスで同時に実行できます。	空
[**セッション Cookie ドメイン**]	既定では、プロキシがインストールされたマシンに対してのみ、セッション Cookie が有効です。この (オプションの) プロパティであれば、より大きいドメインへの有効性を高められます。例: `company.com`	空欄 (既定マシン)
[**Secure 属性あり (https)**]	Secure 属性を持ち、https を使用するセッション クッキー用のオプション。	選択値
[**SameSite 属性 (https)**]	https 用の SameSite 属性値: **属性なし**、**None**、**Lax**、**Strict** 詳しくは「*SameSite クッキー属性 (page 165)*」を参照してください。	Lax
[**Secure 属性あり (http)**]	Secure 属性を持ち、http を使用するセッション クッキー用のオプション。	空
[**SameSite 属性 (http)**]	http 用の SameSite 属性値: **属性なし**、**None**、**Lax**、**Strict** 詳しくは「*SameSite クッキー属性 (page 165)*」を参照してください。	属性なし

追加の応答ヘッダー	クライアントに返す HTTP 応答すべてに付加されるヘッダー。例:
	`Header1: value1`
	`Header2: value2`
		空

プロパティ	説明	デフォルト値
[**ホスト許可リスト**]	Websocket オリジン ホワイト リストに追加されたすべての値は、ボトム レベルから検証されます。たとえば、「*domain.com*」が追加された場合、「*domain.com*」で終わるすべての値が承認されます。「*subdomain.domain.com*」が追加された場合は、「*subdomain.domain.com*」で終わるすべての値が承認されます。 Cross-Origin Resource Sharing (CORS) の使用時にスイッチング スキーマに対応するには、CORS ポリシーによって要求がブロックされないようにするスキーマが、ホストのホワイト リストに含まれている必要があります。 安全でない Web サイト (*http://subdomain.domain.com*) および安全な Web サイト *(https://qlik.sense...*) を実行する Qlik Sense からマッシュアップをロードしている場合、このスキーマ (*http://subdomain.domain.com*) がホストの許可リストに記載されている必要があります。 *許可リストが空の場合でも、Qlik Sense がインストールされたマシンの名前は、表示されませんが許可リストの一部とみなされます。*	空

統合

統合プロパティ

プロパティ	説明	デフォルト値
[**セッション モジュール ベース URI**]	存在する場合、外部セッション モジュールへのアドレス。	空欄 (既定モジュール: インメモリ)
[**負荷分散モジュール ベース URI**]	存在する場合、ユーザーのセッションのために使用する Qlik Sense エンジンを選択する外部の負荷分散モジュールへのアドレス。	空欄 (既定モジュール: ラウンドロビン)

クライアント認証 リンク

クライアント認証 リンクは、Qlik Sense サーバーに対してクライアントの認証を要求するために使用されます。

***クライアント認証 リンク**は、QMC 内の任意の仮想プロキシから生成可能です。ただし、クライアント認証 リンクをハブから取得する場合は、中央ノードの既定の仮想プロキシからリンクを生成する必要があります。*

クライアント認証 リンクのプロパティ

プロパティ	説明	デフォルト値
クライアント認証 リンク ホスト URI	クライアント認証 リンクの一部となる Qlik Sense URI。	空
クライアント認証 リンク フレンドリ名	ユーザーがホストを識別するために役立つ名前。フレンドリ名は、クライアント認証 リンクの一部となります。	空
クライアント認証 リンクの生成	ボタンをクリックすると、コピーしてユーザーに配布できるリンクが生成されます。	-

クライアント認証の構成 (page 501)

タグ

利用可能な QMC タグがない場合、このプロパティグループは表示されません。

テキスト ボックスをクリックすると、利用可能なタグが一覧表示されます。入力を始めると、リストが少なくなります。紐付けられているタグがテキスト ボックスの下に表示されます。

カスタム プロパティ

***カスタム プロパティ**を利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

5. [**適用**] をクリックして変更を保存します。必須の項目が空欄の場合、[**Apply**] は無効になります。
6. [**Associated items**] でフィールドを編集します。

プロキシ

プロキシのプロパティ

プロパティ	説明
ノード	プロキシ名。

プロパティ	説明
状態	次のテキストのいずれかが表示されます。 • **実行中** サービスは正常に実行中です。 • **停止** サービスは停止されました。 • **無効化** サービスは無効になっています。 *状態の詳細については、[**状態**] 列で ⓘ をクリックしてください。* *Qlik Sense サービスの状態を確認する (page 375)*。
サービスの待ち受けポート HTTPS (既定)	既定のプロキシのセキュアな待ち受けポートで、Qlik Sense 通信をすべて管理します。 *ポート443 は他のソフトウェア (Web サーバーなど) によって使用されることがあるため、Qlik Sense Proxy Service (QPS) がこのポートを使用できることを確認してください。*
HTTP 許可	ステータス値:**Yes** または **No** **有効化する**: 暗号化されていない通信を許可します。これは、両方の https (セキュア通信) と (http) の暗号化されていない通信が許可されることを意味しています。 *February 2019 以降のリリースは、ユーザーが http を介してシステムにアクセスすると、セッションの Cookie ヘッダー名にサフィックス (-HTTP) が付加されます。*
サービスの待ち受けポート HTTP	非暗号化待ち受けポート、HTTP 接続が許可されている場合に使用されます。
認証の待ち受けポート	内部認証モジュールの待ち受けポート。 *管理者権限のないユーザーとしてこのポートを編集する場合、変更を有効にするには、起動モードでレポジトリを実行する必要があります。*
Kerberos 認証	ステータス値:**Yes** または **No** **有効化する**: Kerberos 認証を有効にします。

プロパティ	説明
REST API 待ち受けポート	プロキシ API の待ち受けポート。 *管理者権限のないユーザーとしてこのポートを編集する場合、変更を有効にするには、起動モードでレポジトリを実行する必要があります。*
SSL ブラウザ証明書捺印 (署名)	ブラウザからプロキシへのトラフィックの暗号化を扱う、セキュア ソケット レイヤー (SSL) 証明書の捺印。プロキシ証明書および管理者権限のないアカウントでの Qlik Sense サービス実行を編集する場合、以下のように証明書にプライベートキーのアクセス許可を設定する必要があります。
Keep-alive タイムアウト (秒)	接続が切断されるまでの 1 回の HTTP/HTTPS リクエストの最大タイムアウト時間。DoS 攻撃 (サービス拒否攻撃) に対する防御。リクエストがこの時間を超過した場合は、Qlik Sense プロキシによって接続が切断されることを意味しています。ユーザーが接続の遅さと接続の切断で困っている場合は、この値を増やしてください。
ヘッダーの最大サイズ (バイト)	ヘッダーの最大合計サイズ。
最大ヘッダー行数	最大ヘッダー行数。
監査アクティビティ ログ レベル	レベル: [**オフ**] または [**基本**] (制限的なエントリ)
監査セキュリティ ログ レベル	レベル: [**オフ**] または [**基本**] (制限的なエントリ)
サービス ログ レベル	[**エラー**] から [**デバッグ**] までの各レベルには前のレベルよりも多くの情報が含まれます。
監査ログ レベル	プロキシの呼び出しなど、より詳細なユーザーベース メッセージは このロガーに保存されます。 [**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
パフォーマンス ログ レベル	パフォーマンス メッセージはすべて、このロガーに保存されます。パフォーマンス カウンター、および接続、ストリーム、セッション、チケット、ウェブ ソケットの数、負荷分散情報などです。 [**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
セキュリティ ログ レベル	証明書 メッセージはすべて、このロガーに保存されます。 [**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。
システム ログ レベル	標準的なプロキシ メッセージはすべて、このロガーに保存されます。 [**Fatal**] から [**Debug**] までの各レベルには前のレベルよりも多くの情報が含まれます。

プロパティ	説明
パフォーマンスログ間隔 (分)	パフォーマンス ログの間隔。
ID	プロキシの ID。
作成日時	プロキシが作成された日時。
最終変更日	プロキシが最後に変更された日時。
変更者	プロキシを最後に変更したユーザー。
<Custom properties>	カスタム プロパティがある場合はここに一覧表示されます。
▼▲	リストを昇順または降順で並べ替えます。並べ替えをサポートしない列もあります。
	フィルターする文字列を入力するか、利用可能な場合は組込み値を選択します。フィルター条件に一致した行が表示されます。検索を絞り込むために、同時に複数の列でフィルターを使用できます。フィルターが列に適用されると、 が表示されます。 条件を削除するには、テーブル ヘッダー バーで [**Actions**] をクリックして、[**Clear filters and search**] を選択します。 検索とフィルタリングを組み合わせることができます。 *QMC での検索とフィルタリング (page 25)*
編集	選択したプロキシを編集します。
リンクの解除	選択したプロキシからプロキシ サービスのリンクを解除します。 *仮想プロキシを機能させるためにはプロキシ サービスにリンクさせる必要があります。*
リンク	選択したプロキシにプロキシ サービスをリンクします。
アイテムをさらに表示	既定の概要では、アイテムのセット数が表示されます。さらに多くのアイテムを表示するためには、リストの最後までスクロールして、[**Show more items**] をクリックします。アイテムの並べ替えやフィルタリングは、表示中のアイテムだけでなく、常にアイテムの全データベースのリスト上で実行されます。

7. 操作バーで [**適用**] をクリックし、変更内容を保存します。

ほとんどの場合、仮想プロキシに変更内容を適用するときにプロキシを再起動する必要があります。仮想プロキシのリンク先プロキシによって処理されているセッションが終了し、ユーザーはログアウトされます。仮想プロキシの次のリソースを変更すると、プロキシは自動的に再起動しません。タグ、カスタム プロパティ、負荷分散 ノード。タグ、カスタム プロパティ、および負荷分散 ノード。

ページの最下部に [**更新完了**] と表示されます。

仮想プロキシのプロキシへのリンク

仮想プロキシは、使用する前にプロキシ サービスにリンクしておく必要があります。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**仮想プロキシ**] を選択して、概要を表示します。
3. プロキシにリンクする仮想プロキシを選択します。
4. アクション バーで [**編集**] をクリックします。
5. [**仮想プロキシの編集**] ページの右側にある [**関連アイテム**] で、[**プロキシ**] をクリックします。
   [**関連プロキシ**] ページが開きます。
6. In the action bar, click ⊕ **リンク**
   [**プロキシ サービスの選択**] ページが開きます。
7. リンクするノードを選択して [**リンク**] をクリックします。
   リンクされたノードが [**関連プロキシ**] リストに表示されます。プロキシが再起動されたため、セッションが終了します。
8. QMC を再起動します。

仮想プロキシがプロキシにリンクされ、仮想プロキシを使用できるようになりました。

仮想プロキシの削除

削除権限のある仮想プロキシを削除できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**仮想プロキシ**] を選択して、概要を表示します。
3. 削除する仮想プロキシを選択します。複数のプロキシの仮想プロキシを同時に削除することはできません。
4. アクション バーの [**Delete**] をクリックします。
   [**Delete**] ダイアログが表示されます。
5. [**OK**] をクリックします。

スケジューラの編集

更新権限を有するスケジューラを編集できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**スケジューラ**] を選択して、概要を表示します。
3. 編集するスケジューラを選択します。

4. アクション バーで [**編集**] をクリックします。
   複数のスケジューラが選択され、特定の項目の値と異なる場合は、項目名に [**複数の値**] と表示されます。
5. プロパティを編集します。

   一番右側にあるパネルで、プロパティグループの表示/非表示を切り替えることができます。

   ID
   全項目が必須で、空欄のままにはできません。

   ID プロパティ

プロパティ	説明	デフォルト値
[**ノード**]	スケジューラ名。	ノード名を継承します。

   ログ
   [**ログ**] プロパティグループには、Qlik Sense システムのスケジューラ ログ プロパティとトレース プロパティが含まれています。

   ログ プロパティ

プロパティ	説明	デフォルト値
[**監査アクティビティ ログ レベル**]	ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**Basic (基本)**]: 限定的なエントリのセット	基本
[**サービス ログ レベル**]	ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**エラー**]: エラーのエントリのみ • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる	Info

   [**トレース**]

   トレース設定情報

設定	説明	値

[**アプリケーション ログ レベル**]	スケジューラ サービスのアプリケーション メッセージはすべて、このロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info
[**監査 ログ レベル**]	ユーザーベースの詳細なメッセージは、このロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info
[**パフォーマンス ログ レベル**]	パフォーマンス メッセージはすべて、このロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info
[**セキュリティ ログ レベル**]	証明書メッセージはすべて、このロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info

[**システム ログ レベル**]	標準的なスケジューラ メッセージはすべて、このロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info
[**タスク実行 ログ レベル**]	タスク実行 メッセージはすべて、このロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info

Qlik Sense ログ フォルダへの既定のパスは、%ProgramData%\Qlik\Sense\Log\<サービス> です。

詳細設定

詳細設定プロパティ

プロパティ	**説明**	**デフォルト値**
タイプ	上記のプロパティによって有効になると、QSS のタイプは以下のように設定されます。 • [マネージャー]: サイト内のワーカー QSS にタスクを送信します。 • [ワーカー]: マネージャー QSS からタスクを受け取り、タスクを実行します。 • マネージャーとワーカー: シングル ノード サイトで、マネージャー QSS がワーカー QSS としても機能する場合。	ワーカー (セントラル ノードではマネージャー)

プロパティ	説明	デフォルト値
[**同時実行リロード最大数**]	リロード最大数、スケジューラは複数のリロードを同時に実行できます。	4
[**エンジン タイムアウト (分)**]	[**同時実行 リロード最大数**] に達する (個別のプロパティ参照) と、エンジンの新規プロセス開始要求が、稼働中のリロードプロセス数を待機しているキューに置かれて、[**同時実行 リロード最大数**] を下回ります。上記が特定の時間内に起こらなかった場合、エンジンの新規プロセス開始要求はキューから削除されます。	30

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

カスタム プロパティ

***カスタム プロパティ**を利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

[**適用**] をクリックして変更を保存します。必須の項目が空欄の場合、[**Apply**] は無効になります。

6. [**適用**] をクリックして変更を保存します。

ページの最下部に [**更新完了**] と表示されます。

エンジンの編集

更新権限のあるエンジンを編集できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Engines (エンジン)**] を選択して、概要を表示します。
3. 編集するエンジンを選択します。
4. アクション バーで [**編集**] をクリックします。

5. プロパティを編集します。

ID

ID プロパティ

プロパティ	説明	デフォルト値
[ノード]	エンジン名	ノード名を継承します。

アプリ

アプリのプロパティ

プロパティ	説明	デフォルト値
[アプリ自動保存間隔 (秒)]	アプリの自動保存間の秒数。自動保存は常にセッションの最後に実行されます。	30
[アプリのキャッシュ時間 (秒)]	アプリを使用していた最後のセッションが終了した後、Qlik Sense アプリがメモリに残存できる時間 (秒数)。	28800
[テーブルファイルのルートディレクトリ]	関連パスがファイルの場所を決めるために使用される場合、予定されたリロードは、このディレクトリのファイルを検索します。 *この設定は、リロード中のファイルへの相対パス向けの QlikView スクリプトでレガシー機能に対応するために使用されます。この設定を使用して、アプリが保存されているディレクトリを変更することはできません。*	%ProgramData%\Qlik\Sense\Apps
[元に戻す最高回数]	シート、オブジェクト、ブックマーク、ストーリーなどのアプリコンテンツを編集する場合の元に戻す最大回数: 最小 = 0、最大 = 999。	100

詳細設定

詳細設定プロパティ

プロパティ	説明	既定値
[**待ち受けポート**]	Qlik Sense の Web クライアントとの通信のために Qlik Sense Engine Service (QES) によって使用される待ち受けポート。 ⊕ をクリックして、ポートを追加します。⊕ をクリックして、ポートを削除します。	4747
[**データ系統を許可**]	Qlik Sense にデータをロードするロードスクリプトの実行時に、データ系統 (データ元) を保存します。 この設定によって、QVD ファイルに保存するテーブルのロードに使われた **LOAD** ステートメントの情報が許可されます。	選択値
[**最小メモリ使用量**]	[Qlik Sense] によって使用される最小メモリ容量。この制限未満では、キャッシュはクリアされません。この設定と、エンジンのメモリ管理でこの設定が果たす役割の詳細については、[Associative Engine のメモリ管理と CPU 使用率] を参照してください。	70
[**最大メモリ使用量**]	Qlik Sense によって使用される最大メモリ容量。この設定と、エンジンのメモリ管理でこの設定が果たす役割の詳細については、[Associative Engine のメモリ管理とCPU 使用率] を参照してください。	90

プロパティ	説明	既定値
[**メモリ使用量モード**]	オペレーティング システム (Windows) がエンジン プロセスのメモリを管理する方法に影響します。 ドロップダウンを使って、次の方法のいずれかを選択します。 • [**ハード リミット (最大)**]: [**最大メモリ使用量 (%)**] の設定で定義された量よりも多くのメモリを使用しないでください。 この設定では、SetProcessWorkingSetSizeEx ドキュメント (QUOTA_LIMITS_HARDWS_MAX_ENABLE パラメーター) で説明されているように、これをサポートするようにオペレーティング システムを構成する必要があります。 • [**最大リミットを無視**]: [**最大メモリ使用量**] の設定に関わらず、必要最大限のメモリを使用します。 • [**ソフトリミット (最大)**]: 必要かつ利用可能な場合、[**最大メモリ使用量**] の設定で定義された量よりも多くのメモリを使用します。	ハードリミット (最大)

プロパティ	説明	既定値
[**CPU 調整**]	Qlik Sense が使用する CPU 容量。範囲: 0 ~ 100%。 Qlik Sense Engine Service プロセスの優先度の高低を、プロセスが使用している CPU の容量に応じて変えることができます。このようにすると、CPU 容量の一部を他のアプリケーションで使用するために解放して、サーバーの全体的なパフォーマンスを上げることができます。 *Qlik Sense Engine Service プロセスの CPU 使用量がスロットル レベルを超える場合は、オペレーティング システムにより、より多くのリソースが使用可能になるように指定されている可能性があります。*	0 (調整なし)

プロパティ	説明	既定値
[**標準モード**]	選択された場合は、標準モードが使用されます。選択が解除された場合は、レガシーモードが使用されます。標準モードは問題を引き起こす可能性のあるアクションを阻止する既定のモードです。特別な理由がない限り、標準モードを使用します。レガシーモードは、データを Qlik Sense にロードする際に、変更していない QlikView ロードスクリプトを実行するために使用できます。 セキュリティ上の理由から、Qlik Sense の標準モードでは、データロードスクリプトまたは関数、変数に含まれる絶対パスや相対パスはサポートされていません。これは、ファイルシステムが露呈されてしまうからです。 *ただし、標準モードを無効にすると、ファイルシステムが露呈するためセキュリティリスクが生じます。*	選択値
[**HTTP コールバックポート**]	このコールバックポートは、エンジンに HTTP イベントを送信するために、Qlik Sense Repository Service で使用されます。	4748

プロパティ	説明	既定値
[**ハイパーキューブ計算に使用するメモリに対する制限 (バイト)**]	リクエスト中にハイパーキューブ(超立方体)評価が割り当てることのできるメモリの制限です。リクエストで複数のハイパーキューブが計算されている場合、この制限はハイパーキューブの各計算に対し個別に適用されます。 この制限はあらゆる割り当てに対して強制されるのではありません。「0」に設定すると、エンジンは全体にヒューリスティック手法を適用し、計算に多くのメモリを要する同時実行のリクエストの数を制限します。 負の値を指定すると、制限は無効になります。 パフォーマンス上の理由から、メモリの使用/制限は、割り当てごとにではなく、定期的にチェックされます。そのため、場合によっては一時的に制限を超過することがあります。	0
[**メモリのリロードで使用されるメモリに対する制限 (バイト)**]	リロードリクエストに割り当てるメモリの制限です。 負の値または 0 を指定すると、制限は行われなくなります。 パフォーマンス上の理由から、メモリの使用/制限は、割り当てごとにではなく、定期的にチェックされます。そのため、場合によっては一時的に制限を超過することがあります。	-1
[**エクスポートに使用するメモリに対する制限 (バイト)**]	データエクスポートのリクエストの中で、エクスポートが割り当てることのできるメモリの制限です。計算に起因する割り当てはこの制限の対象になりません。 負の値または 0 を指定すると、制限は無効になります。 パフォーマンス上の理由から、メモリの使用/制限は、割り当てごとにではなく、定期的にチェックされます。そのため、場合によっては一時的に制限を超過することがあります。	-1

プロパティ	説明	既定値
[**ハイパーキューブに対する時間制限 (秒)**]	ハイパーキューブ計算で使用できる単一コアCPU稼動時間を制限します。この単一コアCPU稼動時間は、ヒューリスティック手法によるCPU消費時間の概算 (CPU消費時間を計算時に使用されたコア数で除算したもの) です。これはハードリミットではなく、処理される計算の複雑さに依存します。 負の値または0を指定すると、制限は行われなくなります。 パフォーマンス上の理由から、CPU時間に対する厳密な追跡は行われません。	60
[**リロードに対する時間制限 (秒)**]	リロードリクエストで使用できるCPU時間を制限します。 負の値または0を指定すると、制限は行われなくなります。	-1
[**エクスポートに対する時間制限 (秒)**]	データエクスポートのリクエストで、エクスポート処理に許可されるCPU時間の制限です。 負の値または0を指定すると、制限は行われなくなります。	-1
[**リロード中に検索インデックスを作成します。**]	選択すると、サーバー上のアプリがすべてリロード中にインデックス化され、最初の検索セッションの性能が向上します。	選択値

ログ

[**ログ**] プロパティグループには、Qlik Sense システムのエンジン ログ プロパティとトレース プロパティが含まれています。

ログ プロパティ

プロパティ	説明	デフォルト値
[**監査アクティビティ ログ レベル**]	ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**Basic (基本)**]: 限定的なエントリのセット	基本

プロパティ	説明	デフォルト値
[**サービス ログ レベル**]	ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**エラー**]: エラーのエントリのみ • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる	Info

[**トレース**]

トレースの説明

設定	説明	値
パフォーマンス ログ間隔 (分)	パフォーマンスのログ エントリの間隔時間 (分数)。	5
[**システム ログ レベル**]	標準的なエンジン メッセージはすべて、このロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info
[**パフォーマンス ログ レベル**]	パフォーマンス メッセージはすべて、このロガーに保存されます (既定では 5 分ごとに更新)。ログにはアクティブ ユーザー数、開いているセッションの数、CPU ロードなどが含まれます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info

[**QIX パフォーマンス ログ レベル**]	QIX プロトコルのパフォーマンス メッセージはすべて、このロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	オフ
[**監査ログ レベル**]	ユーザーがアプリで選択する場合など、ユーザー ベースの詳細メッセージはこのロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	オフ
[**セッション ログ レベル**]	クライアント セッションが終了すると、ユーザー情報、マシン ID、IP アドレス、ポート番号などすべてのセッション メッセージがこのロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info
[**トラフィック ログ レベル**]	エンジンへの JSON メッセージやエンジンからの JSON メッセージなど、すべてのトラフィック メッセージはこのロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	オフ

分析接続ログ レベル	分析接続メッセージはすべて、このロガーに保存されます。 ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info

Qlik Sense ログ フォルダへの既定のパスは、%ProgramData%\Qlik\Sense\Log\<サービス> です。

タグ

1. テキスト ボックスをクリックすると、利用できる***タグ***がすべて表示されます。
2. 入力を始めると、リストにフィルターが適用されます。

*紐付けられている***タグ***がテキスト ボックスの下に一覧表示されます。*

カスタム プロパティ

カスタム プロパティ*を利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで****カスタム プロパティ****を利用できるようにする必要があります。*

Qlik Analytics Platform を実行している場合は、追加設定を行うことができます。「Qlik Analytics Platform」を参照してください。

6. [**適用**] をクリックして変更を保存します。必須の項目が空欄の場合、[**Apply**] は無効になります。

「**エンジンのプロパティが更新されました**」というメッセージがページの最下部に表示されます。

エンジン サービス設定を変更するには、エンジン サービスを手動で再起動する必要があります。再起動は、手作業での再起動のためサーバーにアクセスする権限のある管理者しか実行できません。

印刷の編集

更新権限を有する印刷サービスを編集できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMCスタート ページから、あるいは [**Start**] ▼ドロップダウン メニューから [**Printing (印刷)**] を選択して、概要を表示します。
3. 編集する印刷サービスを選択します。
4. アクション バーで [**編集**] をクリックします。
5. プロパティを編集します。

一番右側にあるパネルで、プロパティグループの表示/非表示を切り替えることができます。

ID

[**ID**] プロパティグループには、Qlik Sense システムの印刷の基本プロパティが含まれています。
全項目が必須で、空欄のままにはできません。
[**ノード**] プロパティは印刷サービスの名前です。[**ノード**] の既定値はノード名を継承します。

ログ

ログ プロパティ

プロパティ	説明	デフォルト値
[**監査アクティビティ ログ レベル**]	ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**致命的なエラー**]: 致命的なエラーを含むエントリーのみ • [**エラー**]: 致命的なエラーと同じだが、エラーのエントリーも含まれる • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる • [**デバッグ**]: 情報と同じだが、デバッグのエントリーも含まれる	Info
[**サービス ログ レベル**]	ドロップダウンから、ロガーの冗長性を設定します。 • [**オフ**]: エントリーなし • [**エラー**]: エラーのエントリのみ • [**警告**]: エラーと同じだが、警告のエントリーも含まれる • [**情報**]: 警告と同じだが、情報のエントリーも含まれる	Info

Qlik Sense ログ フォルダへの既定のパスは、%ProgramData%\Qlik\Sense\Log\<サービス> です。

タグ

タグ プロパティ

プロパティ	説明
[**タグ**]	*利用可能なタグがない場合、このプロパティグループは空となります。* 紐付けられているタグがテキスト ボックスの下に表示されます。

カスタム プロパティ

***カスタム プロパティ**を利用できない場合、このプロパティグループには何も表示されません (あるいは表示されても空です)。ここで表示する前に、このリソース タイプで**カスタム プロパティ**を利用できるようにする必要があります。*

[**適用**] をクリックして変更を保存します。必須の項目が空欄の場合、[**Apply**] は無効になります。

6. 操作バーで [**適用**] をクリックし、変更内容を保存します。

ページの最下部に [**更新完了**] と表示されます。

カスタム プロパティの使用

カスタム プロパティを作成して、セキュリティ ルールに自分自身の値を使用できるようにします。カスタム プロパティに 1 つまたは複数の値を定義して、リソースのセキュリティ ルールで使用します。

例えば、「Country」という名前のカスタム プロパティを追加し、2 つの値 (USA とUK) を割り当てて、2 つの地域で異なるセキュリティ ルールを作成できるようにしたいと考えているかもしれません。

カスタム プロパティを使用するには

1. QMC へのログイン
2. [***カスタム プロパティ***] を選択します。
3. カスタム プロパティを作成または編集します。
4. リソース タイプを選択します。
5. 値を作成します。
6. リソースを選択して値を適用します。
7. カスタム プロパティを使用してセキュリティ ルールを作成します。

   カスタム プロパティに基づいたアクセス権を実装

カスタム プロパティの新規作成

カスタム プロパティを作成できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Custom properties (カスタム プロパティ)**] を選択して、概要を表示します。
3. データ マネージャーでテーブルの **新規作成** をクリックします。
4. プロパティを編集します。

ID

ID プロパティ

プロパティ	説明
名前	カスタム プロパティ名は必須で、空欄のままにはできません。名前の値では英数字 (A ~ Z および 0 ~ 9) のみを使用し、アルファベット (A ~ Z) で始めなくてはなりません。
説明	オプション。カスタム プロパティの説明を追加します。

リソース タイプ

リソースのプロパティ

プロパティ	説明
[**リソース タイプ**]	カスタム プロパティを利用可能にさせたいリソースを選択します。 カスタム プロパティは以下のリソースに適用できます: • **分析接続** • **アプリ** • [**コンテンツ ライブラリ**] • [**データ接続**] • [**エンジン**] • [**拡張機能**] • [**外部プログラムのタスク**] • [**ノード**] • [**印刷**] • [**プロキシ**] • [**タスクのリロード**] • [**リポジトリ**] • [**スケジューラ**] • [**ストリーム**] • **システム通知** • [**ユーザー同期タスク**] • [**ユーザー**] • [**仮想プロキシ**]

値

作成した値は、セキュリティルールで使用できます。
次の手順を実行します。

1. データ マネージャーでテーブルの [**値**] 見出しで [**新規作成**] をクリックします。値を入力し、[**OK**] をクリックして値を追加します。

   値はセキュリティルールで使用する前にリソースに適用する必要があります。

2. データ マネージャーでテーブルの をクリックして [**値**] リストから値を削除します。
3. [**OK**] をクリックして、削除を確定します。

5. アクション バーで [**Apply**] をクリックし、カスタム プロパティを作成して保存します。
   ページ最下部に [**追加完了**] と表示されます。

これで新しいカスタム プロパティが利用可能となりました。リソースとセキュリティルールでこの値を使用できます。

カスタム プロパティの編集

更新権限を有するカスタム プロパティを編集できます。

複数のカスタム プロパティのプロパティを、一度に編集することはできません。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Custom properties (カスタム プロパティ)**] を選択して、概要を表示します。
3. カスタム プロパティをひとつ選択し、ページの最下部にあるアクション バーで [**編集**] をクリックします。
4. プロパティを編集します。

ID

ID プロパティ

プロパティ	説明
名前	カスタム プロパティ名は必須で、空欄のままにはできません。名前の値では英数字 (A ~ Z および 0 ~ 9) のみを使用し、アルファベット (A ~ Z) で始めなくてはなりません。
説明	オプション。カスタム プロパティの説明を追加します。

リソース タイプ

リソースのプロパティ

プロパティ	説明
[リソース タイプ]	カスタム プロパティを利用可能にさせたいリソースを選択します。 カスタム プロパティは以下のリソースに適用できます: • 分析接続 • アプリ • [コンテンツ ライブラリ] • [データ接続] • [エンジン] • [拡張機能] • [外部プログラムのタスク] • [ノード] • [印刷] • [プロキシ] • [タスクのリロード] • [リポジトリ] • [スケジューラ] • [ストリーム] • システム通知 • [ユーザー同期タスク] • [ユーザー] • [仮想プロキシ]

値

作成した**値**は、セキュリティルールで使用できます。
見出し[**値**] で [**新規作成**] をクリックします。 値を入力して [**OK**] をクリックし、値を追加します。

> *値はセキュリティルールで使用する前にリソースに適用する必要があります。*

をクリックして [**Values**] リストから値を削除し、[**OK**] をクリックして確定します。

5. 操作バーで [**適用**] をクリックします。

ページの最下部に [**更新完了**] と表示されます。

カスタム プロパティの削除

削除権限を有するカスタム プロパティを削除できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMCスタートページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Custom properties (カスタム プロパティ)**] を選択して、概要を表示します。
3. 削除するカスタム プロパティを選択します。
4. アクション バーの [**Delete**] をクリックします。
   [**Delete**] ダイアログが表示されます。
5. [**OK**] をクリックします。

カスタム プロパティ値の適用

セキュリティルールでカスタム プロパティの値 を使用できるようにするには、最初にカスタム プロパティの値をリソースに適用する必要があります。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページまたは [**スタート**] ▼ ドロップダウン メニュー からリソースを選択して、概要を表示します。
3. リソース (複数可) を選択して、[**編集**] をクリックします。
4. [**Properties**] パネルから [**Custom properties**] を選択します。

   > *プロパティパネルで [**Custom properties**] を利用できない場合は、まず、リソースでカスタム プロパティを利用できるようにしなくてはなりません。これは、カスタム プロパティを作成 (または編集) する際に行います。*

5. カスタム プロパティの横のテキスト ボックスをクリックすると、利用できる値が一覧表示されます。
6. 使用したい値を選択します。
   値がテキスト ボックスの下に表示されます。
7. アクション バーで [**適用**] をクリックします。
   ページ最下部に [**追加完了**] と表示されます。

これでカスタム プロパティの値が適用されました。リソースのセキュリティルールを作成する際にこれを使用できます。

カスタム プロパティ: 全リソースへの読み取り専用アクセス権

カスタム プロパティを作成して、セキュリティルールに自分自身の値を使用できるようにします。カスタム プロパティに 1 つまたは複数の値を定義して、リソースのセキュリティルールで使用します。

たとえば、確認作業だけを担当する一部のユーザーに対し、全リソースへの読み取り専用アクセス権を設定する場合があります。その場合は、値を 1 つ指定したカスタム プロパティを作成してセキュリティルールに適用し、そのルールが必要なユーザーに適用します。

カスタム プロパティの作成

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. [**カスタム プロパティ**] を開きます。
3. データ マネージャーでテーブルの新規作成
4. カスタム プロパティに「*AccessAllResources*」という名前を付けます。
5. オプション。説明を追加します。
6. [**リソース タイプ**] で、[**ユーザー**] を選択します。
7. **Values**, click **Create new** and name the value *ReaderOnly*.
8. [**適用**] をクリックします。

1 つの値を持つカスタム プロパティを作成したので、このプロパティを使ってユーザーに全リソースへの読み取り権限を付与できます。作成、更新、公開する権限をユーザーに付与する値など、ニーズに応じてその他の値を簡単に作成できます。

> *必要な場合は、複数のリソース タイプ用のカスタム プロパティを作成できます。この例では、[**ユーザー**] を選択すれば十分です。セキュリティ ルールを作成する場合、リソース フィルターを使って全リソースへのアクセス権を付与します。*

セキュリティ ルールの作成

次の手順を実行します。

1. QMC で [**セキュリティ ルール**] を開きます。
2. データ マネージャーでテーブルの新規作成
3. セキュリティ ルールに「*ReaderAccess*」という名前を付けます。
4. 説明を追加します。このルールにより、カスタム プロパティ グループの *ReaderOnly* メンバーに全リソースへの *AccessAllResources* 読み取りアクセス権が付与されます。

   > *既定で、[**リソース フィルター**] 項目には、全リソースが選択されていることを示すアスタリスクが付いています。データ マネージャーでテーブルの▼next to the text box to view the resources.*

5. [**基本**] で、アクション [**読み取り**] が選択されていることを確認します。
6. ルール作成ボックスで、[**名前**] リストをクリックして、[@AccessAllResources] を選択します。
7. [**値**] の横にある空のテキスト ボックスをクリックして、[ReaderOnly] を選択します。
8. [**詳細設定**] セクションの [**条件**] ボックスには、以下の文字列が入っています。
   ((user.@AccessAllResources="ReaderOnly"))

> *[**コンテキスト**] リストでは、ルールをハブ、QMC、または両方に適用するかどうかを選択できます。*

9. [**適用**] をクリックします。

> *ユーザーディレクトリに接続されている場合、ディレクトリには、セキュリティルールで使用できるプロパティが含まれていることがあります。*

カスタム プロパティのユーザーへの適用

次の手順を実行します。

1. QMCで、[**ユーザー**] を開きます。
2. 1 人以上のユーザーを選択します。

> *複数のユーザーを選択する場合は、Ctrl キーを押しながらクリックします。*

3. [**編集**] をクリックします。
4. 「**ユーザーの編集**」ページで、[**カスタム プロパティ**] セクションが表示されていることを確認します。
5. カスタム プロパティ[AccessAllResources] の横のテキスト ボックスをクリックして、[ReaderOnly] を選択します。
6. [**適用**] をクリックします。

選択したユーザーに、QMC の全リソースへの読み取りアクセス権が付与され、アプリ、ストリーム、コンテンツ ライブなどを表示できるようになりました。

タグを使用する

QMC のリソース概要ページから効率よく環境を検索して管理できるようにするには、タグを作成してリソースに適用します。

タグの作成

タグを作成できます。次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMCスタートページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Tags (タグ)**] を選択して、概要を表示します。
3. データ マネージャーでテーブルの **新規作成** をクリックします。
4. タグ名を入力します。

ID

ID プロパティ

プロパティ	説明
[**名前**]	タグの名前。この名前は、一意にする必要があります。

タグに関連するアイテムの表示

[**タグに関連するアイテムの表示**] プロパティグループは、タグを使用しているリソースを表示します。リソースを編集すると、[**タグ**] プロパティグループから接続が作成されます。
[**タグに関連するアイテムの表示**] プロパティグループには、以下のリソースが含まれます。

- **Apps**
- [**アプリオブジェクト**]
- [**セキュリティルール**]
- [**拡張機能**]
- [**コンテンツ ライブラリ**]
- [**データ接続**]
- [**ノード**]
- [**エンジン**]
- [**プロキシ**]
- [**仮想プロキシ**]
- [**リポジトリ**]
- [**スケジューラ**]
- [**ストリーム**]
- [**ユーザー**]
- [**ユーザー ディレクトリ コネクタ**]
- [**タスクのリロード**]
- [**ユーザー同期タスク**]

5. アクション バーで [**適用**] をクリックして、タグを作成および保存します。
ページの最下部に [**新規タグの追加完了**] と表示されます。

タグの接続

タグをリソースに紐付けることができます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページから、あるいは [**Start**] ▼ ドロップダウン メニューからリソースの種類 ([**Apps (アプリ)**] など) を選択して、概要を表示します。

フィルタリング オプションを使用して列にフィルターを適用できます。

3. タグを紐付けたいアイテムを選択します。
4. 操作バーで [**編集**] をクリックします。
5. [**プロパティ**] セクションで [**タグ**] が選択されていることを確認します。
6. [**Tags**] テキストボックスをクリックして、利用可能なタグのリストを表示します。

   *タグを利用できない場合は、まずタグを作成する必要があります。リソースを編集するときは、タグの作成も削除もできません。スタートページに表示される [**Tags**] セクションでタグを作成します。*

7. リストをフィルタリングするには、タグ名を入力します。
8. タグを選択します。
   タグがテキストボックスの下に青色で追加されます。
9. ページの最下部で [**適用**] をクリックして変更を保存します。
   タグのラベルに **(x)** が追加されます。xはタグを使用している編集中のリソース数を示しています。

これでタグがリソースに紐付けされました。

タグの紐付け解除

タグとリソース間の接続は削除できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**Start**] ▼ ドロップダウン メニューからリソースの種類 ([**Apps (アプリ)**] など) を選択して、概要を表示します。

   フィルタリング オプションを使用して列にフィルターを適用できます。

3. タグを削除したいアイテムを選択し、アクション バーで [**編集**] をクリックします。
4. [**プロパティ**] セクションで [**タグ**] が選択されていることを確認します。
5. [**タグ**] テキストボックスで、⊗ をクリックしてタグを削除します。
6. ページの最下部で [**適用**] をクリックして変更を保存します。

タグの編集

更新権限を有するタグを編集できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Tags (タグ)**] を選択して、概要を表示します。
3. 編集するタグを選択します。
4. アクション バーで [**編集**] をクリックします。
5. プロパティを編集します。

ID

ID プロパティ

プロパティ	説明
[**名前**]	タグの名前。この名前は、一意にする必要があります。

タグの関連付けの表示

[**タグに関連するアイテムの表示**] プロパティグループは、タグを使用しているリソースを表示します。リソースを編集すると、[**タグ**] プロパティグループから接続が作成されます。
[**タグに関連するアイテムの表示**] プロパティグループには、以下のリソースが含まれます。

- **Apps**
- [**アプリオブジェクト**]
- [**セキュリティルール**]
- [**拡張機能**]
- [**コンテンツ ライブラリ**]
- [**データ接続**]
- [**ノード**]
- [**エンジン**]
- [**プロキシ**]
- [**仮想プロキシ**]
- [**リポジトリ**]
- [**スケジューラ**]
- [**ストリーム**]
- [**ユーザー**]
- [**ユーザー ディレクトリ コネクタ**]
- [**タスクのリロード**]
- [**ユーザー同期タスク**]

6. [**適用**] をクリックして変更を保存します。必須の項目が空欄の場合、[**Apply**] は無効になります。

ページの最下部に [**更新完了**] と表示されます。

タグの削除

削除権限を有するタグを削除できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Tags (タグ)**] を選択して、概要を表示します。
3. 削除するタグを選択します。

フィルタリング オプションを使用して列にフィルターを適用できます。

4. アクション バーの [**Delete**] をクリックします。
   [**Delete**] ダイアログが表示されます。
5. [**OK**] をクリックします。

1.7 QMC パフォーマンス – ベストプラクティス

Qlik Management Console (QMC) で最適なパフォーマンスを維持するには、QMC のパフォーマンスに影響を及ぼす主な要因について理解することが重要です。このトピックの助言に従うことにより、応答時間の遅延や、QMC の不適切な使用に起因するその他の問題が生じるリスクを低減できます。

パフォーマンス向上のための提案

QMC の計画、設定、維持の際には、パフォーマンス向上のために次のオプションを検討します。その中には、若干の犠牲を払う価値があるものもあるでしょう。

- 管理者の数:QMC はセルフサービス ツールとしてではなく、限定的な数の管理者用に設計されています。管理者の数を少なくすると、パフォーマンスの向上がみられます。
- アプリの数とサイズ: ハウスキーピングをお勧めします。未使用、またはほとんど使用しないアプリがあるかどうかを確認し、可能であれば削除します。超大型のアプリは、複数の小型アプリに分割できる場合があります。
- セキュリティルールの設計: 適正に設計されたセキュリティルールにより、パフォーマンスの向上が図れます。「*セキュリティルール (page 449)*」を参照してください。
- セキュリティルールのキャッシュについては、「*セキュリティルールのキャッシュ (page 450)*」を参照してください。
- カウンター:QMC で数を表示するクエリは、パフォーマンス向上のために削除できます。
- カスタム フィルター: カスタム フィルターを使用して、操作するデータにすばやくアクセスします。カスタム フィルターに接続されたデータは、ブラウザーにキャッシュされます。カスタムのフィルター ビューを切り替えると、データの変更のみがロードされます。これは、テーブル全体のリロードよりも高速です。「*テーブル ビューでのカスタム フィルターの管理 (page 27)*」を参照してください。

セキュリティルール

セキュリティルールにより、特定の条件を満たしている場合、ユーザーが作成、読み取り、更新、削除などのアクションを実行するためのリソースにアクセスを許可します。

セキュリティルールは常時提供、つまり、ユーザー アクセスを許可するために常時使用されています。セキュリティルールがアクティブにユーザーを除外することはありませんが、アクセス権を付与するセキュリティルールにユーザーが含まれていない場合、そのユーザーのアクセスは事実上拒否されます。しかし重要な点は、ユーザーがリソースにアクセスできるよう、リソースへのユーザー アクセス権を付与するルールが 1 つあるだけでは不十分だということです。多数のルールが、間接的にユーザーを排除することとは無関係です。

セキュリティルールがリソースへのアクセスを許可すると、ルール評価は停止します。ルール評価の最悪のシナリオは、ユーザに権限が全くない場合で、すべてのセキュリティルールが評価されます。

セキュリティルールのキャッシュ

Qlik Sense セキュリティルール メカニズムには、ルール評価のパフォーマンス向上のために、2 つの異なるキャッシュ レイヤーが含まれています。

- セキュリティルール キャッシュ (ルール エンジン)
- セキュリティフィルター結果キャッシュ (Qlik Sense Repository Service)

セキュリティルール キャッシュ

ルール エンジンは、リソースへのアクセスを評価するための解析ルールで使用されるコンポーネントです。セキュリティキャッシュは、ルール エンジン内にあり、解析システム ルールで構成されます。キャッシュはデータベースに保存されず、Qlik Sense Repository Service を再起動すると削除されます。セキュリティルールに変更がない場合、キャッシュは リセットされないため、パフォーマンス向上に貢献します。セキュリティルールの評価は、静的コンテンツ用にはキャッシュされません。

リリース フィルター、コンテキスト、およびアクションに応じて使用するルールをエンジンがフィルターする場合は、最も頻繁にアクセスを許可するルールから順にソートされます。

セキュリティフィルター結果キャッシュ

このキャッシュは Qlik Sense Repository Service にあります。このキャッシュを使用すると、ルール エンジンの使用を回避できます。キャッシュはデータベースに保存されず、Qlik Sense Repository Service を再起動すると削除されます。異なる方法で無効化 (削除) するキャッシュ カテゴリが 3 つあります。

- グローバル キャッシュ: セキュリティルール、負荷分散ルール、ライセンス ルール、または カスタム プロパティになんらかの変更があると、キャッシュの完全無効化がトリガーされます。その結果、セッションの開始後に得られた最適化のメリットは失われます。

- ユーザー キャッシュ: ユーザー属性 または カスタム プロパティに変更があると、ユーザーベースの無効化がトリガーされます。つまり、特定のユーザーに関連付けられたキャッシュが削除されます。

- エンティティ キャッシュ: 単一のエンティティになんらかの変更 (例えば、アプリの名前 または 所有者) があると、エンティティベースの無効化がトリガーされます。つまり、特定のエンティティに関連付けられたキャッシュが削除されます。

関連ログ

セキュリティフィルター結果のキャッシュ無効化に関連したログは次のとおりです。トラブルシューティングや監視のために使用できます。ログがある場所は次のとおりです。
C:\ProgramData\Qlik\Sense\Log\Repository\Trace\HOST_NAME_Audit_Repository.txt

グローバル キャッシュの無効化

`{reason}` によるセキュリティ フィルター結果キャッシュ全体の無効化 (情報 レベルでログに記録)

ユーザー キャッシュの無効化

`ID` があるユーザーのセキュリティ フィルター結果キャッシュを無効化:`{userId}` (デバッグ レベルでログに記録)

エンティティ キャッシュの無効化

エンティティ (type_id) のセキュリティ フィルター結果キャッシュを無効化: {entity.Type.Name}_{entity.Id} (デバッグ レベルでログに記録)

パフォーマンス効率に優れたセキュリティルールの記述ガイドライン

次のガイドラインは、セキュリティルールを記述する際の一般的なベストプラクティスを示したものです。こうした一般的なガイドラインに加えて、自身の特定の環境において、ここに記されている以外にもさらに改善できる場合があります。

特定のリソース フィルターの使用

リソースへのアクセスを評価する前に、リソース フィルターにより該当するリソースに適用されるルールを選別します。そのため、リソース フィルターはできる限り具体的にすることが重要です。フィルターが具体的であればあるほど、ルール エンジンの処理する必要があるルールを減らすことができます。

次の表に、異なる効率のリソース フィルター例を示します。

リソース フィルター

リソース フィルター	評価対象	効率
*	すべてのリソース	効率最小
app*	「app」で始まるすべてのリソース (例えば、*app*、*app.object*)	上記よりも効率的
app_*	アプリ リソース	上記よりも効率的
app_644d2485-d318-45b0-996e-29f5d379cac2	ID が「644d2485-d318-45b0-996e-29f5d379cac2」のアプリ リソース	最も効率的

最後の例は最も効率的ですが、再利用性も大幅に限定されます。一般的な推奨は、ルール内のリソースの種類に対するテストが不必要なレベルまでリソースの種類を指定することです。

正しいコンテキストと対象固有のアクションの使用

リソースへのアクセスを評価する前に、正しいコンテキストとアクションにより該当するリソースに適用されるルールを選別します。

[**ハブ内のみ**]、[**QMC 内のみ**]、または [**ハブ内とQMC の両方**] の 3 つがコンテキストの代替です。ここでも、できる限り具体的にします。最初の 2 つは、1 つのケースのみを評価するため、より効率的です。CRUD すべてへのアクセス (create, read, update, delete) を使用する代わりに、ルールが許可するアクションを指定するようにします。

複数にわたるオブジェクト参照の境界のトラバースを回避

常時とは限りませんが、多くの場合、具体的にすればするほど効率性が向上します。次の 2 つの例では、ユーザーに対し、リロード タスクへの読み取りアクセス権を付与するように設計したルールを示します。

Example 1:

```
user@property=resource.app.stream@property
```

結果: ユーザーは、タスクのアプリのストリームにあるカスタム プロパティに一致するカスタム プロパティを有するユーザであれば、リロード タスクを読み取ることができます。

非効率的。高価なオブジェクト参照の境界 (アプリとストリーム) はトラバースされます。

Example 2:

```
user.@property=resource.@property
```

結果: ユーザーは、タスクに直接あるカスタム プロパティに一致するカスタム プロパティを有するユーザであれば、タスクを読み取ることができます。

より効率的。境界のトラバースを回避します。

カスタム プロパティの数の最小化

場合によっては、少ないほど効率的です。カスタム プロパティの数を最小限に保つとメリットがあります。

Example 3:

```
user.@CustomProperty=resource.@CustomProp2
```

非推奨。リポジトリからフェッチする必要のあるカスタム プロパティが 2 つあるからです。

Example 4:

```
user.@customProperty="ReaderOnly"
```

推奨。リポジトリからフェッチする必要のあるカスタム プロパティは 1 つのみだからです。

ルール構文内の実行順序は重要

ルールを記述するときは、最も高価な演算を最後にするようにします。次の例では、条件の 1 つが true であれば十分です。高価ではない演算が先にあり、true の場合は、より高価な演算の評価が不要になります。

Example 5:

```
resource.app.stream.owner.@a = "b" or user.name = "user1"
```

非効率的。より高価な演算が最初に評価されるからです。

Example 6:

```
user.name = "user1" or resource.app.stream.owner.@a = "b"
```

より効果的。より高価な演算が最後にあり、最初の演算が false の場合にのみ評価されます。

ハード コートの値を回避 – 代わりに属性を使用

`resource.@property == "user1"` や `resource.@property == "user2"` といった、ハード コートの文字列からなる複数のルールよりも、望ましいのは `resource.@property == user.name` といったルールです。

HasPrivilege は非効率的

`HasPrivilege("アクション")` は 2 番目のルールをトリガーするため、できる限り使用を避けるようにします。

Example 7:

```
App.Stream.HasPrivilege("read")
```

ルールの 2 番目の評価をトリガーする、ルール エンジンの新しいインスタンスを作成する機能です。

*Like*演算子は効率が良くありません

ルール評価のパフォーマンスに悪影響を及ぼす可能性があるため、可能であれば、`(EXPRESSION) like (EXPRESSION)` は避けてください。

Example 8:

```
resource.name like unit*"
```

Like 演算子は、文字列全体を比較する等号 (=) 演算子とは対照的に、文字列の各文字で比較します。

参照先:

1.8 Qlik Sense Enterprise on Windowsの構成

Qlik Sense Enterprise on Windows をインストールした後、ユーザーがハブにアクセスして Qlik Sense の使用を開始できるように Qlik Sense 環境を準備する必要があります。以下は、インストール後に Qlik Sense Enterprise on Windows を構成した場合に推奨されるワークフローです。

次の手順を実行します。

1. インストール中に実行されなかった場合は、ライセンスをアクティベートしてください。これにより以下が行われます:
    - サイトのルート管理者になる。
    - 定義されたユーザー数のアナライザー アクセスとプロフェッショナル アクセスを提供する (ユーザーベースのライセンス)
    - アクセス タイプで使用できるトークンを提供する (トークンベースのライセンス)。
2. インストール中に実行されなかった場合は、自分にユーザー アクセスを割り当てる。
3. ユーザーをインポートする準備をするために、ユーザー ディレクトリ コネクタを に追加するQMC。
4. ユーザー ディレクトリ コネクタにより設定されたディレクトリ サービスからユーザーを取得するためにユーザー ディレクトリと同期する。
5. ルート管理者以外の管理者に QMC へのアクセスを与える場合は、それらの管理者ユーザーを追加する。
6. ユーザーにプロフェッショナル アクセスまたはアナライザー アクセス (ユーザーベースのライセンス)、またはユーザー アクセスまたはログイン アクセス (トークンベースのライセンス) のアクセス タイプを割り当てて、ユーザーがハブ内のストリームやアプリにアクセスできるようにする。ユーザーに [**プロフェッショナル アクセス**] または [**アナライザー アクセス**] (ユーザーベースのライセンス)、または [**ユーザー アクセス**] または [**ログイン アクセス**] (トークンベースのライセンス) のアクセス タイプを割り当てて、ユーザーがハブ内のストリームやアプリにアクセスできるようにする。

7. 新しいストリームを作成する。
8. ストリーム用のセキュリティルールを作成して、ユーザーがストリームから読み取り/公開できるようにする。アナライザー アクセスは、公開権限を付与しません。

これで Qlik Sense ユーザーが Qlik Sense Enterprise on Windows 環境を利用できるようになりました。

*既定では、すべての Qlik Sense ユーザーは [**Everyone**] と呼ばれる既定のストリームへの読み取り権限と公開権限があります。*

デフォルトの構成

Qlik Sense インストールには、[**Everyone**] ストリーム、[**Monitoring apps**]、6 つの管理者ロール ([**RootAdmin**]、[**AuditAdmin**]、[**ContentAdmin**]、[**DeploymentAdmin**]、[**HubAdmin**]、[**SecurityAdmin**]) が含まれます。

インストールのデフォルトの構成 Qlik Sense は以下のとおりです。

- すべての認証ユーザーには [**Everyone**] ストリームへの読み取り権限と公開権限があります。
- 匿名ユーザーには [**Everyone**] ストリームの読み取り権限があります。
- 管理者のロールの [**RootAdmin**]、[**ContentAdmin**]、[**SecurityAdmin**] には [**Monitoring apps**] ストリームの読み取り権限と公開権限があります。
- [**RootAdmin**] は、Qlik Sense の全リソースへのフルアクセス権を有します。
- その他の管理者は、Qlik Sense リソースのサブセットにアクセスできます。
- プロキシはローカル エンジンに対してロード バランシングを行います。
- 匿名ユーザーにはコンテンツ作成が許可されていません。
- 所有オブジェクトの所有者は 1 人のみです。
- 公開されていないアプリは、そのオーナーのみが表示できる。
- 公開アプリは編集できません。
- 認証ユーザー (匿名でない) は
    - 所有するアプリを公開します。
    - 未公開アプリのプライベート アプリオブジェクトを新規に作成できます。
    - 公開済アプリのプライベート アプリオブジェクト (シート、ブックマーク、ストーリー) を新規に作成できます。
    - 見ることができるアプリデータをエクスポートできます。
- 誰でも Qlik Sense からデータ接続を管理できますが、フォルダディレクトリタイプのデータ接続を管理できるのは [**RootAdmin**]、[**ContentAdmin**]、[**SecurityAdmin**] のみです。
- 誰でも拡張機能を表示できます
- コンテンツ ライブラリの更新権限を持つユーザーは誰でも その対応ファイルを管理できます。

セキュリティの設定

次の Qlik Sense セキュリティ設定は、QMC から管理します。

- さまざまな範囲の QMC 管理者アクセス権をユーザーに与える管理者ロール
- 異なるユーザー認証方法の認証

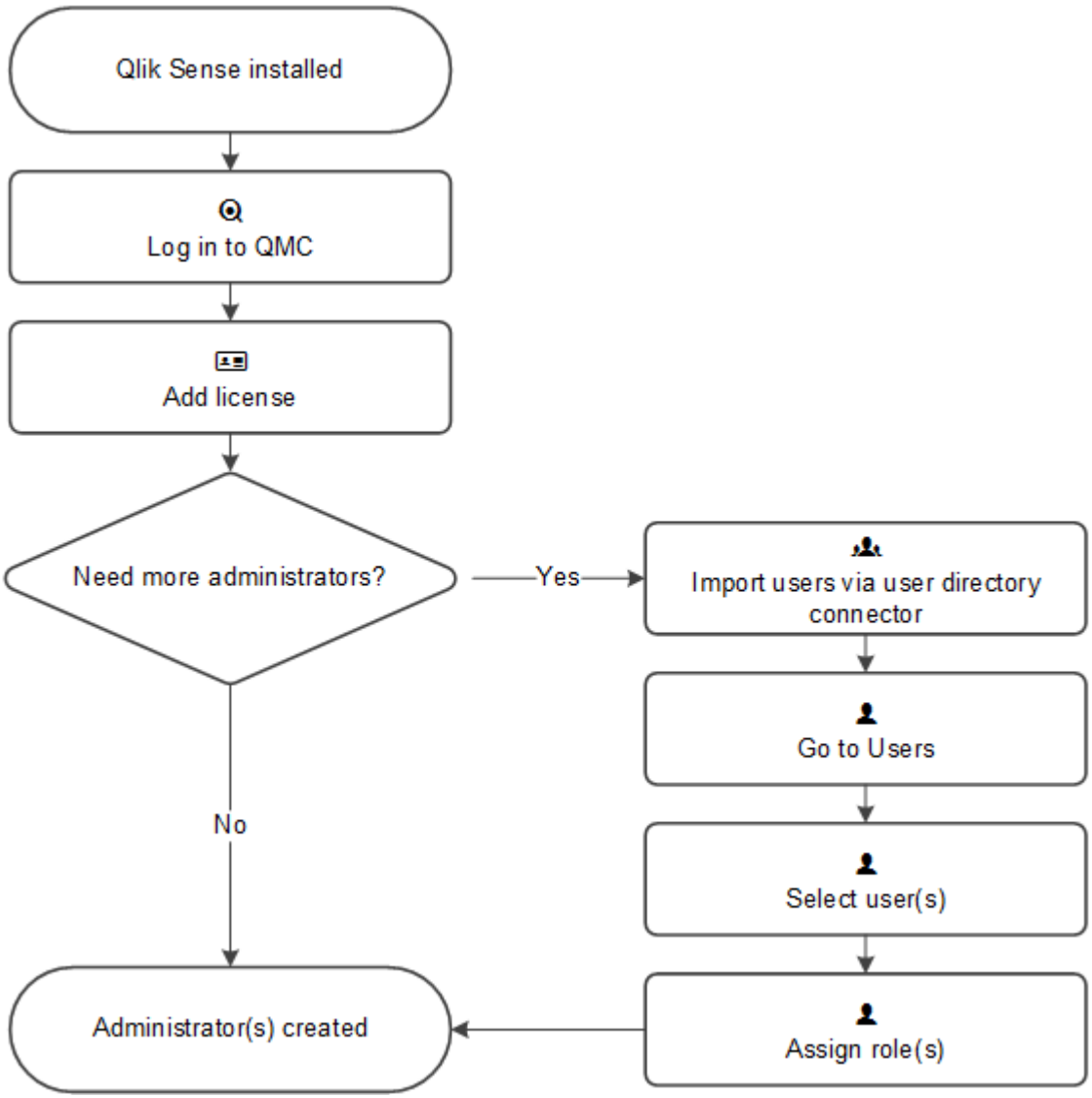
- Web ブラウザとプロキシ間の通信のプロキシ証明書
- URI に基づくさまざまなモジュールを使用して Qlik Sense にアクセスできるようにする仮想プロキシ
- セキュリティルールで独自の値を使用できるカスタム プロパティ
- Qlik Sense リソースにユーザーアクセス権を与えるアクセス制御およびセキュリティルール

QMC での作業に有用なヒントについては、「QMC パフォーマンス – ベストプラクティス (page 449)」を参照してください。

ルート管理者および管理者ユーザーの追加

QMCにアクセスしてサーバー ライセンスを追加する最初のユーザーは、Qlik Senseシステムのルート管理者 (RootAdmin) ロールを取得します。このユーザーは、サイトのあらゆるリソース (セキュリティルール、ストリーム、ノードなど) への完全なアクセス権があります。追加ユーザーを RootAdmin に割り当てることや、異なる管理権限を持つ他の管理者 ロールに割り当てることもできます。

このワークフローは、QMC管理者の追加方法を示しています。



ルート管理者 (RootAdmin) の設定ワークフロー

次の手順を実行します。

1. Qlik Senseがインストールされていることを確認します。
2. ルート管理者 (RoodAdmin) として使用する Windows アカウントを使用して (QMC) にログインします。
3. LEF ライセンスを QMC に追加します。

   LEF を追加すると、Qlik Sense の root 管理者となります。

4. 管理者をさらに追加するには、*管理者ユーザーの設定ワークフロー(page 456)*を参照してください。

これでルート管理者ロールが作成されました。

管理者ユーザーの設定ワークフロー

次の手順を実行します。

1. ルート管理者 (RootAdmin) としてログインします。
2. ユーザーディレクトリコネクタを使用してユーザーをインポートします。
3. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**ユーザー**] を選択して、概要を表示します。
4. 管理権限を設定するユーザーを選択し、[**Edit**] をクリックします。
5. ⊕ [**ロールの追加**] をクリックし、ドロップダウン リストからロールの 1 つを選択します。新しいロールの名前を入力できますが、適切に定義するまでは有効になりません。

   一人のユーザーに複数の管理者ロールを割り当てることができます。

   自分で、自分自身のルート管理者ロールを削除することはできません。これは、QMC を使用することから RootAdmin を誤ってブロックしてしまうのを防止するためです。

これで管理者ロールが作成されました。

Qlik Sense の場合と同様、ユーザーは、QMC のリソースへのアクセス権を持っていない場合には、QMC インターフェースからそのリソースにアクセスすることができません。たとえば、ユーザーのロールを RootAdmin から DeploymentAdmin に変更すると、そのユーザーは QMC のアプリやシート、ストリーム、データ接続ページなどにアクセス不能になります。

*ルート管理者は、Qlik Sense システムで作成されたセキュリティルールを変更または削除することはできません。このようなセキュリティルールは [**セキュリティルール**] 概要ページに一覧表示され、[**タイプ**] は [**既定**] に設定されます。*

既定の管理者ロール

QMC では、管理者ロールのセットがあらかじめ定義されています。各ロールには、特定の目的に合わせて調整されたセキュリティロールが関連付けられています。RootAdmin はインストール時に作成されます。このロールは、QMC に有効なライセンス キーを最初に入力したユーザーに対して自動的に割り当てられます。RootAdmin には、Qlik Senseのすべてのリソースに対するフル アクセス権が付与されています。

管理権限 (page 457) の表に、デフォルトの QMC 管理者 ロール、そのロールで管理可能な QMC の部分、付与されてている管理権限の概要を示します。HubAdmin は QMC のエリアを管理できません。このロールには、ハブでのみ管理権限があります。詳しくは「*HubAdmin (page 551)*」を参照してください。

RootAdmin または SecurityAdmin として、目的に沿った新しいロールを作成することができます。

QMC での作業に有用なヒントについては、「QMC パフォーマンス – ベストプラクティス (page 449)」を参照してください。

管理権限

*凡例 (page 458)*に、この表に示されてるアクションの説明を示します。

管理権限

QMC リソース	AuditAdmin	ContentAdmin	DeploymentAdmin	HubAdmin	SecurityAdmin
Stream_*	R	CRUDPO	R (監視アプリのストリーム)	-	CRUDPO
App*	RA	CRUDEPAO	RUA	-	CRUDEPAO
App.Object*	R	CRUDPO	R (監視アプリ)	-	CRUDPO
DataConnection_*	R	CRUDO	-	-	CRUDO
Extension_*	R	CRUDO	R	-	R
ContentLibrary_*	R	CRUDO	R	-	CRUDO
ContentCacheControl_*	-	R	-	-	R
UserDirectoryConnector*	R	CRUD	CRUD	-	CRUD
ServerNodeConfiguration_*	R	-	CRUD	-	R
Engine*	R	-	CRUD	-	-
Proxy*	R	-	CRUD	-	CRUD
VirtualProxy*	R	-	CRUD	-	CRUD
Repository*	R	-	CRUD	-	-

QMC リソース	AuditAdmin	ContentAdmin	DeploymentAdmin	HubAdmin	SecurityAdmin
Scheduler*	R	-	CRUD	-	-
ReloadTask_*	R	CRUD	CRUD	CRU	-
UserSyncTask_*	R	CRUD	CRUD	-	CRUD
SchemaEvent_*	R	CRUD	CRUD	CRU	-
CompositeEvent_*	R	CRUD	CRUD	-	-
User*	R	CRUD	CRUD	-	CRUD
SystemRule_*	R	CRUD	CRUD	-	CRUD
CustomProperty*	R	CRUD	CRUD	-	CRUD
License_*	R	R	CRUD	-	R
Tag_*	R	CRUD	CRUD	-	CRUD
FileExtension	R	CRD	-	-	CRD
FileExtensionWhiteList	R	RU	-	-	RU
AnalyticConnection_*	R	CRUD	R	-	CRUD
TermsAcceptance_*	R	R	CRUD	-	R
ServiceStatus_*	R	-	CRUD	-	R
ServiceCluster	R	-	CRUD	-	-
LoadBalancingSelectList	R	-	R	-	-
* (監査ビューのすべて)	R	-	-	-	-

凡例

次の表に、管理者が実行可能なアクションを示します。

[キャプション]

アクション	説明
C:作成	リソースの作成
R:読み取り	リソースの読み込み
U:更新プログラム	リソースの更新
D:削除	リソースの削除
E:エクスポート	アプリのエクスポート
A:データのエクスポート	アプリデータのエクスポート

アクション	説明
P:公開	リソースをストリームに公開
O:所有者の変更	リソースの所有者の変更
L:役割の変更	ユーザーの役割の変更
B:負荷分散	ノードおよび仮想プロキシの負荷の分散
M:オフラインでアクセス	オフラインでアプリにアクセス

既定の管理ロールの QMC セクション アクセス

QMC では、管理者ロールのセットがあらかじめ定義されています。各ロールは、ニーズに応じて QMC のセクションへの管理者読み取りアクセス権を付与する QMC セクション アクセス ルールに関連付けられています。RootAdmin は、すべての QMC セクションへのアクセス権を持っています。

QMC セクション アクセス ルールは、QMC セクションへの読み取りアクセス権を付与するだけです。他の権限 (作成、編集、更新など) については、次を参照してください。凡例 (page 458)。HubAdmin はハブにのみアクセスでき、QMC にはアクセスできません。

既定の管理者の読み取りアクセス権

「R」は、管理者がその QMC セクションへの読み取りアクセス権を持っていることを示します。

既定の管理者のアクセス権

QMC	AuditAdmin	ContentAdmin	DeploymentAdmin	SecurityAdmin
QmcSection_Audit	R	R	R	R
QmcSection_Tag	R	R	R	R
QmcSection_Stream	-	R	-	R
QmcSection_App	-	R	R	R
QmcSection_App.Object	-	R	-	R
QmcSection_DataConnection	-	R	-	R
QmcSection_ AnalyticConnection	-	R	-	R
QmcSection_User	-	R	R	R
QmcSection_ CustomPropertyDefinition	-	R	R	R
QmcSection_Task	-	R	R	-
QmcSection_Event	-	R	R	-
QmcSection_SchemaEvent	-	R	-	-
QmcSection_CompositeEvent	-	R	-	-

QMC	AuditAdmin	ContentAdmin	DeploymentAdmin	SecurityAdmin
QmcSection_Extension	-	R	-	-
QmcSection_ReloadTask	-	R	R	-
QmcSection_UserSyncTask	-	R	R	-
QmcSection_ContentLibrary	-	R	-	R
QmcSection_Templates	-	-	R	R
QmcSection_ ServerNodeConfiguration	-	-	R	-
QmcSection_ServiceCluster	-	-	R	-
QmcSection_EngineService	-	-	R	-
QmcSection_ProxyService	-	-	R	R
QmcSection_ VirtualProxyConfiguration	-	-	R	R
QmcSection_ RepositoryService	-	-	R	-
QmcSection_SchedulerService	-	-	R	-
QmcSection_PrintingService	-	-	R	-
QmcSection_Licenses	-	-	R	-
QmcSection_ License.LoginAccessType	-	-	R	-
QmcSection_ License.UserAccessType	-	-	R	-
QmcSection_ License.UserAccessRule	-	-	R	-
QmcSection_ License.ApplicationAccessTyp e	-	-	R	-
QmcSection_Token	-	-	R	-
QmcSection_UserDirectory	-	-	R	-
QmcSection_Certificates	-	-	R	R
QmcSection_ Certificates.Export	-	-	R	R
QmcSection_SyncRule	-	-	R	-
QmcSection_ LoadBalancingRules	-	-	R	-
QmcSection_SystemRule	-	-	-	R

認証

標準的なQlik Senseをインストールすると、Qlik Sense Proxy Service (QPS) に、Microsoft Windows ユーザーの認証を処理するモジュールが組み込まれます。

別の認証方法を使用したり、認証用にカスタマイズされたソリューションを実装することもできます。

相互認証 (双方向認証とも呼ばれます) は Qlik Sense ではサポートされていません。

匿名の認証

ユーザーID や資格情報を入力することなく、ユーザーが Qlik Sense にアクセスできるようにすることができます。これは、仮想プロキシ プロパティ[**匿名アクセス モード**] を編集して行います。匿名使用にはさまざまなレベルがあるので、以下の手順の説明を参照してください。

プロフェッショナル アクセスとアナライザー アクセスを持つユーザーベースのライセンスは、匿名の認証に対応していません。キャパシティベースのライセンスでは、Analyzer Capacity ライセンス (署名付きキー) または トークン ライセンスを使用した匿名認証が可能になります。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**仮想プロキシ**] を選択して、概要を表示します。
3. 認証を取り扱う仮想プロキシを選択して、[**編集**] をクリックします。
4. [**匿名アクセス モード**] を [**認証**] プロパティグループで編集します。
   - 匿名のユーザーがユーザー アカウントに切り替えられるようにしたい場合は、ドロップダウン リストで [**匿名ユーザーを許可**] を選択します。
   - すべてのユーザーを常に匿名にするには、[**常に匿名ユーザー**] を選択します。

   既定値は [**匿名ユーザーなし**] になっているため、Qlik Sense ユーザーはユーザーID と資格情報を入力する必要があります。
5. アクション バーで [**適用**] をクリックし、変更内容を保存します。
   ページの最下部に [**更新完了**] と表示されます。

匿名認証方式を運用するには、匿名ユーザーが Analyzer Capacity ライセンス (署名付きライセンス キーが必要) またはログイン アクセス トークンのいずれかを許可するライセンス ルールを作成する必要があります。

Analyzer Capacity ライセンス

次の手順を実行します。

1. QMC スタートページから、または [**スタート**▼] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
2. **Analyzer Capacity ルール**を選択します。
3. クリックして**新規作成** をクリックします。

4. ID プロパティを編集します。

ID プロパティ

プロパティ	説明
名前	ルールの名前を入力します (必須)。
説明	ルールの簡単な説明を入力します (任意)。

5. 基本ルールまたは高度なルールを作成します。
   a. [**基本**プロパティ] で、次の操作を行います。
      - Select **user**: `userDirectory =`
      - Select **value**:NONE
   b. [高度なプロパティ] で、次の操作を行います。
      - Conditions 項目で、`user.IsAnonymous()` を追加します
6. 操作バーで [**適用**] をクリックします。

これで、Qlik Sense を匿名で使用できるようになりました。

ログイン アクセス トークン

次の手順を実行します。

1. QMC スタート ページから、または [**スタート**▼] ドロップダウン メニューから [**ライセンスの管理**] を選択して、概要を表示します。
2. [**ログイン アクセス ルール**] をクリックします。
3. 編集するルールを選択し、操作バーの [**編集**] をクリックします。
4. [**関連するアイテム**] の [**ライセンス ルール**] をクリックします。
5. 編集するライセンス ルールを選択し、操作バーで [**編集**] をクリックします。
6. [**詳細設定**] セクションの [**条件**] テキスト項目に、「*user.isAnonymous()*」を追加します。

これで、Qlik Sense を匿名で使用できるようになりました。

匿名ユーザーは、ハブで既定の Everyone ストリームを使用できます。これは、匿名アクセス用に既に設定されています。匿名ユーザー専用のストリームを作成することもできます。匿名ユーザー向けのストリームの作成の詳細については、「Qlik Sense Enterprise Client-Managed で匿名ハブ アクセスを許可する方法」を参照してください。

認証方法

認証は、リバース プロキシまたはユーザーを認証するためのフィルタリングを提供するシングル サインオン (SSO) システムと併用して、頻繁に使用されます。

ヘッダーと SAML の認証は、既定の仮想プロキシには使用できません。既定の仮想プロキシしかない場合には、ヘッダーや SAML の認証用に新しい仮想プロキシを作成する必要があります。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**仮想プロキシ**] を選択して、概要を表示します。
3. 認証を取り扱う仮想プロキシを選択して、[**編集**] をクリックします。
4. [**認証**] プロパティグループで必要事項を選択します。
   選択する認証方法によって、追加項目は異なります。

認証プロパティ

プロパティ	説明	既定値
[**匿名アクセスモード**]	• **匿名ユーザーを拒否**: ユーザは、ユーザ ID と資格情報を指定する必要があります。 • **匿名ユーザーを許可**: ユーザは匿名で入力しますが、ユーザアカウントで切り替えてログインすることができます。 • **常に匿名ユーザー**: ユーザーは常に匿名です。	匿名ユーザーなし
[**認証方法**]	• [**Ticket**]: チケットは認証に使用されます。 • [**ヘッダー認証静的ユーザー ディレクトリ**]: 静的ヘッダー認証を許可します。QMC でユーザー ディレクトリを設定します。 • [**ヘッダー認証動的ユーザー ディレクトリ**]: 動的ヘッダー認証を許可します。ヘッダーからユーザー ディレクトリの情報を取得します。 • SAML:SAML2 は認証に使用されます。 • JWT:JSON Web Token は認証に使用されます。 • OIDC:OpenID Connect は認証に使用されます。	チケット
[**ヘッダー認証ヘッダー名**]	ヘッダー認証が許可される場合、ユーザーを識別する HTTP ヘッダー名. ([**Authentication method**] プロパティに [**Header authentication static user directory**] または [**Header authentication dynamic user directory**] のいずれかを選択して) ヘッダー認証を許可する場合、必須です。 *ヘッダー認証は US-ASCII のみをサポートしています (UTF-8 はサポートしていません)。*	空
[**ヘッダー認証静的ユーザー ディレクトリ**]	ヘッダー認証を受けたユーザーの追加情報を取得できるユーザー ディレクトリ名。([**Authentication method**] プロパティに [**Header authentication static user directory**] を選択して) 静的ヘッダー認証を許可する場合は必須です。	空

プロパティ	説明	既定値
[**ヘッダー認証動的ユーザーディレクトリ**]	([**Authentication method**] プロパティに [**Header authentication dynamic user directory**] を選択して) 動的ヘッダー認証を許可する場合、必須です。入力するパターンには '$ud' や '$id' が含まれ、これらを分離する方法も含まれている必要があります。 **ヘッダーの設定および一致の例** `$ud\\$id` – USERDIRECTORY\userid と一致させます (\を追加して、バックラッシュをエスケープする必要があります) `$id@$ud` – userid@USERDIRECTORY と一致させます ($id と$ud の順番は関係ありません) `$ud:::$id` – USERDIRECTORY:::userid と一致させます	空
[**Windows 認証パターン**]	ログイン用に選択された認証パターン。User-Agent ヘッダーに Windows 認証パターン文字列が含まれている場合、Windows 認証が使用されます。一致する文字列がない場合は、フォーム認証が使用されます。	Windows
[**認証モジュールは URI をリダイレクトします**]	外部の認証モジュールを使用する場合、クライアントは認証のため、この URI へリダイレクトされます。	空欄 (既定モジュール: Windows 認証の Kerberos/NTLM)
SAML シングル ログアウト	SAML シングル ログアウト用にサービス プロバイダーが開始するフローを有効にする場合は、このチェック ボックスをオンにします。オンにした場合、仮想プロキシ用に生成されたメタデータ ファイルに、POST およびリダイレクト バインディング用のシングル ログアウトの場所が含められます。	空

プロパティ	説明	既定値
SAML ホスト URI	クライアントに表示されるサーバー名。この名前は、クライアントが QMC などの Qlik サービスにアクセスする際に使用されます。 サーバー名はコンピュータ名と同一である必要はありませんが、ほとんどの場合、同じ名前が使用されます。 URI には http:// または https:// のいずれかを使用できます。http:// を使用するには、仮想プロキシがリンクされているプロキシの編集ページで [**Allow HTTP (HTTP を許可)**] を選択する必要があります。 ([**Authentication method**] プロパティで **SAML** を選択することにより) SAML 認証を許可する場合は必須になります。	空
SAML エンティティ ID	サービスプロバイダーを識別する ID。ID は一意にする必要があります。 ([**Authentication method**] プロパティで **SAML** を選択することにより) SAML 認証を許可する場合は必須になります。	空
[**SAML IdP メタデータ**]	IdP からのメタデータはサービスプロバイダーの構成に使用され、SAML 認証が正常に動作するために必要です。メタデータの一般的な入手方法は、IdP Web サイトからのダウンロードです。 [参照] ボタンをクリックしてアップロード用に IdP metadata .xml ファイルを開きます。エラーを回避するには、[**View content (コンテンツを表示)**] をクリックしてファイルのコンテンツと形式が正しいことを確認します。 メタデータがないと構成は未完了になります。	-
SAML ユーザー ID に使用する属性	ユーザー ID を説明する属性の SAML 属性名。名前やフレンドリな名前を使用して属性を識別できます。 *必須の SAML 属性名が分からない (page 641)*	空
SAML ユーザーディレクトリに使用する属性	ユーザーディレクトリを説明する属性の SAML 属性名。名前やフレンドリな名前を使用して属性を識別できます。名前の値がかっこ内にある場合、その値はコンテンツの属性値として使用されます。[例] では定数属性値「例」を提供しています。 *必須の SAML 属性名が分からない (page 641)*	空

プロパティ	説明	既定値
SAML 署名アルゴリズム	署名 SAML 要求に使用されるハッシュアルゴリズム。SHA-256 を使用するには、関連する秘密キーのプロバイダーが「Microsoft Enhanced RSA and AES Cryptographic Provider」である第三者機関の証明書が必要となります。	-
[**SAML 属性マッピング**]	[**新しい属性の追加**] をクリックして SAML 属性を Qlik Sense 属性にマッピングして、[**必須**] を選択することでこれらを必須とするかどうかを定義します。名前やフレンドリな名前を使用して属性を識別できます。名前の値がかっこ内にある場合、その値はコンテンツの属性値として使用されます。[例] では定数属性値「例」を提供しています。 *SAML 応答ベースの属性は、製品監査を実行するときに考慮に入れられます。*	-

プロパティ	説明	既定値
JWT 証明書	JWT .X509 パブリック キー証明書を PEM 形式で追加します。パブリック キー証明書の例は次の通りです。 -----BEGIN CERTIFICATE----- MIIDYTCCAkmgAwIBAgIJAM/oG48ciCGeMA0GCSqGSIb3DQEBCwUAMEcxEDAOBgNV BAoMB0NvbXBhbnkxEzARBgNVBAMMCkpvaG4gRG9ubmUxHjAcBgkqhkiG9w0BCQEW D2pkZUBjb21wYW55LmNvbTAeFw0xNzAzMjAxMjMxNDhaFw0yNzAzMTgxMjMxNDha MEcxEDAOBgNVBAoMB0NvbXBhbnkxEzARBgNVBAMMCkpvaG4gRG9ubmUxHjAcBgkq hkiG9w0BCQEWD2pkZUBjb21wYW55LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP ADCCAQoCggEBALIaab/y0u/kVIZnUsRVJ9vaZ2coiB3dVl/PCa40fyZdOIK5CvbA dOmJhuM7m/L4PldKmWh7nsPVC6SHAwgVwXASPHZQ6qha9ENChI2NfvqY4hXTH//Y FYaGLuKHD7pE7Jqt7Bhdh1zbBjrzsr1eU4Owwv9W9DxM4tVx3Xx8AUCNRoEWgObz Oqw9CfYY7/AWB8Hnr8G22X/lO/i4uJhiIKDVEisZ55hiNTEyqwW/ewOilI7EAngw L80D7WXpC2tCCe2V3fgUjQM4Q+0jEZGiARhzRhtaceuTBnnKq3+DnHmW4HzBuhZB CLMuWaJowkKaSfCQMel6u0/Evxc8i8FkPeMCAwEAAaNQME4wHQYDVR0OBBYEFNQ9 M2Y5WlRCyftHlD2oIk12YHyBMB8GA1UdIwQYMBaAFNQ9M2Y5WlRCyftHlD2oIk12 YHyBMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAHO46YLxtcMcanol PUC5nGdyYchZVHkd4F5MIe82mypwFszXGvpxKQXyAIPMkTIGb1wnE/wbCfB7moxX oFo+NoASER6wtt6FPHNcCiCXHm3B+2at16nOeMLfDefhQq03Q7qjfoa+7woAYole C9fTHGAl4TMIPThGSluiVLOLgHFUHpZryI6DdiEutXiH4afXaw0mScG36Z1uvHIq dPtjb/vDmIb9jvLITe8mZ8c2isIaBCLOdFvNupARxK7U3UD6HzGIh4x7eqo6g9CK mKIz25FHrKTkyi1n/0+SAlOGp8PSnWrRZKmHkHbpfY5lpCuIBY9Cu2l1Xeq4QW5E	空

プロパティ	説明	既定値
JWT ユーザー ID に使用する属性	ユーザー ID を説明する属性の JWT 属性名。	空
JWT ユーザーディレクトリに使用する属性	ユーザーディレクトリを説明する属性の JWT 属性名。名前の値がかっこ内にある場合、その値はコンテンツの属性値として使用されます。[例] では定数属性値「例」を提供しています。	-
[**JWT 属性マッピング**]	[**新しい属性の追加**] をクリックして JWT 属性を Qlik Sense 属性にマッピングします。名前の値がかっこ内にある場合、その値はコンテンツの属性値として使用されます。[例] では定数属性値「例」を提供しています。	空
オプションのOIDC 属性を無効化	ユーザーディレクトリコネクタを介してユーザーを同期する場合にのみ使用します。選択されている時は、ユーザーディレクトリコネクタの同期から送られてくる**名前**、**グループ**、**メール**、**画像**の属性が、OIDC からの属性で上書きされないように保護されます。	
OpenID Connect メタデータ URI	OpenID Connect プロトコルを使用して ID プロバイダとやり取りする OAuth クライアントに関して、構成情報を提供するエンドポイントへの URL。	
クライアント ID	ユーザ認証用に ID プロバイダーで設定されたクライアントの ID。	
クライアントシークレット	ID プロバイダで構成されているクライアントのシークレット。	
領域	ID プロバイダーに関連付ける名前で、マルチクラウドでの名前の一貫性に使用されます。 サブジェクト属性値の形式が*domainname\username*の場合、**realm**はオプションです。そうでない場合、**realm** は必須です。	
サブジェクト	エンティティ/ユーザーに関するステートメント (名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。 必須。	

プロパティ	説明	既定値
名前	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。 必須。	
グループ	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。	
電子メール	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。 必須。	
client_id:	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。	
写真	エンティティ/ユーザーに関するステートメント(名前/値のペア) および OpenID Connect サービスに関するメタデータ。カンマで区切られた複数の値を使用できます。	
スコープ:	アクセス トークンの発行時にアクセス権限を指定するために、OAuth 2.0 の仕様で使用されます。たとえば、ID プロバイダでユーザー グループ機能をサポートするためにグループ スコープが必要な場合は、このオプションを使用してグループ スコープを追加します。	
OIDC 属性マッピング	[**新しい属性の追加**] をクリックして OIDC 属性を Qlik Sense 属性にマッピングして、[**必須**] を選択することでこれらを必須とするかどうかを定義します。名前やフレンドリな名前を使用して属性を識別できます。	

5. [**適用**] をクリックして変更を保存します。必須の項目が空欄の場合、[**Apply**] は無効になります。ページの最下部に [**更新完了**] と表示されます。

SAML 認証

Security Assertion Markup Language (SAML) は認証と承認のためのデータ形式です。SAML の主なメリットの 1 つは シングル サインオン (SSO) を有効にすることです。これによりユーザーがクラウド アプリケーションや Web サイトにログオンする必要がある回数を最小限に抑えることができます。

認証プロセスには 3 つのエンティティが関与します。

- ユーザー
- ID プロバイダー (IdP)
- サービス プロバイダー (SP)

ID プロバイダーがユーザーを認証します。ID プロバイダーがユーザーの ID を断言すると、サービス プロバイダーはユーザーにサービスへのアクセスが提供できるようになります。ID プロバイダーによって SSO が有効にされているため、ユーザーは各サイトにログインしなくても、複数のサービス プロバイダーのサイトやアプリケーションにアクセスできます。

ID プロバイダーによって開始される SSO

ID プロバイダーによって開始される SSO の場合、ユーザーが ID プロバイダーに直接ログインすると、ID プロバイダーによって SSO 認証が実行されます。

RelayState は常に *https://<machine_name>/<vp_prefix>/hub* に設定することをお勧めします。RelayState が空の場合、一部の ID プロバイダーでは `post` 要求の代わりに `get` 要求が送信されるため、エラーが生じます。

RelayState が空の場合、スペルミスがある場合、またはホストの許可リストに含まれていない場合には、ユーザーは自動的にハブにリダイレクトされます。

IdP から開始する SSO を機能させるには、アサーションに署名する必要があります。

サービス プロバイダーによって開始される SSO

サービス プロバイダーによって開始される SSO の場合、ユーザーはサービス プロバイダー サイトでログインを開始しますが、SP サイトではログインされず、ID プロバイダーによって SSO 認証が開始されます。認証プロセスでは、Qlik Sense がサービス プロバイダーとなります。ユーザーが Qlik Sense にログインすると、ログイン情報は実際の SSO 認証を処理する ID プロバイダーに転送されます。

メタデータ

サービス プロバイダー (Qlik Sense) では、ID プロバイダーからの構成情報が必要になります。この情報は IdP メタデータ ファイルとして利用できます。ユーザーは構成を簡単にするためにこのファイルをダウンロードして、サービス プロバイダーに提供できます。IdP メタデータは QMC からアップロードされます。

すべての IdPs でメタデータ ファイルのダウンロードがサポートされるわけではありません。ダウンロードがサポートされていない場合、メタデータ ファイルは手動で作成できます。

Qlik Sense はサービス プロバイダーとして ID プロバイダーに QMC からダウンロードした SP メタデータを提供します。メタデータには次の情報が含まれています。

- Assertion consumer service (ACS) URL
- エンティティ ID
- セキュリティ証明書

証明書を含まないメタデータ ファイルで仮想プロキシを設定すると、IdP 開始ワークフローは機能しません。

Wikipedia: SAML 2.0

SAML の構成

SAML の設定で、ユーザーがクラウド アプリケーションや Web サイトにログオンする回数を軽減するための シングル サインオン (SSO) ソリューションを有効にできます。SAML の設定には、次の手順があります。

1. 仮想プロキシを構成する。
   この手順には、ID プロバイダの メタデータのアップロードが含まれます。
2. 仮想プロキシをプロキシにリンクする。
3. サービス プロバイダの メタデータを ID プロバイダにアップロードする。
4. 仮想プロキシのプレフィックスを使用して Qlik Sense にアクセスする。

仮想プロキシの構成

次の手順を実行します。

1. 仮想プロキシを作成して、認証方法に SAML を選択します。
   仮想プロキシの作成 (page 398)

   仮想プロキシを機能させるためにはプロキシ サービスにリンクさせる必要があります。ただし、SAML 認証を既定の仮想プロキシで使用することはできません。既定の仮想プロキシしかない場合には、SAML の認証用に新しい仮想プロキシを作成する必要があります

2. (すでに ID プロバイダーの メタデータ ファイルをアップロードした場合は、この手順をスキップして次の手順に進みます)。構成を完了するには、ID プロバイダーからの メタデータ ファイルをアップロードする必要があります (**SAML IdPmetadata**)。ID プロバイダの Web サイトからメタデータを取得できない場合は、ID プロバイダに問い合わせてください。

   次の手順を実行します。

   i. 仮想プロキシの編集ページの [**認証**] で、**SAML IdPmetadata** の メタデータ ファイルを選択するボタンをクリックします。
   ii. ファイルを参照して [**開く**] をクリックします。
   iii. [**内容を表示**] をクリックしてアップロード前にファイルのプレビューを確認します。
   無効なファイル形式やコンテンツがあると、[**適用**] をクリックしたときにエラーが生成されます。

   *[**コンテンツを表示**] のリンクが表示された場合は、メタデータ ファイルが既にアップロードされています。既にアップロードされているファイルと全く同じコンテンツのファイルをアップロードしようとすると、[**適用**] が無効になります。*

3. 引き続き仮想プロキシの編集ページを使用します。

仮想プロキシをプロキシにリンクする

次の手順を実行します。

1. [**仮想プロキシの編集**] ページの右側にある [**関連アイテム**] で、[**プロキシ**] をクリックします。
   [**関連プロキシ**] ページが開きます。

2. 操作バーで、[**リンク**] をクリックします。
   [**プロキシ サービスの選択**] ページが開きます。
3. リンクするノードを選択して [**リンク**] をクリックします。
   リンクされたノードが [**関連プロキシ**] リストに表示されます。プロキシが再起動されたため、セッションが終了します。
4. QMC を再起動します。

サービス プロバイダのメタデータを ID プロバイダにアップロードする

次の手順を実行します。

1. 仮想プロキシの概要ページを開き、ダウンロードするメタデータのあるプロキシを選択します。
2. [**メタデータのダウンロード**] をクリックします。
3. SP メタデータを、Web インターフェース経由か、ID プロバイダーに物理的に配信します。

仮想プロキシのプレフィックスを使用して Qlik Sense にアクセスする
URL の仮想プロキシ プレフィックスを使用して新しい仮想プロキシにアクセスできます。

次の手順を実行します。

- 次の URL を入力します: *https://[node]/[prefix]/*。
  設計した SAML 構成を使用して新しい仮想プロキシ経由で Qlik Sense にアクセスします。

必要な SAML 構成をそれぞれ使用して、複数の仮想プロキシを作成できます。

SAML シングル ログアウト

Security Assertion Markup Language (SAML) にはシングル ログアウト オプションがあり、ユーザーのすべての ID プロバイダー (IdP) セッションを確実に閉じることができます。

SAML シングル サインオン (SSO) を使用すると、1 回ログインするだけでよいので、それ以上ログイン プロンプトが表示されることなく複数の Web サイトにアクセスできます。これは便利ですが、危険を伴う可能性もあります。1 つ以上のセッションが確実に閉じられなかった場合、攻撃を受けやすくなります。SAML シングル ログアウトを使用することでこの危険性を排除できます。

SAML シングル ログアウトには次の 2 つの選択肢があります。

- IdP によって開始されるログアウト
- サービス プロバイダーによって開始されるログアウト

Qlik Sense では、サービス プロバイダーによって開始されるログアウトにのみ対応しています。

サービス プロバイダーによって開始されるシングル ログアウト
サービス プロバイダーによって開始されるシングル ログアウトの使用例は 2 つあります。セッションから自分でログアウトする場合と、セッションがタイム アウトになる場合です。

ユーザー ログアウト

ユーザー ログアウト ユース ケースで、[ログアウト] をクリックするなどして、頻繁にログアウトします。 セッションは終了し、SAML シングル ログアウト要求が IdP に送信されます。次に、IdP ではユーザーの IdP セッションを削除し、ログアウト応答をサービス プロバイダー (Qlik Sense) に送信します。Qlik Sense はその後 ログアウト ページにリダイレクトします。

セッション タイムアウト

セッション タイムアウト ユース ケースでは、セッションがタイムアウトし、Web クライアントに通知され、SAML シングル ログアウト リクエストが IdP に送信されます。次に、IdP ではユーザーの IdP セッションを削除し、ログアウト応答をサービス プロバイダー (Qlik Sense) に送信します。Qlik Sense はその後 ログアウト ページにリダイレクトします。

SAML シングル ログアウトの有効化

Qlik Sense で SAML シングル ログアウトを有効化するには、ID プロバイダーがこれに対応しており、正しく構成されていることを確認します。例えば、一部の ID プロバイダーの場合には、証明書をアップロードする必要があります。証明書が必要な場合は、*%ProgramData%\Qlik\Sense\Repository\Exported Certificates\.Local Certificates* フォルダーにある *server.pem* 証明書を使用するか、サードパーティ証明書へのプロキシが構成されている場合にはそのような証明書を使用することをお勧めします。

アップグレード

Qlik Sense の以前のバージョンからアップグレードする場合、SAML シングル ログアウト用の IdP を設定する必要があります。

次の手順を実行します。

1. 必ず SAML シングル ログアウトに対応する IdP を設定してください。メタデータ ファイルには、Qlik Sense がログアウト要求を送信するログアウトの場所が含まれているはずです。
2. 新しいメタデータを IdP からダウンロードします (通常は ID プロバイダーの Web ページから入手可能です)。
3. 仮想プロキシの編集ページの [**認証**] セクションで、SAML IdP メタデータ ファイルに SAML シングル ログアウト用の設定を追加します。
4. 同じページで [**SAML シングル ログアウト**] を選択します。
5. 新しいメタデータ ファイルをサービス プロバイダー (Qlik Sense) からダウンロードします。
6. サービス プロバイダーのメタデータ ファイルを IdP にアップロードします。
7. SSO の間に IdP で NameID が送信されたことを確認します。例えば、Active Directory Federation Services (ADFS) では NameID を送信するための追加設定が必要です。
8. **QMC** > [**仮想プロキシ**] からダウンロードしたサービス プロバイダーのメタデータ ファイルから証明書を抽出します。関連する仮想プロキシの [**SP メタデータのダウンロード**] をクリックします。
9. ファイル内のタグ *<X509Certificate>* と *</X509Certificate>* の間にある証明書をコピーします。
10. 新しいファイルで、ファイルの最初に *-----BEGIN CERTIFICATE-----* を追加し、ファイルの最後に *-----END CERTIFICATE-----* を追加します。
11. 拡張子が *.pem* または *.crt* のファイルを保存します。

制限事項

- プロキシ サーバーを再起動する場合、またはプロキシ設定を変更する場合は、Web クライアントでセッションが失われます。プロキシを再起動する場合、ログアウト要求を IdP に送信する方法はありません。その結果として、Web クライアントが自動的にログインします。これは、IdP セッションの有効期限が切れていない限り、まだ有効だからです。
- プロキシから IdP に向けたログアウト要求は、SAML HTTP リダイレクト バインディングにのみ対応します。IdP から受信されるログアウト応答は、SAML HTTP リダイレクトおよび SAML HTTP POST バインディングの両方に対応します。

Okta を使用した SAML の構成

Security Assertion Markup Language (SAML) は認証と承認のためのデータ形式です。SAML で シングル サインオン (SSO) を有効化すると、ユーザーが Web サイトや アプリケーションにアクセスするためにログオンする回数を減らすことができます。

SAML はサードパーティ製品による認証用に構成することができます。Okta では、認証は ID プロバイダー (IdP) またはサービス プロバイダー (SP) によって開始されます。

シングル サインオンを ID プロバイダーから開始する場合

ID プロバイダーがユーザーを認証します。ID プロバイダーがユーザーの ID を断言すると、サービス プロバイダーはユーザーにサービスへのアクセスが提供できるようになります。ID プロバイダーによって SSO が有効にされているため、ユーザーは各サイトにログインしなくても、複数のサービス プロバイダーのサイトやアプリケーションにアクセスできます。

シングル サインオンをサービス プロバイダーから開始する場合

サービス プロバイダーはユーザーを ID プロバイダーにリダイレクトし、そこで認証が行われます。認証プロセスでは、Qlik Sense がサービス プロバイダーとなります。認証が正常に行われた後、ユーザーはさらにログインすることなく、複数のサービス プロバイダー サイトおよびアプリケーションにアクセスできます。

Okta を使用して SAML SSO をセットアップするには、Qlik Sense での仮想プロキシの構成が必要です。また、ID プロバイダーである Okta の構成も必要です。

仮想プロキシの作成および構成

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC で、[**仮想プロキシ**] を開きます。
3. データ マネージャーでテーブルの ⊕ 新規作成
4. 右側の [**Properties**] (プロパティ) で、[**Identification**] (ID)、[**Authentication**] (認証)、[**Load balancing**] (負荷分散)、および [**Advanced**] (詳細設定) の各セクションを選択していることを確認します。
5. [**Identification**] (ID) で、[**Description**] (説明) と [**Prefix**] (プレフィックス) に「*okta*」と入力します。
6. [**Session cookie header name**] (セッション クッキー ヘッダー名) で、既存の名前の末尾に「*-okta*」を追加し、ヘッダー名を *X-Qlik-Session-okta* にします。
7. [**Authentication method**] (認証方法) に [**SAML**] を指定します。
8. [**SAML single logout**] (SAML シングル ログアウト) を選択します。SAML シングル ログアウトは、すべての SSO セッションが適切に閉じるようにするためのセキュリティ対策です。

9. [**SAML host URI**] (SAML ホストURI) に、Qlik Sense へのアクセスにユーザーが使用する URL (サーバー名) を *https://myhost.company.com* の形式で入力します。
10. [**SAML entity ID**] (SAML エンティティID) に「*okta*」と入力します。
これは Okta 構成の一意の識別子です。

*[**SAML IdP metadata**] (SAML IdP メタデータ) は以降の段階で追加されます。*

11. [**SAML attribute for user ID**] (ユーザーID に使用する SAML 属性) に「*email*」と入力します。
これは Okta に保存されるユーザーの電子メール アドレスです。Okta 構成内で、別の標準項目またはカスタム項目をユーザーID として使用するように指定することができます。
12. [**SAML attribute for user directory**] (ユーザー ディレクトリに使用する SAML 属性) に「*[okta]*」と入力します。
これは、括弧を必要とする静的属性です。
13. [**SAML signing algorithm**] (SAML 署名アルゴリズム) に [**SHA-1**] を指定します。
14. [**SAML attribute mapping**] (SAML 属性マッピング) で、⊕ [**Add new attribute**] (新しい属性の追加) をクリックします。
15. [**SAML attribute**] (SAML 属性) として「*groups*」、[**Qlik Sense attribute**] (Qlik Sense 属性) として「*group*」を入力します。[**Mandatory**] (必須) の選択を解除します。
名前 *groups* は SAML アサーションでの属性名です。セキュリティルールでこの属性を使用している場合、Qlik Sense はこの属性名 *group* に応答します。
16. [**Load balancing nodes**] (負荷分散ノード) で、⊕ [**Add new server node**] (新しいサーバー ノードの追加) をクリックします。
17. この仮想プロキシが接続を負荷分散するエンジン ノードを選択します。
18. [**Advanced**] (詳細設定) の [**Host white list**] (ホスト許可リスト) セクションで、⊕ [**Add new value**] (新しい値の追加) をクリックします。
19. Qlik Sense サーバー ([**SAML host URI**] (SAML ホストURI) で入力したのと同じサーバー) のホスト名を追加します。
20. [**Apply**] (適用) をクリックし、[**OK**] をクリックしてサービスを再起動します。
21. 右側の [**Associated items**] (関連するアイテム) メニューで、[**Proxies**] (プロキシ) を選択します。
22. [**Link**] (リンク) をクリックし、この構成を使用するプロキシ (1 つまたは複数) に仮想プロキシをリンクさせます。
プロキシ サービスが再起動します。
23. [**Virtual proxies**] (仮想プロキシ) 概要ページに移動します。
24. 作成した *okta* 構成を選択し、操作バーの [**Download SP metadata**] (SP メタデータのダウンロード) をクリックします。
25. Qlik Sense で生成されたメタデータを開きます。以下を確認してください。
    - *entityID*: この値は、Okta が Qlik Sense サーバーと通信できるようにするために必要です。
    - *SingleLogoutService*URL (*Location*): これは、SAML ホストURI を入力して末尾に仮想プロキシ パスを追加すると Qlik Sense によって生成される URL です。末尾に *samlauthn* と *slo* が追加されていることに留意してください。これは、Okta が SAML シングル ログアウトを ID プロバイダーに伝達するために使用する URL です。

- *AssertionConsumerService* URL (*Location*): これは、SAML ホスト URI を入力して末尾に仮想プロキシ パスを追加すると Qlik Sense によって生成される URL です。末尾に *samlauthn* が追加されていることに留意してください。これは、Okta が SAML アサーションを Qlik Sense に伝達するために使用する URL です。
- *NameIDFormat*: 既定では、*transient* 名の形式はメタデータとして指定されます。SAML 構成においてこの方法で設定することが常に必要とは限りませんが、適切な操作性を確保するには、この値を記録しておき構成に適切に適用する必要があります。

これで、とりあえず仮想プロキシの設定が完了しました。このページに戻り、IdP メタデータ ファイル (ID プロバイダーの Web ページから入手可能) をアップロードします。次のステップでは、Okta を構成します。

Okta の構成

Okta は構成での ID プロバイダーとなるため、Okta の構成を行う前にアカウントを登録する必要があります。詳細については https://www.okta.com/ を参照してください。

Qlik Sense Enterprise on Windows, with Multi-Cloud をインストールする場合には、Okta の開発者アカウントを使用する必要があります。

この構成にはサードパーティ製品が含まれているため、構成が本項の説明の通りであると保証することはできません。サードパーティ製品に変更が行われ、弊社が認識していない場合もあります。

次の手順を実行します。

1. Okta でトップ メニューの [**Developer Console**] (開発者コンソール) にマウスを合わせ、[**Classic UI**] (クラシック UI) を選択します。
2. トップ メニューで、[**Applications**] (アプリケーション) を選択します。
3. [**Add Application**] (アプリケーションの追加) をクリックします。
4. [**Create New App**] (アプリの新規作成) をクリックします。
5. [**Platform**] (プラットフォーム) として [**Web**] を選択します。
6. [**Sign on method**] (サインオン方法) として [**SAML 2.0**] を選択します。
7. [**Create**] (作成) をクリックします。
   構成画面が表示されます。
8. このアプリに「*Qlik Sense SAML configuration*」という名前をつけます。
9. オプション: ロゴを追加します。
10. [**Next**] (次へ) をクリックします。
    [**SAML Settings**] (SAML 設定) ページが表示されます。
11. [**Single sign on URL**] (シングル サインオン URL) として、SP メタデータ ファイルからの *AssertionConsumerService* URL を項目に入力します。*samlauthn* の後ろに必ず末尾のスラッシュを挿入してください。これを怠ると、Qlik Sense で SAML アサーションが受け入れられません。
12. [**Audience URI (SP Entity ID)**] (オーディエンス URI (SP エンティティ ID)) として、前に開いた SP メタデータからの *entityID* 値を入力します (*okta*)。
13. [**Name ID format**] (名前 ID の形式) に [**Transient**] (一時的) を指定します。

14. [**Show Advanced Settings**] (詳細設定の表示) をクリックします。
15. [**Enable Single Logout**] (シングル ログアウトの有効化) に、[**Allow application to initiate Single Logout**] (シングル ログアウトの開始をアプリケーションに許可する) を指定します。
16. [**Single Logout URL**] (シングル ログアウトURL) には、*https://<machine_name>/<vp_prefix>/samlauthn/slo/* の形式を使用します。
17. [**SP issuer**] (SP 発行元) には、仮想プロキシの SAML entity ID を使用します (*okta*)。
18. **QMC** > [**仮想プロキシ**] からダウンロードしたサービス プロバイダーのメタデータ ファイルから証明書を抽出します。関連する仮想プロキシの [**SP メタデータのダウンロード**] をクリックします。
19. ファイル内のタグ *<X509Certificate>* と *</ X509Certificate>* の間にある証明書をコピーします。
20. 新しいファイルで、ファイルの最初に *-----BEGIN CERTIFICATE-----* を追加し、ファイルの最後に *-----END CERTIFICATE-----* を追加します。
21. 拡張子が *.pem* または *.crt* のファイルを保存します。
22. [**Upload Certificate**] (証明書のアップロード) をクリックします。
23. [**ATTRIBUTE STATEMENTS**] (属性ステートメント) セクションで、[**Name**] (名前) に「*email*」と入力し、[**値**] には [*user.email*] を指定します。
24. [**GROUP ATTRIBUTE STATEMENTS**] (グループ属性ステートメント) セクションで、[**Name**] (名前) に「*groups*」と入力し、[**Filter**] (フィルター) に [**Regex**] を指定して文字列「*^[A-Za-z0-9_.]+$*」を追加します。

    > *正規表現を使用して検索パターンを定義します。検索パターンの条件に適合する文字列のみが検索されます。検索パターンが ^[A-Za-z0-9_.]+$ の場合、グループ名は、A ~ Z と a ~ z の文字、0 ~ 9 の数字、アンダースコア(_)、ピリオド(.) のいずれかが含まれている場合にのみ検索されます。名前にダッシュ(-) が含まれている場合は、検索パターンに適合しないため検索されません。詳しくは、「Wikipedia: 正規表現」を参照してください。*

25. [**次へ**] をクリックします。
    フィードバック セクションが開きます。
26. [**Are you a customer or partner?**] (顧客/パートナーのいずれに該当しますか?) の問いに対し、[**I'm an Okta customer adding an internal app**] (社内アプリを追加しようとしている Okta 顧客です) を選択します。
27. オプション: [**This is an internal app that we have created**] (これは社内アプリとして作成したアプリです) を選択します。
28. [**Finish**] (完了) をクリックします。
    [**Sign On**] (サインオン) ページが表示されます。このページから IdP メタデータをダウンロードできます。
29. 下にスクロールして、[**dentity Provider metadata**] (IDプロバイダーメタデータ) リンクをクリックします。Qlik Sense ではメタデータ ファイルの拡張子が xml でなければならないため、ファイルは必ず *metadata.xml* として保存してください。
30. 上向きにスクロールし、トップ メニューで [**People**] (ユーザー) を選択します。
31. 作成した接続をユーザーが使用できるように、ユーザーをアプリに割り当てる必要があります。[**Assign to People**] (ユーザーへの割り当て) をクリックし、ユーザーを追加します。(ユーザーが Okta アカウントを持っていることが前提となります。)

これで Okta の構成が完了しました。接続をテストするには、最後のステップとして IdP メタデータを仮想プロキシにアップロードする必要があります。

IdP メタデータ ファイルのアップロード

次の手順を実行します。

1. QMC に戻り、編集のために *okta* 仮想プロキシを開きます。
2. [**Authentication**] (認証) の [**SAML IdP metadata**] (SAML IdP メタデータ) で、[**Choose File**] (ファイルの選択) をクリックします。
3. Okta からダウンロードしたメタデータ ファイルを選択します。
4. [**View content**] (コンテンツを表示) をクリックしてメタデータを確認します。
5. [**Apply**] (適用) をクリックします。
6. [**OK**] をクリックし、仮想プロキシへの変更を承諾します。
7. [**Refresh QMC**] (QMC データの更新) をクリックします。

これで構成をテストできます。

Okta SAML 構成のテスト

前述したように、シングル サインオン (SSO) はサービス プロバイダーまたは ID プロバイダーを介して開始できます。

シングル サインオンをサービス プロバイダーから開始する場合

次の手順を実行します。

1. 新しいブラウザー ウィンドウを開いて、仮想プロキシ パスを含む Qlik Sense サーバー URL に移動します。
   例: *https://myhost.company.com/okta/*
   ログイン要求の認証のために、ブラウザーが Okta にリダイレクトされます。
2. ユーザー資格情報を入力します。
   Okta によって Qlik Sense ハブにリダイレクトされます。

シングル サインオンを ID プロバイダーから開始する場合

1. ブラウザーを開いて www.okta.com に移動します。
2. ユーザー資格情報を使用してログインします。
3. 上部のメニューで、[**My Applications**] (マイ アプリケーション) をクリックします。
   使用可能なアプリケーションが表示されます。
4. Qlik Sense SAML アプリケーションをクリックします。
   Qlik Sense ハブが新しいタブで開きます。

RelayState は常に https://<machine_name>/<vp_prefix>/hub に設定することをお勧めします。RelayState が空の場合、一部の ID プロバイダーでは `post` 要求の代わりに `get` 要求が送信されるため、エラーが生じます。RelayState が空の場合、スペルミスがある場合、またはホストの許可リストに含まれていない場合には、ユーザーは自動的にハブにリダイレクトされます。

IdP から開始する SSO を機能させるには、アサーションに署名する必要があります。

OneLogin を使用した SAML の構成

Security Assertion Markup Language (SAML) は認証と承認のためのデータ形式です。SAML でシングル サインオン (SSO) を有効化すると、ユーザーが Web サイトや アプリケーションにアクセスするためにログオンする回数を減らすことができます。

SAML はサードパーティ製品による認証用に構成することができます。OneLogin では、認証は ID プロバイダー (IdP) またはサービス プロバイダー (SP) によって開始されます。

シングル サインオンを ID プロバイダーから開始する場合

ID プロバイダーがユーザーを認証します。ID プロバイダーがユーザーの ID を断言すると、サービス プロバイダーはユーザーにサービスへのアクセスが提供できるようになります。ID プロバイダーによって SSO が有効にされているため、ユーザーは各サイトにログインしなくても、複数のサービス プロバイダーのサイトやアプリケーションにアクセスできます。

シングル サインオンをサービス プロバイダーから開始する場合

サービス プロバイダーはユーザーを ID プロバイダーにリダイレクトし、そこで認証が行われます。認証プロセスでは、Qlik Sense がサービス プロバイダーとなります。認証が正常に行われた後、ユーザーはさらにログインすることなく、複数のサービス プロバイダー サイトおよびアプリケーションにアクセスできます。

OneLogin を使用して SAML SSO をセットアップするには、Qlik Sense での仮想プロキシの構成が必要です。また、ID プロバイダーである OneLogin の構成も必要です。

仮想プロキシの作成および構成

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC で、[**仮想プロキシ**] を開きます。
3. データ マネージャーでテーブルの ⊕ 新規作成
4. 右側の [**Properties**] (プロパティ) で、[**Identification**] (ID)、[**Authentication**] (認証)、[**Load balancing**] (負荷分散)、および [**Advanced**] (詳細設定) の各セクションを選択していることを確認します。
5. [**Identification**] (ID) で、[**Description**] (説明) と [**Prefix**] (プレフィックス) に「*onelogin*」と入力します。
6. [**Session cookie header name**] (セッション クッキー ヘッダー名) で、既存の名前の末尾に「*-onelogin*」を追加し、ヘッダー名を *X-Qlik-Session-onelogin* にします。
7. [**Authentication method**] (認証方法) に [**SAML**] を指定します。
8. [**SAML single logout**] (SAML シングル ログアウト) を選択します。SAML シングル ログアウトは、すべての SSO セッションが適切に閉じるようにするための方法です。
9. [**SAML host URI**] (SAML ホスト URI) に、Qlik Sense へのアクセスにユーザーが使用する URL (サーバー名) を *https://myhost.company.com* の形式で入力します。
10. [**SAML entity ID**] (SAML エンティティ ID) に「*onelogin*」と入力します。
    これは OneLogin 構成の一意の識別子です。

    > *[**SAML IdP metadata**] (SAML IdP メタデータ) は以降の段階で追加されます。*

11. [**SAML attribute for user ID**] (ユーザー ID に使用する SAML 属性) に「*userid*」と入力します。

これは OneLogin に保存されるユーザーの電子メール アドレスです。OneLogin 構成内で、別の標準項目またはカスタム項目をユーザー ID として使用するように指定することができます。

12. [**SAML attribute for user directory**] (ユーザー ディレクトリに使用する SAML 属性) に「*[onelogin]*」と入力します。
これは、括弧を必要とする静的属性です。
13. [**SAML signing algorithm**] (SAML 署名アルゴリズム) に [**SHA-1**] を指定します。
14. [**SAML attribute mapping**] (SAML 属性マッピング) で、⊕ [**Add new attribute**] (新しい属性の追加) をクリックします。
15. [**SAML attribute**] (SAML 属性) として「*Email*」、[**Qlik Sense attribute**] (Qlik Sense 属性) として「*email*」を入力します。[**Mandatory**] (必須) の選択を解除します。(必須の属性が SAML 応答に含まれていないと、認証要求は Qlik Sense で拒否されます。)
16. 別の属性を追加するため、⊕ [**Add new attribute**] (新しい属性の追加) を再度クリックします。
17. [**SAML attribute**] (SAML 属性) として「*userid*」、[**Qlik Sense attribute**] (Qlik Sense 属性) として「*name*」を入力します。[**Mandatory**] (必須) の選択を解除します。
18. [**Load balancing nodes**] (負荷分散ノード) で、⊕ [**Add new server node**] (新しいサーバー ノードの追加) をクリックします。
19. この仮想プロキシが接続を負荷分散するエンジン ノードを選択します。
20. [**Advanced**] (詳細設定) の [**Host white list**] (ホスト許可リスト) セクションで、⊕ [**Add new value**] (新しい値の追加) をクリックします。
21. Qlik Sense サーバー ([**SAML host URI**] (SAML ホスト URI) で入力したのと同じサーバー) のホスト名を追加します。
22. [**Apply**] (適用) をクリックし、[**OK**] をクリックしてサービスを再起動します。
23. 右側の [**Associated items**] (関連するアイテム) メニューで、[**Proxies**] (プロキシ) を選択します。
24. [**Link**] (リンク) をクリックし、この構成を使用するプロキシ (1 つまたは複数) に仮想プロキシをリンクさせます。
プロキシ サービスが再起動します。
25. [**Virtual proxies**] (仮想プロキシ) 概要ページに移動します。
26. 作成した *onelogin* 構成を選択し、操作バーの [**Download SP metadata**] (SP メタデータのダウンロード) をクリックします。
27. Qlik Sense で生成されたメタデータを開きます。以下を確認してください。
    - *entityID*: この値は、OneLogin が Qlik Sense サーバーと通信できるようにするために必要です。
    - *AssertionConsumerService* URL (*Location*): これは、SAML ホスト URI を入力して末尾に仮想プロキシ パスを追加すると Qlik Sense によって生成される URL です。末尾に *samlauthn* が追加されていることに留意してください。これは、OneLogin が SAML アサーションを Qlik Sense に伝達するために使用する URL です。

これで、とりあえず仮想プロキシの設定が完了しました。このページに戻り、IdP メタデータ ファイル (ID プロバイダーの Web ページから入手可能) をアップロードします。次のステップでは、OneLogin を構成します。

OneLogin の構成

OneLogin は構成での ID プロバイダーとなるため、OneLogin の構成を行う前にアカウントを登録する必要があります。詳細については https://www.onelogin.com/ を参照してください。

この構成にはサードパーティ製品が含まれているため、構成が本項の説明の通りであると保証することはできません。サードパーティ製品に変更が行われ、弊社が認識していない場合もあります。

次の手順を実行します。

1. OneLogin トップ メニューで、[**Applications**] (アプリケーション) を選択します。
2. [**Add App**] (アプリの追加) をクリックします。
3. 検索ボックスに「*SAML*」と入力します。
   SAML テンプレートのリストが表示されます。
4. [**SAML Custom Connector (Advanced)**] (カスタム コネクタ (詳細)) を選択します。
5. [**Display Name**] (表示名) を「*Qlik Sense SAML configuration*」に変更します。
6. [**SAVE**] (保存) をクリックします。
7. [**Configuration**] (構成) タブをクリックします。
8. [**Audience**] (オーディエンス) で、SAML 仮想プロキシの エンティティID「*onelogin*」を入力します。
9. [**Recipient**] (受信者)、[**ACS (Consumer) URL Validator**] (ACS (コンシューマー) URL 検証)、および [**ACS (Consumer) URL**] (ACS (コンシューマー) URL) に、SP メタデータ ファイルからの *AssertionConsumerService* URL をそれぞれ入力します。*samlauthn* の後ろに必ず末尾のスラッシュを挿入してください。これを怠ると、Qlik Sense で SAML アサーションが受け入れられません。
10. [**Single Logout URL**] (シングル ログアウト URL) には、*https://<myhost.company.com>/<vp_prefix>/samlauthn/slo/* の形式を使用します。
11. **SAML** [**signature element**] (署名要素) には、値 [**Assertion**] (アサーション) を選択します。
12. [**Parameters**] (パラメータ) タブをクリックします。
13. 既定では、OneLogin により*NameID (fka Email)* 属性が提供されます。
    これは仮想プロキシのセットアップで追加した 2 つの属性の 1 つです。
14. 仮想プロキシのセットアップ時に追加した 2 つ目の属性を加えるため、[**Add parameter**] (パラメータの追加) をクリックします。
    [**New Field**] (新しい項目) ウィンドウが開きます。
15. [**Field name**] (項目名) に「*userid*」と入力します。
16. [**Include in SAML assertion**] (SAML アサーションに含める) を選択し、[**SAVE**] (保存) をクリックします。
17. [*userid*] 属性をクリックします。
    [**Edit Field Userid**] (項目 Userid の編集) ウィンドウが開きます。
18. [**Value**] (値) リストで、[**Email name part**] (電子メール名部分) を選択し、[**SAVE**] (保存) をクリックします。
19. 右側の [**SAVE**] (保存) をクリックします。
20. トップ メニューで [**Users**] (ユーザー) をクリックし、[**Users**] (ユーザー) を選択します。
21. アプリを追加するユーザーをクリックします。
22. [**Applications**] (アプリケーション) タブをクリックし、[**Applications**] の右側にある [**+**] 記号をクリックします。
23. [**Assign New Login to <user>**] (<user> への新しいログインの割り当て) ウィンドウで、前に作成した [*Qlik Sense SAML configuration*] (Qlik Sense 構成) を選択し、[**CONTINUE**] (続行) をクリックします。
24. [**Edit Qlik Sense SAML Configuration Login for <user>**] (<user> の Qlik Sense 構成ログインの編集) ウィンドウで、[**CANCEL**] (キャンセル) をクリックします。

25. トップメニューで、[**Applications**] (アプリケーション) をクリックし、[**Applications**] (アプリケーション) を選択します。
26. [*Qlik Sense SAML Configuration*] (Qlik Sense SAML 構成) をクリックします。
27. [**MORE ACTIONS**] (追加アクション) リストで、[**SAML Metadata**] (SAML メタデータ) を選択します。

これで OneLogin の構成が完了しました。接続をテストするには、最後のステップとして IdP メタデータを仮想プロキシにアップロードする必要があります。

IdP メタデータファイルのアップロード

次の手順を実行します。

1. QMC に戻り、編集のために *onelogin* 仮想プロキシを開きます。
2. [**Authentication**] (認証) の [**SAML IdP metadata**] (SAML IdP メタデータ) で、[**Choose File**] (ファイルの選択) をクリックします。
3. OneLogin からダウンロードしたメタデータファイルを選択します。
4. [**View content**] (コンテンツを表示) をクリックしてメタデータを確認します。
5. [**Apply**] (適用) をクリックします。
6. [**OK**] をクリックし、仮想プロキシへの変更を承諾します。
7. [**Refresh QMC**] (QMC データの更新) をクリックします。

これで構成をテストできます。

OneLogin SAML 構成のテスト

前述したように、シングル サインオン (SSO) はサービス プロバイダーまたは ID プロバイダーを介して開始できます。

シングル サインオンをサービス プロバイダーから開始する場合

次の手順を実行します。

1. 新しいブラウザー ウィンドウを開いて、仮想プロキシ パスを含む Qlik Sense サーバー URL に移動します。
   例: *https://myhost.company.com/onelogin/*
   ログイン要求の認証のために、ブラウザーが OneLogin にリダイレクトされます。
2. ユーザー資格情報を入力します。
   OneLogin によって Qlik Sense ハブにリダイレクトされます。

シングル サインオンを ID プロバイダーから開始する場合

1. ブラウザーを開いて www.onelogin.com に移動します。
2. ユーザー資格情報を使用してログインします。
3. 上部のメニューで、[**My Applications**] (マイ アプリケーション) をクリックします。
   使用可能なアプリケーションが表示されます。
4. Qlik Sense SAML アプリケーションをクリックします。
   Qlik Sense ハブが新しいタブで開きます。

RelayState は常に https://<machine_name>/<vp_prefix>/hub に設定することをお勧めします。RelayState が空の場合、一部の ID プロバイダーでは `post` 要求の代わりに `get` 要求が送信されるため、エラーが生じます。RelayState が空の場合、スペルミスがある場合、またはホストの許可リストに含まれていない場合には、ユーザーは自動的にハブにリダイレクトされます。

IdP から開始する SSO を機能させるには、アサーションに署名する必要があります。

AD FS を使用した SAML の構成

Security Assertion Markup Language (SAML) は認証と承認のためのデータ形式です。SAML でシングル サインオン (SSO) を有効化すると、ユーザーが Web サイトや アプリケーションにアクセスするためにログオンする回数を減らすことができます。

SAML はサードパーティ製品による認証用に構成することができます。Active Directory Federation Services (AD FS) では、認証はサービスプロバイダー (SP) によって開始されます。

シングル サインオンをサービス プロバイダーから開始する場合

サービス プロバイダーはユーザーを ID プロバイダーにリダイレクトし、そこで認証が行われます。認証プロセスでは、Qlik Sense がサービス プロバイダーとなります。認証が正常に行われた後、ユーザーはさらにログインすることなく、複数のサービス プロバイダー サイトおよびアプリケーションにアクセスできます。

AD FS を使用して SAML SSO をセットアップするには、Qlik Sense での仮想プロキシの構成が必要です。また、ID プロバイダーである AD FS の構成も必要です。ここでは、AD FS がインストール済みであることを前提としています。このトピックでは、AD FS をインストールする方法については説明していません。

Windows Server に AD FS をインストールする方法については、次のビデオをご覧ください:「Qlik Sense SAML: ADFS Integration Part One of Three」。

仮想プロキシの作成および構成

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC で、[**仮想プロキシ**] を開きます。
3. データ マネージャーでテーブルの ⊕新規作成
4. 右側の [**Properties**] (プロパティ) で、[**Identification**] (ID)、[**Authentication**] (認証)、[**Load balancing**] (負荷分散)、および [**Advanced**] (詳細設定) の各セクションを選択していることを確認します。
5. [**Identification**] (ID) で、[**Description**] (説明) と [**Prefix**] (プレフィックス) に「*adfs*」と入力します。
6. [**Session cookie header name**] (セッション クッキー ヘッダー名) で、既存の名前の末尾に「*-adfs*」を追加し、ヘッダー名を *X-Qlik-Session-adfs* にします。
7. [**Authentication method**] (認証方法) に [**SAML**] を指定します。
8. [**SAML single logout**] (SAML シングル ログアウト) を選択します。SAML シングル ログアウトは、すべての SSO セッションが適切に閉じるようにするためのセキュリティ対策です。

9. [**SAML host URI**] (SAML ホストURI) に、Qlik Sense へのアクセスにユーザーが使用する URL (サーバー名) を *https://myhost.company.com* の形式で入力します。
10. [**SAML entity ID**] (SAML エンティティID) に「*adfs*」と入力します。
これは AD FS 構成の一意の識別子です。
11. AD FS サーバー *https://<adfs_server>/FederationMetadata/2007-06/FederationMetadata.xml* からIdP メタデータをダウンロードします。
12. [**Authentication**] (認証) の [**SAML IdP metadata**] (SAML IdP メタデータ) で、[**Choose File**] (ファイルの選択) をクリックします。
13. AD FS からダウンロードしたメタデータファイルを選択します。
14. [**View content**] (コンテンツを表示) をクリックしてメタデータを確認します。
15. [**SAML attribute for user ID**] (ユーザーID に使用するSAML 属性) で、
「*http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn*」と入力します。
これは、ユーザープリンシパル名 (UPN) のスキーマ定義です。この定義は、AD FS マネージャーの [**Service] (サービス) > [Claim Descriptions**] (要求記述) で確認できます。
16. [**SAML attribute for user directory**] (ユーザーディレクトリに使用するSAML 属性) に「*[adfs]*」と入力します。
これは、括弧を必要とする静的属性です。
17. [**SAML signing algorithm**] (SAML 署名アルゴリズム) に [**SHA-1**] を指定します。
これは、Qlik Sense サーバーがメタデータに追加する署名証明書です。
18. [**SAML attribute mapping**] (SAML 属性マッピング) で、[**Add new attribute**] (新しい属性の追加) をクリックします。
19. [**SAML attribute**] (SAML 属性) として「*http://schemas.xmlsoap.org/claims/Group*」、[**Qlik SenseGroup**] (属性) として「*Group*」と入力します。[**Mandatory**] (必須) の選択を解除します。選択をそのままにすると、SAML 応答に属性が含まれず、Qlik Sense によって認証要求が拒否されます。SAML 属性の説明は、AD FS マネージャーの [**Service] (サービス) > [Claim Descriptions**] (要求記述) で確認できます。
20. [**Load balancing nodes**] (負荷分散ノード) で、[**Add new server node**] (新しいサーバーノードの追加) をクリックします。
21. この仮想プロキシが接続を負荷分散するエンジンノードを選択します。
22. [**Advanced**] (詳細設定) の [**Host white list**] (ホスト許可リスト) セクションで、[**Add new value**] (新しい値の追加) をクリックします。
23. Qlik Sense サーバー ([**SAML host URI**] (SAML ホストURI) で入力したのと同じサーバー) のホスト名を追加します。
24. [**Apply**] (適用) をクリックし、[**OK**] をクリックしてサービスを再起動します。
25. 右側の [**Associated items**] (関連するアイテム) メニューで、[**Proxies**] (プロキシ) を選択します。
26. [**Link**] (リンク) をクリックし、この構成を使用するプロキシ (1 つまたは複数) に仮想プロキシをリンクさせます。
プロキシ サービスが再起動します。
27. [**Virtual proxies**] (仮想プロキシ) 概要ページに移動します。
28. 作成した *adfs* 構成を選択し、操作バーの [**Download SP metadata**] (SP メタデータのダウンロード) をクリックします。
AD FS を構成するときに、このメタデータファイルが必要になります。
29. Qlik Sense で生成されたメタデータを開きます。以下を確認してください。

- *entityID*: この値は、AD FS が Qlik Sense サーバーと通信できるようにするために必要です。
- *AssertionConsumerService* URL (*Location*): これは、SAML ホスト URI を入力して末尾に仮想プロキシ パスを追加すると Qlik Sense によって生成される URL です。末尾に *samlauthn* が追加されていることに留意してください。これは、AD FS が SAML アサーションを Qlik Sense に伝達するために使用する URL です。
- *NameIDFormat*: 既定では、*transient* 名の形式は メタデータとして指定されます。SAML 構成においてこの方法で設定することが常に必要とは限りませんが、適切な操作性を確保するには、この値を記録しておき構成に適切に適用する必要があります。

これで、仮想プロキシの設定が完了しました。次のステップでは、AD FS を構成します。

AD FS の構成

このトピックでは、AD FSを構成する方法について説明しますが、AD FS をインストールする方法については、説明していません。AD FS は構成内で ID プロバイダーとなるため、構成を開始するためには AD FS のアクセス権が必要です。

この構成にはサードパーティ製品が含まれているため、構成が本項の説明の通りであると保証することはできません。サードパーティ製品に変更が行われ、弊社が認識していない場合もあります。

次の手順を実行します。

1. AD FS で、サーバー マネージャーを開きます。
2. 右側のメニューで、[**Tools] (ツール) > [AD FS Management**] (AD FS の管理) を選択します。
3. 左側の [**Trust Relationships**] (信頼関係) フォルダーをクリックします。
   ウィザードが開きます。
4. 右側の [**Actions**] (操作) で、[**Add Relying Party Trust**] (証明書利用者信頼の追加) を選択します。
5. [**Start**] (開始) をクリックします。
6. オプション [**Import data about the relying from a file**] (証明書利用者についてのデータをファイルからインポートする) を選択し、仮想プロキシの構成後にダウンロードした SP メタデータ ファイルに移動して、[**Next**] (次へ) をクリックします。
7. 証明書利用者の表示名を入力し、[**Next**] (次へ) をクリックします。
8. [**I do not want to configure multi-factor authentication settings for this relying party trust at this time**] (現時点ではこの証明書利用者信頼に多要素認証を構成しない) を選択し、[**Next**] (次へ) をクリックします。
9. [**Permit all users access to this relying party**] (すべてのユーザーに対してこの証明書利用者へのアクセスを許可する) を選択し、[**Next**] (次へ) をクリックします。
10. [**Ready to Add Trust**] (信頼の追加の準備完了) ウィンドウで、[**Next**] (次へ) をクリックします。
11. [**Close**] (閉じる) をクリックします。
    [**Edit Claim Rules for <display name>**] (<表示名> の要求規則の編集) ダイアログが開きます。
12. [**Add Rule**] (規則の追加) をクリックします。
    規則テンプレート ページのウィンドウが開きます。
13. [**Next**] (次へ) をクリックします。
    [Rule Configuration] (ルールの構成) ウィンドウが開きます。

14. 要求規則名を入力し、[**Attribute store**] (属性ストア) で [**Active Directory**] を選択します。
15. **LDAP 属性**の一覧で [*User-Principal-Name*] を選択し、[**Outgoing Claim Type**] (出力方向の要求の種類) で [*UPN*] を選択します。
16. **LDAP 属性**の一覧の 2 行目で [*User-Principal-Name*] を再度選択し、[**Outgoing Claim Type**] (出力方向の要求の種類) で [*Name ID*] (名前 ID) を選択します。
17. **LDAP 属性**の一覧の 3 行目で [*Token-Groups - Unqualified Names*] (Token-Groups - 名前の指定なし) を選択し、[**Outgoing Claim Type**] (出力方向の要求の種類) で [*Group*] (グループ) を選択します。
18. [**Finish**] (完了) をクリックします。
19. [**Apply**] (適用) をクリックして [**OK**] をクリックします。
20. 新しい証明書利用者信頼をダブルクリックし、[**Advanced**] (詳細設定) タブを開きます。
21. [**Secure hash algorithm**] (セキュア ハッシュ アルゴリズム) を [*SHA-1*] に変更します。
22. [**Apply**] (適用) をクリックして [**OK**] をクリックします。

証明書の PowerShell 設定

証明書は自己署名であるため、署名証明書と暗号化証明書に対して失効状態の確認をオフにする必要があります。これを Windows PowerShell で実行します。

次の手順を実行します。

1. **PowerShell** を開きます。
2. 次の文字列を入力します。
   `Set-ADFSRelyingPartyTrust -targetname "<ターゲット名>" -SigningCertificateRevocationCheck "none"`
3. 新しい行に次の文字列を入力します。
   `Set-ADFSRelyingPartyTrust -targetname "<ターゲット名>" -EncryptionCertificateRevocationCheck "none"`
4. **Enter** を押します。

これで AD FS の構成が完了しました。これで構成をテストできます。

AD FS SAML 構成のテスト

サービス プロバイダーで シングル サインオン (SSO) を開始します。

シングル サインオンをサービス プロバイダーから開始する場合

次の手順を実行します。

1. 新しいブラウザー ウィンドウを開いて、仮想プロキシ パスを含む Qlik Sense サーバー URL に移動します。
   例: *https://myhost.company.com/adfs/*
   ブラウザーが AD FS にリダイレクトされてログイン要求が認証されます。
2. ユーザー資格情報を入力します。
   AD FS によって Qlik Sense ハブにリダイレクトされます。

JWT 認証

JSON Web Token (JWT) is an open standard for secure transmission of information between two parties as a JavaScript Object Notation (JSON) object. JWT is used for authentication and authorization.JWT により single sign-on (SSO) を有効化できるため、ユーザーがクラウド アプリケーションや Web サイトにログオンする回数を最小限にすることができます。

JWT の構造

JWT は、ヘッダー、ペイロード、シグネチャーの 3 つの部分で構成されています。

ヘッダー

ヘッダーは通常、タイプ (typ) および アルゴリズム (alg) の 2 つの部分で構成されています。アルゴリズムを使用して、シグネチャーが生成されます。

```
{
"typ": "JWT",
"alg": "RS256"
}
```

RS256 は、このトークンの署名に RS256 - RSA シグネチャーと SHA256 が使用されていることを示します。

ペイロード

ペイロードは、作成するクレームで構成された JSON オブジェクトです。クレームとは、エンティティ(通常はユーザー) と追加のメタデータに関するステートメントです。

```
{
"userId":"jde",
"name":"John Donne",
"email":"jde@company.com",
"roles":["RootAdmin"],
"exp": 1472034208
}
```

シグネチャー

シグネチャーは、差出人の ID を確認し、メッセージが改ざんされていないことを保証するために使用します。JWT シグネチャーは、エンコードされたヘッダーとペイロードのことで、秘密鍵で署名されています。通常、シグネチャーの生成と有効化にX.509 証明書が使用されます。QMC の仮想プロキシでは、証明書 (公開鍵を含む) を構成して、シグネチャーを有効化します。

認証は、シグネチャーを確認することで行われます。シグネチャーが有効な場合、Qlik Sense に対してアクセスが許可されます。

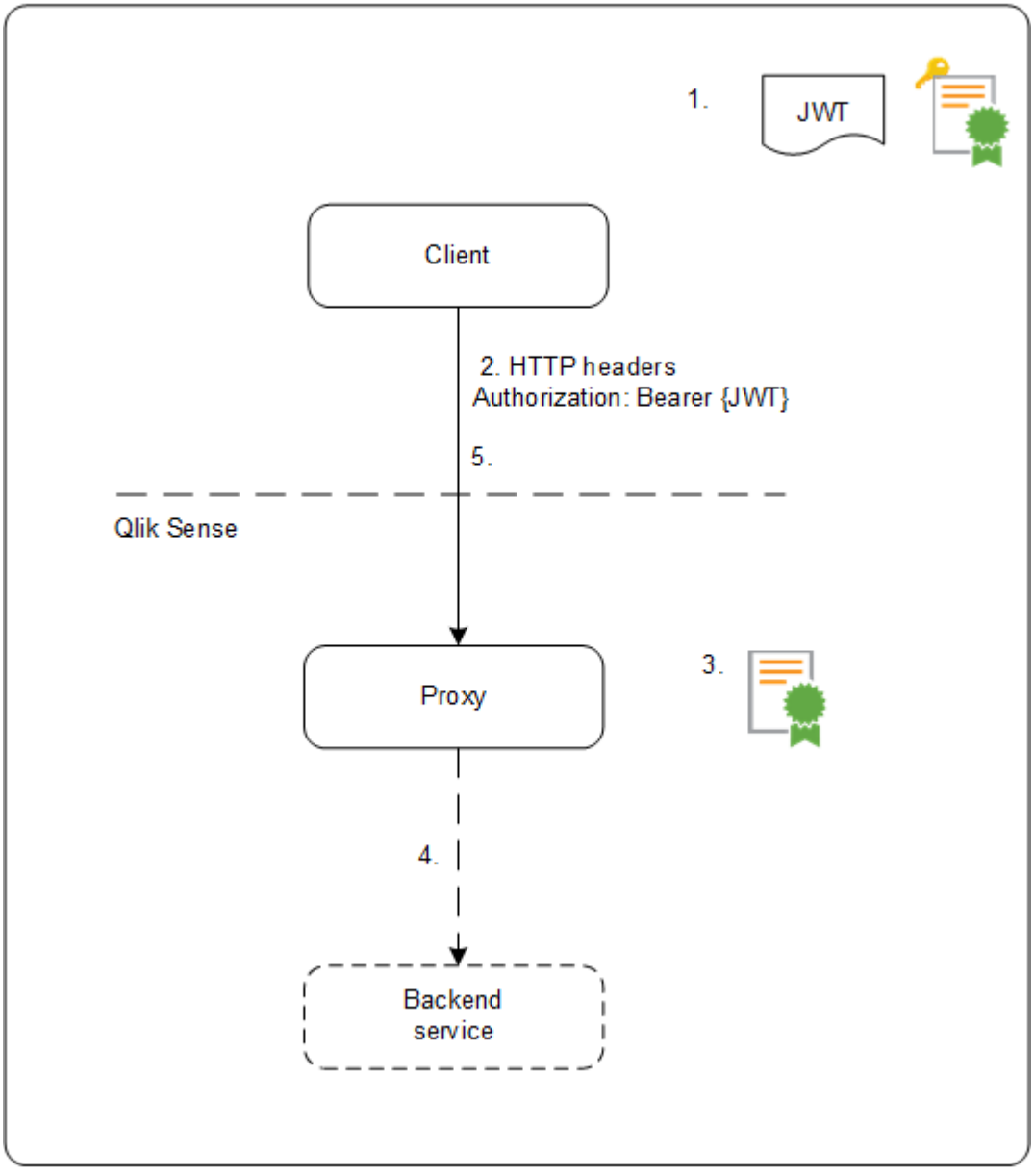
サポートするシグネチャー アルゴリズム

Qlik Sense では以下のシグネチャーをサポートしています。

- RS256 - RSA シグネチャーとSHA256
- RS384 - RSA シグネチャーとSHA384
- RS512 - RSA シグネチャーとSHA512

例: 署名付き JWT による Qlik Sense へのアクセス

次の例は、署名付き JWT を使用して Qlik Sense にアクセスする場合の手順です。



1. クレームのセットを含む JWT が生成され、構成した証明書用の秘密鍵で署名されます。
2. HTTP 承認ヘッダーで、署名付き JWT を含め、要求がプロキシに送信されます。
3. プロキシは、構成された証明書の公開鍵を使用して JWT のシグネチャーを有効化します。

4. プロキシは、構成された属性マッピングを含む Qlik Sense ヘッダーを出力し、バックエンド サービスに呼び出しを転送します。
5. クライアントはセッションを受信し、その後の呼び出しには JWT を含める必要はありません。
    a. 呼び出しに JWT が含まれている場合、その JWT は有効化され、無効な場合はそのユーザーからのアクセスが拒否されます。
    b. JWT に含まれるユーザーがセッションのために保存されたユーザーと異なる場合、そのユーザーは新しいセッションを取得します。

標準的なフィールド

JWT クレーム内では以下のフィールドを使用できます。

- Issuer (iss): JWT を発行したプリンシパルを識別します。
- Subject (sub): JWT のサブジェクトを識別します。
- Audience (aud): JWT の受信者を識別します。
- Expiration time (exp): JWT が受領されなくなるまでの有効期限を識別します。
- Not before (nbf): JWT の受領が開始される時間を識別します。
- Issued at (iat): JWT が発行された時刻を識別します。
- JWT ID (jti): トークンを識別します。

制限事項

以下の制限事項があります。

- 暗号化された JWT はサポートされていません。

    HTTPS を使用する場合、JWT を含むすべてのトラフィックは転送中に暗号化されます。

- 以下の署名アルゴリズムのみサポートしています。
    - RS256 - RSA シグネチャーと SHA256
    - RS384 - RSA シグネチャーと SHA384
    - RS512 - RSA シグネチャーと SHA512

AD FS を使用した OIDC の設定

OpenID Connect (OIDC) は、認可フレームワークである OAuth 2.0 の上位の認証層です。OIDC でシングル サインオン (SSO) を有効化すると、ユーザーが Web サイトやアプリケーションにアクセスするためにログオンする回数を減らすことができます。OIDC はサードパーティ製品による認証用に構成することができます。

AD FS の構成

このトピックでは、AD FS を構成する方法について説明しますが、AD FS をインストールする方法については、説明していません。AD FS は構成内で ID プロバイダーとなるため、構成を開始するためには AD FS のアクセス権が必要です。

この構成にはサードパーティ製品が含まれているため、構成が本項の説明の通りであると保証することはできません。サードパーティ製品に変更が行われ、弊社が認識していない場合もあります。

次の手順を実行します。

1. AD FS で、サーバー マネージャーを開きます。
2. 右側のメニューで、[**ツール**] > [**AD FS管理**] を選択します。
3. AD FS管理ペインで、[**アプリケーショングループ**] > [**アクション**] > [**アプリケーショングループの追加**] を選択します。
4. [**サーバーアプリケーション**] を選択します。[名前] と[説明] を入力します。[**次へ**] をクリックします。
5. クライアントIDは、[**サーバーアプリケーション**] の下にあります。それをメモしてください。
6. リダイレクトURI: *https://<QSEhostname>/<VirtualProxyPrefix>/oidcauthn* を入力して、[URIの**追加**] ボタンをクリックします。

   仮想プロキシのプレフィックスとして adfs を使用します。
7. [**次へ**] をクリックします。
8. [**共有秘密キーの生成**] を選択します。秘密鍵が生成されます。それをメモしてください。
   設定の概要が表示されます。[**次へ**] をクリックして、アプリケーション グループの追加 ステップを完了します。
9. 作成したアプリケーション グループを開きます。
   [**プロパティ**] ウィンドウが表示されます。
10. [**アプリケーションの追加**] をクリックします。
    新しいウィンドウが表示されます:**<app group name> に新しいアプリケーションを追加します**。
11. [**Web API**] のテンプレートを選択します。[**次へ**] をクリックします。
12. 任意で、[**Web API**] の名前を編集します。
13. [**識別子**] に、このアプリケーション グループにサーバー アプリケーションを作成するときにメモしたクライアントID を追加します。[**次へ**] をクリックします。
14. [**アクセスコントロールポリシーの適用**] で、[**全員を許可**] を選択します。[**次へ**] をクリックします。
15. [**アプリケーション権限の設定**] > [**クライアントアプリケーション**] で、サーバアプリケーションが選択されています。これは変更しないで下さい。[**許可されているスコープ**]について、**allatclaims**、**email**、**openid**、および **profile** を選択します。[**次へ**] をクリックします。
16. 設定の概要が表示されます。[**次へ**] をクリックして、Web API の追加 ステップを完了します。
17. **Web API** > **発行変換ルール** を開きます。
18. [**Add Rule**] (規則の追加) をクリックします。ルールの名前を入力し、[**属性ストア**] として [**Active Directory**] を選択してから、「*メール アドレス*」-「*メール アドレス*」および「*トークングループ- 名前の指定なし*」-「*グループ*」マッピングを追加します。変更内容を保存します。
19. **ADFS Management** ツールで **証明書利用者の信頼** に移動します。
20. 以下の証明書利用者の信頼があることを確認してください。**識別子**は *https://<ADFShostname>/adfs/services/trust*である必要があります。

21. 証明書利用者の信頼が使用できない場合は、新規で追加する必要があります。*https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/create-a-relying-party-trust#to-create-a-claims-aware-relying-party-trust-manually* で説明されている手順に従いますが、**「証明書の構成」**および**「URLの構成」**の手順はスキップします。
22. AD FS 認証による Qlik Sense Enterprise サイトを使用するユーザーの電子メールアドレスを必ず追加してください。
    a. AD サーバーで [**Active Directory ユーザーとコンピューター**] を開きます。
    b. [**Users**] フォルダに移動し、ユーザーを右クリックして [**プロパティ**] を選択します。
    c. [**全般**] で、[**電子メール**] フィールドに、ユーザーの電子メールアドレスを入力します。
    d. [**OK**] をクリックして、変更を保存します。

仮想プロキシの作成および構成

次の手順を実行します。

1. Qlik Management Console (QMC) で、[**Virtual proxies**] (仮想プロキシ) を開きます。
2. クリック 新規作成
3. 右側の [**Properties**] (プロパティ) で、[**Identification**] (ID)、[**Authentication**] (認証)、[**Load balancing**] (負荷分散)、および [**Advanced**] (詳細設定) の各セクションを選択していることを確認します。
4. [**Identification**] (ID) で、[**Description**] (説明) と [**Prefix**] (プレフィックス) に「*adfs*」と入力します。
5. [**Session cookie header name**] (セッション クッキー ヘッダー名) で、既存の名前の末尾に「*-adfs*」を追加し、ヘッダー名を *X-Qlik-Session-adfs* にします。
6. [**Authentication method**] (認証方法) に [**OIDC**] を選択します。
7. [**OpenID 接続メタデータ URI**] フィールドに、「OpenID Configuration」のURLを入力します。URLの形式は、次のようにする必要があります: *https://<ADFShostname>/adfs/.well-known/openid-configuration*。
8. メモしたクライアント ID とクライアント シークレットを対応するフィールドに入力します。
9. **Realm**に、*adfs* と入力します。OIDC 認証によってリポジトリに追加されたユーザーのユーザー ディレクトリ名は「adfs」に設定されます。

   サブジェクト属性値の形式が domainname\username の場合、realm はオプションです。そうでない場合、realm は必須です。
   属性 sub、name、email は必須です。その他の属性は必須ではありませんが、値は必要です。空の属性がある構成はエラーを発生します。

10. [**name**] (名前) フィールドで、値を *unique_name* に変更します。
11. [**groups**] (グループ) フィールドで、値を *group* に変更します。
12. [**client_id**] (クライアント ID) フィールドで、値を *appid* に変更します。
13. [**scope**] (範囲) フィールドで、値を *openid allatclaims profile email* と入力します。

    OpenID は必須です。他のスコープは追加できますが、ID プロバイダー側での設定と一致する必要があります。

14. [**Load balancing nodes**] (負荷分散ノード) で、[**Add new server node**] (新しいサーバー ノードの追加) をクリックします。
15. この仮想プロキシが接続を負荷分散するエンジン ノードを選択します。
16. [**Advanced**] (詳細設定) の [**Host allow list**] (ホスト許可リスト) セクションで、[**Add new value**] (新しい値の追加) をクリックします。
17. AD FS サーバーのホスト名を追加します。
18. [**Apply**] (適用) をクリックし、[**OK**] をクリックしてサービスを再起動します。
19. 右側の [**Associated items**] (関連するアイテム) メニューで、[**Proxies**] (プロキシ) を選択します。
20. [**Link**] (リンク) をクリックし、この構成を使用するプロキシ (1 つまたは複数) に仮想プロキシをリンクさせます。
    プロキシ サービスが再起動します。

OpenID Connect Metadata URI、*https://{IdP_hostname}/.well-known/openid-configuration* を選択した時に、IdP サーバーで構成した要求とスコープが、**claims_supported** と **scopes_supported** タグで返されることを確認します。

これで AD FS の構成が完了しました。

> *例えば、属性の確認のためにトークンが使用される場合は、Qlik Sense を参照してください。OIDC トークンを手動でリクエストし、正しい属性が含まれるかどうかを確認する方法 (PowerShell)*

Auth0を使用した OIDC の設定

OpenID Connect (OIDC) は、認可フレームワークである OAuth 2.0 の上位の認証層です。OIDC でシングル サインオン (SSO) を有効化すると、ユーザーが Web サイトやアプリケーションにアクセスするためにログオンする回数を減らすことができます。OIDC はサードパーティ製品による認証用に構成することができます。

Auth0 の構成

> *この構成にはサードパーティ製品が含まれているため、構成が本項の説明の通りであると保証することはできません。サードパーティ製品に変更が行われ、弊社が認識していない場合もあります。*

次の手順を実行します。

1. *https://auth0.com/* にログインして、メールアドレスを使用してアカウントを作成します。
2. Auth0 の左メニューで、[**Applications**] (アプリケーション) を開きます。
3. [**Create application**] (アプリケーションの作成) をクリックします。
4. アプリケーションの名前を指定し、[**Single Page Web Applications**] (シングル ページ Web アプリケーション) を選択して、[**作成**] をクリックします。
5. 必要に応じて、Web アプリテクノロジーを選択します。
6. [**設定**] を選択します。

7. [**Allowed Callback URLs**] (許可されたコールバックURL) ボックスで、*https://<QSEhostname>/<VirtualProxyPrefix>/oidcauthn* の書式でホストに URL を追加します。

仮想プロキシのプレフィックスとして auth0 を使用します。

8. 下にスクロールし、[**Save changes**] (変更を保存) をクリックします。
9. [**クライアント ID**] と[**クライアント シークレット**] の値を書き留めます。
10. 一番下までスクロールし、[**詳細設定**] を選択します。
11. [**エンドポイント**] を選択します。
12. [**OpenID configuration**] (OpenID 構成) の URL を書き留めます。

仮想プロキシの作成および構成

次の手順を実行します。

1. Qlik Management Console (QMC) で、[**Virtual proxies**] (仮想プロキシ) を開きます。
2. クリック 新規作成
3. 右側の [**Properties**] (プロパティ) で、[**Identification**] (ID)、[**Authentication**] (認証)、[**Load balancing**] (負荷分散)、および [**Advanced**] (詳細設定) の各セクションを選択していることを確認します。
4. [**Identification**] (ID) で、[**Description**] (説明) と[**Prefix**] (プレフィックス) に「*auth0*」と入力します。
5. [**Session cookie header name**] (セッション クッキー ヘッダー名) で、既存の名前の末尾に「*-auth0*」を追加し、ヘッダー名を *X-Qlik-Session-auth0* にします。
6. [**Authentication method**] (認証方法) に [**OIDC**] を選択します。
7. [**OpenID 接続メタデータ URI**] フィールドに、メモした「OpenID Configuration」のURLを入力します。URLの形式は、次のようにする必要があります: *https://<Auth0hostname>/.well-known/openid-configuration*。
8. メモしたクライアントID とクライアント シークレットを対応するフィールドに入力します。
9. **Realm**に、*auth0*と入力します。OIDC 認証によってリポジトリに追加されたユーザーのユーザー ディレクトリ名は「auth0」に設定されます。

サブジェクト属性値の形式がdomainname\usernameの場合、realmはオプションです。そうでない場合、realm は必須です。
属性 sub、name、email は必須です。その他の属性は必須ではありませんが、値は必要です。空の属性がある構成はエラーを発生します。

10. [**client_id**] (クライアントID) フィールドで、値を *aud* に変更します。
11. [**scope**] (範囲) フィールドで、値を *openid profile email* と入力します。

OpenID は必須です。他のスコープは追加できますが、ID プロバイダー側での設定と一致する必要があります。

12. [**Load balancing nodes**] (負荷分散ノード) で、[**Add new server node**] (新しいサーバー ノードの追加) をクリックします。
13. この仮想プロキシが接続を負荷分散するエンジン ノードを選択します。

14. [**Advanced**] (詳細設定) の [**Host allow list**] (ホスト許可リスト) セクションで、[**Add new value**] (新しい値の追加) をクリックします。
15. Auth0 テナント ([**OpenID Connect Metadata URI**] (OpenID 接続のメタデータURI) で入力したのと同じホスト名) のホスト名を追加します。
16. [**Apply**] (適用) をクリックし、[**OK**] をクリックしてサービスを再起動します。
17. 右側の [**Associated items**] (関連するアイテム) メニューで、[**Proxies**] (プロキシ) を選択します。
18. [**Link**] (リンク) をクリックし、この構成を使用するプロキシ (1 つまたは複数) に仮想プロキシをリンクさせます。
    プロキシ サービスが再起動します。

OpenID Connect Metadata URI、*https://{IdP_hostname}/.well-known/openid-configuration* を選択した時に、IdP サーバーで構成した要求とスコープが、**claims_supported** と**scopes_supported** タグで返されることを確認します。

https://{IdP_hostname}/.well-known/openid-configuration アクセス時に返される値の例

これで Auth0 の構成が完了しました。

*例えば、属性の確認のためにトークンが使用される場合は、*Qlik Sense を参照してください。 OIDC トークンを手動でリクエストし、正しい属性が含まれるかどうかを確認する方法 (PowerShell)

OKTAを使用した OIDC の設定

OpenID Connect (OIDC) は、認可フレームワークである OAuth 2.0 の上位の認証層です。OIDC でシングル サインオン (SSO) を有効化すると、ユーザーが Web サイトやアプリケーションにアクセスするためにログオンする回数を減らすことができます。OIDC はサードパーティ製品による認証用に構成することができます。

OKTA の構成

この構成にはサードパーティ製品が含まれているため、構成が本項の説明の通りであると保証することはできません。サードパーティ製品に変更が行われ、弊社が認識していない場合もあります。

次の手順を実行します。

1. 管理者アカウントを使用して、*https://www.okta.com/* にログインします。
2. [**セキュリティ**] > [**API**] に移動します。
3. [**承認サーバー**] タブで、[**承認サーバーの追加**] を選択し、承認サーバーの名前、オーディエンス、説明を入力します。
    a. 承認サーバーを作成したら、[**クレーム**] タブに移動します。
        i. [**クレームの追加**] をクリックします。
        ii. クレームの [**名前**] を [*グループ*] として入力します。
        iii. [**トークン タイプに含める**] ドロップダウンで、[**ID トークン**] と [**常に**] を選択します。
        iv. [**値の種類**] を [**グループ**] に設定します。
        v. [**フィルター**] を [**regex .* と一致**] に設定します。
        vi. [**作成**] をクリックします。
    b. [**Scopes**] (スコープ) タブに移動します。
        i. [**Scopes**] (スコープ) タブを開きます。
        ii. [**スコープの追加**] をクリックします。
        iii. スコープの [**名前**] を [*グループ*] として入力します。
        iv. [**公開メタデータに含める**] を選択します。
        v. [**作成**] をクリックします。
    c. [**アクセス ポリシー**] タブに移動します。
        i. [**Add Policy**] (ポリシーの追加) をクリックします。新しいポリシーの名前と説明を入力し、[**割り当て先**] を [*すべてのクライアント*] オプションに設定したままにします。[**ポリシーの作成**] をクリックします。
        ii. 新しいポリシーが作成されたら、[**ルールの追加**] をクリックしてポリシーの新しいルールを追加します。ルール名を入力します。すべての項目の既定値をそのままにして、[**ルールの作成**] をクリックします。
    d. 承認サーバーの [**設定**] タブにある発行者 URI に注意してください。この URI は次の形式になります: *https://<yourOktaDomain>/oauth2/<authServerId>*

    上記の変更を行うことにより、新しい認証サーバーを作成する代わりに、OKTA で使用可能な既定の認証サーバーを利用できます。
4. トップ メニューで、[**Applications**] (アプリケーション) を選択します。
5. [**Add Application**] (アプリケーションの追加) をクリックします。
6. [**Create New App**] (アプリの新規作成) をクリックします。
7. [**Platform**] (プラットフォーム) として [**Web**] を選択します。

8. [**Sign on method**] (サインオン方法) として [**OpenID Connect**] を選択します。
9. [**作成**] をクリックします。
構成ウィンドウが表示されます。
10. アプリに *Qlik SenseOIDC 設定と名前を付けます。*
11. 必要に応じて、ロゴを追加します。
12. [**Login Redirect URI**] に、*https://<QSEhostname>/<VirtualProxyPrefix>/oidcauthn* と入力します。

> *仮想プロキシのプレフィックスとして Okta を使用します。*

13. [**保存**] をクリックします。
アプリケーションの詳細 ページが表示されます。
14. [**全般**] > [**クライアント認証情報**] にある、[**クライアント ID**] と [**クライアント シークレット**] の値を書き留めます。
15. 作成した接続をユーザーが使用できるように、ユーザーをアプリに割り当てる必要があります。[**Assign to People**] (ユーザーへの割り当て) をクリックし、ユーザーを追加します。(ユーザーが OKTA アカウントを持っていることが前提となります。)

仮想プロキシの作成および構成

次の手順を実行します。

1. Qlik Management Console (QMC) で、[**Virtual proxies**] (仮想プロキシ) を開きます。
2. クリック 新規作成
3. 右側の [**Properties**] (プロパティ) で、[**Identification**] (ID)、[**Authentication**] (認証)、[**Load balancing**] (負荷分散)、および [**Advanced**] (詳細設定) の各セクションを選択していることを確認します。
4. [**Identification**] (ID) で、[**Description**] (説明) と [**Prefix**] (プレフィックス) に「*okta*」と入力します。
5. [**Session cookie header name**] (セッション クッキー ヘッダー名) で、既存の名前の末尾に「*-okta*」を追加し、ヘッダー名を *X-Qlik-Session-okta* にします。
6. [**Authentication method**] (認証方法) に [**OIDC**] を選択します。
7. [**OpenID 接続メタデータ URI**] 項目に、Okta の承認サーバー設定から指定された発行者 URI を次の形式で入力します: *https://<yourOktaDomain>/oauth2/<authServerId>/.well-known/openid-configuration*。
8. メモしたクライアント ID とクライアント シークレットを対応するフィールドに入力します。
9. **Realm**に、「okta」と入力します。OIDC 認証によってリポジトリに追加されたユーザーのユーザー ディレクトリ名は「okta」に設定されます。

> *サブジェクト属性値の形式が domainname\username の場合、realm はオプションです。そうでない場合、realm は必須です。*
> *属性 sub、name、email は必須です。その他の属性は必須ではありませんが、値は必要です。空の属性がある構成はエラーを発生します。*

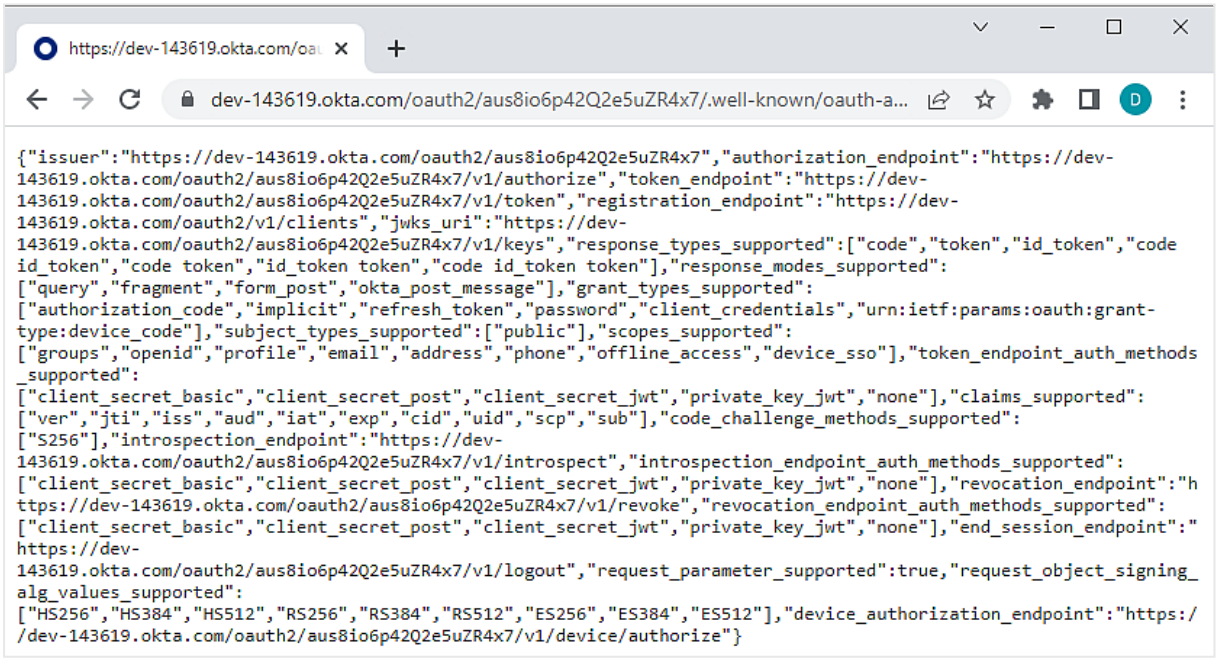
10. [**client_id**] (クライアント ID) フィールドで、値を *aud* に変更します。
11. [**scope**] (範囲) フィールドで、値を *openid profile email* と入力します。

> *OpenID は必須です。他のスコープは追加できますが、ID プロバイダー側での設定と一致する必要があります。*

12. [**Load balancing nodes**] (負荷分散ノード) で、[**Add new server node**] (新しいサーバー ノードの追加) をクリックします。
13. この仮想プロキシが接続を負荷分散するエンジン ノードを選択します。
14. [**Advanced**] (詳細設定) の [**Host allow list**] (ホスト許可リスト) セクションで、[**Add new value**] (新しい値の追加) をクリックします。
15. OKTA ([**OpenID Connect Metadata URI**] (OpenID 接続のメタデータURI) で入力したのと同じホスト名) の名前を追加します。
16. [**Apply**] (適用) をクリックし、[**OK**] をクリックしてサービスを再起動します。
17. 右側の [**Associated items**] (関連するアイテム) メニューで、[**Proxies**] (プロキシ) を選択します。
18. [**Link**] (リンク) をクリックし、この構成を使用するプロキシ (1 つまたは複数) に仮想プロキシをリンクさせます。
    プロキシ サービスが再起動します。

OpenID Connect Metadata URI、*https://{IdP_hostname}/.well-known/openid-configuration* を選択した時に、IdP サーバーで構成した要求とスコープが、**claims_supported** と**scopes_supported** タグで返されることを確認します。

https://{IdP_hostname}/.well-known/openid-configuration アクセス時に返される値の例



これで OKTA の構成が完了しました。

例えば、属性の確認のためにトークンが使用される場合は、Qlik Sense を参照してください。OIDC トークンを手動でリクエストし、正しい属性が含まれるかどうかを確認する方法 (PowerShell)

Qlik Sense との SAML シングル サインオン (SSO) を実現するための、SAP HANA の構成

SAP HANA でアクセス権が異なるユーザーが多くいる場合でも、複数の ODBC コネクターと資格情報を作る必要はありません。代わりに、SAP HANA への シングル サインオン (SSO) ODBC コネクターを作成し、SAP HANA のセキュリティ認証を使用できます。

Qlik Sense ユーザーは、Qlik と SAP HANA 間で一貫して識別され認証されます。そのため、Qlik Sense ハブからアプリケーションを閲覧するユーザーは、SAP HANA で閲覧が許可されている値や属性しか閲覧できません。これは、Qlik アプリケーションにロードされた静的データには適用されません。しかし、ユーザーが新しい接続を作成したり、データをリロードしたり、Direct Discovery を使用する場合には適用されます。

これはアプリのデザイナーやユーザーが多く存在する場合に便利です。重要なことは、ユーザーが Qlik アプリにログインして、接続文字列に対してユーザー ID を動的に渡すことで、各ユーザーが自分のデータベース ログイン情報を使ってデータソースに効率的に接続できるようにすることです。これによって、データソースに対しても、行やテーブル レベルでのセキュリティを維持することができます。

SSO を設定するには、次の操作を行います。

手順 1 ~ 4 は SAP HANA Studio で行います。

1. 証明書と秘密キーを生成します。
2. SAP HANA に証明書をインストールします。
3. SAP HANA Studio で ID プロバイダー (IdP) とユーザー マッピングを作成します。
4. SAP HANA の構成を検証します。
5. Qlik Sense インストールのすべてのノードに PEM ファイルを配布して Qlik Sense を構成します。すべてのノードに同じ証明書を使います。
   - 各コンピューターの証明書フォルダーに証明書と秘密キーのファイルをコピーします。初期設定では、これは *C:\ProgramData\Qlik\Sense\Engine\Certificates* です。

     証明書に Qlik.pem および Qlik_key.pem という名前が付けられていることを確認してください。
6. SAP HANA への ODBC 接続を作成します。
   - [**現在のユーザー**] を選択します。
     あらゆるデータ接続の使用が SAP HANA からエンド ユーザーの資格情報を使って実行できるようになります。
   - データを選択し、マッピングされたデータベース ユーザーの権限と利用可能なデータが合致することを確認します。

C:\ProgramData\Qlik\Sense\Engine に移動し、*Settings.ini* を開いて、Qlik Sense の設定を有効にします。次のテーブルに、SSO 設定の選択肢を定義します。

SSO 設定

名前	初期設定	説明
SSOCertificateFolder	デフォルトのエンジン フォルダ	証明書が作成されるフォルダ
SSOCertificate	”qlik.pem”	証明書ファイルの名前
SSOPrivateKey	「qlik_key.pem」	秘密キーの名前
SSOCasing	0	0: 大文字/小文字を区別 >0: 大文字 <0: 小文字
SSOExternalId	0	0: QlikId (ドメイン\ユーザー名) 1: UPN (username@domain.com) 2: (ユーザー名)

シングル サインオン のための Cloudera Impala の構成

シングル サインオン (SSO) ソリューションの場合、アプリや Web サイトにユーザーがログオンする回数を最小限にすることができます。

Qlik Sense で Cloudera Impala をデータ ソースとして設定する場合、Cloudera Impala を SSO で構成できます。Qlik Sense ユーザー資格情報を保存し、信頼関係を定義することで、Qlik Sense 資格情報が Qlik Sense から Cloudera Impala に渡されます。

Cloudera Impala への SSO データ接続を使ってアプリを作成するユーザーは、Cloudera Impala で認証されます。アプリデータがインメモリでロードされる場合、データへのアクセスは Qlik Sense 内から制御されます。他の Cloudera Impala データ ソース接続が作成されることを防ぐために、QMC でセキュリティ ルールを設定して ODBC データ接続を作成できないようにします。

*Qlik ODBC Connector Package の Cloudera Impala も SSO に対応しています。ODBC コネクタパッケージでこのコネクターを使用する場合は、次の設定指示に従ってください。*Cloudera Impala コネクターの SSO の設定。

この構成では、ベンダー提供のドライバーのみ動作し、Qlik Connector Package のドライバーは動作しません。

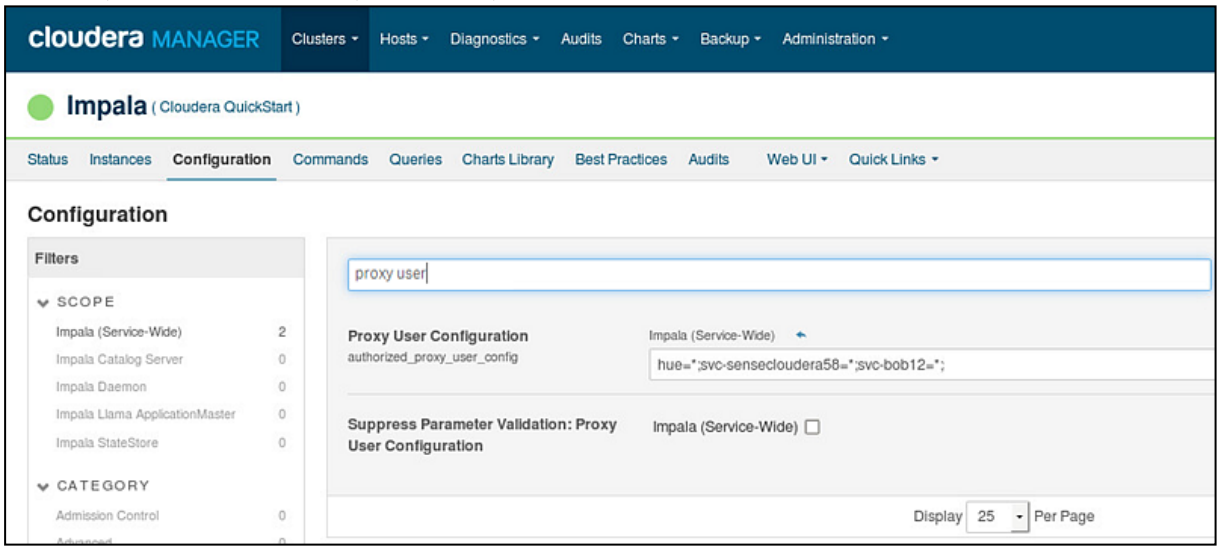
この構成は Cloudera Impala のみを対象としています。Hive には別の構成オプションが必要です。

Cloudera Impala 用の SSO の設定

Cloudera Impala 用に SSO を設定するには、最初に「kerberized」クラスターを設定する必要があります。このクラスターでは Kerberos 認証が要求され、承認には Sentry が使用されます。次に、Cloudera Manager で権限を借用できるユーザーの追加、ベンダーの ODBC ドライバーのインストール、Cloudera Impala へのデータ ソースの作成、Qlik Sense の構成、および Cloudera Impala への ODBC 接続の作成を行う必要があります。

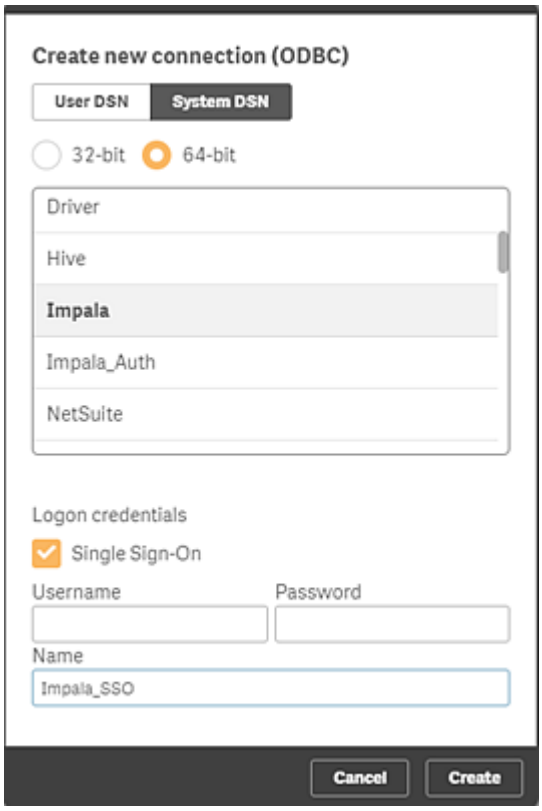
次の手順を実行します。

1. Kerberos 認証を要求する「kerberized」クラスターを設定し、承認には Sentry を使用します。
   詳細については、Cloudera のドキュメントを参照してください。 Cloudera
2. Cloudera Manager で権限を借用できるユーザーを追加します。
   a. Cloudera Manager で Impala クラスターを表示し、[**構成**] を選択します。
   b. *プロキシ ユーザー*を探します。
   c. [**プロキシ ユーザーの構成**] で、他のユーザーの権限を借用することを許可されているサービス アカウント ユーザーを追加します。
   次の例では、サービス アカウント ユーザーの svc-bob12 がユーザーの権限を借用できます。
   例: *hue=*;svc-senseclouderа58=*;svc-bob12=*;*



Cloudera Impala のみが対象のプロキシ ユーザー構成

   d. Cloudera サービスを再起動します。
3. ベンダーの ODBC ドライバーをインストールします。
4. Cloudera Impala へのデータ ソースを作成します。
5. Qlik Sense を構成します (必要な場合)。
   a. *%ProgramData%\Qlik\Sense\Engine* に移動し、*Settings.ini* を開きます。
   b. 設定を編集し *Settings.ini の SSO 設定 (page 501)* を確認して、保存します。
   c. Qlik Sense Engine Service を再起動します。
6. Qlik Sense を使用し、Cloudera Impala への ODBC 接続を作成します。
   a. データ ロード エディターを開きます。
   b. ODBC 接続を作成し、[**ログオン資格情報**] の下の [**シングル サインオン**] を選択します。



c. データ モデル ビューアーで、マッピングされたデータベース ユーザーの権限と利用可能なデータが合致することを確認します。

設定はこれで完了です。

Settings.ini の SSO 設定

SSO 設定

設定	既定値	絞込値
SSODisableLogOn	0	• 0:SSO の有効化 • 1:SSO の無効化
SSOCasing	0	• 0: 大文字/小文字を区別 • >0: 大文字 • <0: 小文字
SSOExternalId	0	• 0: QlikId (ドメイン\ユーザー名) • 1: UPN (username@domain.com) • 2: ユーザー名

クライアント認証の構成

Qlik Sense 管理者は、Qlik Sense に対するクライアントの認証実行をユーザーに許可できます。それには、Qlik Management Console (QMC) で認証リンクを生成して、そのリンクをクライアント ユーザーに配布する必要があります。認証リンクの有効期限はありません。

任意のノードの認証リンクを生成し、そのリンクを手動で配布することができます。ただし、Qlik Sense ハブから取得されることになるリンクを生成する場合は、セントラル ノードの既定の仮想プロキシを選択する必要があります。

ユーザーには必ずユーザー アクセスまたはプロフェッショナル アクセスを割り当てます。

アクセスの詳細については、「*ユーザー アクセスの管理 (page 319)*」と「*Professional アクセスの管理 (page 309)*」を参照してください。

クライアント認証はテスト サーバーでは対応していません。

認証リンクの生成と配布

1. Qlik Sense 管理者として QMC を開きます。
2. [**仮想プロキシ**] タブをクリックし、プロキシを選択して [**編集**] をクリックします。
3. [**仮想プロキシの編集**] ページの [**クライアント認証 リンク**] タブをクリックします。
4. クライアント認証 リンク ホスト URI を入力します。これは、Qlik Sense サーバーの認証ページを表示する URL です。
5. クライアント認証用の Qlik Sense ホスト サーバーにフレンドリ名を付けます。この名前は認証時に、クライアント ユーザーに対してサーバーを識別するために使用されます。
6. [**生成**] をクリックします。認証 リンクが生成されます。リンクをテキスト エディターにコピーしてファイルを保存します。同じ設定のリンクを後で再び生成する必要がある場合は、同じリンクが生成されます。
7. [**適用**] ボタンをクリックします。適用後、仮想プロキシに関連付けられたすべてのプロキシが再起動されます。
8. リンクを次のいずれかの方法で配布します。
    a. リンクを Qlik Sense ハブから取得できることをクライアント ユーザーに知らせます。Qlik Sense ハブの上部ツール バーにある ••• から [**クライアント認証**] を選択すると、どの Qlik Sense ユーザーもこのリンクを利用できます。ユーザーがリンクを選択すると、クライアントによって認証ボタンが「ようこそ」ページに追加されます。上記の手順で Qlik Sense サーバーに付けたフレンドリ名がボタンの名前になります。ユーザーはボタンをクリックし、自分の Qlik Sense 資格情報を使ってクライアントにログインできます。
    b. メールや別の方法で認証リンクをクライアント ユーザーに配布します。ユーザーがリンクを選択すると、クライアントによって認証ボタンが「ようこそ」ページに追加されます。上記の手順で Qlik Sense サーバーに付けたフレンドリ名がボタンの名前になります。ユーザーはボタンをクリックし、自分の Qlik Sense 資格情報を使ってクライアントにログインできます。
    c. *hubs.ini* ファイルを構成し、これを配布します。
        i. テキスト エディタを使って *hubs.ini* というファイルを作成します。
        ii. 変更内容を保存します。
        iii. 認証リンクを新しい行に追加します。
        iv. Qlik Sense への認証を許可するクライアント ユーザーにファイルを配布します。
        v. 配布されたファイルを C:\Users\<ユーザー名>\Documents\Qlik\Sense\Hubs\ に貼り付けるようユーザーに指示します。*C:\Users\<ユーザー名>\Documents\Qlik\Sense\Hubs*.
        次回ユーザーがクライアントを起動する際、Qlik Sense の資格情報を使用して Qlik Sense サーバーで認証されます。

システム関数計算の設定

管理者として、一部のシステム関数がエンドユーザに値を返さないようにしたり、API呼び出しを防ぐことができます。この設定は任意です。

次の関数は、値を戻さないようにブロックできます。

- ComputerName()
- EngineVersion()
- OSName()
- OSVersion()
- ProductVersion()
- QTProduct()

一部の現在のアプリケーションでは、条件付きの計算で関数を使用する場合があります。

1. *%ProgramData%\Qlik\Sense\Engine* に移動し、*Settings.ini* を開きます。
2. 設定を編集し *Settings.iniのシステム関数計算の設定 (page 503)* を確認して、保存します。
3. Qlik Sense Engine Service を再起動します。

設定はこれで完了です。

*Settings.ini*のシステム関数計算の設定

設定	既定値	絞込値
BlockSystemInfo	BlockSystemInfo=0	• 0: システム関数計算の有効化 • 1: システム関数計算の無効化

プロキシ証明書の変更

Qlik Sense では、サービスとQlik Sense Web クライアント間のすべての通信は、ウェブプロトコルに基づいています。Web プロトコルは、以下のためにセキュア ソケット レイヤー (SSL) を使用します。

- 暗号化と情報の交換とキー
- 通信を行う当事者の認証の証明書

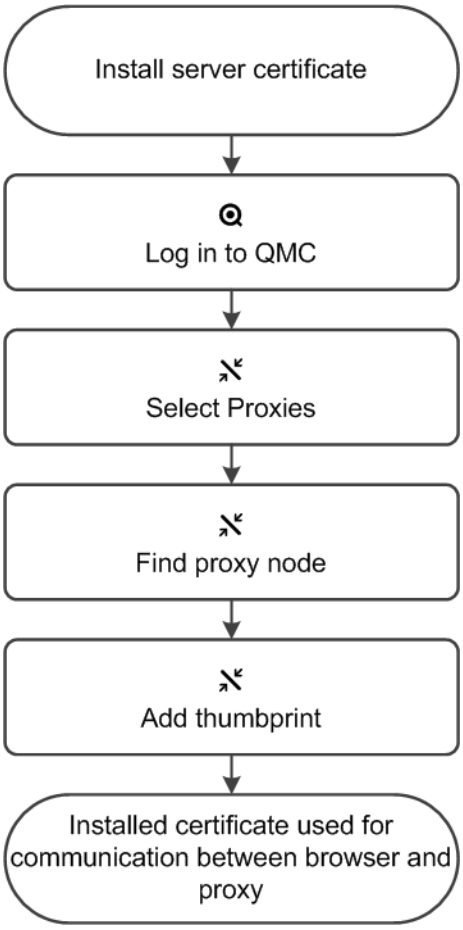
標準的なQlik Senseをインストールすると、Qlik Sense Proxy Service (QPS) に、ブラウザからプロキシへのトラフィックの暗号化を処理するモジュールが組み込まれます。Web ブラウザーとプロキシ間の通信の証明書が置き換わります。

サードパーティの証明書は、Qlik Sense Proxy Service HTTPS ポート(443) にバインドされています。API ポート(4243) 経由の通信は、常に Qlik Sense サーバー証明書を使用します。

プロキシ証明書および管理者権限のないアカウントでのQlik Sense サービス実行を編集する場合、以下のように証明書にプライベートキーのアクセス許可を設定する必要があります。

管理者権限のないユーザーがプロキシを実行している場合、管理者はグループ「Qlik Sense サービス ユーザー」の証明書の秘密キーに読み取りアクセス権を追加する必要があります。そうしないと、プロキシは証明書にアクセスできません。

このフローは、プロキシ証明書の変更を説明したものです。



次の手順を実行します。

1. 新規サーバー証明書をインストールします:
    a. 新規証明書のサムプリントを書き留めます。
    b. [*ローカル コンピューター/個人*] の [Windows 証明書ストア] で新規サーバー証明書をプロキシ ノードにインストールします。

> *有効にするには、証明書が秘密キーを含む必要があります。証明書は、Qlik Sense Proxy Service を実行するために使用されるユーザー アカウントのローカル コンピューター/コンピューター アカウント> MMC の個人部分にインストールされている必要があります。*

> *サードパーティの証明書を使用する場合、その証明書が Windows で信頼されること、その証明書を使って秘密キーが Windows 証明書ストアに保存されていることが必要です。証明書は、Qlik Sense Proxy Service を実行するために使用されるユーザー アカウントのローカル コンピューター/コンピューター アカウント> MMC の個人部分にインストールされている必要があります。*

> *Qlik Sense は SHA-1 や SHA-256 に基づいた署名アルゴリズムを使用して作成される証明書をサポートします。*

2. QMC を開く: *https://<QPS サーバー名>/qmc*
3. QMC スタート ページから、あるいは [**Start (スタート)**] ▼ ドロップダウン メニューから [**Proxies (プロキシ)**] を選択して、概要を表示します。
4. 概要から関連するプロキシを探し、[**編集**] を選択します。
5. [**セキュリティ**] プロパティ グループの [**SSL ブラウザ証明書捺印 (署名)**] を編集し、この手順のステップ 1 からインストール済みサーバー証明書のサムプリントを追加します。
6. アクション バーで [**適用**] をクリックし、変更内容を保存します。
   ページの最下部に [**更新完了**] と表示されます。
7. プロキシを再開します。

これでインストールされた証明書は、Web ブラウザーとプロキシ間の通信のために使用できます。お使いのインターネット ブラウザに QMC のアドレスを入力すると、緑の南京錠 (ブラウザによっては南京錠に似たアイコン) が表示されます。これは、ブラウザーが証明書を信頼して、サーバー コンピューターを特定できたことを意味しています。QMC の既定のアドレスは、*https://<QPS サーバー名>/qmc*です.

署名済みサーバープロキシ証明書への変更

既定で、ウェブ ブラウザ (クライアント) と Qlik Sense プロキシの間のセキュアな通信には自己署名証明書が使用されます。その結果、クライアント ウェブ ブラウザに、「このサイトのセキュリティ証明書は信頼できません」(Chrome) または「接続の安全性を確認できません」(Firefox) といった警告が表示されることがあります。この問題を解決するには、ウェブ ブラウザ (クライアント) とプロキシの間の通信に使用される証明書を、信頼できる認証局 (CA) の署名済みサーバー証明書に置き換える必要があります。

> *既存の自己署名証明書は安全です。証明書が安全かどうかを判別するための情報がウェブ ブラウザに十分にないため、警告が表示されます。ここで説明する手順に従えば、クライアント ウェブ ブラウザの警告を排除することができます。*

主な手順

署名済みサーバープロキシに変更する場合は、以下の主な手順に従う必要があります。手順 2 ~ 4 には、サブセクションの詳細な手順が含まれています。

1. 信頼できる CA (VeriSign、GlobalSign など) から、プロキシ ノードの URL に適合する有効な署名済みサーバー証明書を入手します。
2. Windows ローカル コンピューターの証明書ストアに上記証明書をインポートします。
3. 上記証明書のサムプリントを見つけます。
4. 上記証明書を使用するようにプロキシ ノードを構成します。

Qlik Sense のバージョンに関係なく、証明書自体に秘密キーが含まれている必要があります。Microsoft Management Console (MMC) で証明書を確認することで、キーが存在するかどうかを検証できます。次の確認メッセージが表示されます。「この証明書に対応する秘密キーを持っています。」

証明書のインポート

次の手順を実行します。

1. プロキシ ノード上でMMC を起動します。
2. MMC で、[**ファイル > スナップインの追加と削除...**] の順に開きます。
3. [**証明書**] を選択して [**追加**] をクリックします。
4. [**コンピューター アカウント**] を選択して [**次へ**] をクリックし、[**ローカル コンピューター**] を選択して [**完了**] をクリックします。
5. MMC で、[**証明書 (ローカル コンピューター)/個人**] を開きます。
6. MMC で、[**他の操作 > すべてのタスク > インポート...**] を開きます。
7. CA から提供された証明書ファイルに移動します。
8. 画面の説明に従って、秘密キーを含む証明書をインポートします。
9. 新しい証明書が **[証明書 (ローカル コンピューター)] > [個人] > [証明書]** にインポートされ、秘密キーを含んでいることを確認します。
10. **[証明書] > [証明のパス]** をダブルクリックして、**「この証明書は問題ありません」**と表示されることを確認します。

*Qlik Sense サービスを実行するサービス アカウントで新しい証明書を利用できることを確認する必要があります。そのための最適な方法は、サービス アカウントとして MMC を実行し、**[個人] > [証明書]** に新しい証明書が表示されているかどうかを確認することです。ローカル システムでサービスを実行している場合、Psexec などのツールを使用してローカル システムとして MMC を実行し、新しい証明書を利用できることを確認できます。*

証明書にプライベート キーのアクセス許可を設定します。

プロキシ証明書および管理者権限のないアカウントでの Qlik Sense サービス実行を編集する場合、以下のように証明書にプライベートキーのアクセス許可を設定する必要があります。

1. プロキシ ノード上で **MMC** を起動します。
2. **MMC** で、[**証明書 (ローカル コンピューター)/個人**] を開きます。
3. CA から提供された証明書を選択します。
4. [**アクション] > [All Tasks] (すべてのタスク) > [Manage Private Keys**] (プライベート キーの管理) を選択します。
5. [**Permissions**] (権限) ポップアップで、**「Qlik Senseサービス ユーザー」**グループまたは Qlik Sense サービスを実行中の特定のサービス ユーザーに読み取り権限を追加します。
6. Qlik Sense Proxy Service を再起動します。

証明書サムプリントの確認

次の手順を実行します。

1. MMC で、インポートした証明書を右クリックして [**開く**] を選択します。
2. [**詳細**] タブで、下にスクロールして [**拇印**] を選択します。
3. サムプリントのハッシュ値をマーク/ハイライトし、Ctrl キーを押しながらC キーを押して、クリップボードにハッシュ値をコピーします。
4. テキスト エディターにハッシュ値を貼り付け、すべてのスペースを削除します。

プロキシ ノードの構成

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. [**Proxies (プロキシ)**] を開きます。
3. プロキシを選択して、[**Edit (編集)**] をクリックします。
4. 右側の [**Properties (プロパティ)**] で [**Security (セキュリティ)**] を選択します。
5. 下にスクロールして、[**Security (セキュリティ)**] セクションで [**SSL browser certificate thumbprint (SSL ブラウザ証明書サムプリント)**] を見つけます。
6. 新しい証明書のサムプリントのハッシュ値を (テキスト エディターから) 貼り付けます。
7. [**適用**] をクリックします。

これで、ブラウザの警告が表示されることなく、Qlik Sense プロキシにアクセスできます。

QMC を使用して証明書をエクスポートする

お使いの Qlik Sense インストールにサードパーティ製ツールを追加したい場合、証明書をエクスポートする必要があります。

エクスポートした証明書は、以下を行うために使用できます。

- 認証、セッション、負荷分散といった外部モジュールを使用します。
- 新しいノードを作成したときに、QMC 機能を使う代わりに手動で証明書を移動する。

QMC から証明書をエクスポートする目的は、サイトのバックアップや復元ではありません。そのためにリポジトリスナップショット マネージャーか Microsoft Management Console を使用することを推奨します。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページまたは メニューから [**証明書**] を▼選択します。
   [**証明書**] の [**エクスポート**] ページが表示されます。
3. [**コンピュータ名**] ボックスで、証明書を作成しているコンピュータの完全な名前 (*MYMACHINE.mydomain.com*)、または [*IP アドレス*] を選択します。

   IPv6 アドレスをホスト名として使用する方法もサポートされています。

   複数のコンピュータの証明書をエクスポートできます。新しいボックスを追加するには、⊕[**コンピュータ名を追加**] をクリックします。同じコンピュータ名を複数回使うことはできません。ボックスを削除するには、⊗ をクリックします。
4. パスワードの使用はオプションです。パスワードを使用する場合は、エクスポートされたクライアント証明書とサーバー証明書に同じパスワードが適用されます。

   セキュリティ上の理由により、エクスポートするルート証明書には秘密キーが含まれません。

   a. [**証明書のパスワード**] ボックスでパスワードを入力します。
   b. [**パスワードの再入力**] ボックスでパスワードを再入力します。
      パスワードは一致しなくてはなりません。
5. パブリック キーに秘密のキーを追加したい場合は、[**秘密のキーを含める**] を選択します。

   新しいノードの証明書をエクスポートする場合は秘密のキーを含める必要があります。秘密キーは新規ノード上でパスワードなどのエントリーを復号化するために使用します。これらのエントリはデータベースに含まれます。

6. [**Export file format for certificates**] ドロップダウン リストでファイル形式を選択します。
   Windows 形式は .pfx です。
7. アクション バーで [**証明書のエクスポート**] をクリックします。
   証明書のエクスポートが始まり、[**証明書のエクスポート中**] と表示されます。
   エクスポートが完了したら、[**証明書がエクスポートされました**] というダイアログが表示されます。
   [**証明書はこのディスクの場所にエクスポートされます**] と表示され、コンピュータごとに 1 つのフォルダが追加されるターゲット ディレクトリが示されます。各フォルダでは、client.pfx、root.cer、service.pfx の証明書が作成されます。エクスポートに失敗すると、[**証明書のエクスポートを完了できませんでした**] というダイアログが表示されます。

共有コンテンツへのリンクの公開をユーザーに許可するための Qlik Sense の構成

Qlik Sense セキュリティルールを作成し、QlikView が Qlik Sense ハブでリンクを公開できるように Qlik Sense リポジトリを構成する必要があります。

共有コンテンツのセキュリティルールの追加

QMC で新しいセキュリティルールを作成することで、共有コンテンツを有効にします。

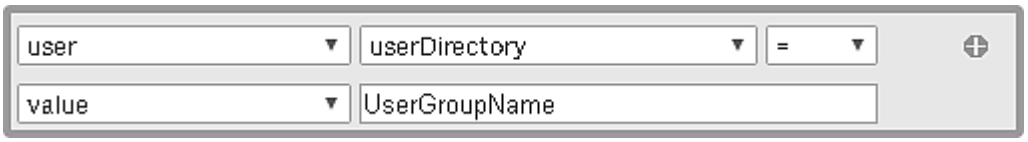
次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC で [**セキュリティルール**] を開きます。
3. ページの下部で [**新規作成**] をクリックします。
4. [**ID**] セクションで、名前とルールの説明を追加します。以下の表の提案を使用できます。

ID の項目と値の提案

項目	値
[**名前**]	*SharedContentCreate-AllUsersFromUserGroupName*
[**説明**]	*UserGroupName ドメインのすべてのユーザーが共有コンテンツの作成を許可されます*

5. [**基本設定**] セクションで、[**リソース フィルタ**] として *SharedContent_** と入力します。
6. [**作成**] アクションを選択し、[**読み取り**] アクションがクリアされていることを確認します。
7. 以下の図の値を使用してルール定義アクションを完了します。*UserGroupName* は、各自の認証ユーザーグループの名前と置き換えます。



8. (オプション) すべての認証ユーザーに対して QlikView コンテンツの共有を許可する場合、[**条件**] ボックスに *!user.IsAnonymous()* と入力します。
9. [**適用**] をクリックします。

認証ユーザーに対するセキュリティルールが QMC に追加されます。

Qlik Sense リポジトリでの共有コンテンツの有効化

Qlik Sense リポジトリで共有コンテンツを有効にするには、構成ファイルを更新する必要があります。デフォルトでは、*Repository.exe.config* ファイルは マシンの *C:\Program Files\Qlik\Sense\Repository* にあります。Qlik Sense構成ファイルを編集し、`SharedContentEnabled` キーの値を `true` に変更します。Windows のサービス アプリケーションを使用して Qlik Sense Repository Service を再起動し、この構成を有効にします。

Qlik Sense 証明書を使用した QlikView Distribution Service の構成

Qlik Sense 証明書を使用して各 QlikView Distribution Service (QDS) を構成し、Qlik Sense ハブに公開される QlikView ドキュメントへのリンクを許可する必要があります。

開始する前に

QDS を構成するには、各 QDS マシンに、client.pfx、root.cer、server.pfx などの新しい証明書セットをコピーする必要があります。構成する各 QDS マシンでは、新しい Qlik Sense 証明書セットが必要となります。

QDS マシンでの Qlik Sense 証明書のインポート

証明書は、ネイティブ Windows の証明書のインポート ウィザードを使用してインポートできます。

root.cer 証明書は、他のすべての証明書よりも前にインポートする必要があります。

root.cer 証明書のインポート

1. 証明書をダブルクリックして開きます。
2. [**証明書のインストール**] をクリックします。
   証明書のインポート ウィザードが開始されます。
3. [**現在のユーザー**] を選択します。
4. [**証明書をすべて次のストアに配置する**] を選択します。
5. [**参照**] をクリックし、[**信頼されたルート証明機関**] フォルダーを選択します。
6. 証明書情報を確認し、[**完了**] をクリックします。
   root.cer 証明書が QDS マシンでインポートされます。

client.pfx 証明書および server.pfx 証明書のインポート

1. 証明書をダブルクリックして開きます。
   証明書のインポート ウィザードが開始されます。
2. [**現在のユーザー**] を選択します。
3. [**秘密キーの保護**] 画面で、証明書のパスワードを入力します。
4. [**証明書の種類に基づいて、自動的に証明書ストアを選択する**] を選択します。
5. 証明書情報を確認し、[**完了**] をクリックします。
   証明書が QDS マシンでインポートされます。

Qlik Sense 証明書およびマシン情報を使用した QDS プロパティの構成

関連する証明書サムネイルと Qlik Sense および QDS のマシン情報を使用して、QDS 構成ファイルを各マシンで更新する必要があります。デフォルトでは、QDS の構成ファイル *QVDistributionService.exe.config* は、*C:\Program Files\QlikView\Distribution Service* にあります。

1. In the `<appSettings>` セクションで、`<add key="QRSMachineName" value="MySenseMachine.domain.com" />` と入力します。`QlikSenseMachineName.domain.com` は、Qlik Sense リポジトリを実行しているマシンの名前で置き換えます。

   マシン名はドメインを含んでおり、Qlik Sense 証明書の作成時に使用した名前と一致する必要があります。

2. 別の行で、<add key="QVWSMachineName" value="QlikViewMachineName" /> と入力します。
   QlikViewMachineName は、QlikView Web Server を実行しているマシンの名前で置き換えます。

   ドメインは必要ありません。

3. (オプション) 別の行で、<add key="AjaxClientPath" value="/MyAjaxURL/opendoc.htm" /> と入力します。MyAjaxURL は、使用している Ajax Client の URL で置き換えます。この構成オプションを追加しない場合、デフォルトの /QvAJAXZfc/opendoc.htm が使用されます。
4. Windows の [Microsoft 管理コンソール] を開きます。
5. [**証明書 - 現在のユーザー**] ドロップダウン矢印をクリックします。
6. [**個人 > 証明書**] フォルダーを開きます。
7. [QlikClient] 証明書をダブルクリックします。
   証明書のプロパティが表示されます。
8. [**詳細**] タブで、拇印の値をコピーします。
9. *QVDistributionService.exe.config* ファイルの別の行で、<add key="SenseClientCertificateThumbprint" value="ThumprintID" /> と入力します。**ThumbprintID** は、証明書のプロパティに表示される拇印の値で置き換えます。
10. 変更内容を保存します。
    QDS が、Qlik Sense ハブの QlikView ドキュメントへのリンクを公開できるように構成されます。

QlikView ドキュメントへのリンクを Qlik Sense ハブで公開するタスクの作成

QMC を使用して、Qlik Sense ハブで QlikView ドキュメントへのリンクを作成できます。

Qlik Sense ハブの QlikView ドキュメントでは、Ajax クライアントを使用した操作のみがサポートされます。

開始する前に

Qlik Sense の QlikView ドキュメントへのリンクを公開するには、Active Directory およびソース ドキュメントとの接続が設定されている QlikView Server が必要です。

QlikView Management Console の設定

Qlik Sense マシンと接続するための QlikView Web Server のアクセス ポイントを構成する必要があります。

次の手順を実行します。

1. [**システム**] タブをクリックします。
2. QlikView Web Server フォルダーで、現在の QlikView Web Server マシンを開きます。
3. [**アクセス ポイント**] タブで、[**サーバー接続**] をクリックします。
4. ドロップダウン メニューを使用して、QlikView Web server の名前を ***local*** からマシン名に変更します。

QlikView ドキュメントへのリンクの公開

QlikView Management Console で次のタスクを実行して、ドキュメントへのリンクを公開します。

1. [**ドキュメント**] タブをクリックします。
   [**ソース ドキュメント**] ページが開きます。

   > *公開できるのは、ソース ドキュメントだけです。*

2. QDS インスタンスを展開して、共有するドキュメントを見つけます。
3. をクリックして、新しいタスクを作成します。
4. [**配布**] タブで、をクリックして受信者を追加します。
5. [**特定のユーザー**] というユーザーのタイプを選択します。
6. をクリックして、ユーザーを追加します。

   > *このユーザーは、QlikView および Qlik Sense で、Active Directory ユーザー グループのメンバーである必要があります。*

7. [**ドキュメント情報**] タブで、をクリックして属性を追加します。
8. [**名前**] 項目に *ShowInSenseHub*、[**Value**] (値) 項目に *true* と入力します。
9. [**適用**] をクリックします。
   タスクが起動し、Qlik Sense ハブに QlikView ドキュメントへのリンクが追加されます。

Qlik Sense ハブでの QlikView ドキュメントの表示

次の手順を実行します。

1. Qlik Sense ドキュメントを共有している特定のユーザーと同じ資格情報を使用して、ハブにログインします。QlikView
2. ハブで、[**QlikView ドキュメント**] をクリックします。
3. ドキュメントへのリンクをクリックして、QlikView AccessPoint を新しいウィンドウで開きます。

> *QlikView ドキュメントは Qlik Sense ハブからは削除できません。*

負荷分散ルールを設定する

マルチノード サイト内では、ノードごとに Qlik Sense Repository Service (QRS) の 1 つのインスタンスが実行されます。セントラル ノードで稼働している QRS は、プライマリとみなされます。プライマリ QRS は、中央リポジトリのデータベースの負荷分散を行います。

Qlik Sense アプリの負荷分散ルールを設定します。

負荷分散ルールを作成する

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**負荷分散ルール**] を選択します。
3. データ マネージャーでテーブルの **新規作成** をクリックします。
   左側に編集パネル (すべてのプロパティを保持)、右側に監査ページが配置された分割ページが表示されます。
4. [**ID**] の、[**テンプレートからルールを作成**] ドロップダウン リストで、ルールを作成するリソースのタイプを選択します。

   *[**基本**] セクションの [**リソース フィルター**] テキスト ボックスの横にある矢印をクリックしてポップオーバーを開き、フィルターに複数のリソースを選択できます。*

   不特定
   [**ノード間でアプリを開くときの負荷分散**]
5. [**Identification (ID)**] で、ルールに名前を付け、説明を入力します。
6. この時、ルールを有効にしたくない場合は、[**無効**] を選択します。
7. [**基本**] ビューで、ルールを作成するアクションのタイプを選択します。
8. ドロップダウン リストでリソース条件を選択します。
   たとえば、リソース条件 [**name**] および設定 [**name**]= *MyApp* を選択すると、*MyApp* という名前のアプリにルールが適用され、設定 [**name**]= *MyApp** により名前が *MyApp* で始まるすべてのアプリにルールが適用されます。

   *複数の条件を使用すると、[**Group**] をクリックして 2 つの条件をグループ化できます。条件のグループ化後、[**Ungroup**] をクリックして、グループ化を解除できます。この他に、サブグループ化オプションには [**Split**] および [**Join**] があります。条件間の既定の演算子は、OR です。これは、演算子のドロップダウン リストで変更できます。AND が OR より上位になるように、条件をグループ化します。*

   *[**Create rule from template**] の選択を変更すると、自動的にすべての [**アクション**] がクリアされ、[**Advanced**] セクションの [**Conditions**] テキスト ボックスが変更されます。*

   リソース

   プロパティの説明

プロパティ名	説明
@<customproperty>	リソースと関連付けられているカスタム プロパティ。
name	関連アプリの名前。
owner.@<customproperty>	アプリに関連付けられた所有者のプロパティ。対応する所有者のプロパティの説明を参照してください。

プロパティ名	説明
owner.environment.browser	アプリに関連付けられた所有者のプロパティ。対応する所有者のプロパティの説明を参照してください。
owner.environment.context	アプリに関連付けられた所有者のプロパティ。対応する所有者のプロパティの説明を参照してください。
owner.environment.device	アプリに関連付けられた所有者のプロパティ。対応する所有者のプロパティの説明を参照してください。
owner.environment.ip	アプリに関連付けられた所有者のプロパティ。対応する所有者のプロパティの説明を参照してください。
owner.environment.os	アプリに関連付けられた所有者のプロパティ。対応する所有者のプロパティの説明を参照してください。
owner.environment.secureRequest	アプリに関連付けられた所有者のプロパティ。対応する所有者のプロパティの説明を参照してください。
owner.name	リソース所有者のユーザー名。
owner.userDirectory	リソース所有者のユーザーディレクトリ。
owner.userId	リソース所有者のユーザーID。
stream.@<customproperty>	アプリに関連付けられた所有者のプロパティ。対応する所有者のプロパティの説明を参照してください。
stream.name	関連のあるストリームの名前。

9. [**プレビュー**] をクリックすると、現在定義されている監査グリッド内のルールのアクセス権が表示されます。
10. [**適用**] をクリックして、ルールを作成し、保存します。
ページ最下部に [**追加完了**] と表示されます。

負荷分散ルールを編集する

更新権限を有する負荷分散ルールは編集できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**負荷分散ルール**] を選択します。
3. 編集したい規則を選択します。
4. アクション バーで [**編集**] をクリックします。
左側に編集パネル (すべてのプロパティを保持)、右側に監査ページが配置された分割ページが表示されます。
5. 規則に該当する項目を編集します。

*複数の条件を使用すると、[**Group**] をクリックして2 つの条件をグループ化できます。条件のグループ化後、[**Ungroup**] をクリックして、グループ化を解除できます。この他に、サブグループ化オプションには [**Split**] および [**Join**] があります。条件間の既定の演算子は、OR です。これは、演算子のドロップダウン リストで変更できます。AND が OR より上位になるように、条件をグループ化します。*

*[**基本**] セクションの [**リソース フィルター**] テキスト ボックスの横にある矢印をクリックしてポップオーバーを開き、フィルターに複数のリソースを選択できます。*

リソース

プロパティの説明

プロパティ名	説明
@<customproperty>	リソースと関連付けられているカスタム プロパティ。
name	関連アプリの名前。
owner.@<customproperty>	アプリに関連付けられた所有者のプロパティ。対応する所有者のプロパティの説明を参照してください。
owner.environment.browser	アプリに関連付けられた所有者のプロパティ。対応する所有者のプロパティの説明を参照してください。
owner.environment.context	アプリに関連付けられた所有者のプロパティ。対応する所有者のプロパティの説明を参照してください。
owner.environment.device	アプリに関連付けられた所有者のプロパティ。対応する所有者のプロパティの説明を参照してください。
owner.environment.ip	アプリに関連付けられた所有者のプロパティ。対応する所有者のプロパティの説明を参照してください。
owner.environment.os	アプリに関連付けられた所有者のプロパティ。対応する所有者のプロパティの説明を参照してください。
owner.environment.secureRequest	アプリに関連付けられた所有者のプロパティ。対応する所有者のプロパティの説明を参照してください。
owner.name	リソース所有者のユーザー名。
owner.userDirectory	リソース所有者のユーザー ディレクトリ。
owner.userId	リソース所有者のユーザー ID。
stream.@<customproperty>	アプリに関連付けられた所有者のプロパティ。対応する所有者のプロパティの説明を参照してください。
stream.name	関連のあるストリームの名前。

6. この時、ルールを有効にしたくない場合は、[**無効**] をクリックします。

7. [**プレビュー**] をクリックすると、現在定義されている監査グリッド内のルールのアクセス権が表示されます。
8. [**適用**] をクリックして、編集したルールを保存します。
   ページの最下部に [**更新完了**] と表示されます。

負荷分散ルールを削除する

削除権限を有する負荷分散ルールは、削除できます。

リソースが削除されると、そのリソースに関連付けられている負荷分散ルールとセキュリティルールはすべて自動的に削除されます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**負荷分散ルール**] を選択します。
3. 削除するルールを選択します。

   フィルタリング オプションを使用して列にフィルターを適用できます。

4. アクション バーの [**Delete**] をクリックします。
   [**Delete**] ダイアログが表示されます。
5. [**OK**] をクリックします。

カスタム プロパティのある負荷分散ルールを作成する

所属先の会社には複数のマルチ ノード Qlik Sense が設置されており、あらゆるノードを対象とした負荷分散ルールを作成する必要があります。個々のノードで負荷分散ルールを設定できます。ただし、マルチノードのシナリオでは、ノードをグループ化すると負荷分散を管理しやすくなります。

以下の例では、機能別にノードをグループ化する方法を示しています。セントラル ノードで、該当する部門のストリームにアプリを公開している各サイト ノードの負荷を分散させる負荷分散ルールを作成すると想定してみましょう。

同じ方法をスケジューラやプロキシ、エンジンにも適用できます。

次の手順を実行します。

1. 「*Departments*」という名前のカスタム プロパティを作成します。
   a. このカスタム プロパティをリソース タイプ [**ノード**] および [**ストリーム**] に適用します。
   b. 「Departments」カスタム プロパティの値: [*Sales*]、[*Development*]、[*Test*] を作成します。
2. カスタム プロパティ「Departments」をノードに追加します。
   a. [**ノード**] 概要で複数選択を使用して適切なノードを選択します。
   b. [**編集**] をクリックします。

c. [**カスタム プロパティ**] セクションで、「Departments」カスタム プロパティを「*Sales*」に設定します。
d. 部門「Development」および「Test」に対して繰り返します。

3. カスタム プロパティ「Departments」をストリームに追加します。
a. [**ストリーム**] 概要で複数選択を使用して適切なストリームを選択します。
b. [**編集**] をクリックします。
c. [**カスタム プロパティ**] セクションで、「Departments」カスタム プロパティを「*Sales*」に設定します。
d. 部門「Development」および「Test」に対して繰り返します。
4. 負荷分散ルールを作成してセントラル ノード上の「Sales」ストリームで「Sales」ノードがアプリの負荷分散をできるようにします。
a. 以下の条件を使用して、リソース「*App_**」の負荷分散ルールを作成します ([**詳細設定**] セクション)。
node.@Department= Sales and resource.stream.@Department = Sales
つまり、この負荷分散ルールは、「Departments」カスタム プロパティが「*Sales*」という値に設定されているストリームのアプリすべてに適用されます。
b. すべての部門に対して繰り返します。

これで部門を使用してノードの負荷分散を管理できるようになりました。

コンテンツのキャッシュ制御の構成

コンテンツのキャッシュ制御を使用すると、ブラウザのキャッシュ動作を変更できます。キャッシュ制御は、リポジトリ サービスによって処理されるエンドポイントで使用されます。この機能はデフォルトで無効になっており、ファイル *Repository.exe.conf* と *capabilities.json* を変更して有効にできます。その後、Qlik Sense Service Dispatcher と Qlik Sense Repository Service を再起動します。

次の手順を実行します。

1. *C:\Program Files\Qlik\Sense\Repository\Repository.exe.conf* を開き、次のキーを true に設定します。
```
<add key="ContentCacheControl" value="true" />
```
2. *C:\Program Files\Qlik\Sense\CapabilityService\capabilities.json* を開き、次のフラグを追加します。
```
{"contentHash":"2ae4a99c9f17ab76e1eeb27bc4211874","originalClassName":"FeatureToggle","
flag":"QMC_CONTENT_CACHE_CONTROL","enabled":true}
```

コンテンツ キャッシュ制御は、Qlik Management Console (QMC) のコンテンツ ライブラリ関連項目セクションで追加または変更されます。*コンテンツ ライブラリ: 関連するアイテム (page 45)* を参照してください。構成が完了すると、コンテンツ キャッシュ制御は特定のコンテンツ ライブラリに自動的に関連付けられ、そのコンテンツをターゲットとするリクエストにのみ影響します。他のリクエストを対象とするコンテンツ キャッシュ制御、いわゆる一般的なコンテンツ キャッシュ制御を作成するには、コンテンツ ライブラリへの参照を削除する必要があります。これを行うには、利用可能な API PUT メソッドを使用して `contentLibrary` 値を `null` に設定します。次の例を参照してください。コンテンツ キャッシュ制御は、POST メソッドを使用して API 要求から直接作成することもできます。

```
PUT /qrs/contentcachecontrol/33774a23-ad86-44f7-96bc-0e346c062cc2
{
  "id": "33774a23-ad86-44f7-96bc-0e346c062cc2",
  "createdDate": "2021-12-09T11:59:20.728Z",
  "modifiedDate": "2021-12-09T11:59:20.728Z",
  "modifiedByUserName": "RDLUND\\svc-silver",
  "name": "api",
  "contentLibrary": null,
```

```
  "filter": "test",
  "maxAge": 3600,
  "cachePolicy": 0,
  "privileges": null,
  "schemaPath": "ContentCacheControl"
}
```

定義されたコンテンツ キャッシュ制御に該当するリクエストは、QMC で見られるユーザー定義の正規表現 (正規表現フィルター)、または ContentCacheControl モデルで見られるフィルター項目の値に基づいてフィルター処理されます。例については *コンテンツ ライブラリ: 関連するアイテム (page 45)* を参照してください。評価される URI の要求の一部は、ホスト名の後のテキストで構成され、仮想プロキシのプレフィックスは含まれません。Qlik Sense Repository Service が一致を探す場合、コンテンツ ライブラリに関連付けられたコンテンツ ライブラリ コントロールが一般的なものよりも優先されます。それらはスタックに実装されます。つまり、最初の一致でそれ以降のルックアップが終了します。複数のコントロールがユーザー定義のフィルターに一致する場合、最新の変更日 (modifiedDate) との一致が優先されます。規定のセキュリティ ルール セットでは、RootAdmin ロールのみがコンテンツ キャッシュ制御への完全な CRUD アクセス権を持っています。さらに、ContentAdmin および SecurityAdmin ロールには、すべてのコンテンツ キャッシュ制御への読み取りアクセス権があります。対応するコンテンツ ライブラリに対する読み取り権限を持つユーザーは、それらのコンテンツ ライブラリに関連付けられたコンテンツ キャッシュ制御への読み取りアクセス権を持ちます。*Qlik Sense に含まれるセキュリティ ルール (page 540)* の ReadContentCacheControl ルールを参照してください。

URI に api を含むハブ固有のリクエストのコンテンツ キャッシュ制御は、Hub サービスの起動時に取得されます。新しく追加または変更されたコンテンツ キャッシュ制御の場合、これらのリクエストを適用することを目的として、Qlik Sense Service Dispatcher を再起動するか、対応する node.js プロセス - *"..\HubService\index.js*を終了することにより、Hub サービスを再起動する必要があります。他のタイプのリクエストの場合、新しいエントリを作成した後、または既存のエントリを変更した後に再起動する必要はありません。

Repository Main API の Open API 仕様に基づく新しいメソッドについては、以下を参照してください。 Contentcachecontrol。

Repository Main API の Open API 仕様に従って対応するモデルについては、以下を参照してください。 ContentCacheControl および ContentCacheControlCondensed。

1.9 アクセス制御の設計

Qlik Sense でアクセス制御を設計する方法を理解する上で欠かせないコンセプトがあります。

このセクションのトピックでは、これらのコンセプトとともに、属性に基づくセキュリティ ルールを構築するためのルール、ルール構文、エディタについて説明します。

- プロパティに基づくアクセス制御
- 設計により提供されているセキュリティ ルール

プロパティ

Qlik Senseでは、属性はプロパティと呼ばれます。プロパティは、アクセスをリクエストしているユーザーや、リクエストの影響を受けるリソース、リクエストが行われている環境を識別するために使われます。Qlik Sense では、すぐに利用できる既定のタイプのプロパティを使用するか、ユーザー ディレクトリ コネクター経由でディレクトリ サービスから提供されるプロパティを使用するか、カスタマイズした独自のプロパティを定義することができます。

カスタム プロパティ (page 519)

既定のプロパティ

Qlik Sense は、対象 (ユーザー)、環境、リソースの説明に使用できる既定のプロパティを提供します。「*条件のうちひとつのプロパティ値ペア: (page 520)*」の例では、ユーザーを識別するためのプロパティとしてユーザー グループ メンバーシップ (AD グループ) が使用されました。また、IP やリクエストの種類といった環境プロパティが、1 つまたは複数の IP アドレスへのアクセスや HTTPS リクエストの種類を制限するために追加されました。

ディレクトリ サービスのプロパティ

QMC のユーザー ディレクトリ コネクターを使用して Qlik Sense をディレクトリ サービスに接続すると、ディレクトリ サービスのユーザー プロパティが利用できるようになります。ルールの作成時にユーザー条件 ドロップダウン リストでプロパティを確認できます。

カスタム プロパティ

カスタム プロパティを使うと、独自のプロパティを定義して、絞込値を割り当てることができます。これにより、既定の環境プロパティに独自のプロパティを補足できます。カスタム プロパティでは、ユーザーのロールやタイプも使用できます。

たとえば、組織内でQlik Senseの開発者、貢献者、消費者を設定できます。これらのユーザー タイプがディレクトリ サービスでグループとして定義されていないと想定してみましょう。カスタム プロパティでは、UserType プロパティを定義するオプションがあります。これで、開発者、貢献者、消費者という値をユーザーに割り当て、個人やユーザー グループ メンバーシップではなくユーザーのタイプに基づいてルールを適用できます。

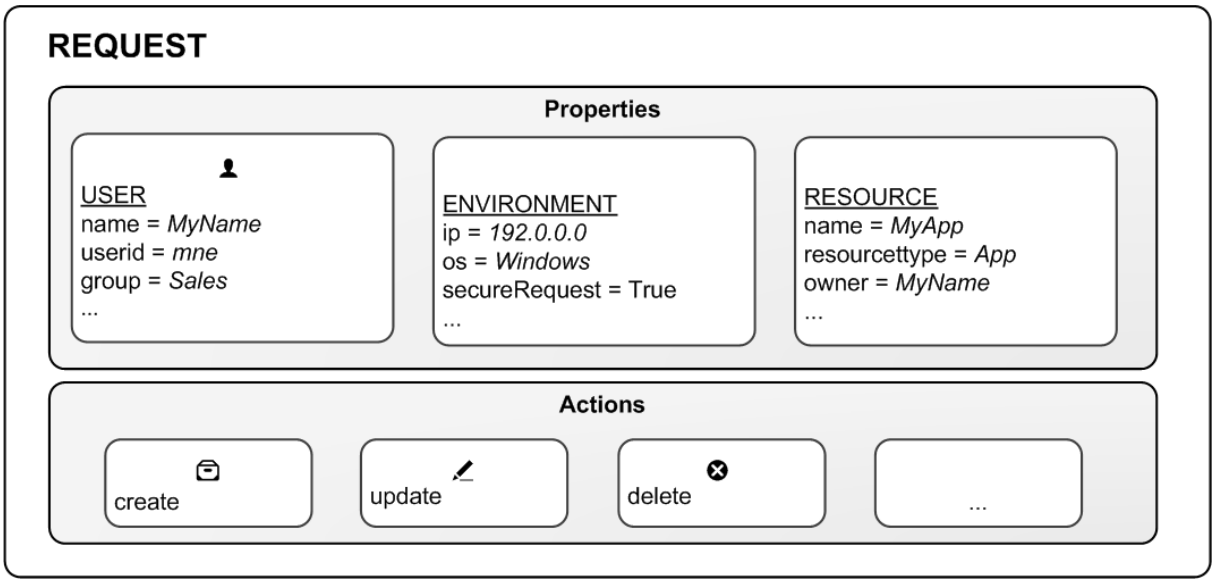
ルールの作成時にユーザー条件 ドロップダウン リストでカスタム プロパティを確認できます。リストでは、カスタム プロパティに「@」というサフィックスが付いています。

プロパティベースのアクセス制御

アクセス制御はプロパティベースで、プロパティはアクセス リクエストの関係者について説明するために使われます。この場合、関係者は以下の通りです。

- リクエストを行っている*ユーザー*
- リクエストが行われる*環境*
- リクエストが適用される*リソース*

各プロパティは、"group = Sales" や "resourcetype = App" などのいわゆるプロパティ値ペアの値によって定義されます。また、各リクエストには、要請者がリソースでの実行を求めているアクション (作成、更新、削除など) とともに、リクエストに関与しているユーザー、環境、リソースのプロパティ値ペアが含まれます。



アクセスのリクエスト

ルールを使用したアクセスの評価

プロパティ値ペアに基づいてルールを作成することができます。これは、要請者のプロパティ値がリソースのセキュリティルールで定義されたプロパティ値の条件に一致する場合にのみ、当該リソースでのアクションのリクエストが受け入れられることを意味します。

通常、ルールは文章として読み取ることができます:

"[条件] の場合、要請者に [リソース] の [アクション] を許可する"

各ルールでは、アクションと、アクションを適用するリソースについて説明する必要があります。リソースのルールを定義しなければ、どのユーザーもそのリソースにアクセスできません。

> *条件を定義する必要はありませんが、条件を定義しなければ、すべてのユーザーとリソースにルールが適用されます。*

リクエストを受け取ると、ルール エンジンは該当するすべてのルールに照らし合わせてリクエストを評価します。該当するルールとは、リクエストと同じタイプのリソースに適用されるルールを指します。各ルールにはリソース フィルタが付随しているため、ルール エンジンはすべてのリソースに対してリクエストを評価する必要がありません。最後に、条件にリソースのプロパティ条件を与えることにより、ルールがどのリソースに適用されるのか正確に指定することができます。

ルール評価のワークフロー

条件のうちひとつのプロパティ値ペア:

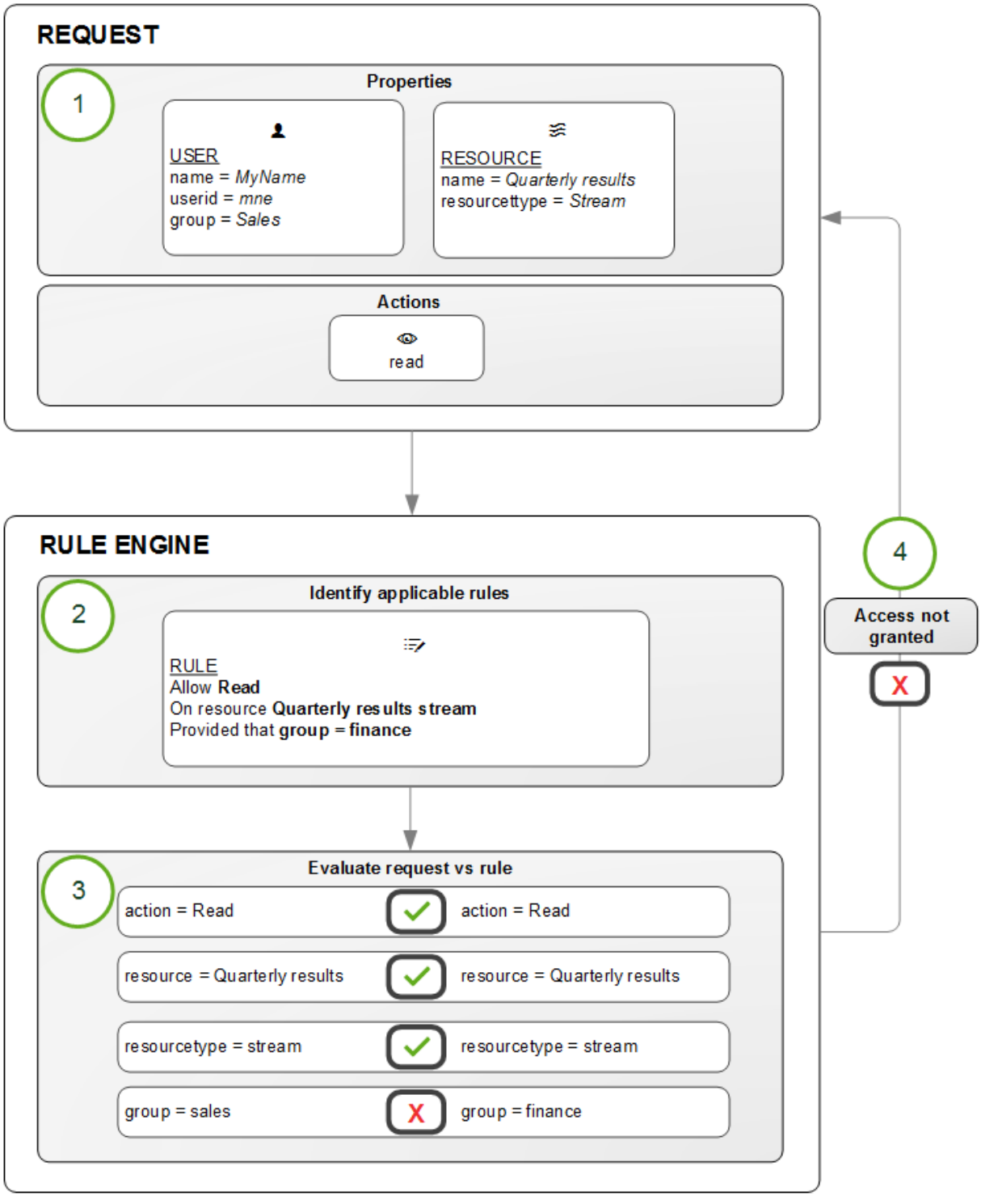
たとえば、あなたが会社の営業部に勤務しており、財務部が発表した四半期業績ストリームを読みたいとします。たとえば、あなたが会社の営業部に勤務しており、財務部が発表した四半期業績ストリームを読みたいとします。 この場合は、「財務」アクティブ ディレクトリグループに属するユーザーのみがストリームを読み取れるという

ルールがこのストリームにはあります。

これをルールに置き換えると、以下のようになります:

「[グループ=財務] の場合、ユーザーに [四半期決算のストリーム] を [読み取る] ことを許可」

この例では、ルールの評価で「False」という結果が出ます。つまり、あなたのグループは「財務」でないため、読み取りアクセス権がありません。実際には、ストリームのアイコンさえ表示されません。



ルールの評価

ルール評価のワークフローは次のとおりです。

1. ユーザーによって送信された [Quarterly results stream (四半期業績ストリーム)] の [read (読み取り)] リクエスト
2. ルール エンジンが、リクエストを評価するルールがどれであるか特定します
3. ルール エンジンによってリクエストが評価されます
4. 基準を満たしていない場合、アクセス権は与えられません

条件の複数のプロパティ値ペア:

ルール評価のワークフローの例は基本的なもので、1 つの条件を持つ 1 つのリソースに 1 つのアクションがあります。しかし、Qlik Sense セキュリティルールの長所は、1 つのルールで条件の異なる複数のリソースに対して複数のアクションを適用できるという点です。四半期業績の例を見ると、入力にアクティブ ディレクトリグループを使用して、財務部と管理部の双方への読み取りおよび更新アクセス権を提供するようルールを拡張できます。

「グループ=財務 またはグループ=管理の場合、ユーザーに [四半期決算のストリーム] の読み出しおよび更新を許可」

Qlik Sense で事前に定義されたセキュリティルール

Qlik Sense には、[**ReadOnly**] および [**Default**] ルールと呼ばれる予め定義されたルールが含まれています。これらのルールは、QMC 管理者が Qlik Sense システムを管理し、セキュリティルールを作成、更新、管理できるようにするために提供されています。ReadOnly ルールはセキュリティにとって重要で、編集できません。既定のルールは、会社とシステムの要件に合わせて編集できます。

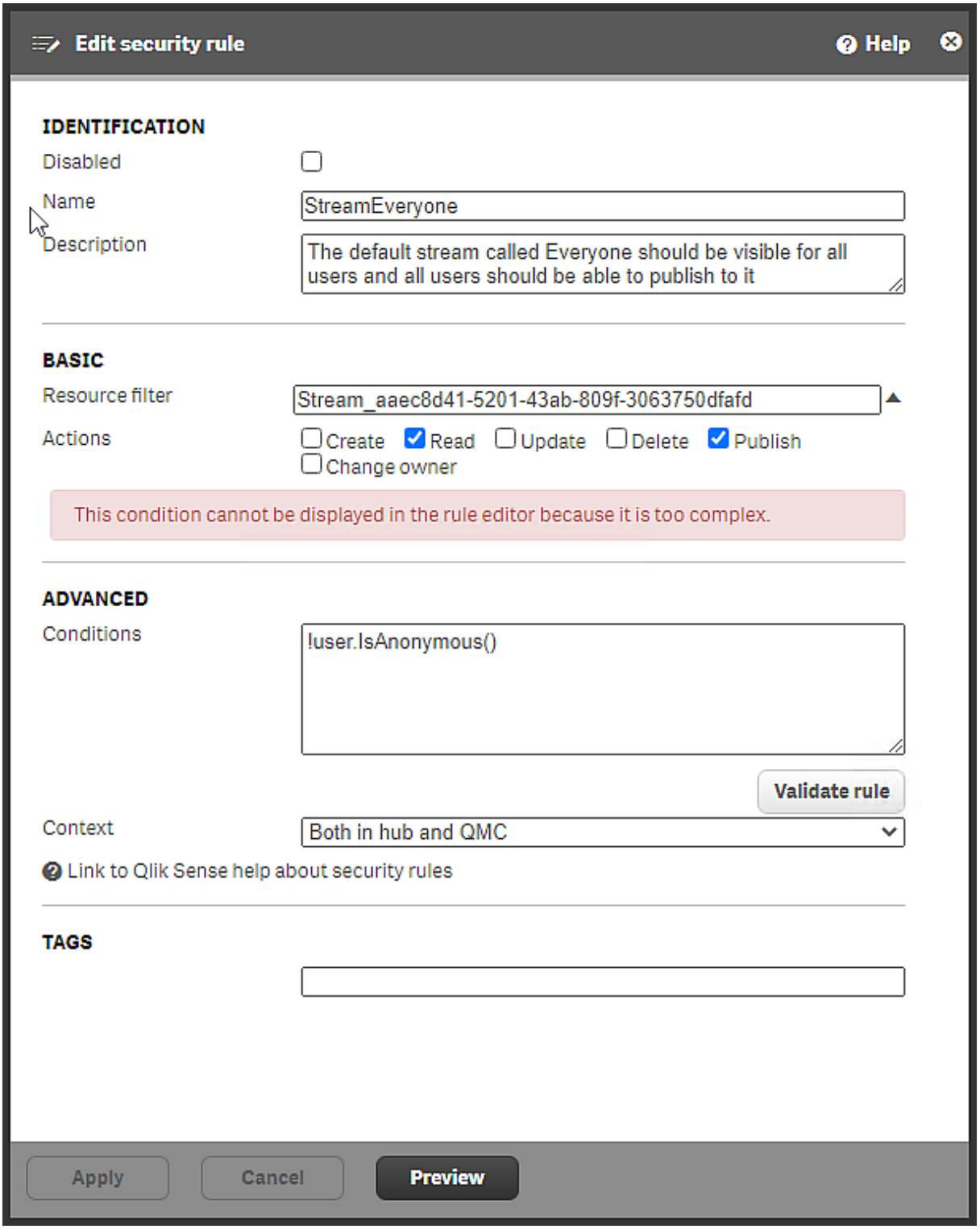
> *Qlik Sense が提供する既定のルールを編集する場合、ルールのタイプの定義は [**既定**] から [**カスタム**] に変更されます。既定のルールを変更したり、既定のルールに影響が及ぶ新しいルールを追加したりすると、Qlik Sense において予期せぬ動作を引き起こす場合があります。既定のルールに変更を加える前に、ルールのプレビュー機能を使用して、ルールの動作を確認してください。Qlik Sense を新しいバージョンにアップグレードする場合は、読み取り専用ルールおよび既定のルールのみが自動で更新されることに、注意してください。*

セキュリティルールのしくみ

Qlik Sense Enterprise on Windows では、セキュリティル ールを使用して、アプリやストリームなどのリソースへのアクセスをユーザーに許可できます。すべてのセキュリティルールは本質的に包括的です。つまり、常にユーザーにリソースへのアクセスを許可し、ユーザーのアクセスを拒否するルールを作成することはありません。セキュリティルールの目的は、通常、一部のユーザーのみにリソースへのアクセスを許可することです。適切なユーザーだけがリソースにアクセスできるようにすることは、セキュリティルール管理者 (SecurityAdmin) のタスクです。

2 つの簡単なセキュリティルール

簡単なスタートとして、Qlik Sense Enterprise on Windows、*StreamEveryone*、*StreamEveryoneAnonymous* のインストールに含まれている 2 つのセキュリティルールを見てみましょう。



Qlik Sense Enterprise on Windows とともにインストールされるセキュリティルール StreamEveryone

[**ID**] セクションでは、ルールが無効になっていないため、ルールがアクティブであることがわかります。ルールの目的は、[**説明**] ボックスに記載されています。

[**基本**] セクションでは、リソース フィルターが特定のストリームを特定します。フィルターの最初の部分はリソース タイプ *Stream* を識別し、2 番目の部分はグローバル一意識別子 (GUID) です。リソース フィルターはルールの範囲を示します。ここで、ルールがカバーするエンティティのタイプを定義します。リソース フィルターを使用すると、例えば、ユーザーが表示できるアプリを定義するルールと比較して、ユーザーが表示できるデータ接続に影響を与えるさまざまなルールのセットを設定できます。

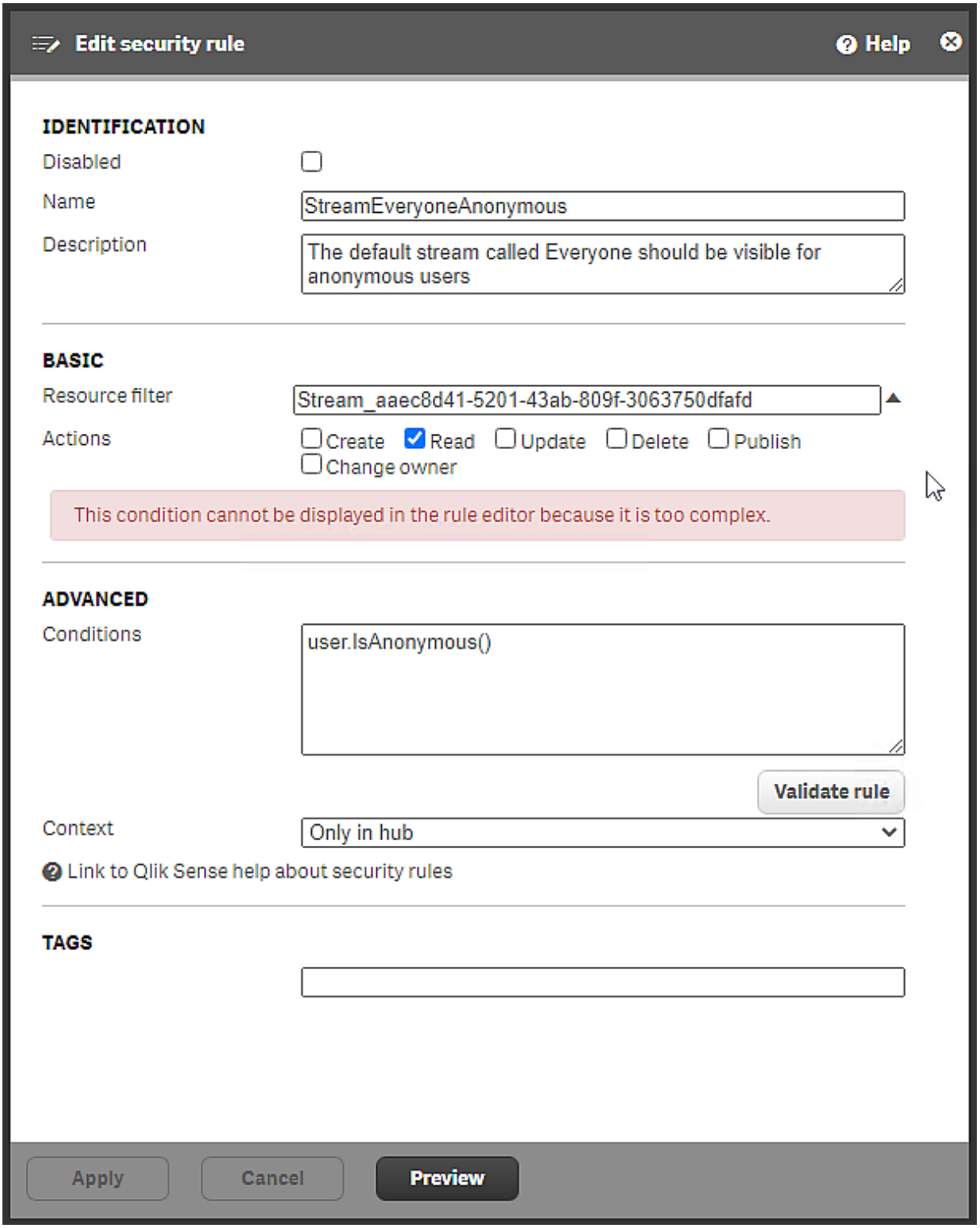
参照先: *リソース フィルターの定義 (page 572)*

ユーザーが実行できるアクションは *Read* と *Publish* です。すべてのユーザーは、アプリやアプリオブジェクトなど、ストリーム内のコンテンツにアクセスできます。ユーザーは、アプリとアプリオブジェクトをストリームに公開することもできます。

[**詳細**] セクションでは、条件は [`!userIsAnonymous()`] です。このルールは匿名ユーザーを除外するため、[**説明**] の記述はすべてのユーザーに当てはまるわけではありません。[`IsAnonymous()`] 関数の詳細については、*IsAnonymous アクセスを要求しているユーザーが匿名でログインしている場合に「True」を返すユーザー条件のブール型機能。その他の場合は「False」を返します。user.IsAnonymous() 例と結果例と結果例結果 リソース フィルター: Stream_*条件: user.IsAnonymous() アクション: read匿名ユーザーはストリームの読み取りを許可されます。リソース フィルター: Stream_*条件: !user.IsAnonymous() アクション: read, publish匿名でないユーザー(条件の前に NOT 演算子「!」が付いたもの) は全員、ストリームを読み取って公開することができます。匿名でないユーザー(条件の前に NOT 演算子「!」が付いたもの) は全員、ストリームを読み取って公開することができます。匿名ユーザーはストリームにアクセスできません。(page 1)* を参照してください。

コンテキスト: このルールは、ハブと QMC から *Everyone* ストリームにアクセスするユーザーの両方に適用されます。

匿名ユーザーはルール *StreamEveryone* を介してストリーム *Everyone* にアクセスできないため、別のルールが必要です。



Qlik Sense Enterprise on Windows とともにインストールされるセキュリティルール StreamEveryoneAnonymous

ルールは *StreamEveryoneAnonymous* で、3 つの例外を除いて *StreamEveryone* ルールに似ています。

- 実行できる唯一のアクションは *Read* であり、*Publish* は不可能です。
- 条件は [`userIsAnonymous()`] です。これは、ルールが匿名ユーザーにのみ適用されることを意味します。
- コンテキストは [*ハブでのみ*] です。匿名ユーザーは QMC にアクセスできません。

Everyone ストリームに 2 つのルールが必要なのは、アクションとコンテキストの違いによるものです。それらの違いがなかったら、*StreamEveryone* で十分だったでしょう。

カスタム プロパティを使用したストリームとセキュリティルールの作成

Qlik Sense Enterprise on Windows でインストールされているルールが多数ある場合でも、組織の特定のニーズを満たす新しいセキュリティルールを作成する必要があります。セキュリティルールを作成するときは、カスタム プロパティまたはユーザー ロールを使用して管理を容易にすることができます。ここでは、カスタム プロパティを紹介します。ユーザー ロールについては、*セキュリティルールのユーザー ロールの定義 (page 533)* を参照してください。

カスタム プロパティを使用すると、セキュリティルールを変更せずに、ユーザー アクセスを簡単に追加または削除できます。この例では、カスタム プロパティはまだ定義されていません。

カスタム プロパティの定義

[*財務*] と [*営業*] の 2 つのユーザー グループが、四半期レポート アプリが公開される [*四半期報告書*] と呼ばれるストリームにアクセスする必要があると想定します。これらのグループはまだユーザー ディレクトリで定義されていないため、定義する必要があります。これを行うには、[*財務*] と [*営業*] の値を使用してカスタム プロパティを作成します。

カスタム プロパティの新規作成

値が [*財務*] と [*営業*] の [*部門*] というカスタム プロパティを作成します。

1. QMC スタート ページで、[**カスタム プロパティ**] を選択します。
2. [**新規作成**] をクリックします。
   カスタム プロパティ編集ページが開きます。
3. 名前 [*部門*] を入力します。
4. [**リソース タイプ**] で、[**ストリーム**] および [**ユーザー**] を選択します。
   これらは、セキュリティルールに必要なリソースです。
5. [**値**] で [**新規作成**] をクリックします。
6. 値 [*財務*] を追加し、[**新規作成**] をクリックします。
7. 値 [*営業*] を追加します。
8. [**適用**] をクリックします。

[*部門*] という新しいカスタム プロパティが、[*財務*] と [*営業*] の 2 つの値で作成され、それぞれのグループのユーザーに割り当てます。

カスタム プロパティ値をユーザーに割り当て

1. QMC で、[**ユーザー**] を開きます。
2. 列セレクター ( ) を開き、[*@Department*] を選択します。これは、リストの最後の項目である可能性があります。
3. [*財務*] グループに追加するユーザーを選択します。複数選択が可能です。
4. [**編集**] を選択します。

5. [**プロパティ**] セクションで、[**カスタム プロパティ**] が選択されていることを確認します。
   [**カスタム プロパティ**] セクションが表示され、[*部門*] はオプションです。
6. [*部門*] のボックスをクリックし、値 [*財務*] を選択します。
7. [財務] のすべてのユーザーの値が [*財務*] になるまで、このステップを繰り返します。
8. [**適用**] をクリックします。
9. [*営業*] グループのメンバーに対して対応するアクションを実行します。

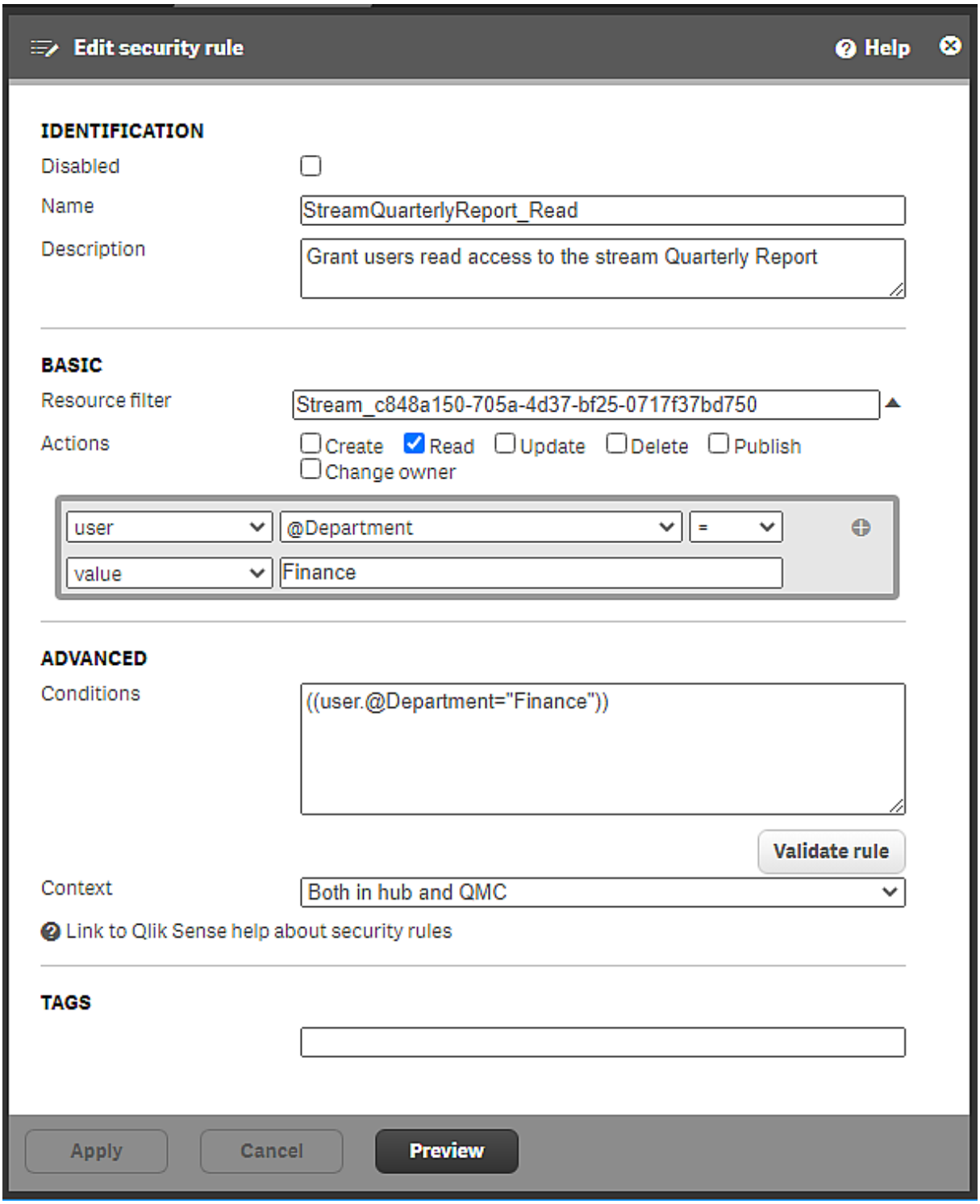
これで、[*財務*] と[*営業*] の 2 つのカスタム プロパティグループができました。これらは、いくつかの異なるセキュリティルールで使用できます。ユーザーは簡単に追加または削除できます。カスタム プロパティの値として部門を追加することもできます。

グループが会社のさまざまな部門の人々で構成されているためにグループを簡単に定義できない場合は、その目的を明確に示す名前でカスタム プロパティを定義できます。現在の例では、StreamQuarterlyReport_Read が可能な名前です。そのカスタム プロパティに必要な唯一の値は Read です。

ストリームとセキュリティルールの作成

これでカスタム プロパティ値が得られ、ストリームの [*四半期報告書*] と、ユーザー グループにストリームへのアクセスを許可するセキュリティルールを作成できます。

1. QMC スタート ページから [**ストリーム**] に移動し、[**新規作成**] をクリックします。
2. ストリームに [*四半期報告書*] という名前を付けます。
3. [**適用**] をクリックします。
   セキュリティルール エディタが表示されます。セキュリティルールの作成をキャンセルする場合、ストリームにはセキュリティルールがなく、すべてのユーザーがそのストリームにアクセスできます。それはおそらくあなたが望むものではありません。
4. セキュリティルールに [*StreamQuarterlyReport_Read*] という名前を付けます。(セクション [**ID**] を選択する必要があります)
5. 必要に応じて、説明を追加します。
6. [**リソース フィルター**] は、一意のストリーム ID で既に存在しています。
7. [**アクション**] の場合は、[**読み取り**] を保持したまま、[**公開**] の選択をクリアします。
8. ルール エディタで、画像に示すように、*user*、*@Department*、=、*value*、*Finance* を選択します。

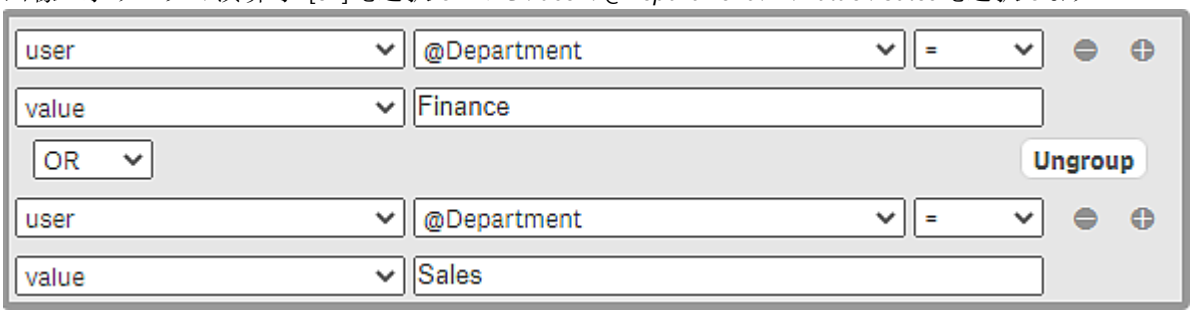


セキュリティルール [StreamQuarterlyReport_Read]

9. [**ルールの検証**] をクリックして、ルール構文が正しいことを確認します。ルールのロジックはテストされていません。
10. [**適用**] をクリックして、ルールを保存します。

[*営業*] グループに何が起こったのか疑問に思われるかもしれません。そのユーザー グループを追加するには、さまざまな方法があります。[**条件**] ボックスで直接変更を加えることができますが、最も安全な方法はルール エディタを使用することです。

1. [**関連するアイテム**] で、[**セキュリティ ルール**] を選択します。
2. [*StreamQuarterlyReport_Read*] をダブル クリックします。
3. [**基本**] セクションで、ルール エディタの [**+**] をクリックします。
4. 画像に示すように、演算子 [OR] を選択してから、*user*、*@Department*、=、*value*、*Sales* を選択します。



条件が更新されたルール エディタ

[**条件**] ボックスの文字列は、ルール エディタでの変更を反映するように更新され、次のようになります: `((user.@Department="Finance" or user.@Department="Sales"))`。代わりに、[**条件**] ボックスで直接変更を加えた場合は、それに応じてルール エディタが更新されます。

5. [**適用**] をクリックします。

[*営業*] グループの別のオプションは、[*営業*] グループに関連する可能性のあるアクション [*読み取り*]、[*公開*]、[*更新*] を使用して個別のセキュリティ ルールを作成することです。

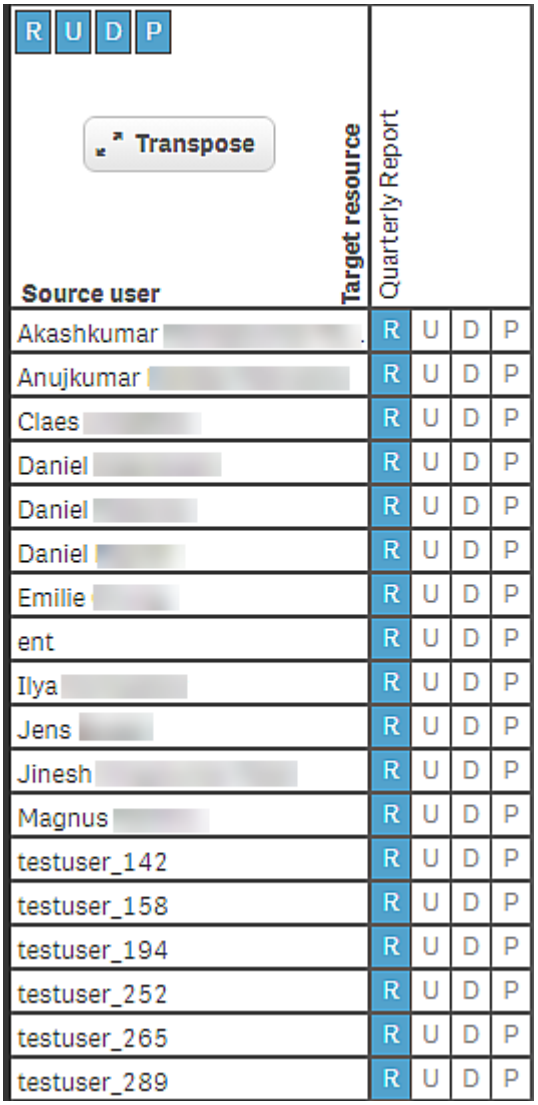
セキュリティ ルール エディタの詳細については、セキュリティ ルール エディタ(page 566) を参照してください。

新しいルールの監査

新しいセキュリティ ルールが適切なユーザーに適切な種類のアクセスを許可していることを確認することが重要です。

1. 引き続き [*ストリーム: 関連するアイテム*] ページで、[**ルールの監査**] をクリックして、新しく作成したルールを編集および監査するためのページを開きます。
2. ストリームの監査が設定されているので、[**監査**] をクリックするだけです。

新しいセキュリティ ルールがユーザー ディレクトリに対してテストされるようになり、[*営業*] および [*財務*] のユーザーのリストに、ストリームへの読み取り権限があることを示す [**R**] が表示されるはずです。



R U D P Transpose Source user	Target resource: Quarterly Report			
Akashkumar	R	U	D	P
Anujkumar	R	U	D	P
Claes	R	U	D	P
Daniel	R	U	D	P
Daniel	R	U	D	P
Daniel	R	U	D	P
Emilie	R	U	D	P
ent	R	U	D	P
Ilya	R	U	D	P
Jens	R	U	D	P
Jinesh	R	U	D	P
Magnus	R	U	D	P
testuser_142	R	U	D	P
testuser_158	R	U	D	P
testuser_194	R	U	D	P
testuser_252	R	U	D	P
testuser_265	R	U	D	P
testuser_289	R	U	D	P

ストリーム四半期報告書への読み取りアクセス権を持つ[財務] および[営業] のユーザーの監査結果

既存のグループのカスタム プロパティを使用したストリームとセキュリティ ルールの作成

多くの場合、会社には Active Directory などのユーザー ディレクトリがあり、カスタム プロパティで使用して、すべてのユーザーにストリームへのアクセスを許可できます。

カスタム プロパティの新規作成

[*ADGroupStream_Read*] というカスタム プロパティを作成します。

1. QMC スタート ページで、[**カスタム プロパティ**] を選択します。
2. [**新規作成**] をクリックします。
   カスタム プロパティ編集ページが開きます。
3. [*ADGroupStream_Read*] という名前を入力します。
4. [**リソース タイプ**] で、[**ストリーム**] および [**ユーザー**] を選択します。
   これらは、セキュリティ ルールに必要なリソースです。
5. [**適用**] をクリックします。

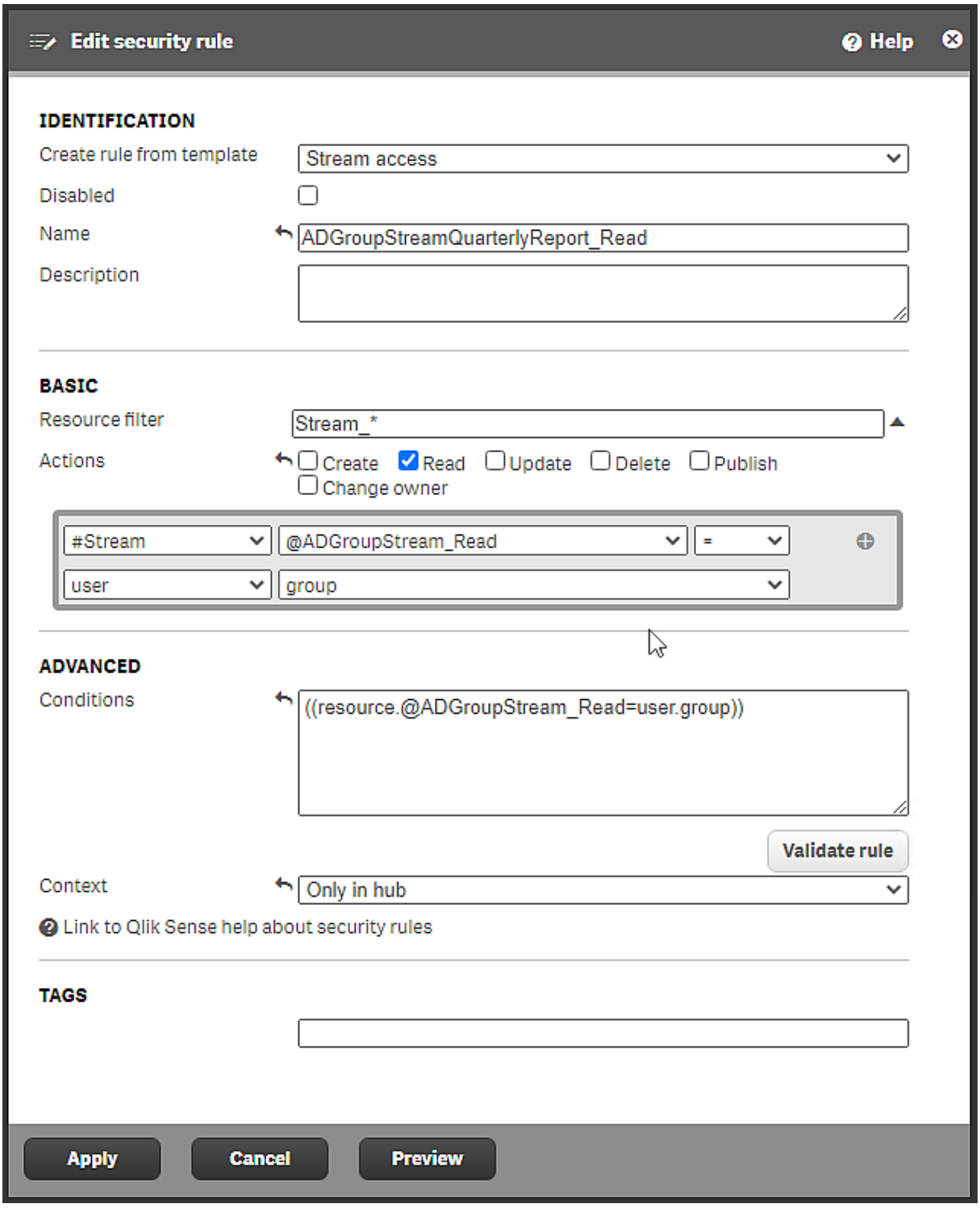
この場合、特定のカスタム プロパティ値は必要ありません。すべてのユーザーは同じユーザー ディレクトリに属しているため、セキュリティ ルールでカスタム プロパティ名を使用できます。そのディレクトリのメンバーになると、ストリームへのアクセスが許可されます。

ディレクトリ サービスのプロパティの詳細については、*プロパティ(page 518)* を参照してください。

セキュリティ ルールの作成

これでカスタム プロパティが作成され、ユーザーにストリーム [*四半期報告書*] へのアクセスを許可するセキュリティ ルールを作成できます。

1. QMC スタート ページから [**セキュリティ ルール**] に移動し、[**新規作成**] をクリックします。
2. セキュリティ ルールに「*ADGroupStreamQuarterlyReport_Read*」という名前を付けます。
3. [**リソース フィルター**] に *Stream_** と入力します。
4. [**アクション**] で、[**読み取り**] を選択します。
5. ルール エディタで、画像に示すように、*#Stream*、*@ADGroupStream_Read*、=、*user*、*group* を選択します。



セキュリティルール ADGroupStreamQuarterlyReport_Read

6. [**コンテキスト**] で、[*Only in hub*] を選択します。
   このルールは、ハブからストリームにアクセスするユーザーにのみ適用されます。
7. [**適用**] をクリックして、ルールを保存します。

新しいセキュリティルールが作成され、Active Directory グループのすべてのユーザーがストリーム [*四半期報告書*] への読み取りアクセス権を持ちます。

セキュリティルールのユーザー ロールの定義

ユーザー ロールは、カスタム プロパティを使用せずにルール管理を容易にする方法です。ロールを定義し、それらをユーザーに割り当てます。ロールをいくつかのセキュリティルールで使用して、その役割を持つすべてのユーザーにアクセスを許可できます。

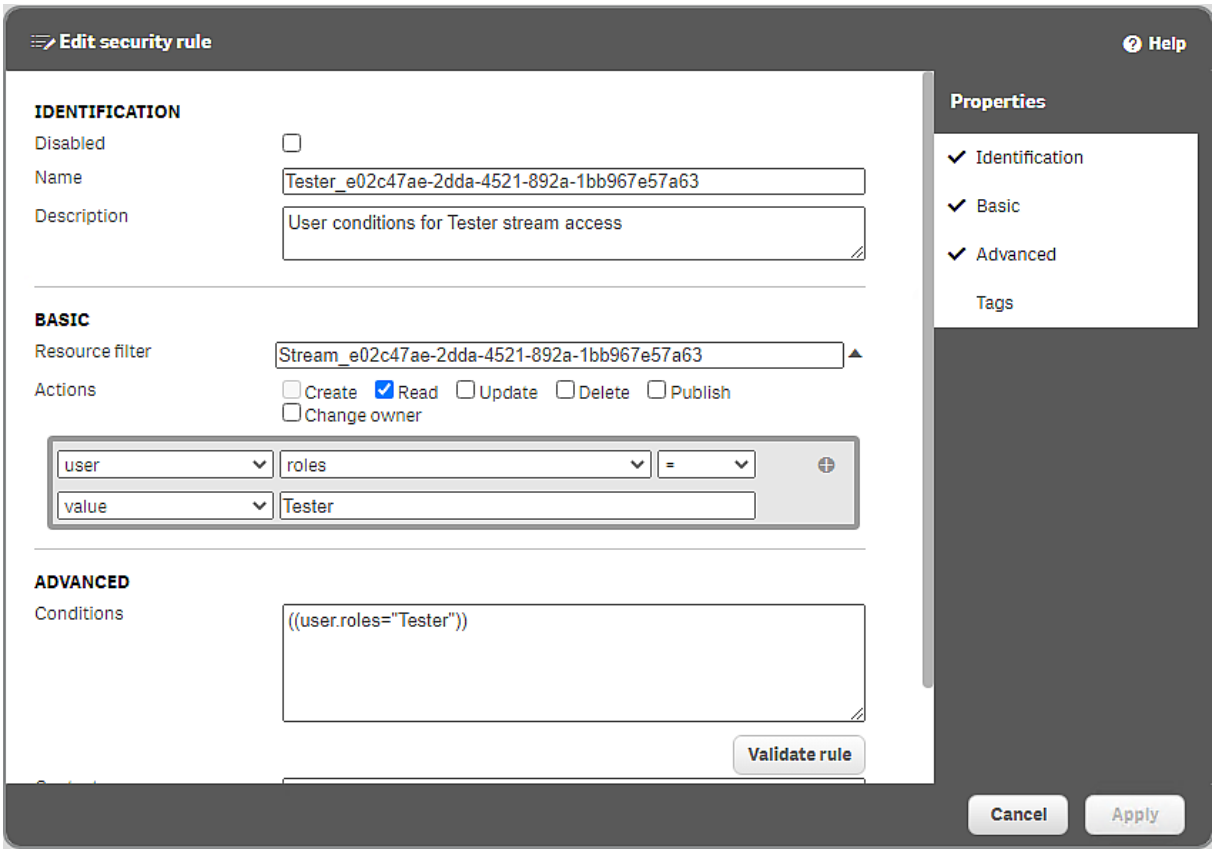
ユーザー ロールを使用したストリームおよびセキュリティルールの作成

開発者用とテスター用の 2 つのユーザー ロールが必要であると仮定します。これらの役割には異なるアクセス ニーズがあるため、2 つのセキュリティルールが必要です。

テスターと開発者向けのセキュリティルールの定義

また、テスターがストリームへの読み取りアクセス権を持っていれば十分であると想定します。

1. QMC スタート ページから [**ストリーム**] に移動し、[**新規作成**] をクリックします。
2. ストリーム に [*TestStream1*] という名前を付けます。
3. [**適用**] をクリックします。
   [**セキュリティルールの編集**] ページが表示されます。セキュリティルールの作成をキャンセルする場合、ストリームにはセキュリティルールがなく、すべてのユーザーがそのストリームにアクセスできます。それはおそらくあなたが望むものではありません。

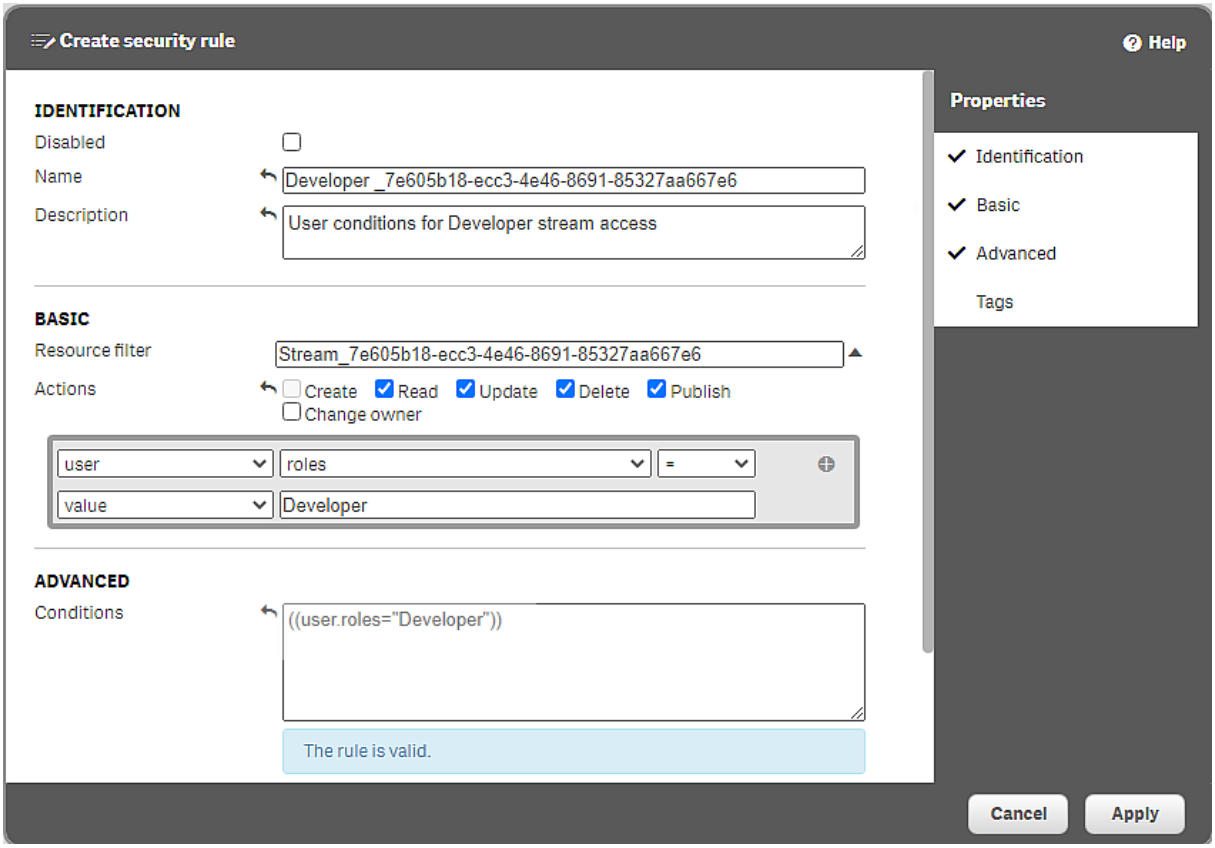


[TestStream1] へのテスター アクセスのセキュリティルール

4. [**プロパティ**] で、[**ID**] を選択します。
5. [**名前**] に、*Tester_<ストリームの GUID>* ([**リソース フィルター**] からの GUID) と入力します。
6. [**アクション**] の場合は、[**読み取り**] を保持したまま、[**公開**] の選択をクリアします。
7. ルール エディタで、画像に示すように、*user*、*roles*、=、*value* を選択し、*Tester* を手動で入力します。[**リソース フィルター**]、[**条件**]、[**アクション**] 項目で定義されているアクセス権は、ユーザー ロール [*テスター*] に適用されます。この役割は、ユーザーに適用できるようになります。
8. [**ルールの検証**] をクリックして、ルール構文が正しいことを確認します。ルールのロジックはテストされていません。
9. [**適用**] をクリックして、ルールを保存します。
10. [**関連するアイテム**] で、[**セキュリティ ルール**] をクリックします。

> *ここには、この特定のストリームに関連付けられているすべてのセキュリティ ルールがあります。*

11. [**関連付けルールの作成**] をクリックして、同じストリームに対して別のルールを作成します。今回は開発者向けです。
12. [**名前**] に、*Developer_<ストリームの GUID>* ([**リソース フィルター**] からの GUID) と入力します。
13. [**アクション**] では、[**読み取り**]、[**更新**]、[**削除**]、[**公開**] をすべて選択する必要があります。
14. ルール エディタで、画像に示すように、*user*、*roles*、=、*value* を選択し、*Developer* を手動で入力します。この役割は、ユーザーに適用できるようになります。



[TestStream1] への開発者アクセスのセキュリティ ルール

15. [**ルールの検証**] をクリックして、ルール構文が正しいことを確認します。ルールのロジックはテストされていません。
16. [**適用**] をクリックして、ルールを保存します。

これで、いくつかの異なるセキュリティルールで使用できる 2 つのユーザー ロール、[*テスター*] と [*開発者*] ができました。ユーザーは簡単に追加または削除できます。同じ方法で、追加のユーザー ロールを作成できます。

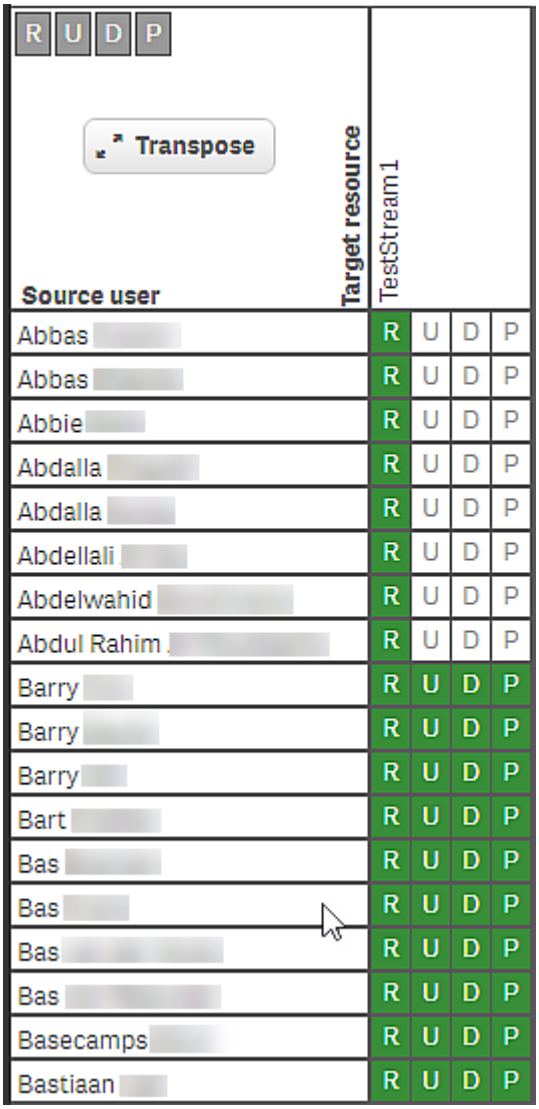
ユーザーへの役割の割り当て

1. QMC で、[**ユーザー**] を開きます。
2. [*テスター*] の役割を希望するユーザーを選択します。複数選択が可能です。
3. [**編集**] をクリックします。
4. [**ロールの追加**] をクリックして、リストから [*テスター*] を選択します。
5. [**適用**] をクリックします。
6. [**ユーザー**] をクリックして、ユーザーの概要を開きます。
   [**管理者 ロール**] 列で、ユーザーの役割が [*テスター*] であることを確認します。
7. [*開発者*] の役割を持つ必要があるユーザーに対して、対応するアクションを実行します。

新しいルールの監査

新しいセキュリティルールが適切なユーザーに適切な種類のアクセスを許可していることを確認することが重要です。

1. [**ストリーム**] に移動し、[*TestStream1*] をダブルクリックします。
   [**ストリームの編集**] ページが表示されます。
2. [**関連するアイテム**] で、[**セキュリティ ルール**] をクリックします。
   このストリームに関連付けられているセキュリティルールが表示されます。
3. [*Tester_<GUID>*] を選択し、[**ルールの監査**] をクリックします。
   ([*Developer_<GUID>*] を選択することもできます。これは、対象となるのと同じストリームです)
4. [**監査**] をクリックします。
   このストリームのセキュリティルールはユーザー ディレクトリに対してテストされるようになり、テスターが読み取りアクセスを示す [**R**] のみを持つユーザーと、[**RUDP**] ([**読み取り**]、[**更新**]、[**削除**]、[**公開**]) を持つ開発者のリストが作成されるはずです。



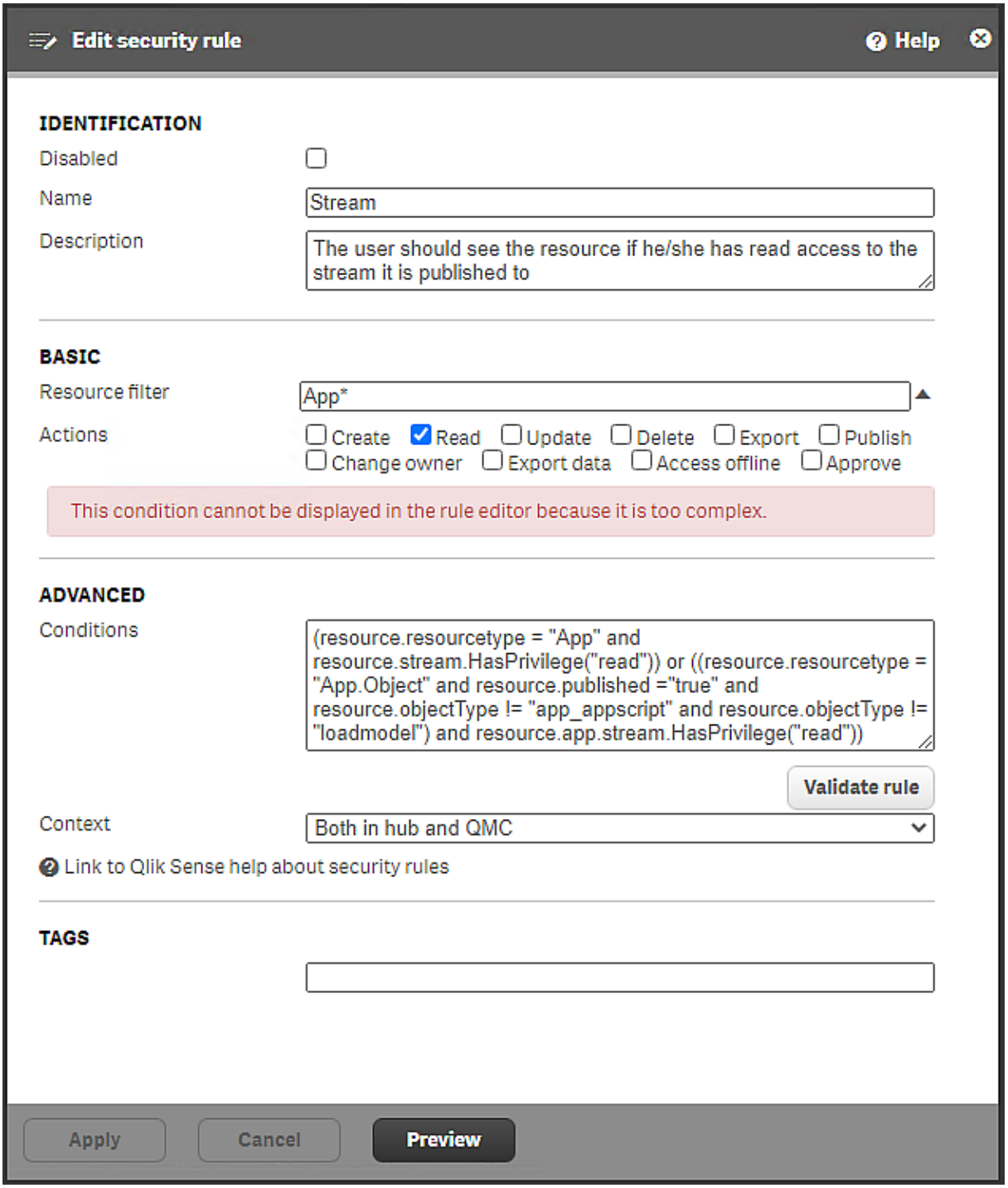
[テスター] または [開発者] の役割を持つユーザーの監査結果

ルール階層

セキュリティルールを設計するときは、さまざまなリソースフィルター間の階層関係を理解することが重要です。このような関係を認識していないと、ルールが意図したとおりに機能しなくなる可能性があります。多くの場合、アイテムへのアクセスには複数のセキュリティルールが含まれます。アプリを使用できるようにするには、そのアプリへの読み取りアクセス権を持っているだけでは不十分です。アプリが公開されているストリームへのアクセス権も必要です。アプリ内のアプリオブジェクトも編集する場合は、そのアプリオブジェクトに更新権限を付与する追加のルールが必要になります。

ルール階層。アプリオブジェクトへのアクセスにはアプリアクセスが必要であり、アプリアクセスにはストリーム アクセスが必要です。

これまでに達成したことを検討し、ユーザーにストリームへのアクセスを許可すると、ユーザーがアプリを開いてアプリオブジェクトを表示する前に、より多くのセキュリティルールが必要になるようです。しかし、それは必要ではなく、その理由はそのようなルールが既に存在しているからです。前述のように、Qlik Sense Enterprise on Windows にはいくつかのセキュリティルールがインストールされています。これらのルールの一部は、システムが機能するために不可欠であるため、編集または削除できません。他のルールは便宜上存在しますが、この場合、セキュリティルール *Stream* が存在すると便利です。これはルールがどのように見えるかです。



Qlik Sense Enterprise on Windows インストールに含まれるセキュリティルール Stream

ルールの説明には、「*ユーザーは、公開先のストリームへの読み取りアクセス権がある場合、リソースを表示する必要があります*」と記載されています。ストリームへの読み取りアクセス権がある場合は、このルールを通じて、そのストリームに追加されたコンテンツも表示できます。このルールが存在するため、ユーザーにアプリやアプリオブジェクトへの読み取りアクセスを許可するルールを作成する必要はありません。すべて処理されています。

[**リソース フィルター**] の値は [App*] であることに注意してください。[App*] 値は、アプリとアプリオブジェクトの両方をカバーします。テンプレートからルールを作成するときのアプリアクセスの既定値は [App_*] であり、アプリオブジェクトではなくアプリのみが対象となります。

ルールの条件は少し難しく見えるかもしれませんが、1 つずつ見てみましょう。

最初の部分: `resource.resourcetype = "App" and resource.stream.HasPrivilege("read")`。

この条件では、アプリが公開されているストリームへの読み取りアクセス権が必要です。読み取りアクセス権がある場合、アプリへの読み取りアクセス権が付与されます ([**アクション**] セクションに記載されています)。

2 番目の部分: `or ((resource.resourcetype = "App.Object" and resource.published ="true" and resource.objectType != "app_appscript" and resource.objectType != "loadmodel") and resource.app.stream.HasPrivilege("read"))`

条件のこの部分は、アプリオブジェクトが公開されているストリームへの読み取り権限を持っていることにも依存します。読み取り権限がある場合、アプリオブジェクトが公開されている場合、アプリオブジェクト ([`app_appscript`] と [`loadmodel`] を除く) への読み取りアクセス権が付与されます。

Stream などの一般的なセキュリティルールを設定することは、ストリーム内のコンテンツへのアクセス権の付与を簡素化するための便利なソリューションです。ただし、アプリまたはアプリオブジェクトへのアクセスを制限する場合は、特定の条件で新しいルールを作成し、アクセス権を付与する既存のルールを無効にする必要があります。ユーザーがアクセスできるように、リソースへのアクセス権をユーザーに付与するセキュリティルールが 1 つあれば十分であることを忘れないでください。アクセス権が付与されていない別のルールが存在する場合でも、リソースにアクセスできるようになります。

既存のルールに基づいての新しいルールの作成

Qlik Sense Enterprise on Windows には、既定で含まれているいくつかのセキュリティルールが付属しています。ルールには、2 つのタイプがあります。(Default および Read only) が保存されます。Read only ルールは、システムが機能するために不可欠であるため、編集または削除できません。Default ルールは編集できます。編集すると、ルールタイプが 3 番目のタイプ Custom に変更されます。既存の Default ルールを編集する場合は、コピーを作成して編集することを強くお勧めします。後で既存のルールが必要になる場合があります。

Qlik Sense に含まれるセキュリティルール (page 540)

パフォーマンス

セキュリティルールを設計するときは、パフォーマンスについて考慮することが重要です。アプリ、ストリーム、セキュリティルールの数が増えると、ハブの起動が遅くなり、応答時間が長くなるため、パフォーマンスが問題になる可能性があります。パフォーマンスに役立つセキュリティルールを設計できるようにするには、ルールの評価プロセスを理解する必要があります。

評価手順の概要については、*評価 フロー (page 596)* を参照してください。

QMC のベストプラクティスと効率的なセキュリティルールを作成するためのガイドラインについては、*QMC パフォーマンス – ベストプラクティス (page 449)* を参照してください。

Qlik Sense に含まれるセキュリティルール

Qlik Sense インストールでは、多くのセキュリティルールがあらかじめに含まれており、QMC で使用できます。セキュリティルールを使用して、Qlik Sense の領域へのアクセス権をユーザーに付与することができます。ルールには次の 3 つのタイプがあります。Default、Read only、Custom。Read only ルールは Qlik Sense の必須ルールであり、編集または削除することはできません。Default ルールは編集可能です。Default ルールを編集するか、新しいルールを作成すると、タイプが Custom に変更されます。

Default ルールを編集する場合、後で元のルールを使用する必要が生じることがあるため、元のルールからコピーを作成、編集することを強くお勧めします。コピーを使用する前に、元のルールを必ず無効化してください。

Qlik Sense インストールには次のセキュリティルールがあらかじめ含まれています。

AuditAdmin

AuditAdmin セキュリティルールのプロパティ

プロパティ	詳細
名前	AuditAdmin
説明	監査管理者には、エンティティを監査するための読み取り権限が必要です
リソース フィルター	*
アクション	読み取り
コンテキスト	QMC 専用
タイプ	初期設定
条件	user.roles = "AuditAdmin" and !(resource.resourcetype = "TransientObject" and resource.name like "QmcSection_*")

AuditAdminQmcSections

AuditAdminQmcSections セキュリティルールのプロパティ

プロパティ	詳細
名前	AuditAdminQmcSections
説明	監査管理者には、関連セクションを監査するための読み取り権限が必要です
リソース フィルター	License_*,TermsAcceptance_*,QmcSection_AppDistributionStatus,QmcSection_CloudDistribution, QmcSection_Tag,QmcSection_Audit,QmcSection_DeploymentSetup
アクション	読み取り
コンテキスト	QMC 専用
タイプ	初期設定
条件	((user.roles="AuditAdmin"))

コンテンツ ライブラリのコンテンツ

コンテンツ ライブラリのコンテンツのセキュリティルールのプロパティ

プロパティ	詳細
名前	コンテンツ ライブラリのコンテンツ
説明	コンテンツ ライブラリへの読み取り権限のある全ユーザーは、該当ファイルへの読み取り権限も必要です
リソース フィルター	StaticContentReference_*
アクション	読み取り
コンテキスト	ハブとQMC の両方
タイプ	Read only (読み取り専用)
条件	resource.ContentLibrarys.HasPrivilege("Read")

コンテンツ ライブラリ管理 コンテンツ

コンテンツ ライブラリ管理 コンテンツのセキュリティルールのプロパティ

プロパティ	詳細
名前	コンテンツ ライブラリ管理 コンテンツ
説明	コンテンツ ライブラリへの更新権限のある全ユーザーは、該当ファイルを管理するための権限も必要です
リソース フィルター	StaticContentReference_*
アクション	作成、読み取り、更新、削除
コンテキスト	ハブとQMC の両方
タイプ	Read only (読み取り専用)
条件	resource.ContentLibrarys.HasPrivilege("Update")

ContentAdmin

ContentAdmin セキュリティルールのプロパティ

プロパティ	詳細
名前	ContentAdmin
説明	コンテンツ管理者には、コンテンツ関連エンティティを管理するための権限が必要です
リソース フィルター	Stream_*,App*,ReloadTask_*,ExternalProgramTask_*,UserSyncTask_*, SchemaEvent_*,User*,CustomProperty*,Tag_*,DataConnection_*,CompositeEvent_*,Extension_*,ContentLibrary_*,FileExtension_*,FileExtensionWhiteList_*,SystemNotification_*
アクション	作成、読み取り、更新、削除、エクスポート、公開、所有者の変更

プロパティ	詳細
コンテキスト	QMC 専用
タイプ	初期設定
条件	((user.roles="ContentAdmin"))

ContentAdminQmcSections

ContentAdminQmcSections セキュリティルールのプロパティ

プロパティ	詳細
名前	ContentAdminQmcSections
説明	コンテンツ管理者には、コンテンツ関連セクションへの読み取り権限が必要です
リソース フィルター	License_*,TermsAcceptance_*,QmcSection_Stream,QmcSection_App,QmcSection_App.Object, QmcSection_AppDistributionStatus,QmcSection_CloudDistribution,QmcSection_DataConnection, QmcSection_Tag,QmcSection_User,QmcSection_CustomPropertyDefinition,QmcSection_Task, QmcSection_Event, QmcSection_SchemaEvent,QmcSection_CompositeEvent,QmcSection_Extension, QmcSection_ReloadTask,QmcSection_UserSyncTask,QmcSection_ContentLibrary, QmcSection_Audit,QmcSection_AnalyticConnection,QmcSection_SystemNotification, QmcSection_SystemNotificationPolicy,QmcSection_DeploymentSetup
アクション	読み取り
コンテキスト	QMC 専用
タイプ	初期設定
条件	((user.roles="ContentAdmin"))

ContentAdminRulesAccess

ContentAdminRulesAccess セキュリティルールのプロパティ

プロパティ	詳細
名前	ContentAdminRulesAccess
説明	コンテンツ管理者には、ストリーム、データ接続、コンテンツ ライブラリ、拡張のセキュリティルールを管理するための権限が必要です
リソース フィルター	SystemRule_*
アクション	作成、読み取り、更新、削除
コンテキスト	QMC 専用
タイプ	初期設定

プロパティ	詳細
条件	user.roles = "ContentAdmin" and (resource.category = "Security" and (resource.resourcefilter matches "Stream_\w{8}-\w{4}-\w{4}-\w{4}-\w{12}" or resource.resourcefilter matches "DataConnection_\w{8}-\w{4}-\w{4}-\w{4}-\w{12}" or resource.resourcefilter matches "ContentLibrary_\w{8}-\w{4}-\w{4}-\w{4}-\w{12}" or resource.resourcefilter matches "Extension_\w{8}-\w{4}-\w{4}-\w{4}-\w{12}") or (resource.category = "Generic" and resource.subcategory = "SystemNotification"))

CreateApp

CreateApp セキュリティルールのプロパティ

プロパティ	詳細
名前	CreateApp
説明	匿名ユーザー以外の全ユーザーにアプリを作成するための権限が必要です
リソース フィルター	App_*
アクション	作成
コンテキスト	ハブでのみ
タイプ	初期設定
条件	!user.IsAnonymous()

CreateAppObjectsPublishedApp

CreateAppObjectsPublishedApp セキュリティルールのプロパティ

プロパティ	詳細
名前	CreateAppObjectsPublishedApp
説明	公開済みアプリへの読み取り権限を持つ全ユーザーは、そのアプリに属するシート、ストーリー、ブックマーク、スナップショットを作成する権限も必要です
リソース フィルター	App.Object_*
アクション	作成
コンテキスト	ハブでのみ
タイプ	初期設定
条件	!resource.App.stream.Empty() and resource.App.HasPrivilege("read") and (resource.objectType = "userstate" or resource.objectType = "sheet" or resource.objectType = "story" or resource.objectType = "bookmark" or resource.objectType = "snapshot" or resource.objectType = "embeddedsnapshot" or resource.objectType = "hiddenbookmark") and !user.IsAnonymous()

CreateAppObjectsUnPublishedApp

CreateAppObjectsUnPublishedApp セキュリティルールのプロパティ

プロパティ	詳細
名前	CreateAppObjectsUnPublishedApp
説明	未公開アプリへの読み取り権限を持つ全ユーザーは、そのアプリに属するアプリオブジェクトを作成する権限も必要です
リソース フィルター	App.Object_*
アクション	作成
コンテキスト	ハブでのみ
タイプ	初期設定
条件	resource.App.stream.Empty() and resource.App.HasPrivilege("read") and !user.IsAnonymous()

CreateOdagLinks

CreateOdagLinks セキュリティルールのプロパティ

プロパティ	詳細
名前	CreateOdagLinks
説明	ODAG テンプレートアプリへの読み取りアクセス権を持っている非匿名ユーザーはリンクを作成することができ、最初にテンプレートアプリを知らなくてもリンクを作成することが可能です
リソース フィルター	OdagLink_*
アクション	作成
コンテキスト	ハブでのみ
タイプ	初期設定
条件	!user.IsAnonymous() and (resource.templateApp.Empty() or resource.templateApp.HasPrivilege("read"))

CreateOdagLinkUsage

CreateOdagLinkUsage セキュリティルールのプロパティ

プロパティ	詳細
名前	CreateOdagLinkUsage
説明	SelectionApp に対する読み取りアクセス権とリンクに対する読み取りアクセス権を持っている非匿名ユーザーは、OdagLinkUsages を作成できます

プロパティ	詳細
リソース フィルター	OdagLinkUsage_*
アクション	作成
コンテキスト	ハブでのみ
タイプ	初期設定
条件	!user.IsAnonymous() and (resource.selectionApp.Empty() or resource.selectionApp.HasPrivilege("read")) and (resource.link.Empty() or resource.link.HasPrivilege("read"))

CreateOdagRequest

CreateOdagRequest セキュリティルールのプロパティ

プロパティ	詳細
名前	CreateOdagRequest
説明	リンクに対する読み取りアクセス権を持っている非匿名ユーザーは、そのリンクを使用して新しい要求を作成できます
リソース フィルター	OdagRequest_*
アクション	作成
コンテキスト	ハブでのみ
タイプ	初期設定
条件	!user.IsAnonymous() and (resource.link.HasPrivilege("read"))

DataConnection

DataConnection セキュリティルールのプロパティ

プロパティ	詳細
名前	DataConnection
説明	「folder」を除くすべてのリソース タイプ用のデータ接続を作成することができます
リソース フィルター	DataConnection_*
アクション	作成
コンテキスト	ハブでのみ
タイプ	初期設定
条件	((resource.type!="folder"))

DataPrepAppCacheAccessRule

DataPrepAppCacheAccessRule セキュリティルールのプロパティ

プロパティ	詳細
名前	DataPrepAppCacheAccessRule
説明	匿名ユーザー以外の全ユーザーにデータ接続への読み取り権限が必要です
リソース フィルター	DataConnection_<Connection_ID>
アクション	読み取り
コンテキスト	ハブとQMC の両方
タイプ	Custom (カスタム)
条件	!user.isAnonymous()

既定のコンテンツ ライブラリ

既定のコンテンツ ライブラリのセキュリティルールのプロパティ

プロパティ	詳細
名前	既定のコンテンツ ライブラリ
説明	全ユーザーに、既定のコンテンツ ライブラリへの読み取り権限が必要です
リソース フィルター	ContentLibrary_<コンテンツ ライブラリID>
アクション	読み取り
コンテキスト	ハブとQMC の両方
タイプ	初期設定
条件	true

DeleteOdagLinkUsage

DeleteOdagLinkUsage セキュリティルールのプロパティ

プロパティ	詳細
名前	DeleteOdagLinkUsage
説明	選択アプリでの読み取りアクセス権を持っている非匿名ユーザーは、そのアプリの OdagLinkUsages を削除できます
リソース フィルター	OdagLinkUsage_*
アクション	読み取り、削除
コンテキスト	ハブでのみ

プロパティ	詳細
タイプ	初期設定
条件	!user.IsAnonymous() and resource.selectionApp.HasPrivilege("read")

DeploymentAdmin

DeploymentAdmin セキュリティルールのプロパティ

プロパティ	詳細
名前	DeploymentAdmin
説明	展開管理者には、展開関連のエンティティに対するアクセス権が必要です
リソース フィルター	ServiceCluster_*,ServerNodeConfiguration_ *,Engine*,Proxy*,VirtualProxy*,Repository*,Printing*,Scheduler*, User*,CustomProperty*,Tag_*,License*, TermsAcceptance_*,ReloadTask_ *,ExternalProgramTask_*, UserSyncTask_*,SchemaEvent_*,CompositeEvent_*, Deployment_*,IdentityProviderSettings_*, SystemNotification_*
アクション	作成、読み取り、更新、削除
コンテキスト	QMC 専用
タイプ	初期設定
条件	((user.roles="DeploymentAdmin"))

DeploymentAdminAppAccess

DeploymentAdminAppAccess セキュリティルールのプロパティ

プロパティ	詳細
名前	DeploymentAdminAppAccess
説明	展開管理者には、負荷分散ルールを扱うために、アプリへの読み取り権限と更新権限が必要です
リソース フィルター	App_*
アクション	読み取り、更新
コンテキスト	QMC 専用
タイプ	初期設定
条件	((user.roles="DeploymentAdmin"))

DeploymentAdminQmcSections

DeploymentAdminQmcSections セキュリティルールのプロパティ

プロパティ	詳細
名前	DeploymentAdminQmcSections
説明	展開管理者には、展開関連セクションへの読み取り権限が必要です
リソース フィルター	License_*,TermsAcceptance_*,ServiceStatus_*,QmcSection_AppDistributionStatus, QmcSection_CloudDistribution,QmcSection_Tag,QmcSection_Templates,QmcSection_ ServiceCluster, QmcSection_ServerNodeConfiguration,QmcSection_ EngineService,QmcSection_ProxyService, QmcSection_VirtualProxyConfig,QmcSection_ RepositoryService, QmcSection_SchedulerService,QmcSection_ PrintingService,QmcSection_License*,QmcSection_Token, LoadbalancingSelectList,QmcSection_User,QmcSection_UserDirectory,QmcSection_ CustomPropertyDefinition, QmcSection_Certificates,QmcSection_ Certificates.Export,QmcSection_Task,QmcSection_App,QmcSection_SyncRule, QmcSection_LoadBalancingRule,QmcSection_Event,QmcSection_ ReloadTask,QmcSection_UserSyncTask,QmcSection_Audit, QmcSection_ DistributionPolicy,QmcSection_SystemNotification,QmcSection_SystemNotificationPolicy, QmcSection_DeploymentSetup
アクション	読み取り
コンテキスト	QMC 専用
タイプ	初期設定
条件	((user.roles="DeploymentAdmin"))

DeploymentAdminRulesAccess

DeploymentAdminRulesAccess セキュリティルールのプロパティ

プロパティ	詳細
名前	DeploymentAdminRulesAccess
説明	展開管理者には、同期ルールとライセンス ルールを管理するための権限が必要です
リソース フィルター	SystemRule_*
アクション	作成、読み取り、更新、削除
コンテキスト	QMC 専用
タイプ	初期設定
条件	user.roles = "DeploymentAdmin" and (resource.category = "Sync" or resource.category = "License" or resource.category = "Generic")

ExportAppData

ExportAppData セキュリティルールのプロパティ

プロパティ	詳細
名前	ExportAppData
説明	匿名ユーザーを除くすべてのユーザーが、表示を許可されているアプリデータのエクスポートを許可されます
リソース フィルター	App_*
アクション	データのエクスポート
コンテキスト	ハブとQMC の両方
タイプ	初期設定
条件	resource.HasPrivilege("read") and !user.IsAnonymous()

拡張機能

拡張機能のセキュリティルールのプロパティ

プロパティ	詳細
名前	拡張機能
説明	全ユーザーに、拡張への読み取り権限が必要です
リソース フィルター	Extension_*
アクション	読み取り
コンテキスト	ハブとQMC の両方
タイプ	初期設定
条件	true

拡張管理コンテンツ

拡張管理コンテンツのセキュリティルールのプロパティ

プロパティ	詳細
名前	拡張管理コンテンツ
説明	拡張への更新権限のある全ユーザーは、該当ファイルを管理するための権限も必要です
リソース フィルター	StaticContentReference_*
アクション	作成、読み取り、更新、削除
コンテキスト	ハブとQMC の両方

プロパティ	詳細
タイプ	Read only (読み取り専用)
条件	resource.Extensions.HasPrivilege("Update")

拡張静的コンテンツ

拡張静的コンテンツのセキュリティルールのプロパティ

プロパティ	詳細
名前	拡張静的コンテンツ
説明	拡張への読み取り権限のある全ユーザーに、該当ファイルへの読み取り権限が必要です
リソースフィルター	StaticContentReference_*
アクション	読み取り
コンテキスト	ハブとQMC の両方
タイプ	Read only (読み取り専用)
条件	resource.Extensions.HasPrivilege("Read")

ファイル アップロード接続オブジェクト

ファイル アップロード接続オブジェクトのセキュリティルールのプロパティ

プロパティ	詳細
名前	ファイル アップロード接続オブジェクト
説明	匿名ユーザー以外の全ユーザーに、サーバーにファイルをアップロードするために使われるデータ接続への読み取り権限が必要です
リソースフィルター	DataConnection_<data_connection_ID>
アクション	読み取り
コンテキスト	ハブとQMC の両方
タイプ	初期設定
条件	!user.IsAnonymous()

FolderDataConnection

FolderDataConnection セキュリティルールのプロパティ

プロパティ	詳細
名前	FolderDataConnection
説明	管理者には、フォルダデータ接続を管理するための権限が必要です

プロパティ	詳細
リソース フィルター	DataConnection_*
アクション	作成、読み取り、更新、削除
コンテキスト	ハブでのみ
タイプ	初期設定
条件	resource.type = "folder" and (user.roles = "RootAdmin" or user.roles = "ContentAdmin" or user.roles = "SecurityAdmin")

HubAdmin

HubAdmin セキュリティルールのプロパティ

プロパティ	詳細
名前	HubAdmin
説明	ハブ管理者は、タスクとスキーマ イベントをリロードするための読み取り、作成、更新の権限を持っている必要があります
リソース フィルター	ReloadTask_*,SchemaEvent_*
アクション	作成、読み取り、更新
コンテキスト	ハブでのみ
タイプ	初期設定
条件	((user.roles="HubAdmin"))

HubSectionHome

HubSectionHome セキュリティルールのプロパティ

プロパティ	詳細
名前	HubSectionHome
説明	すべてのユーザーがホーム ハブ セクションにアクセスできるようにします
リソース フィルター	HubSection_Home
アクション	読み取り
コンテキスト	ハブとQMC の両方
タイプ	初期設定
条件	true

HubSectionTask

HubSectionTask セキュリティルールのプロパティ

プロパティ	詳細
名前	HubSectionTask
説明	すべてのユーザーがタスク ハブ セクションにアクセスできるようにします
リソース フィルター	HubSection_Task
アクション	読み取り
コンテキスト	ハブでのみ
タイプ	初期設定
条件	true

インストール済み静的コンテンツ

インストール済み静的コンテンツのセキュリティルールのプロパティ

プロパティ	詳細
名前	インストール済み静的コンテンツ
説明	全ユーザーに、インストール済みの静的コンテンツへの読み取り権限が必要です
リソース フィルター	StaticContentReference_*
アクション	読み取り
コンテキスト	ハブとQMC の両方
タイプ	Read only (読み取り専用)
条件	((resource.StaticContentSecurityType="Open"))

ManageAnalyticConnection

ManageAnalyticConnection セキュリティルールのプロパティ

プロパティ	詳細
名前	ManageAnalyticConnection
説明	RootAdmin ロール、ContentAdmin ロールおよび SecurityAdmin ロールは、分析接続を管理できる必要があります
リソース フィルター	AnalyticConnection_*
アクション	作成、読み取り、更新、削除
コンテキスト	ハブとQMC の両方

プロパティ	詳細
タイプ	初期設定
条件	((user.roles="RootAdmin" or user.roles="ContentAdmin" or user.roles="SecurityAdmin"))

オフライン アクセス

オフライン アクセスのセキュリティルールのプロパティ

プロパティ	詳細
名前	オフライン アクセス
説明	匿名ユーザーを除くすべてのユーザーが、表示を許可されているアプリに対してオフライン アクセスを許可されます
リソース フィルター	App_*
アクション	読み取り
コンテキスト	ハブとQMC の両方
タイプ	初期設定
条件	resource.HasPrivilege("read") and !user.IsAnonymous()

Owner

Owner セキュリティルールのプロパティ

プロパティ	詳細
名前	Owner
説明	リソースがストリームに公開されていない場合、リソースの所有者には、更新権限と削除権限が必要です
リソース フィルター	*
アクション	更新、削除
コンテキスト	ハブとQMC の両方
タイプ	初期設定
条件	resource.IsOwned() and (resource.owner = user and !((resource.resourcetype = "App" and !resource.stream.Empty()) or (resource.resourcetype = "App.Object" and resource.published = "true")))

OwnerAnonymousTempContent

OwnerAnonymousTempContent セキュリティルールのプロパティ

プロパティ	詳細
名前	OwnerAnonymousTempContent
説明	テンポラリコンテンツの匿名所有者は、これにアクセスして削除できる必要があります
リソース フィルター	TempContent_*
アクション	読み取り、削除
コンテキスト	ハブとQMC の両方
タイプ	Read only (読み取り専用)
条件	user.IsAnonymous() and resource.anonymousOwnerUserId = user.userId

OwnerAppApproveAppObject

OwnerAppApproveObject セキュリティルールのプロパティ

プロパティ	詳細
名前	OwnerAppApproveAppObject
説明	アプリの所有者は、アプリに属するアプリオブジェクトを承認できる必要があります
リソース フィルター	App.Object_*
アクション	承認
コンテキスト	ハブとQMC の両方
タイプ	初期設定
条件	resource.App.owner = user

OwnerPublishAppObject

OwnerPublishAppObject セキュリティルールのプロパティ

プロパティ	詳細
名前	OwnerPublishAppObject
説明	アプリオブジェクトが承認されていない場合、アプリオブジェクトの所有者にはアプリオブジェクトへの公開権限が必要です
リソース フィルター	App.Object_*
アクション	公開
コンテキスト	ハブとQMC の両方

プロパティ	詳細
タイプ	初期設定
条件	resource.IsOwned() and resource.owner = user and resource.approved = "false" and resource.app.stream.HasPrivilege("publish")

OwnerPublishDuplicate

OwnerPublishDuplicate セキュリティルールのプロパティ

プロパティ	詳細
名前	OwnerPublishDuplicate
説明	アプリまたはストリームの所有者は公開することができ、アプリの所有者は複製できる必要があります。
リソース フィルター	App_*,Stream_*
アクション	公開、複製
コンテキスト	ハブとQMC の両方
タイプ	初期設定
条件	resource.IsOwned() and resource.owner = user

OwnerRead

OwnerRead セキュリティルールのプロパティ

プロパティ	詳細
名前	OwnerRead
説明	リソースがストリームに公開されている場合、リソースの所有者にはリソースへの読み取り権限が必要です
リソース フィルター	*
アクション	読み取り
コンテキスト	ハブとQMC の両方
タイプ	Read only (読み取り専用)
条件	resource.IsOwned() and resource.owner = user

OwnerUpdateApp

OwnerUpdateApp セキュリティルールのプロパティ

プロパティ	詳細
名前	OwnerUpdateApp

プロパティ	詳細
説明	アプリの所有者は、更新ができる必要があります
リソース フィルター	App_*
アクション	更新プログラム
コンテキスト	ハブとQMC の両方
タイプ	初期設定
条件	resource.IsOwned() and resource.owner = user

QMCCachingSupport

QMCCachingSupport セキュリティルールのプロパティ

プロパティ	詳細
名前	QMCCachingSupport
説明	QMC キャッシュをサポートするには、このルールを QmcCacheEnabled フラグとともに有効にします。
リソース フィルター	ExecutionSession_*,ExecutionResult_*,*TaskOperational*
アクション	読み取り
コンテキスト	QMC 専用
タイプ	初期設定
条件	((user.roles="ContentAdmin" or user.roles="DeploymentAdmin"))

ReadAnalyticConnectionEveryone

ReadAnalyticConnectionEveryone セキュリティルールのプロパティ

プロパティ	詳細
名前	ReadAppContentFiles
説明	匿名ユーザー以外のユーザーが分析接続を読み取ることができます
リソース フィルター	AnalyticConnection_*
アクション	読み取り
コンテキスト	ハブでのみ
タイプ	Read only (読み取り専用)
条件	!user.IsAnonymous()

ReadAppContentFiles

ReadAppContentFiles セキュリティルールのプロパティ

プロパティ	詳細
名前	ReadAppContentFiles
説明	アプリへの読み取り権限のある全ユーザーには、そのコンテンツ ファイルへの読み取り権限も必要です
リソース フィルター	StaticContentReference_*
アクション	読み取り
コンテキスト	ハブとQMC の両方
タイプ	Read only (読み取り専用)
条件	resource.AppContents.App.HasPrivilege("Read")

ReadAppContents

ReadAppContents セキュリティルールのプロパティ

プロパティ	詳細
名前	ReadAppContents
説明	アプリへの読み取り権限を持つ全ユーザーには、そのアプリに属するアプリコンテンツへの読み取り権限も必要です
リソース フィルター	App.Content_*
アクション	読み取り
コンテキスト	ハブとQMC の両方
タイプ	Read only (読み取り専用)
条件	resource.App.HasPrivilege("read")

ReadAppDataSegments

ReadAppDataSegments セキュリティルールのプロパティ

プロパティ	詳細
名前	ReadAppDataSegments
説明	アプリへの読み取り権限を持つ全ユーザーには、そのアプリに属するアプリデータセグメントへの読み取り権限も必要です
リソース フィルター	App.DataSegment_*
アクション	読み取り

プロパティ	詳細
コンテキスト	ハブとQMC の両方
タイプ	Read only (読み取り専用)
条件	resource.App.HasPrivilege("read") and !user.IsAnonymous()

ReadAppInternals

ReadAppInternals セキュリティルールのプロパティ

プロパティ	詳細
名前	ReadAppInternals
説明	アプリへの読み取り権限を持つ全ユーザーには、そのアプリに属するアプリ内部への読み取り権限も必要です
リソース フィルター	App.Internal_*
アクション	読み取り
コンテキスト	ハブとQMC の両方
タイプ	Read only (読み取り専用)
条件	resource.App.HasPrivilege("read")

ReadContentCacheControl

ReadContentCacheControl セキュリティルールのプロパティ

プロパティ	詳細
名前	ReadContentCacheControl
説明	親コンテンツ ライブラリへの読み取りアクセスは、コンテンツ キャッシュ コントロールを参照するための読み取りアクセスも提供する必要があります
リソース フィルター	ContentCacheControl_*
アクション	読み取り
コンテキスト	ハブとQMC の両方
タイプ	初期設定
条件	((user.roles="ContentAdmin" or user.roles="SecurityAdmin" or resource.contentLibrary.HasPrivilege("read")))

ReadCustomProperties

ReadCustomProperties セキュリティルールのプロパティ

プロパティ	詳細
名前	ReadCustomProperties
説明	非匿名ユーザーは、カスタムプロパティ定義および値を読み取ることができます。
リソースフィルター	CustomProperty*
アクション	読み取り
コンテキスト	ハブとQMC の両方
タイプ	初期設定
条件	!user.IsAnonymous()

ReadOdagLinks

ReadOdagLinks セキュリティルールのプロパティ

プロパティ	詳細
名前	ReadOdagLinks
説明	非匿名ユーザーは ODAG リンクを読み取ることができます
リソースフィルター	OdagLink_*
アクション	読み取り
コンテキスト	ハブでのみ
タイプ	初期設定
条件	!user.IsAnonymous()

ReadOdagLinkUsage

ReadOdagLinkUsage セキュリティルールのプロパティ

プロパティ	詳細
名前	ReadOdagLinkUsage
説明	選択アプリに対する読み取りアクセス権を持っている非匿名ユーザーは、その OdagLinkUsages を読み取ることができます
リソースフィルター	OdagLinkUsage_*
アクション	読み取り
コンテキスト	ハブでのみ

プロパティ	詳細
タイプ	初期設定
条件	!user.IsAnonymous()

RootAdmin

RootAdmin セキュリティルールのプロパティ

プロパティ	詳細
名前	RootAdmin
説明	ルート管理者には、完全なアクセス権が必要です
リソース フィルター	*
アクション	作成、読み取り、更新、削除、エクスポート、公開、所有者の変更、ロールの変更、データのエクスポート
コンテキスト	QMC 専用
タイプ	Read only (読み取り専用)
条件	((user.roles="RootAdmin"))

SecurityAdmin

SecurityAdmin セキュリティルールのプロパティ

プロパティ	詳細
名前	SecurityAdmin
説明	セキュリティ管理者には、セキュリティ関連エンティティへのアクセス権が必要です
リソース フィルター	Stream_*,App*,Proxy*,VirtualProxy*,User*,SystemRule_*,CustomProperty*,Tag_*,DataConnection_*, ContentLibrary_*,FileExtension_*,FileExtensionWhiteList_*,Deployment_*, IdentityProviderSettings_*
アクション	作成、読み取り、更新、削除、エクスポート、公開、所有者の変更
コンテキスト	QMC 専用
タイプ	初期設定
条件	((user.roles="SecurityAdmin"))

SecurityAdminQmcSections

SecurityAdminQmcSections セキュリティルールのプロパティ

プロパティ	詳細
名前	SecurityAdminQmcSections

プロパティ	詳細
説明	セキュリティ管理者には、セキュリティ関連セクションへの読み取り権限が必要です
リソース フィルター	License_*,TermsAcceptance_*,ServiceStatus_*,QmcSection_Stream,QmcSection_App, QmcSection_App.Object,QmcSection_AppDistributionStatus,QmcSection_ CloudDistribution,QmcSection_SystemRule, QmcSection_DataConnection,QmcSection_ Tag,QmcSection_Templates,QmcSection_Audit,QmcSection_ProxyService,QmcSection_ VirtualProxyConfig,QmcSection_User,QmcSection_CustomPropertyDefinition, QmcSection_Certificates,QmcSection_Certificates.Export,QmcSection_ContentLibrary, QmcSection_AnalyticConnection,QmcSection_DeploymentSetup
アクション	読み取り
コンテキスト	QMC 専用
タイプ	初期設定
条件	((user.roles="SecurityAdmin"))

SecurityAdminServerNodeConfiguration

SecurityAdminServerNodeConfiguration セキュリティルールのプロパティ

プロパティ	詳細
名前	SecurityAdminServerNodeConfiguration
説明	セキュリティ管理者には、ServerNodeConfiguration エンティティへの読み取り権限が必要です
リソース フィルター	ServerNodeConfiguration_*
アクション	読み取り
コンテキスト	QMC 専用
タイプ	初期設定
条件	((user.roles="SecurityAdmin"))

ServiceAccount

ServiceAccount セキュリティルールのプロパティ

プロパティ	詳細
名前	ServiceAccount
説明	サービス アカウントには、全アクションを実行するための権限が必要です
リソース フィルター	*
アクション	作成、読み取り、更新、削除、エクスポート、公開、所有者の変更、ロールの変更、データのエクスポート

プロパティ	詳細
コンテキスト	ハブとQMC の両方
タイプ	Read only (読み取り専用)
条件	((user.UserDirectory="INTERNAL" and user.UserId like "sa_*"))

共有コンテンツ管理コンテンツ

共有コンテンツ管理コンテンツのセキュリティルールのプロパティ

プロパティ	詳細
名前	共有コンテンツ管理コンテンツ
説明	共有コンテンツへの更新権限のある全ユーザーには、該当ファイルを管理するための権限も必要です
リソースフィルター	StaticContentReference_*
アクション	作成、読み取り、更新、削除
コンテキスト	ハブとQMC の両方
タイプ	Read only (読み取り専用)
条件	resource.SharedContents.HasPrivilege("Update")

共有コンテンツ確認コンテンツ

共有コンテンツ確認コンテンツのセキュリティルールのプロパティ

プロパティ	詳細
名前	共有コンテンツ確認コンテンツ
説明	共有コンテンツへの読み取り権限のある全ユーザーは、該当ファイルへの読み取り権限も必要です
リソースフィルター	StaticContentReference_*
アクション	読み取り
コンテキスト	ハブとQMC の両方
タイプ	Read only (読み取り専用)
条件	resource.SharedContents.HasPrivilege("Read")

ストリーム

ユーザーがストリーム内の公開されたアプリを編集できるようなルールを作成することは推奨されません。

ストリームのセキュリティルールのプロパティ

プロパティ	詳細
名前	ストリーム
説明	ストリームへの読み取り権限を持つ全ユーザーには、そのストリームに公開されたリソースへの読み取り権限も必要です
リソース フィルター	App*
アクション	読み取り
コンテキスト	ハブとQMC の両方
タイプ	初期設定
条件	(resource.resourcetype = "App" and resource.stream.HasPrivilege("read")) or ((resource.resourcetype = "App.Object" and resource.published ="true" and resource.objectType != "app_appscript" and resource.objectType != "loadmodel") and resource.app.stream.HasPrivilege("read"))

StreamEveryone

StreamEveryone セキュリティルールのプロパティ

プロパティ	詳細
名前	StreamEveryone
説明	匿名ユーザー以外の全ユーザーに、Everyone という既定のストリームへの読み取り権限と公開権限が必要です
リソース フィルター	Stream_<stream_ID>
アクション	読み取り、公開
コンテキスト	ハブとQMC の両方
タイプ	初期設定
条件	!user.IsAnonymous()

StreamEveryoneAnonymous

StreamEveryoneAnonymous セキュリティルールのプロパティ

プロパティ	詳細
名前	StreamEveryoneAnonymous
説明	匿名ユーザーには、Everyone という既定のストリームへの読み取り権限が必要です
リソース フィルター	Stream_<stream_ID>

プロパティ	詳細
アクション	読み取り
コンテキスト	ハブでのみ
タイプ	初期設定
条件	user.IsAnonymous()

StreamMonitoringAppsPublish

StreamMonitoringAppsPublish セキュリティルールのプロパティ

プロパティ	詳細
名前	StreamMonitoringAppsPublish
説明	RootAdmin、ContentAdmin、SecurityAdmin には、Monitoring apps という既定のストリームへの公開権限が必要です
リソース フィルター	Stream_<stream_ID>
アクション	公開
コンテキスト	ハブでのみ
タイプ	初期設定
条件	((user.roles="RootAdmin" or user.roles="ContentAdmin" or user.roles="SecurityAdmin"))

StreamMonitoringAppsRead

StreamMonitoringAppsRead セキュリティルールのプロパティ

プロパティ	詳細
名前	StreamMonitoringAppsRead
説明	既定の管理者には、Monitoring apps という既定のストリームへの読み取り権限が必要です
リソース フィルター	Stream_<stream_ID>
アクション	読み取り
コンテキスト	ハブとQMC の両方
タイプ	初期設定
条件	((user.roles="RootAdmin" or user.roles="ContentAdmin" or user.roles="SecurityAdmin" or user.roles="DeploymentAdmin" or user.roles="AuditAdmin"))

テンポラリコンテンツ

テンポラリコンテンツのセキュリティルールのプロパティ

プロパティ	詳細
名前	テンポラリコンテンツ
説明	匿名ユーザー以外の全ユーザーに一時コンテンツを作成するための権限が必要です
リソースフィルター	TempContent_*
アクション	作成
コンテキスト	ハブとQMC の両方
タイプ	Read only (読み取り専用)
条件	!user.IsAnonymous()

UpdateAppContentFiles

UpdateAppContentFiles セキュリティルールのプロパティ

プロパティ	詳細
名前	UpdateAppContentFiles
説明	アプリへの更新権限のある全ユーザーには、そのコンテンツファイルを管理するための権限も必要です
リソースフィルター	StaticContentReference_*
アクション	作成、読み取り、更新、削除
コンテキスト	ハブとQMC の両方
タイプ	Read only (読み取り専用)
条件	resource.AppContents.App.HasPrivilege("Update")

UpdateAppContents

UpdateAppContents セキュリティルールのプロパティ

プロパティ	詳細
名前	UpdateAppContents
説明	アプリへの更新権限を持つ全ユーザーには、そのアプリに属するアプリコンテンツへの更新権限も必要です
リソースフィルター	App.Content_*
アクション	更新プログラム

プロパティ	詳細
コンテキスト	ハブとQMC の両方
タイプ	Read only (読み取り専用)
条件	resource.App.HasPrivilege("update")

UpdateAppDataSegments

UpdateAppDataSegments セキュリティルールのプロパティ

プロパティ	詳細
名前	UpdateAppDataSegments
説明	アプリへの更新権限を持つ全ユーザーには、そのアプリに属するアプリデータセグメントを管理するための権限も必要です
リソース フィルター	App.DataSegment_*
アクション	作成、読み取り、更新、削除
コンテキスト	ハブとQMC の両方
タイプ	Read only (読み取り専用)
条件	resource.App.HasPrivilege("update") and !user.IsAnonymous()

UpdateAppInternals

UpdateAppInternals セキュリティルールのプロパティ

プロパティ	詳細
名前	UpdateAppInternals
説明	アプリへの更新権限を持つ全ユーザーには、そのアプリに属するアプリ内部を管理するための権限も必要です
リソース フィルター	App.Internal_*
アクション	作成、読み取り、更新、削除
コンテキスト	ハブとQMC の両方
タイプ	Read only (読み取り専用)
条件	resource.App.HasPrivilege("update")

セキュリティルール エディタ

セキュリティルール エディタではセキュリティルールを新規作成できます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**セキュリティ ルール**] を選択します。
3. データ マネージャーでテーブルの ⊕ [**新規作成**] するか、既存のルールを選択して [**編集**] をクリックします。

必要に応じて、シンプルなルール用の [**基本**] セクション、または詳細なルールを作成するための [**詳細**] セクションの [**条件**] テキスト ボックスを使用できます。

*[**詳細**] セクションでルールを作成する場合は、**[基本]** セクションで **[アクション]** を指定する必要があります。*

ストリームやデータ接続といった一部のリソース タイプでは、セキュリティ ルール セクションにアクセスすることなく、関連するルールを直接編集したり、作成することができます。親オブジェクトを削除すると、関連するルールも削除されるという点に注意してください。

[基本] セクションを使用するケース

[**基本**] セクションを使用すると、次のいずれかの操作を効率的に行うことができます。

- 1 つのリソース タイプのみに適用されるルールの作成
- より詳細なルールの基盤の作成

1 つのリソース タイプのみのルール作成

[**ID**] セクションの [**テンプレートからルールを作成**] ドロップダウン リストを使用してリソース タイプを選択すると、選択したリソース タイプが [**基本**] セクションの [**リソース フィルター**] に設定されます。また、明示的にこのリソース タイプを示すリソース フィルターが自動的に生成されます。例えば、[**アプリ アクセス**] を選択した場合、リソース フィルタに「App_*」が設定されます。これは、QMC がアプリのルールのみを評価することを意味します。

リソース フィルタでのリソースの命名 (page 572)

基本ビューからさらにリソース タイプを追加するには、[**リソース フィルター**] テキスト ボックスの右側にある矢印をクリックして、リソースを選択します。

より詳細なルールの基盤の作成

[**基本**] セクションを使用すると、ルールのベースをすばやく作成できます。例えば、[**詳細**] セクションの [**条件**] テキスト フィールドでは、ルールを適用するリソースのタイプを 1 つと、AND/OR 以外の演算子を使用した条件を定義できます。[**詳細**] セクションで、エディタの内蔵機能を使用することもできます。

[詳細設定] セクションと [基本設定] セクションのバックトラック

[**基本**] セクションと [**詳細**] セクションの間での同期 (いわゆるバックトラッキング) を有効にするには、[**基本**] セクションで作成された条件にかっこを追加します。同様に、[**基本**] セクションでリソースを追加すると、[**Conditions (条件)**] テキスト フィールドに、条件が空欄のユーザー定義が自動的に設定されます。ただし、[**詳細**] セクションのみでルールを作成し、バックトラッキングの必要がなければ、上記の方法に従う必要はありません。

セキュリティルールの作成

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**セキュリティルール**] を選択します。
3. データ マネージャーでテーブルの **新規作成** をクリックします。
   左側に編集パネル (すべてのプロパティを保持)、右側に監査ページが配置された分割ページが表示されます。
4. [**ID**] の、[**テンプレートからルールを作成**] ドロップダウン リストで、ルールを作成するリソースのタイプを選択します。

   [基本] セクションの [リソース フィルター] テキスト ボックスの横にある矢印をクリックしてポップオーバーを開き、フィルターに複数のリソースを選択できます。

   リソース

   リソースのプロパティ

プロパティ	セキュリティ規則が適用されます
Unspecified	すべてのリソース タイプ
App access	アプリ
App object access	オブジェクト シート、ストーリー、ブックマーク、メジャー、軸など、オブジェクトのオブジェクト タイプ。
Content library access	コンテンツ ライブラリ
Data connection access	データ接続
Extension access	拡張機能
Reload task access	タスクのリロード
Node access	Qlik Sense ノードの構成
Stream access	ストリーム
User access	ユーザー
Security rule access	セキュリティルール
User directory connector access	ユーザー ディレクトリ
User synchronization task access	ユーザー同期タスク
Analytic connection access	分析接続

たとえば、[**アプリ アクセス ルール**] を作成し、リソース条件の [**名前**] を「*MyApp*」に設定すると、ルールは「*MyApp*」という名前のアプリに適用されます。ただし、[**名前**] を「*MyApp**」に設定すると、名前が「*MyApp*」で始まるすべてのアプリにルールが適用されます。

> *[**Create rule from template**] の選択を変更すると、自動的にすべての [**アクション**] がクリアされ、[**Advanced**] セクションの [**Conditions**] テキストボックスが変更されます。*

5. [**Identification (ID)**] で、ルールに名前を付け、説明を入力します。
6. この時、ルールを有効にしたくない場合は、[**無効**] を選択します。
7. 必要に応じて、リソース フィルターに新たなリソースを追加します。データマネージャーでテーブルの ▼next to the **Resource filter** text box to open a pop-up with the available resources.
8. In the **Basic** section, click ⊕to add more conditions (optional).

   複数の条件を使用すると、[**Group**] をクリックして 2 つの条件をグループ化できます。条件のグループ化後、[**Ungroup**] をクリックして、グループ化を解除できます。この他に、サブグループ化オプションには [**Split**] および [**Join**] があります。条件間の既定の演算子は、OR です。これは、演算子のドロップダウンリストで変更できます。AND が OR より上位になるように、条件をグループ化します。

   > *ワイルドカード(*) を使用する際は、"=" の代わりに "`like`" 演算子を使用する必要があります。*

   リソース条件のプレゼンテーションについては、次を参照してください。*利用可能なリソース条件 (page 582)*。
9. 次を参照して、リソース フィルターを定義します。*リソース フィルターの定義 (page 572)*。
10. リソースのユーザーにアクセス権限を割り当てるには、該当する [**アクション**] を選択します。

アクション プロパティ

アクセス ルールの説明

アクション	説明
Create	リソースを作成します。
Read	リソースを読み取ります。
Update	リソースを更新します。
Delete	リソースを削除します。
Export	Qlik Sense Enterpriseからqvfファイルにアプリをエクスポートします。
Duplicate	アプリの複製。
Publish	リソースをストリームに公開します。
Approve	アプリに属するオブジェクトを承認します。
Change owner	リソースの所有者を変更します。

アクション	説明
Change role	ユーザー ロールを変更します。
Export data	オブジェクトからデータをエクスポートします。これには、次のアクションが含まれます。 • ビジュアライゼーションの「画像としてエクスポート」。 • ビジュアライゼーションの「PDF としてエクスポート」。 • ビジュアライゼーションの「データのエクスポート」。 • メニューの「シートのエクスポート」。 • ストーリーテリングの「ストーリーのエクスポート」。 *これらのアクションのサブセットのみにアクセス権を付与することはできません。* *匿名ユーザーがデータをエクスポートできるようにするには、セキュリティ ルール ExportAppData のコピーを作成し、そのコピーを変更して、`resource.HasPrivilege("read")` のみを[**条件**] に含めるようにします。「Qlik Sense に含まれるセキュリティルール (page 540)」を参照してください。*
Access offline	アプリにオフラインでアクセスします。

11. ルールが適用されるユーザーを指定するユーザー条件を選択します。

OS やブラウザのタイプなど外部コールから受け取った環境データは、Qlik Sense システムによって安全を確保されません。

ユーザー条件プロパティ

接続されたユーザー ディレクトリに含まれるユーザープロパティはすべて、ドロップダウン リストに表示されます。これは、メール アドレスや部門名などです。

条件のプロパティ

プロパティ	説明
@<customproperty>	ユーザーに関連付けられたカスタム プロパティ。
name	ユーザーのフル ネーム
userdirectory	ユーザー ディレクトリ名。
userid	ユーザーの ID。
description	ユーザー ディレクトリから取得した所有者の説明。

プロパティ	説明
email	接続されたユーザーディレクトリに含まれる利用可能なメール アドレス。
group	ユーザーディレクトリから取得した所有者のグループ メンバーシップ。
environment.browser	セキュリティルールは、ブラウザのタイプに適用されます。対応ブラウザ:Chrome、Firefox、Safari、MSIE、または Unknown. **Example 1:** ブラウザとバージョンの定義: Firefox 22.0 Chrome 33.0.1750.154 *ブラウザ情報に斜線 (/) が含まれる場合は、空白文字で置き換えてください。* **Example 2:** ブラウザのすべてのバージョンを含める場合は、ワイルドカード (*) を使用します: 環境ブラウザ = Chrome*
environment.context	セキュリティルールは、コールが起こる Qlik Sense 環境にのみ適用されます。 利用可能なプリセット値: ManagementAccess または AppAccess.
environment.device	セキュリティルールは、デバイスのタイプに適用されます。 利用可能なプリセット値:iPhone、iPad、または Default.
environment.ip	セキュリティ規則は IP 番号に適用されます。 *セキュリティルールの例: IP アドレス別のストリーム アクセス権 (page 613)*
environment.os	セキュリティルールは、オペレーティング システムのタイプに適用されます。 利用可能なプリセット値:Windows、Linux、Mac OS X、または Unknown.
environment.secureRequest	セキュリティルールは、リクエスト タイプに適用されます。 利用可能なプリセット値: SSL True または False

12. [**詳細**] ビューでは、ルールの適用先を [**コンテキスト**] ドロップダウン リストから選択できます。

コンテキストプロパティ
コンテキスト ルールの適用対象を指定します。[**Both in hub and QMC**]、[**Only in hub**]、[**Only in QMC**] のいずれかに指定できます。

13. [**プレビュー**] をクリックすると、ルールが作成するアクセス権や、そのアクセス権が適用されるユーザーが表示されます。
14. [**適用**] をクリックして、ルールを作成し、保存します。
ページ最下部に [**追加完了**] と表示されます。

リソース フィルターの定義

ルール適用の効率化を図るには、ルール エディタでルール評価を行うリソースの数を絞り込むことが推奨されます。これは、セキュリティルールにリソース フィルタを適用すると実行できます。リソース フィルタは明示的または黙示的にルールが適用されるリソースのタイプを定義します。

リソースやユーザー条件を追加すると、リソースの数を絞り込むことができます。監査ページ、セキュリティルール概要ページ、またはセキュリティルール編集ページのいずれかで、セキュリティルールに使用されているリソース フィルターを確認できます。

リソース フィルタでのリソースの命名

リソース フィルターを定義する際は以下のルールを利用できます:

- 明示的な命名
リソース GUID を使用してリソースを定義します。
たとえば "Stream_88ee46c6-5e9a-41a7-a66a-f5d8995454ec"。

  各概要ページを使用してリソースのアクセス権を作成した場合と、セキュリティルール概要ページ> リソース フィルタで、データ接続、ログイン アクセス、ストリームの GUID を確認できます。

- ワイルドカード (_*) を使用した明示的なタイプの命名
「_*」ワイルドカードを使うと、ルールを適用するリソースのタイプを明示的に定義できます。
たとえば、「App_*」とすると、すべての App リソースにのみルールが適用されます。
- ワイルドカード (*) を使用した黙示的なタイプの命名
ワイルドカードを使用するとリソースを定義できます。
たとえば、「App*」とすると、「App」で始まるすべてのリソースにルールが適用されます。つまり、このルールはアプリ、シート、ストーリー、データ、オブジェクトに適用されます。

単一のリソースの指定

単一のリソースのタイプを定義するには、セキュリティルールの編集ページの基本ビューで [**リソース**] ドロップダウンリストからリソースのタイプを選択します。[**詳細**] ビューでは、[**リソース**] と [**条件**] 項目が自動的に入力されます。

例と結果

例と結果

例	結果
[アプリ] を [リソース] ドロップダウン リストから選択します。	以下のテキストが詳細ビューに表示されます。 リソース App* 条件 resource.resourcetype="App" and ( )
Stream_88ee46c6-5e9a-41a7-a66a-f5d8995454ec	ルールは、GUID が指定されているストリームに適用されます。

複数リソース タイプの定義

リソース フィルタ フィールドでルールに適用したいリソース タイプの名前を入力します。リソース GUID を含む明示的なリソースの名前を書き込むか、ワイルドカードを使用して特定タイプのあらゆるリソースを示唆することができます。

例と結果

例と結果

例	結果
App*, Streams*	ルールは アプリ、シート、ストーリー、データ、オブジェクト、ストリームに適用されます。
App_*, Streams*	ルールはアプリとストリームに適用されます。
Stream_\w{8}-\w{4}-\w{4}-\w{4}-\w{12}	ルールはリソース ID を使用している既存のストリームすべてに適用されます。

複合ユーザー イベントにおける複数の許可

複雑なユーザー イベントに対処するには、すべての必要条件を考慮するため複数のルールが必要になることが一般的です。次の許可の例には、複数のルールが関係しており、さまざまなリソース タイプ、条件、アクションに対処しています。表に、各タスクとそのタスクで必要とされるアクションを示します。

Import, Start user sync task, Start reload task

インポート権限、ユーザー同期タスク開始権限、リロード タスク開始権限

Task	App	Data Connection	UserSyncTask	ReloadTask	UserDirectory
Import	Create また、Update	Create (インポートしたアプリに新しいデータ接続が含まれている場合)			

Start UserSyncTask			Read		Update
Start ReloadTask	Update			Read	

Duplicate, Publish, Publish and replace

複製権限、公開権限、公開して置換権限

Task	App	Stream	App.Object
Duplicate	Read また、Duplicate		Read (それ以外の場合にはアプリが複製されますが、ユーザーが読み取り権限を持っているアプリオブジェクトのみが複製されたアプリに組み込まれます。)
Publish	Read また、Publish	Read また、Publish	Read (それ以外の場合にはアプリが公開されますが、ユーザーが読み取り権限を持っているアプリオブジェクトのみが公開されます。)
Publish and replace	Read、Update、および Publish のインポート	Read また、Publish	Read また、Update

タスクの詳細

Import

説明

新しいデータ接続が含まれるアプリをインポートできるようにするには、リソース タイプDataConnectionでの [**追加**] 許可と、リソースタイプAppでの [**追加**] および [**更新**] 許可が必要です。

ルール 1

リソース フィルター = App_*

条件 = (アプリのインポートを許可するユーザーを選択するための条件。)

Actions = Create, Update

ルール 2

リソース フィルター = DataConnection_*

条件 = (アプリのインポートを許可するユーザーを選択するための条件。)

Actions = Create

Start UserSyncTasks

説明

ユーザー同期タスクを実行できるようにするには、リソース タイプ での [**追加**] 許可 と、リソース タイプでの [更新] 許可が必要です。UserSyncTaskUserDirectory

ルール 1

リソース フィルター = UserSyncTask_*

条件 = (実行を許可するユーザーまたはユーザー同期タスクを選択するための条件。)

Actions = Read

ルール 2

リソース フィルター = UserDirectory_*

条件 = (更新を許可するユーザーまたはユーザー ディレクトリを選択するための条件。)

Actions = Update

Start ReloadTasks

説明

リロード タスクを実行できるようにするには、リソース タイプ ReloadTask での [**読み取り**] 許可 と、リソース タイプ App での [**更新**] 許可が必要です。

ルール 1

リソース フィルター = App_*

条件 = (リロードを許可するユーザーまたはアプリを選択するための条件。)

Actions = Update

ルール 2

リソース フィルター = ReloadTask_*

条件 = (実行を許可するユーザーまたは リロード タスクを選択するための条件。)

Actions = Read

Duplicate

説明

アプリを複製できるようにするには、リソース タイプ App とApp.Objects (複製されるアプリの一部となるオブジェクト) での [**読み取り**] 許可 と、アプリの [**複製**] 許可が必要です。

ルール 1

リソース フィルター = App_*

条件 = (アプリの複製を許可するユーザーを選択するための条件。)

Actions = Create and Read

ルール 2

リソース フィルター = App.Object_*

条件 = (複製を許可するユーザーまたはアプリを選択するための条件。)

Actions = Read

Publish

説明

アプリを公開できるようにするには、アプリでの [**読み取り**] および [**公開**] 許可、リソース タイプStreamでの [**読み取り**] および [**公開**] 許可、およびリソース タイプApp.Objects (公開されるアプリに組み込まれるオブジェクト) での [**読み取り**] 許可が必要です。

ルール 1

リソース フィルター = App_*、Stream_*

条件 = (ストリームへのアプリの公開を許可するユーザーを選択するための条件。)

Actions = Read, Publish

ルール 2

リソース フィルター = App.Object_*

条件 = (ユーザー、または公開されるアプリに組み込まれるApp.Objects を選択するための条件。)

Actions = Read

Publish and replace アプリ

説明

アプリを公開および置換できるようにするには、リソース タイプAppでの [**読み取り**]、[**更新**]、および [**公開**] 許可、リソース タイプStreamでの [**読み取り**] および [**公開**] 許可、およびリソース タイプApp.Objects (公開されるアプリに組み込まれるオブジェクト) での [**読み取り**] および [**更新**] 許可が必要です。

ルール 1

リソース フィルター = App_*

条件 = (アプリの公開および置換を許可するユーザーを選択するための条件。)

Actions = Read, Publish, Update

ルール 2

リソース フィルター = Stream_*

条件 = (公開を許可するユーザーまたはストリームを選択するための条件。)

Actions = Read, Publish

ルール 3

リソース フィルター = App.Object_*

条件 = (ユーザー、または公開されるアプリに含めるApp.Objects を選択するための条件。)

Actions = Read, Update

利用可能なリソース フィルター

以下の表は、リソース オブジェクトと、これをターゲットにするために使用できるリソース フィルターを示しています。

このリストにはすべて表示されているわけではなく、よく使用されるリソース フィルターの例のみを表示しています。

App 関連のリソース

アプリ フィルター

リソース フィルター	フィルターのターゲット
App	アプリケーション
App.Content	アプリ固有のコンテンツ ライブラリに保存されているコンテンツ
App.DataSegment	アプリケーションによってロードされ、使用されるデータの表現
App.Internal	アプリケーション内部の必須パラメータ
App.Object	シート、ストーリー、スクリプト、軸、メジャー、マスターオブジェクト、スナップショット、ブックマークなどのすべての App.Object リソース
appprops	テーマとシート タイトルの視覚的なスタイリング。
ColorMap	軸の値と色の間のマッピング。
Extension	Qlik Sense にインストールされている拡張機能
IAChat	コンテンツ Insight Advisor Chat
WebExtensionLibrary	Web 拡張機能のライブラリ
Widgets	Qlik Sense にインストールされているウィジェット

タスク リソース

タスク フィルター

リソース フィルター	フィルターのターゲット
CompositeEvent	スケジューラーのタスク トリガー
ExecutionResult	タスクの実行の詳細
ExecutionSession	タスクのアクティブ セッションの詳細
ExternalProgramTask	サードパーティプログラムをトリガーするタスク
ReloadTask	アプリでリロードを実行するタスク。これは配布タスクにも当てはまります。
SchemaEvent	スケジュールされたタスクがいつ実行されるかの詳細
UserSyncTask	外部ユーザー ディレクトリのユーザーを同期するタスク

コンテンツ ライブラリ関連のリソース

コンテンツ ライブラリ フィルター

リソース フィルター	フィルターのターゲット
ContentLibrary	コンテンツ ライブラリ
FileReference	ノード間でファイルを同期するためにバイナリ同期によって使用されるディスクに格納されるファイルの表現
SharedContent	QlikView ドキュメント、Qlik NPrinting で生成されたレポートへのリンク
StaticContentReference	コンテンツ ライブラリのファイルへのリンク
TempContent	エクスポートからのファイルなどの一時コンテンツ用のコンテンツ ライブラリ

ハブ セクション リソース

ハブへのユーザー アクセスを無効にするために、次のフィルターを使用できます。

ハブ セクション フィルター

リソース フィルター	フィルターのターゲット
HubSection_Home	ハブを開くアクセス権を付与し、アクセス権のあるリソースを表示します。既定では、オンです。 *ハブへのユーザー アクセスのみを無効化すると、[ナビゲーション] メニューの [**ハブの表示**] が表示されなくなります。この場合でも、ハブへのアクセスは URL を編集することで可能です。*
HubSection_Task	タスク ハブ セクションへのアクセスを許可します。既定では、オンです。

QMC セクション リソース

異なる QMC セクションへのアクセス権を付与するには、次のフィルターを使用します。QMC セクションへのアクセス権を持つユーザーはそのセクションを開けますが、ユーザーのアクセス権に応じたオブジェクトのみが表示されます。

使用可能なリソースの概要を取得するには、QMC に RootAdmin としてログインし、ネットワーク トラフィックを確認することができます。

QMC セクション フィルター

リソース フィルター	フィルターのターゲット
QmcSection_AnalyticConnection	QmcSection_AnalyticConnection リソース

リソース フィルター	フィルターのターゲット
QmcSection_App	QmcSection_App リソース
QmcSection_App.Object	QmcSection_App.Object リソース
QmcSection_Audit	QmcSection_Audit リソース
QmcSection_Certificates	QmcSection_Certificate リソース
QmcSection_Certificates.Export	QmcSection_Certificates.Export リソース
QmcSection_CompositeEvent	QmcSection_CompositeEvent リソース
QmcSection_ContentLibrary	QmcSection_ContentLibrary リソース
QmcSection_CustomPropertyDefinition	QmcSection_CustomPropertyDefinition リソース
QmcSection_DataConnection	QmcSection_DataConnection リソース
QmcSection_DistributionPolicy	QmcSection_DistributionPolicy リソース
QmcSection_EngineService	QmcSection_EngineService リソース
QmcSection_Event	QmcSection_Event リソース
QmcSection_Extension	QmcSection_Extension リソース
QmcSection_License	QmcSection_License リソース
QmcSection_Licenses	QmcSection_Licenses リソース
QmcSection_License.AnalyzerAccessRule	QmcSection_License.AnalyzerAccessRule リソース
QmcSection_License.AnalyzerAccessType	QmcSection_License.AnalyzerAccessType リソース
QmcSection_License.ApplicationAccessType	QmcSection_License.ApplicationAccessType リソース
QmcSection_License.LoginAccessType	QmcSection_License.LoginAccessType リソース
QmcSection_License.ProfessionalAccessRule	QmcSection_License.ProfessionalAccessRule リソース
QmcSection_License.ProfessionalAccessType	QmcSection_License.ProfessionalAccessType リソース
QmcSection_License.UserAccessRule	QmcSection_License.UserAccessRule リソース
QmcSection_License.UserAccessType	QmcSection_License.UserAccessType リソース
QmcSection_LoadBalancingRule	QmcSection_LoadBalancingRule リソース
QmcSection_OdagService	QmcSection_OdagService リソース
QmcSection_PrintingService	QmcSection_PrintingService リソース
QmcSection_ProxyService	QmcSection_ProxyService リソース
QmcSection_ReloadTask	QmcSection_ReloadTask リソース
QmcSection_RepositoryService	QmcSection_RepositoryService リソース
QmcSection_SchedulerService	QmcSection_SchedulerService リソース
QmcSection_SchemaEvent	QmcSection_SchemaEvent リソース

リソース フィルター	フィルターのターゲット
QmcSection_ServerNodeConfiguration	QmcSection_ServerNodeConfiguration リソース
QmcSection_ServiceCluster	QmcSection_ServiceCluster リソース
QmcSection_Stream	QmcSection_Stream リソース
QmcSection_SyncRule	QmcSection_SyncRule リソース
QmcSection_SystemRule	QmcSection_SystemRule リソース
QmcSection_Tag	QmcSection_Tag リソース
QmcSection_Task	QmcSection_Task リソース
QmcSection_Token	QmcSection_Token リソース
QmcSection_User	QmcSection_User リソース
QmcSection_UserDirectory	QmcSection_UserDirectory リソース
QmcSection_UserSyncTask	QmcSection_UserSyncTask リソース
QmcSection_VirtualProxyConfig	QmcSection_VirtualProxyConfig リソース

ライセンス関連のリソース

ライセンス フィルター

リソース フィルター	フィルターのターゲット
License	実際のライセンス エンティティQlik Sense .
License.AnalyzerAccessGroup	アナライザー アクセス タイプの自動割り当てに使用されるルールのリソース。
License.AnalyzerAccessType	アナライザー アクセスのタイプ。ユーザー (名前付き) に手動でアクセス権を割り当てるための CRUD。
License.AnalyzerAccessUsage	アナライザー アクセス タイプの使用状況を追跡するためのタイプ。リソース フィルターでは使用しないでください。
License.LoginAccessType	ログイン アクセスのタイプ。(時間制限付きの) ログイン アクセスにトークンを割り当て、関連したルールを設定するための CRUD。
License.LoginAccessUsage	ログイン アクセス タイプの使用を追跡するためのタイプ。リソース フィルターでは使用しないでください。
License.ProfessionalAccessGroup	プロフェッショナル アクセス タイプの自動割り当てに使用されるルールのリソース。
License.ProfessionalAccessType	プロフェッショナル アクセスのタイプ。ユーザー (名前付き) に手動でアクセス権を割り当てるための CRUD。
License.ProfessionalAccessUsage	プロフェッショナル アクセス タイプの使用状況を追跡するためのタイプ。リソース フィルターでは使用しないでください。

リソース フィルター	フィルターのターゲット
License.UserAccessGroup	ユーザー アクセス タイプの自動割り当てに使用されるルールのリソース。
License.UserAccessType	ユーザー アクセスのタイプ。ユーザー(名前付き) アクセス権に手動でトークンを割り当てるための CRUD。
License.UserAccessUsage	ユーザー アクセス タイプの使用を追跡するためのタイプ。リソース フィルターでは使用しないでください。
TermsAcceptance	QMC での利用規約ページにアクセスするためのリソース。

ノードまたはサービス関連のリソース

これらのフィルターは、QMC の関連したセクションにある個別のエントリを参照します。

ノード/サービス フィルター

リソース フィルター	フィルターのターゲット
Certificates	Certificates リソース
Deployment	Deployment リソース
EngineService	EngineService リソース
IdentityProviderSettings	IdentityProviderSettings リソース
LoadbalancingSelectList	LoadbalancingSelectList リソース
OdagService	OdagService リソース
PrintingService	PrintingService リソース
ProxyService	ProxyService リソース
RepositoryService	RepositoryService リソース
SchedulerService	SchedulerService リソース
ServerNodeConfiguration	ServerNodeConfiguration リソース
ServiceCluster	ServiceCluster リソース
ServiceStatus	ServiceStatus リソース
VirtualProxyConfig	VirtualProxyConfig リソース

その他のリソース

これらのフィルターは、QMC の関連したセクションにある個別のエントリを参照します。

その他のフィルター

リソース フィルター	フィルターのターゲット
AnalyticConnection	AnalyticConnection リソース
CustomPropertyDefinition	CustomPropertyDefinition リソース

リソース フィルター	フィルターのターゲット
DataConnection	DataConnection リソース
FileExtension	FileExtension リソース
FileExtensionWhiteList	FileExtensionWhiteList リソース
OdagLink	OdagLink リソース
OdagLinkUsage	OdagLinkUsage リソース
OdagRequest	OdagRequest リソース
Stream	Stream リソース
SystemRule	SystemRule リソース
Tag	Tag リソース
User	User リソース
UserDirectory	UserDirectory リソース

利用可能なリソース条件

次のテーブルは利用可能なリソース条件のリストです。

このリストにはすべて表示されているわけではなく、よく使用されるリソース条件の例のみを表示しています。

基本設定

基本プロパティの説明と例

プロパティ	説明	例
resource.@<customproperty>	リソースに関連付けられているカスタム プロパティ。この例では、@Department はカスタム プロパティ名です。	`resource.@Department = Finance`。 `resource.@Department = user.userDirectory`
resource.name	リソース名。	`resource.name like "*US*"`。「US」を含む文字列が条件に一致します。
resource.id	リソースの ID。	`resource.id=5dd0dc16-96fd-4bd0-9a84-62721f0db427`。この場合のリソースはアプリです。

リソース ユーザーとオブジェクトの所有者

リソース ユーザーとオブジェクトの所有者 のプロパティ

プロパティ	説明	例
user.email owner.email	ユーザーの メール。 所有者の メール。	`user.email="user@domain.com"` `owner.email="owner@domain.com"`
user.environment.browser	ブラウザのセッション ベースの属性。「=」ではなく「like」演算子を使用します。ブラウザ データは、「Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0」のように、バージョンとその他の詳細を含む形式で送信されるためです。代わりに「=」演算子を使用することはできますが、その場合は値全体を指定する必要があります。	`user.environment.browser like "*Firefox*"`
user.environment.context	コンテキストのセッション ベースの属性。(QMC にはコンテキスト用の個別の設定があります)。	`user.environment.context="Management Access"`
user.environment.device	デバイスのセッション ベースの属性。	`user.environment.device="iPhone"`
user.environment.ip	IP アドレスのセッション ベースの属性。	*セキュリティルールの例: IP アドレス別のストリーム アクセス権 (page 613)*
user.environment.os	オペレーティング システムのセッション ベースの属性。	`user.environment.os like "Windows*"`
user.environment.secureRequest	secureRequest のセッション ベースの属性。値 true - SSL が使用される場合。それ以外の場合は false。	`user.environment.secureRequest="true"`

プロパティ	説明	例
user.environment.[SAML attribute]	認証時に入力されたセッションベースの属性 (user.environment.group など)。	`user.environment.xxx="<attribute name>"`
user.environment.[ticket attribute]	認証時に入力されたセッションベースの属性 (user.environment.group など)。	`user.environment.xxx="<attribute name>"`
user.environment.[session attribute]	認証時に入力されたセッションベースの属性 (user.environment.group など)。	`user.environment.xxx="<attribute name>"`

user.group
owner.group
	ユーザーが属するグループ。
	所有者が属するグループ。
		`user.group=resource.app.stream.@AdminGroup`
		
		`owner.group=@Developers`

user.userdirectory
owner.userdirectory
	ユーザーが属するユーザーディレクトリ。
	所有者が属するユーザーディレクトリ。
		`user.userdirectory="Employees"`
		
		`owner.userdirectory="Employees"`

user.userId
owner.userId
	ユーザーの ID。
	所有者の ID。
		`user.userId="<userID>"`
		
		`owner.userId="<ownerID>"`

user.roles
owner.roles
	ユーザーのロール。
	所有者のロール。
		`user.roles="AuditAdmin"`
		
		`owner.roles="SystemAdmin"`

*user.environment 条件を使用するには、仮想プロキシ内の [**仮想セキュリティ環境**] を有効にする必要があります。*

参照先: 仮想プロキシ (page 157)

リソース アプリ

リソース アプリのプロパティ

プロパティ	説明	例
stream.name	アプリの公開先のストリームの名前。	`stream.name="Finance"`

app.object リソース

app.object リソースのプロパティ

プロパティ	説明	例
app.stream.name	アプリオブジェクトの公開先のストリームの名前。	`app.stream.name="Test"`
app.name	オブジェクトが属するアプリの名前。	`app.name="Q3_Report"`
approved	そのオブジェクトが、アプリの公開時のオリジナルアプリの一部であったかどうかを示すインジケーター。値: true または false。	`resource.approved="true"`
description	オブジェクトの説明。	`resource.description="old"`
objectType	考えられる値: • app_appscript • bookmark • dimension • embeddedsnapshot • genericvariableentry • hiddenbookmark • loadmodel • masterobject • measure • odagapplink • sheet • snapshot • story	`resource.objectType="sheet"`
published	オブジェクトが公開されているかどうかを示すインジケーター。値: true または false。	`resource.published="false"`

app.content や reloadtask などのアプリ関連のリソース

app.content や reloadtask などのアプリ関連リソースのプロパティ

プロパティ	説明	例
app.stream.name	アプリの公開先のストリームの名前。	`app.stream.name="Test"`
app.name	アプリの名前。	`app.name="Q3_Report"`

リソース DataConnection

リソース DataConnection のプロパティ

プロパティ	説明	例
Type	データ接続のタイプ。 考えられる値: • OLEDB • ODBC • フォルダ • Internet • カスタム (すべてのカスタム コネクター向け)	`resource.type!="folder"`

SystemRule リソース

SystemRule リソースのプロパティ

プロパティ	説明	例
Category	システム ルール カテゴリ。 考えられる値: • セキュリティ • ライセンス • 同期	`resource.category="license"`
ResourceFilter	ルールのリソース フィルター。	`resource.resourcefilter matches "DataConnection_\w{8}-\w{4}-\w{4}-\w{4}-\w{12}"`
RuleContext	ルールのコンテキスト。 考えられる値: • BothQlikSenseAndQMC • QlikSenseOnly • QMCOnly	`resource.rulecontext="BothQlikSenseAndQMC"`
Type	ルールのタイプ。 考えられる値: • 初期設定 • Read only (読み取り専用) • Custom (カスタム)	`resource.type!="custom"`

ContentLibrary リソース

ContentLibrary リソースのプロパティ

プロパティ	説明	例
Type	考えられる値: • media	`resource.type="media"`

ServerNodeConfiguration リソース

ServerNodeConfiguration リソースのプロパティ

プロパティ	説明	例
IsCentral	セントラル ノードのインジケーター。値: true または false。	`resource.iscentral="true"`
nodePurpose	ノードの目的。development または production。	`resource.nodepurpose="production"`

UserDirectory リソース

UserDirectory リソースのプロパティ

プロパティ	説明	例
userDirectoryName	ユーザー ディレクトリの名前。	`resource.userDirectoryname="Employees"`

UserSyncTask リソース

UserSyncTask リソースのプロパティ

プロパティ	説明	例
userDirectory.name	ユーザー ディレクトリ コネクタの名前。	`resource.userDirectory.name="Employees"`
userDirectory.userDirectoryName	ユーザー ディレクトリの名前。	`userDirectory.userdirectoryname="Employees"`

Widget リソース

Widget リソースのプロパティ

プロパティ	説明	例
library.name	そのウィジェットが属するライブラリの名前。	`resource.library.name="Dev"`

*一部のリソース(environment.browser など) では、プロキシ設定で [**拡張セキュリティ環境**] を選択する必要があります。*

演算子と条件の関数

QMC には予め定義されている関数が複数含まれており、対象リソースからプロパティ値を返すために使用できます。

論理演算子の適用順位付け

1 つ以上の論理演算子が条件内で使用されている場合は、NOT がまず評価され、その次に AND、最後に OR が評価されます。s 丸括弧を使えば、必要でない場合であっても条件が読みやすくなり、演算子の適用順位付けができるため間違いのリスクを減らすことができます。

A OR B AND C は Qlik Sense セキュリティルールでどのように解釈されますか。

A OR (B AND C)として解釈されます。

AND

この演算子は 2 つの数式を比較して、両者とも「True」の場合にのみ、「True」を返します。

構文:

```
(EXPRESSION) && (EXPRESSION)
(EXPRESSION) and (EXPRESSION)
```

例と結果:

AND 演算子の例と結果

例	結果
`(resource.@org = "UK") && (user.name = "John Doe")`	双方の式が「True」の場合にのみ「True」になります。
`(resource.@org = "UK") and (user.name = "John Doe")`	前と同じですが「&&」の代わりに「and」を使用します。

EQUAL

この演算子では、大文字と小文字が区別されません。比較対象の数式と等しい場合は True を返します。リストが使用される場合、1 つの値だけが一致する必要があります。

構文:

```
(EXPRESSION) = (EXPRESSION)
```

例と結果:

EQUAL 演算子の例と結果

例	結果
アクセス リクエストで@orgがukの場合。	`resource.@org = "UK"`は「True」になります。演算子では大文字と小文字が区別されないためです。
アクセス リクエストで@orgがUKの場合。	`resource.@org = "UK"` は「True」になります。
アクセス リクエストで@orgがUnited Kingdomの場合。	`resource.@org = "UK"` は「False」になります。
アクセス リクエストでresource@groupがSalesで、user.groupがSalesを含む場合。	`resource.@group = "Sales"`は「True」になります。user.groupがSalesを含むためです。

LIKE

セキュリティルールは、正規表現の演算子「like」をサポートしています。この比較演算子は、大文字と小文字は区別されません。

構文:

```
(EXPRESSION) like (EXPRESSION)
```

例と結果:

LIKE 演算子の例と結果

例	結果
`resource.name like "mya*"`	大文字か小文字かにかかわらず、「*mya*」で始まる名前のすべてのリソースは「True」になります。 *例には、[**詳細設定**] セクションの[**条件**] ボックスに表示される構文が示されています。引用符は検索文字列として認識されますが、検索文字列として認識されるべきではない場合が多いため、[**基本**] セクションでは引用符を使用しないでください。[基本] セクションに表示されるべき検索文字列は次のとおりです: `mya*`。*

ルール評価のパフォーマンスに悪影響を及ぼす可能性があるため、可能であれば、like 演算子の使用は避けてください。

NOT

この演算子は数式のブール値を反転し、数式が「False」の場合は「True」を返し、数式が「True」の場合は「False」を返します。

構文:

```
!(EXPRESSION)
```

例と結果:

NOT 演算子の例と結果

例	結果
アクセス リクエストで@orgがUKの場合	`!(resource.@org = "UK")` は「True」になります。
アクセス リクエストで@orgがUSの場合	`!(resource.@org = "UK")` は「True」になります。

MATCHES

セキュリティルール エディタは、正規表現の演算子「matches」をサポートしています。この演算子は大文字と小文字を区別しないので、大文字か小文字かにかかわらず表現に合致した結果を返します。Regex の開始および終了アンカーは暗黙的に追加されます。

構文:

```
(EXPRESSION) matches (EXPRESSION)
```

例と結果:

MATCHES 演算子の例と結果

例	結果
`resource.name matches ".*yAp.*"`	大文字か小文字かにかかわらず、名前に「*yap*」が含まれるすべてのリソースは「True」になります。
`resource.resourcefilter matches "Stream_\\w{8}-\\w{4}-\\w{4}-\\w{4}-\\w{12}"`	アクセス リクエストのリソース フィルターが適正な書式になっていれば「True」になります。

NOT EQUAL

この演算子では、大文字と小文字が区別されません。比較対象の数式と等しくない場合は True を返します。リストが使用される場合、1 つの値だけが一致する必要はありません。

構文:

```
(EXPRESSION) != (EXPRESSION)
```

例と結果:

NOT EQUAL 演算子の例と結果

例	結果
アクセス リクエストで@orgがukの場合	`resource.@org != "UK"`は「False」になります。演算子では大文字と小文字が区別されないためです。
アクセス リクエストで@orgがUKの場合	`resource.@org != "UK"` は「False」になります。
アクセス リクエストで@orgがUnited Kingdomの場合	`resource.@org != "UK"` は「True」になります。
アクセス リクエストでresource@groupがSalesで、user.groupがSalesを含む場合。	`resource.@group != "Sales"`は「False」になります。user.groupがSalesを含むためです。

OR

この演算子は 2 つの数式を比較して、一方あるいは両方の数式が「True」の場合に「True」を返します。

構文:

```
(EXPRESSION) || (EXPRESSION)
(EXPRESSION) or (EXPRESSION)
```

例と結果:

OR 演算子の例と結果

例	結果
`(resource.@org = "UK") || (resource.@org = "US")`	いずれかの式が「True」の場合にのみ「True」になります。
`(resource.@org = "UK") or (resource.@org = "US")`	上記と同じですが「||」の代わりに「or」を使用します。

STRICT EQUAL

この演算子では、大文字と小文字の区別がなされます。比較対象の数式と完全に等しくなる場合は True を返します。値が使用されている数式がリストに存在する場合、完全なリストは必ずしも一致しません。

構文:

```
(EXPRESSION) == (EXPRESSION)
```

例と結果:

STRICT EQUAL 演算子の例と結果

例	結果
アクセス リクエストで@orgがunited Statesの場合	は「False」になります。演算子では大文字と小文字が区別されるためです。resource.@org == "United States"
アクセス リクエストで@orgがUnited Statesの場合	`resource.@org == "United States"` は「True」になります。
アクセス リクエストで@orgがUSの場合	`resource.@org == "United States"` は「False」になります。

STRICT NOT EQUAL

この演算子では、大文字と小文字の区別がなされます。比較対象の数式と等しくない場合は True を返します。値が使用されている数式がリストに存在する場合、完全なリストは必ずしも一致しません。

構文:

```
(EXPRESSION) !== (EXPRESSION)
```

例と結果:

STRICT NOT EQUAL 演算子の例と結果

例	結果
アクセス リクエストで@orgがunited statesの場合	は「True」になります。演算子では大文字と小文字が区別されるためです。resource.org !== "United States"
アクセス リクエストで@orgがUnited Statesの場合	`resource.org !== "United States"` は「False」になります。
アクセス リクエストで@orgがUSの場合	`resource.org !== "United States"` は「True」になります。

HasPrivilege

要求しているユーザーが対象となるリソース (複数可) に指定されたアクセス権を有する場合に「True」を返すリソース条件のブール型機能。その他の場合は「False」を返します。

構文:

```
resource.HasPrivilege("アクション")
```

プロパティ:

構文プロパティ

プロパティ	説明
アクション	必須。アクセス権の評価を希望するアクションです。

例と結果

例と結果

例	結果
リソース フィルター: * **条件:** resource.resourcetype = "App" and resource.Stream.HasPrivilege ("read") **アクション:** read	ユーザーにリソースの公開先のストリームの読み取り権限がある場合、アプリの読み取りアクセス権が与えられます。

IsAnonymous

アクセスを要求しているユーザーが匿名でログインしている場合に「True」を返すユーザー条件のブール型機能。その他の場合は「False」を返します。

構文:

```
user.IsAnonymous()
```

例と結果

例と結果

例	結果
リソース フィルター: Stream_* **条件:** user.IsAnonymous() **アクション:** read	匿名ユーザーはストリームの読み取りを許可されます。
リソース フィルター: Stream_* **条件:** !user.IsAnonymous() **アクション:** read, publish	匿名でないユーザー(条件の前にNOT演算子「!」が付いたもの)は全員、ストリームを読み取って公開することができます。匿名でないユーザー(条件の前にNOT演算子「!」が付いたもの)は全員、ストリームを読み取って公開することができます。匿名ユーザーはストリームにアクセスできません。

空

指定リソースに接続がない(値がない)場合に「True」を返すリソース条件のブール関数。その他の場合は「False」を返します。

構文:

```
resource.resourcetype.Empty()
```

例と結果

例と結果

例	結果
リソース フィルター: App_* **条件:** resource.stream.Empty() **アクション:** update	このルールでは、アプリがストリームに接続 (公開) されていない場合には、ユーザーがアプリを更新できます。
リソース フィルター: App.Sheet_* **条件:** resource.app.stream.Empty() **アクション:** update	このルールでは、シートが属するアプリがストリームに公開されていない場合には、ユーザーがシートを更新できます。

IsOwned

指定リソースに所有者がいる場合に「True」を返す [**リソース条件**] のブール型機能。その他の場合は「False」を返します。

構文:

```
resource.IsOwned()
```

例と結果

例と結果

例	結果
リソース フィルター: * **条件:** resource.IsOwned() and resource.owner = user **アクション:** read, export, publish	リソースの所有者は自分のリソースの読み取り、エクスポート、公開を実行できなくてはなりません。この条件は、リソースが所有されなくてはならないこと、また、所有者がルールの適用を要請しているユーザーでなくてはならないことを指定します。 *これは、OwnerNonModificationActions ルール (QMC とともに提供されているカスタム ルール) の定義です。リソースがストリームに公開されていない場合、リソース所有者にあらゆるアクションを提供する所有者ルールを補完します。*

セキュリティルールの編集

更新権限を有するセキュリティルールを編集できます。Qlik Sense が提供する既定のルールを編集する場合、ルールのタイプの定義は [**既定**] から [**カスタム**] に変更されます。既定のルールを変更したり、既定のルールに影響が及ぶ新しいルールを追加したりすると、Qlik Sense において予期せぬ動作を引き起こす場合があります。既

定のルールに変更を加える前に、ルールのプレビュー機能を使用して、ルールの動作を確認してください。Qlik Sense を新しいバージョンにアップグレードする場合は、読み取り専用ルールおよび既定のルールのみが自動で更新されることに、注意してください。

ユーザーがストリーム内の公開されたアプリを編集できるようなルールを作成することは推奨されません。

ストリームやデータ接続といった一部のリソースタイプでは、セキュリティルール セクションにアクセスすることなく、関連するルールを直接編集したり、作成することができます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**セキュリティルール**] を選択します。
3. 編集したい規則を選択します。
4. アクション バーで [**編集**] をクリックします。
   左側に編集パネル (すべてのプロパティを保持)、右側に監査ページが配置された分割ページが表示されます。

   [基本] セクションの [リソース フィルター] テキスト ボックスの横にある矢印をクリックしてポップオーバーを開き、フィルターに複数のリソースを選択できます。
5. [**プレビュー**] をクリックすると、現在定義されている監査グリッド内のルールのアクセス権が表示されます。
6. [**適用**] をクリックして、編集したルールを保存します。
   ページの最下部に [**更新完了**] と表示されます。

クライアントで複数のタブを開いている場合、セキュリティルールへの更新はすぐには有効になりません。その場合は、ログアウトしてから再度ログインします。開いているタブが 1 つのみの場合、更新するだけで十分です。

セキュリティルールの削除

削除権限を有するセキュリティルールを削除できます。

リソースが削除されると、そのリソースに関連付けられている負荷分散ルールとセキュリティルールはすべて自動的に削除されます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**セキュリティ ルール**] を選択します。
3. 削除するルールを選択します。
4. アクション バーの [**Delete**] をクリックします。
   [**Delete**] ダイアログが表示されます。
5. [**OK**] をクリックします。

セキュリティルールの評価

ユーザーがリソースへのアクセスを要求するたびに、Qlik Sense は Qlik Sense システムでセキュリティルールに照らし合わせてその要求を評価します。少なくとも 1 つのルールが「True」と評価されると、Qlik Sense はセキュリティルールで説明されている条件とアクションに従ってユーザーにアクセス権を与えます。ルールの評価で「True」という結果が出なければ、ユーザーはアクセスを拒否されます。Qlik Sense セキュリティルールはプロパティに基づいているため、Qlik Sense は非常に拡張性に優れており、ユーザーのグループに適用されるプロパティに基づいてルールを構築できます。

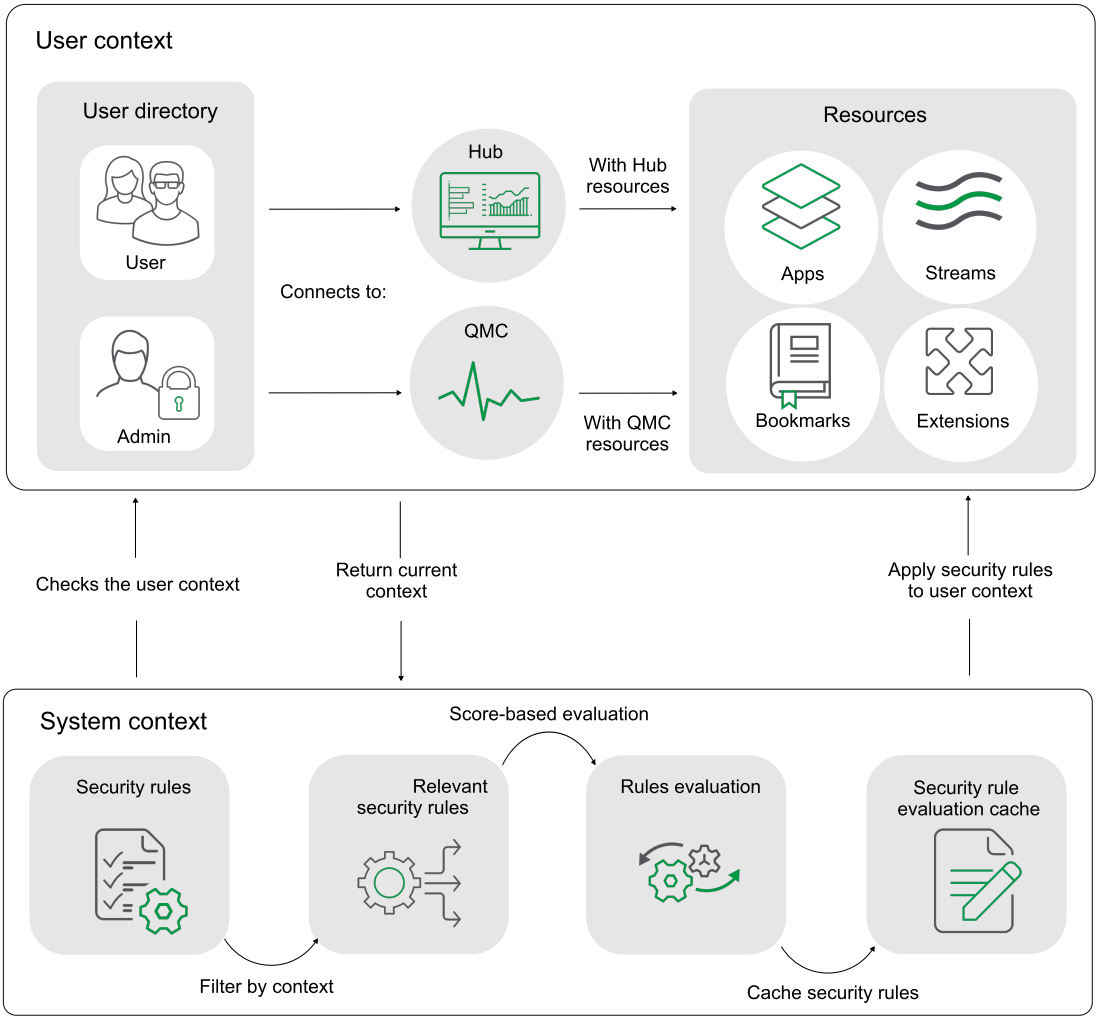
このようにセキュリティルール評価には包括的な方法を採用しており、Qlik Sense でリソースのセキュリティを設計する際は以下の原則を念頭におく必要があります:

- 当該リソースの少なくとも 1 つのルールに、アクセスをリクエストしているユーザーのアクセス権が含まれている場合は、アクセスが提供されます。
- 明示的にユーザーを除外するルールを作成する必要はありません。
- ルールを作成する際は、なるべくユーザーのロール、ユーザー タイプ、グループのプロパティを使用します。

その後、ルールのプレビューおよび監査ツールを使用して、ルールが実際に機能することを確認・検証できます。

評価フロー

次の画像は、ユーザーが Qlik Sense のハブにアクセスした場合のセキュリティルールの評価方法を示しています。ルール評価の手順、およびルールがパフォーマンスに与える影響の詳細については、ブログ記事「セキュリティルールと Qlik Sense のパフォーマンス」を参照してください。また、ここでキャッシュの無効化についても説明します。



セキュリティルールの例

セキュリティルール作成の一般的な例を次に示します。

Example 1: ユーザーにアクセス権を提供するには 1 つのルールのみが必要です

財務部は財務結果を*四半期業績*と呼ばれるストリームに公開します。まず、財務部のユーザーのみがこのストリームを読み取ることができるようにします。この場合は、*四半期業績*ストリームの読み取りアクションを提供する財務部ユーザー向けのセキュリティルールのみを作成する必要があります。

このセキュリティルールを作成する最も簡単な方法は、QMC で [**ストリーム**] 概要に進み、[**Associated items**] の [**System rules**] で、リストからストリームを選択して [**Edit**] をクリックし、ユーザーの [**Read**] 条件をストリームに追加することです。既存のルールを編集することも、ユーザーの [**Read**] 条件を含むルールを新規で作成することもできます。条件には、ディレクトリサービスからいずれかのグループプロパティを使用するとよいでしょう。利用可能な場合、ディレクトリサービスのグループプロパティプロパティは、[**基本**] ビューのドロップダウンメニューに表示されます。ディレクトリサービスに適切なグループプロパティが含まれていない場合は、QMC でカスタムプロパティを作成できます (たとえば、値が [**財務**] の [**部署**] プロパティ)。

Example 2: 複数のルールがユーザーに適用される場合

*四半期業績*の例では、Active Directory グループ「財務」に属するユーザーが四半期業績ストリームを読み取れるようにするルール (ルール 1) を作成しました。別のルール (ルール 2) でも、Active Directory (AD) グループ「経営陣」に属するユーザーが四半期業績ストリームに読み取りアクセス権を付与すると想定します。

最後に、Active Directory グループ「営業」と「経営陣」の双方に営業部長が属していると想定します。

セキュリティルールの例 2

-	ルール 1	ルール 2
ユーザーは以下が可能	読み取り	読み取り
対象リソース	四半期結果ストリーム	四半期結果 ストリーム
前提	group=Finance	group=Management
評価結果	FALSE	True
結果的に営業部長が得たアクセス権	読み取りアクセス権の提供	

Example 3: 複数のルールに異なるアクセス権がある場合

四半期業績の例では、Active Directory グループ「財務」に属するユーザーが四半期業績ストリームを読み取れるようにするルール (ルール 1) を作成しました。別のルール (ルール 2) でも、Active Directory (AD) グループ「経営陣」に属するユーザーが四半期業績ストリームに読み取りアクセス権を提供すると想定します。最後に、ルール 3 では、「経営陣」ユーザーが読み取りアクセス権のあるストリームでアプリを更新できます。

Active Directoy グループ「営業」と「経営陣」の双方に営業ディレクターが属していると想定します。

セキュリティルールの例 3

-	ルール 1	ルール 2	ルール 3
ユーザーは以下が可能	読み取り	読み取り	更新プログラム
対象リソース	四半期結果ストリーム	四半期結果ストリーム	ユーザーがストリームの読み取りアクセス権を持っている場合はすべてのアプリとシート
前提	group=Finance	group=Management	group=Management
評価結果	FALSE	True	True
結果的に営業部長が得たアクセス権	読み取りおよび更新アクセス権を提供		

Example 4: すぐに利用できる Qlik Sense ルール

英国の財務オフィスが、英国四半期報告書と呼ばれるアプリを四半期結果 ストリームに公開しました。このアプリで読み取りアクセス権のあるユーザーは英国オフィスの財務ユーザーのみにしたいと考えています。この目的で、英国の管理者はルール 3 を作成し、AD グループ「財務」と英国オフィスに属するユーザーのみに読み取りアクセス権があると明示的に規定します。また、例 1 のルール 2 や、すぐに利用できるストリーム ルールもあると想定します。

この場合、英国の財務は、営業部長が英国四半期報告書アプリを読み取れないものと想定している可能性があります。ただし、ルール 2 では経営陣が四半期報告書ストリームを読み取ることができ、ストリーム ルールでは四半期報告書に読み取りアクセスのあるユーザー全員がこのストリームのあらゆるアプリを読み取れるため、これは「True」ではありません。

セキュリティルールの例 4

-	ルール 2	ルール 3	ストリーム ルール
ユーザーは以下が可能	読み取り	読み取り	読み取り
対象リソース	四半期報告書ストリーム	四半期報告書ストリームで公開された英国の四半期報告書アプリ	ストリームのすべてのアプリとシート
前提	group=Management	group=Finance AND office=UK	ユーザーはストリームの読み取りアクセスがあります
評価結果	True	FALSE	True
結果的に営業部長が得たアクセス権	読み取りアクセス権の提供		

重複しているルール

ルールを作成していくと、最終的には重複するルールが存在するようになります。つまり、2 つ以上のルールに規定されている条件が同じユーザー (複数可) を対象にすることがあります。ルールが重複する場合はアクセス権を提供するルールが優先されます。

Qlik Senseは順番に各ルールを評価します。1 つのルールであるタイプのアクセス権が与えられる場合、Qlik Senseはそのアクセス権を付与します。

2 つのルールが重複する場合、通常は以下のタイプの重複が起こります:

- 同一
  双方のルールがユーザーに読み取りアクセス権を提供します。この場合は読み取りアクセス権が提供されます。

- 補足
  1 つのルールで読み取りを提供し、もう片方のルールでは更新を提供します。この場合、ユーザーには読み取りと更新の双方のアクセス権が提供されます。

QMC の監査ページでは、リソースに適用されるユーザー セキュリティルールを確認できます。

監査 (page 72)

ルールの効果もプレビューできます。

セキュリティルールの編集 (page 594)

Example 1:

例えば、「*条件のうちひとつのプロパティ値ペア: (page 520)*」では、Active Directory グループ「Finance」に属するユーザーが四半期業績ストリームを読み取れるようにするルール (ルール 1) を作成しました。別のルール (ルール 2) でも、Active Directory (AD) グループ「経営陣」に属するユーザーが四半期業績ストリームに読み取りアクセス権を付与すると想定します。

最後に、Active Directory グループ「営業」と「経営陣」の双方に営業部長が属していると想定します。

ルールの結果

結果	**ルール 1**	**ルール 2**
ユーザーは以下が可能	読み取り	読み取り
対象リソース	四半期報告書ストリーム	四半期報告書ストリーム
前提	group=Finance	group=Management
評価結果	FALSE	TRUE
結果的に営業部長が得たアクセス権	読み取りアクセス権の提供	読み取りアクセス権の提供

Example 2:

英国の財務オフィスが、英国四半期見通しと呼ばれるアプリを四半期報告書ストリームに公開しました。このアプリで読み取りアクセス権のあるユーザーは英国オフィスの財務ユーザーのみにしたいと考えています。この目的で、英国の管理者はルール 3 を作成し、AD グループ「財務」と英国オフィスに属するユーザーのみに読み取りアクセス権があると明示的に規定します。また、例 1 のルール 2 や、すぐに利用できるストリーム ルールもあると想定します。

この場合、英国の財務は、営業部長が英国四半期報告書アプリを読み取れないものと想定している可能性があります。ただし、ルール 2 では経営陣が四半期報告書ストリームを読み取ることができ、ストリーム ルールではこのストリームに読み取りアクセスのあるユーザー全員がこのストリームのあらゆるアプリを読み取れるため、これは「True」ではありません。

ルールの結果

結果	ルール 3	ルール 2	ストリーム ルール
ユーザーは以下が可能	読み取り	読み取り	読み取り
対象リソース	四半期報告書ストリームで公開された英国の四半期報告書	四半期報告書ストリーム	ストリームのすべてのアプリとシート
前提	group=Finance AND office=UK	group=Management	ユーザーはストリームの読み取りアクセスがあります
評価結果	FALSE	TRUE	TRUE
結果的に営業部長が得たアクセス権	読み取りアクセス権の提供	読み取りアクセス権の提供	読み取りアクセス権の提供

セキュリティルールの例

以下の例では、幾つかのシナリオでのセキュリティルールの使い方と書き方を示します。

セキュリティルールの例: カスタム管理者 ロールの作成 (page 601)

セキュリティルールの例: ユーザー タイプ別 Qlik Sense アクセス権の適用 (page 606)

セキュリティルールの例:QMC アプリ管理者の作成によって文書管理者を再作成する(page 609)

セキュリティルールの例: ユーザー属性別のストリーム アクセス権 (page 612)

セキュリティルールの例: IP アドレス別のストリーム アクセス権 (page 613)

セキュリティルールの例: ユーザー属性別のアプリへの Qlik Sense Mobile Client Managed オフライン アクセス権 (page 615)

セキュリティルールの例: ある顧客のケース(page 616)

セキュリティルールの例: カスタム管理者 ロールの作成

Qlik Sense には、デフォルトの管理者 ロールが 6 つ設定されています。カスタム管理者 ロールを作成する場合は、セキュリティルールをいくつか定義する必要があります。この例では、ストリーム、アプリ、アプリオブジェクト、およびリロード タスクを管理するカスタム管理者 ロールを作成します。

次のセキュリティルールが必要です。

- 必要なリソースへのアクセスを可能にするルール。
- QMC での必要なセクションへのアクセス権を管理者に付与するための QMC セクション アクセス ルール。

特定のユーザーに対するセキュリティルールを作成するのではなく、汎用管理者 ロールを作成することにより、ルールを再利用可能にします。カスタム管理者 ロールは、いずれのセキュリティルールも変更することなく、数人のユーザーに割り当てることができます。

リソース ルール

リソース ルールを作成することにより、1 人以上のユーザーに同じ管理者アクセス権を付与することができます。

次の手順を実行します。

1. [**セキュリティ ルール**] を選択して新規作成
2. [**名前**] フィールドに、「*CustomAdmin*」と入力します。
3. ストリーム、アプリ、アプリオブジェクト (シートやストーリーなど)、およびタスクをフィルターするためのリソース フィルターを設定します。
   [**基本**] セクションで、[**リソース フィルター**] フィールドに次のように入力します。
   `Stream_*, App_*, App.Object_*, ReloadTask_*`
4. 指定されたリソース向けにルールが提供すべきアクションを設定します。
   [**基本**] セクションで、次のようにして [**アクション**] を選択します。
   作成、読み取り、更新、削除、エクスポート、公開、データのエクスポート
5. ユーザーの役割を指定するための条件を設定します。
   [**拡張**] セクションで、[**条件**] 項目に次のように入力します。
   `user.roles = "CustomAdmin"`
6. [**適用**] をクリックします。
7. カスタム管理者となるユーザーにその役割を割り当てます。
   QMC スタート ページ、[**ユーザー**] の順に進みます。
8. ユーザーを選択して、[**編集**] をクリックします。
9. [管理者 ロール] で をクリックし、`CustomAdmin` を選択します。
10. [**適用**] をクリックします。

以下の表に、ユーザーの役割 CustomAdmin のセキュリティ ルールの項目をまとめます。

セキュリティルールの項目

項目	コード	コメント
リソース フィルター	`Stream_*, App_*, App.Object_*, ReloadTask_*`	リソース タイプ `Stream`、`App`、`AppObjects`、および `ReloadTasks` のフィルタリングを行います。 *また、`App_*, App.Object_*` の代わりに`App*` と書くこともできます。下線 (_) のないワイルドカード(*) では `App` で始まるすべてのリソースタイプが対象になるためです。*
アクション	作成、読み取り、更新、削除、エクスポート、公開、データのエクスポート	条件を満たす場合には、これらのアクションが許可されます。
条件	`user.roles = "CustomAdmin"`	ユーザーの役割 `CustomAdmin`は、[**ユーザー**] > [**役割**] で選択できます。

QMC セクション アクセス

コンテンツを管理するため、管理者には、QMC の関連セクションに対するセクション アクセス権が必要です。

次の手順を実行します。

1. [**セキュリティルール**] を選択して新規作成
2. [**名前**] フィールドに、「*QMC_Sections_CustomAdmin*」と入力します。
3. リソース フィルターを設定して、*CustomAdmin* がアクセスする必要のある QMC のセクションをフィルターします。
   [**基本**] セクションで、[**リソース フィルター**] フィールドに次のように入力します。
   `License_*,QmcSection_Stream,QmcSection_App,QmcSection_App.Object,QmcSection_Task`
4. 指定されたリソース向けにルールが提供すべきアクションを設定します。
   [**基本**] セクションで、次のようにして [**アクション**] を選択します。
   読み取り
5. ユーザーの役割を指定するための条件を設定します。
   [**拡張**] セクションで、[**条件**] フィールドに次のように入力します。
   `user.roles = "CustomAdmin"`
6. ルールのコンテキストを設定します。

[**拡張**] セクションの [**コンテキスト**] フィールドで、[**QMCでのみ**] を選択します。

7. [**適用**] をクリックします。

以下の表に、*QMC_Sections_CustomAdmin* のセキュリティルールをまとめます。

セキュリティルールのプロパティ

項目	コード	コメント
リソース フィルター	`License_*,QmcSection_Stream,QmcSection_App,QmcSection_App.Object,QmcSection_Task`	QMC セクション アクセス ルールにより、QMC セクションへの読み取りアクセス権のみが付与されます。
アクション	読み取り	条件を満たす場合にはそのアクションが許可されます。
条件	`user.roles = "CustomAdmin"`	管理者 ロール `CustomAdmin` のユーザーには、これらのセクションへのアクセス権が付与されます。
コンテキスト	QMC 専用	このルールは、QMC に対してのみ適用されます。

セキュリティルールの例:QMC 組織管理者 ロールを作成する

この例では、以下を行うことで、部門のアクセス権の管理を体系化します。

- 各部門の管理者を作成する
- 各管理者に、その部門に属するユーザーが作成したコンテンツへの完全なアクセス権を与える

組織管理者 ロールを作成するには、新しいセキュリティルールを作成し、カスタム プロパティを使ってロールをアプリに接続する必要があります。

セキュリティルール

セキュリティルール	ルールの結果
DepartmentAdminQmcSections	管理者が QMC のどのセクションを表示できるかを制御します。
DepartmentAdminApp	管理者が管理できるリソースを制御します。

手順

次の手順を実行します。

1. 新しいカスタム プロパティを作成します。
   a. プロパティに「*Department*」と名前を付けます。
   b. [**リソース タイプ**] で、[**アプリ**]、[**タスクの リロード**]、[**ユーザー**] を選択します。
   c. [**新規作成**] をクリックして値「*Finance*」を入力します。
   d. [**値**] エリアの外側をクリックします。

e. [**新規作成**] をクリックして値「*Sales*」を入力します。
f. [**適用**] をクリックします。

2. 新しいセキュリティルール (*DepartmentAdminQmcSections* と *DepartmentAdminApp*) を作成します。
   a. Select **Security rules** and click 新規作成
   b. [**詳細設定**] セクションと[**基本設定**] セクションで、*セキュリティルール コード(page 605)* に基づいて、[**リソース フィルター**]、[**条件**]、[**アクション**]、[**コンテキスト**] を入力します。
3. 部門の管理者ユーザーにロールを適用します (追加するすべての管理者に対してこのステップを繰り返します)。
   a. [**ユーザー**] を選択してユーザーを選択し、[**終了**] をクリックします。
   b. データ マネージャーでテーブルの under **Admin roles** and select *DepartmentAdmin*.
   c. [**カスタム プロパティ**] で「*Department (部門)*」カスタム プロパティの値を選択します (*[Sales (販売)]* または *[Finance (財務)]*)。
   d. [**適用**] をクリックします。
4. 組織管理ユーザーが管理できるようにするアプリを選択します。
   a. QMC スタート ページ、[**アプリ**] の順に進み、アプリを選択して、[**編集**] をクリックします。
   b. 「*Department (部門)*」カスタム プロパティの値を選択します (*[Sales (販売)]* または *[Finance (財務)]*)。
   c. [**適用**] をクリックします。

これで、組織管理者ロールを作成し、割り当てしました。

セキュリティルール コード

以下に、この例のセキュリティルール コードと説明用のコメントを示します。

「DepartmentAdminQmcSections」のセキュリティルール コード

DepartmentAdminQmcSections のセキュリティルール コード情報

項目	コード	コメント
リソース フィルター	`QmcSection_Stream,QmcSection_App,QmcSection_App.Sheet, QmcSection_App.Story,QmcSection_Tag, QmcSection_Task, QmcSection_ReloadTask, QmcSection_Event, QmcSection_ SchemaEvent, QmcSection_CompositeEvent`	ストリーム、アプリ、シート、ストーリー、タグ、タスク、トリガーをフィルタリングします。
条件	`user.roles = "DepartmentAdmin"`	このルールは、ユーザー ロールが `DepartmentAdmin` に設定されているユーザー全員に適用されます。
アクション	`read`	条件が満たされると、読み取りアクションが与えられます。
コンテキスト	[**QMC専用**]	このルールは QMC を使用するときにのみ有効です。

「DepartmentAdminApp」のセキュリティルール コード

DepartmentAdminApp のセキュリティルール コード情報

項目	コード	コメント
リソース フィルター	`App*,ReloadTask_*,SchemaEvent_*,Tag_*,CompositeEvent_*`	アプリ、シート、ストーリー、タスク、タグ、トリガーをフィルタリングします。
条件	`user.roles="DepartmentAdmin" and resource.@Department=user.@Department and (resource.resourcetype="App" or (resource.resourcetype="ReloadTask" or resource.resourcetype="App.Object") or resource.resourcetype="SchemaEvent" or resource.resourcetype="CompositeEvent" or resource.resourcetype="Tag")`	このルールは、ユーザー ロールが `DepartmentAdmin` に設定されているユーザー全員に適用されます。
アクション	`create, read, update, delete, publish`	条件が満たされると、指定されたアクションが許可されます。
コンテキスト	[**QMC専用**]	このルールは QMC を使用するときにのみ有効です。

セキュリティルールの例: ユーザー タイプ別 Qlik Sense アクセス権の適用

この例では、ユーザー タイプに従ってアクセス権を設定します。開発部門には以下のユーザー タイプがあります。

- 開発者: アプリ、シート、ストーリー、オブジェクトを作成することができ、データ接続の使用と作成も可能です。
- 貢献者: 公開済みのアプリ向けにストーリーとシートを作成できますが、新しいアプリは作成できません。
- 消費者: コンテンツを使用できますが作成できません。

対応するアクセス権 のある以下の業務が識別されています:

業務アクセス権

業務	開発者	貢献者	消費者
アプリの追加	許可	許可なし	許可なし
アプリオブジェクトの作成	許可	許可	許可なし
データ接続を作成	許可	許可なし	許可なし

以下では、ユーザーが読み取りアクセスのあるストリームでアプリへの読み取りアクセスをユーザーに与えるためのすぐに利用できるルール ストリームがあるものと想定します。以下では、ユーザーが読み取りアクセスのあるストリームでアプリへの読み取りアクセスをユーザーに与えるためのすぐに利用できるルール ストリームがあるものと想定します。これにより消費者がアプリを読み取れるようになります。また、この例に従ってアクセス権 を設定する場合は、同梱のセキュリティルール を無効にする必要があります。CreateApp、CreateAppObjectsPublishedApp、CreateAppObjectsUnPublishedApp、および DataConnection です。

以下の主なステップでセキュリティルールを使用し、ユーザーのタイプに従ってアクセス権を設定します。

1. 個別のユーザーではなくユーザーの種類に規則を適用できるように各ユーザー タイプを定義します。
2. カスタム プロパティを適切なユーザーに適用します。

   また、対応するグループを含むユーザー ディレクトリを所有している場合は、カスタム プロパティの代わりにそのユーザー ディレクトリを利用することもできます。

3. 業務のタイプごとに 1 つのルールを作成します。

手順

次の手順を実行します。

1. カスタム プロパティの値として ユーザー タイプを定義します。
   a. 「UserType」という名前のカスタム プロパティを作成します。
   b. 作成したカスタム プロパティを、リソース タイプ [Users (ユーザー)] に適用します。
   c. カスタム プロパティの値を Developer、Contributor、Consumer として定義します。
   d. [**適用**] をクリックします。
2. 「UserType」カスタム プロパティを [**ユーザー**] ページで適切なユーザーに適用します。
3. 4 つの新しいセキュリティルール (CreateApp、CreateAppObjectsPublishedApp、CreateAppObjectsUnPublishedApp、DataConnection) を作成します。
   a. [**セキュリティルール**] を選択して [**新規作成**] をクリックします。
   b. [**Advanced**] セクションと [**Basic**] セクションで、[**Resource filter**]、[**Conditions**]、[**Actions**]、[**Context**] を入力します。
   "Create app" のセキュリティ コード(page 608)。
   c. 業務に対応するように [**名前**] を設定します。
   d. [**適用**] をクリックします。
4. 以下のセキュリティルールが無効または削除されていることを確認してください。
   a. **CreateApp**
   b. **CreateAppObjectsPublishedApp**
   c. **CreateAppObjectsUnPublishedApp**
   d. **DataConnection**

これでユーザーのタイプに従ってアクセス権を授与するルールが作成されました。

セキュリティルール コード

以下に、この例のセキュリティルール コードと説明用のコメントを示します。

"Create app" のセキュリティ コード

セキュリティルール コード項目

項目	コード	コメント
リソース フィルター	`App_*,FileReference_*`	特にリソース タイプ App のフィルタリングを行います。

条件	`!user.IsAnonymous() and (user.@usertype="Developer")`	`!user.IsAnonymous()`
		この条件では、ユーザーが匿名でログインしているかどうかの評価に使用できるセキュリティルール関数 **IsAnonymous()** が使用されます。この場合、ユーザーが匿名ユーザーとしてログインしていると、条件は満たされません。
		`(user.@usertype="Developer")`
		カスタム プロパティ`@usertype` が `Developer` に設定されているユーザ全員がこの条件を満たしています。
		また、対応するグループを含むユーザー ディレクトリを所有している場合は、カスタム プロパティの代わりにそのユーザー ディレクトリを利用することもできます。この場合、条件は `user.group="Developer"` のようになります。

[アクション]	`create`	条件が満たされると、指定されたアクションが許可されます。

「Create app object (アプリ オブジェクトの作成)」(シート、ストーリー、アプリ オブジェクト) のセキュリティ ルール コード

セキュリティルール コード項目

項目	コード	コメント
リソース フィルター	`App.Object_*`	特にリソース タイプ App.Object のフィルタリングを行います。

項目	コード	コメント
条件	resource.App.HasPrivilege ("read") and !user.IsAnonymous() and (user.@usertype=「開発者」or user.@usertype=「貢献者」)	resource.App.HasPrivilege("read") この条件では、セキュリティルールの **HasPrivilege()** 関数を使います。これはリソース タイプのアクセス権を評価する際に使用できます。 この例では、関数はリソース タイプ ユーザーがリソース シートでアクションの更新を実行できるかどうかを評価します。貢献者は、自分が所有しているシートのオブジェクトを作成することができます。
[アクション]	create	条件が満たされると、指定されたアクションが許可されます。

「データ接続」のセキュリティ コード

セキュリティルール コード項目

項目	コード	コメント
リソース フィルター	DataConnection_*	特に DataConnection リソース タイプのフィルタリングを行います。
条件	resource.resourcetype = "DataConnection" and (user.@usertype="Developer")	resource.resourcetype = "DataConnection" このルールは、DataConnection という種類のリソースに適用されます。 user.@usertype="Developer" このルールは、@usertype カスタム プロパティが「Developer」に設定されているユーザーに適用されます。
[アクション]	create	条件が満たされると、指定されたアクションが許可されます。

セキュリティルールの例:QMC アプリ管理者の作成によって文書管理者を再作成する

この例では、文書管理者を QlikView で再作成します。Qlik Sense次のいずれかを行って管理者を再作成できます。

- ロール (アプリ管理者) の新規作成
- このロールをアプリに接続するためのカスタム プロパティの作成

次のテーブルでは、アプリの管理者 ロールに対するセキュリティルールを示しています。

セキュリティルールとその結果

セキュリティルール	ルールの結果
AppAdminQmcSections	管理者が確認できる QMC のセクションを制御します。
AppAdminRead	管理者が読み取りできるリソースを制御します。
AppAdminModify	管理者が変更できるリソースを制御します。

変更と読み取りのアクセスを授与するルールは分割されます。こうすることで、アプリ管理者がアプリを操作するときに理解しておく必要のある重要な情報 (この例ではストリームの情報) を読み取り/表示 (変更なし) できるようになります。

手順

次の手順を実行します。

1. 3 つの新しいセキュリティルール (AppAdminQmcSections、AppAdminRead、AppAdminModify) を作成します:
    a. Select **Security rules** and click 新規作成
    b. [**Advanced**] セクションと[**Basic**] セクションで、*「AppAdminQmcSections」のセキュリティコード(page 611)*に基づいて、[**Resource filter**]、[**Conditions**]、[**Actions**]、[**Context**] を入力します。
    c. 業務に対応するように名前を設定します。
    d. [**適用**] をクリックします。
2. アプリ管理者にするユーザーにロールを適用します。
    a. [**ユーザー**] を選択してユーザーを選択し、[**終了**] をクリックします。
    b. データマネージャーでテーブルの under **Admin roles** and select *AppAdmin*.
    c. [**適用**] をクリックします。
3. 新しいカスタムプロパティを作成し、値としてユーザーを追加します。
    a. [**カスタム プロパティ**] を選択して、[**新規作成**] をクリックします。
    b. [**名前**] 項目に *AppAdmin* と入力します。
    c. [**リソース タイプ**] で、[**アプリ**] を選択します。
    d. **Values**, click **Create new**, add the **User ID** as a value and click **OK**.
    e. [**適用**] をクリックします。
4. このユーザーが管理できるようにするアプリを選択します。
    a. (複数のアプリを選択するには Ctrl キーを押しながらアプリをクリックして) [**アプリ**] を選択し、[**編集**] をクリックします。
    b. 「**AppAdmin**」カスタムプロパティの [**ユーザー ID**] を選択します。
    c. [**適用**] をクリックします。

これで、アプリ管理者ロールを作成し、割り当てしました。このロールのユーザーが にログインすると、アプリ、タスク、シート、ストリームにアクセスできます。QMC

セキュリティルール コード

以下に、この例のセキュリティルール コードと説明用のコメントを示します。

「AppAdminQmcSections」のセキュリティ コード

AppAdminQmcSections のセキュリティ ルール コード

項目	コード	コメント
リソース フィルター	`QmcSection_Stream, QmcSection_App, QmcSection_App.Sheet,QmcSection_App.Story, QmcSection_Tag,QmcSection_Task, QmcSection_ReloadTask, QmcSection_Event, QmcSection_SchemaEvent, QmcSection_CompositeEvent`	ストリーム、アプリ、シート、ストーリー、タグ、タスク、トリガーをフィルタリングします。
条件	`user.roles = "AppAdmin"`	このルールは、ユーザー ロールが「AppAdmin」に設定されているユーザー全員に適用されます。
アクション	`read`	条件が満たされると、読み取りアクセス権が与えられます。
コンテキスト	[**QMC でのみ**]	このルールは QMC を使用するときにのみ有効です。

「AppAdminRead」のセキュリティ コード

AppAdminRead のセキュリティ ルール コード

項目	コード	コメント
リソース フィルター	`Stream_*,App*,ReloadTask_*,SchemaEvent_*,Tag_*,CompositeEvent_*,User*`	ストリーム、アプリ、シート、ストーリー、タグ、タスク、トリガーのリソースタイプをフィルタリングします。
条件	`user.roles = "AppAdmin" and ((resource.resourcetype="App" and resource.@AppAdmin=user.userId and user.userDirectory="QVNCycles") or ((resource.resourcetype="ReloadTask" or resource.resourcetype="App.Object") and resource.app.@AppAdmin=user.userId and user.userDirectory="QVNCycles") or resource.resourcetype="SchemaEvent" or resource.resourcetype="CompositeEvent" or resource.resourcetype="Tag" or resource.resourcetype="Stream" or resource.resourcetype="User")`	このルールは、アプリに接続されている「AppAdmin」カスタム プロパティと同じ userId を持つユーザー全員に適用されます。
アクション	`read`	条件が満たされると、読み取りアクセス権が与えられます。

項目	コード	コメント
コンテキスト	[**QMC でのみ**]	このルールは QMC を使用するときにのみ有効です。

「AppAdminModify」のセキュリティ コード

このルールは、QMC 内でアプリ管理者が何を変更できるかを決めます。これは、ストリームを変更できないことを除き、読み取りと同じルールです。

AppAdminModify のセキュリティルール コード

項目	コード	コメント
リソース フィルター	`App*,ReloadTask_*,SchemaEvent_*,Tag_*,CompositeEvent_*`	ストリーム、アプリ、シート、ストーリー、タグ、タスク、トリガーのリソースタイプをフィルタリングします。
条件	`user.roles = "AppAdmin" and ((resource.resourcetype="App" and resource.@AppAdmin=user.userId and user.userDirectory="QVNCycles") or ((resource.resourcetype="ReloadTask" or resource.resourcetype="App.Object") and resource.app.@AppAdmin=user.userId and user.userDirectory="QVNCycles") or resource.resourcetype="SchemaEvent" or resource.resourcetype="CompositeEvent" or resource.resourcetype="Tag")`	このルールは、アプリに接続されている「AppAdmin」カスタム プロパティと同じ userId を持つユーザー全員に適用されます。
アクション	`create, update, delete, changeowner`	条件が満たされると、指定されたアクションが授与されれます。
コンテキスト	[**QMC専用**]	このルールは QMC を使用するときにのみ有効です。

セキュリティルールの例: ユーザー属性別のストリーム アクセス権

この例では、チケット認証またはセッションとSAML 属性で取得されたユーザー属性を使用して、特定のストリームへのアクセス権を作成します。

ユーザー属性を使用可能にするには、まずプロキシ API 経由でチケットを追加する必要があります。

手順

次の手順を実行します。

1. [**セキュリティルール**] を選択して [**新規作成**] をクリックします。
2. ルールのリソース フィルターは特定のストリームに設定します。
   [**Advanced**] セクションで、[**Resource filter**] 項目には、*セキュリティルール コード(page 613)*に基づいてテキストを入力します。
3. その後、ルールを適用するユーザーを指定する条件を設定する必要があります。
   [**Advanced**] セクションで、[**Conditions**] 項目には、*セキュリティルール コード(page 613)*に基づいてテキストを入力します。
4. ルールで提供するアクションを設定します。
   [**Basic**] セクションで、*セキュリティルール コード(page 613)*に基づいて、[**Actions**] を選択します。
5. [**名前**] 項目にセキュリティルールの名前を入力します。
6. [**適用**] をクリックします。

これで、チケット認証ユーザー属性に基づいて特定のストリームへのアクセス権を作成しました。

セキュリティルール コード

以下に、この例のセキュリティルール コードと説明用のコメントを示します。

セキュリティルール コード項目

項目	コード	コメント
リソース フィルター	`Stream_<GUID>`	特定の GUID でストリームをフィルタします。

条件	`resource.resourcetype="Stream" and (user.environment.<Attribute1>="<Value1a>")`	`resource.resourcetype="Stream"`
		このルールはストリームに適用されます。
		
		`(user.environment.<Attribute1>="<Value1a>")`
		属性が指定値に一致するユーザーにルールを適用します。

アクション	`read`	条件が満たされると、読み取りアクションが許可されます。

セキュリティルールの例: IP アドレス別のストリーム アクセス権

この例では、IP アドレスを通じて特定のストリームへのアクセス権を作成します。

次の事例では、アクセス権に IP アドレスを使用できます。

- アプリを社内ネットワークからのみ利用可能にする場合。
- アプリをモバイル ユーザーのみが利用可能にする場合。

手順

次の手順を実行します。

1. [**仮想プロキシ**] を開きます。
2. 編集する仮想プロキシを選択し、[**編集**] をクリックします。
3. [**詳細設定**] セクションで、[**拡張セキュリティ環境**] を選択します。
4. [**適用**] をクリックします。
5. [**仮想プロキシへの変更を適用**] ポップアップで [**OK**] をクリックします。
6. [**ストリーム**] を開いて新しいストリームを作成します。
7. [**セキュリティルール**] を開いて [**新規作成**] をクリックします。
8. [**テンプレートからルールを作成**] リストで、[**ストリーム アクセス**] を選択します。
9. ルールの名前を入力します。
10. 特定のストリームにリソース フィルターを設定します:
    [**詳細設定**] セクションで、[**リソース フィルター**] 項目を、*セキュリティルール コード(page 614)* に基づいて入力します。
    例:*Stream_aaec8d41-5201-43ab-809f-3063750dfafd*
11. ルールを適用する IP アドレスとリソースを指定する条件を設定します:
    [**詳細設定**] セクションで、[**条件**] 項目を、*セキュリティルール コード(page 614)* に基づいて入力します。
    例: *user.environment.ip = "::ffff:10.88.0.5"*
12. ルールで提供するアクションを設定します:
    [**Basic**] セクションで、*セキュリティルール コード(page 614)*に基づいて、[**Actions**] を選択します。
    アクション [**読み取り**] および [**公開**] を選択します。
13. [**適用**] をクリックします。

これで、接続デバイスの IP アドレスに基づいて特定のストリームへのアクセス権を作成しました。

セキュリティルール コード

以下に、この例のセキュリティルール コードと説明用のコメントを示します。

セキュリティルール コード項目

項目	コード	コメント
リソース フィルター	`Stream_<GUID>`	特定のストリームにフィルター。

項目	コード	コメント
条件	`(user.environment.ip="<Your_IP_address>")` `user.environment.ip` 条件には異なるフォーマットがあります。ハイブリッドデュアルスタック IPv6/IPv4 の実装で、使用されるのは常に IPv6 フォーマットです。クライアントが IPv6 の使用を決めた場合は、その IPv6 アドレスはプロキシにより追加されます。クライアントが IPv4 を使用する場合は、IPv4-mapped アドレスが使われます。 **Example 1:** *IPv4 address: 10.88.0.5 => ::ffff:10.88.0.5 (IPv6)* この場合、ルール条件は次のように設定できます: • user.environment.ip like "*10.88.0*" • user.environment.ip like "::ffff:10.88*" • user.environment.ip = "::ffff:10.88.0.5" **Example 2:** *IPv6 address: 2001:0db8:85a3:0000:0000:8a2e:0370:7334* この場合、ルール条件は次のように設定できます: • user.environment.ip like "*0db8:85a3:0000:0000:8a2e*" • user.environment.ip like "2001:0db8:85a3:0000:0000*" • user.environment.ip = "2001:0db8:85a3:0000:0000:8a2e:0370:7334" *サンプル中のアスタリスク(*) は付加文字を意味します。*	`(user.environment.ip="<Your_IP_address>")` 値に対応する IP アドレスから接続してくるデバイスにルールが適用されます。
アクション	`Read,Publish`	Read とPublish 条件が満たされると、アクションが許可されます。

セキュリティルールの例: ユーザー属性別のアプリへの Qlik Sense Mobile Client Managed オフライン アクセス権

この例では、チケット認証またはセッションと属性で取得されたユーザー属性を使用して、特定のアプリへのオフライン アクセス権を作成します。SAML

ユーザー属性を使用可能にするには、まずプロキシ API 経由でチケットを追加する必要があります。

手順

次の手順を実行します。

1. Select **Security rules** and click 新規作成
2. ルールのリソース フィルターは、アプリのフィルターに設定します。
   [**基本**] セクションで、[**リソース フィルター**] 項目には、*セキュリティルール コード(page 616)* に基づいてテキストを入力します。
3. その後、ルールを適用するユーザーを指定する条件を設定する必要があります。
   [**Advanced**] セクションで、[**Conditions**] 項目には、*セキュリティルール コード(page 616)*に基づいてテキストを入力します。
4. ルールで提供するアクションを設定します。
   [**基本**] セクションで、セキュリティルール コード (page 616) に基づいて、[**アクション**] を選択します。
5. [**名前**] 項目にセキュリティルールの名前を入力します。
6. [**適用**] をクリックします。

これで、チケット認証ユーザー属性に基づいて特定のストリームへのアクセス権を作成しました。

セキュリティルール コード

以下に、この例のセキュリティルール コードと説明用のコメントを示します。

セキュリティルール

項目	コード	コメント
リソース フィルター	`App_*`	特に、リソース タイプ アプリをフィルタリングします。

条件	`resource.resourcetype="App_*" and (user.environment.<Attribute1>="<Value1a>")`	`resource.resourcetype="App_*"`
		このルールはアプリに適用されます。
		
		`(user.environment.<Attribute1>="<Value1a>")`
		属性が指定値に一致するユーザーにルールを適用します。

アクション	`read`	条件が満たされると、読み取りアクションが許可されます。

セキュリティルールの例: ある顧客のケース

以下の例は、セキュリティルールに関する顧客のニーズに合わせて柔軟なソリューションが開発された顧客のケースを示しています。

ユーザー ディレクトリ構造

顧客は次のユーザー ディレクトリ構造を持っており、それを再利用する必要がありました。

プロジェクト

ユーザー ディレクトリ構造の例 1

ロール	アクセス	コンテンツ
開発者	フォルダの接続	Excel ファイル
管理者	QMCアクセス	アプリ、アプリオブジェクト、タスク
オーディエンス1	ストリーム	ダッシュボード1、ダッシュボード2、ダッシュボード3
オーディエンス2	ストリーム	ダッシュボード4、ダッシュボード5、ダッシュボード6

この構造は顧客のQlik Sense展開において複数のプロジェクトを持ち、その展開が複数のロールで構成されていることを示しています。

- 開発者: フォルダ接続を使って、このプロジェクトのための資料を作成することを許可されている。
- 管理者: プロジェクトのリソース管理を許可されているスーパー ユーザーの一種。
- オーディエンス: 各オーディエンスに関連付けられたストリームを通じてダッシュボードの定義済みセットの使用を許可されているユーザー

セキュリティ ロールとプロジェクト グループの追加

次のテーブルでは元のユーザー ディレクトリ構造を再利用します。ただし2つの新しいプロパティとして、セキュリティ ロールとプロジェクト グループを追加します。

プロジェクト (proj_X)

ユーザー ディレクトリ構造の例 2

ロール (セキュリティ ロール)	プロジェクト (プロジェクト グループ)	コンテンツ
開発者 (role_dev)	DC_ProjectX (projX_dev)	Excel ファイル
管理者 (role_admin)	QMCアクセス (projX_admin)	アプリ、アプリオブジェクト、タスク
オーディエンス1 (role_ext) (ロールなし = 読み取りアクセス)	Proj1_Aud1 (projX_aud1)	ダッシュボード1、ダッシュボード2、ダッシュボード3
オーディエンス2 (role_ext) (ロールなし = 読み取りアクセス)	Proj1_Aud2 (projX_aud2)	ダッシュボード4、ダッシュボード5、ダッシュボード6

新しいプロパティはさまざまなグループを定義するために使用されます。

- セキュリティ ロール: ユーザーが実行できる操作 (アプリの作成、シートの追加、データのエクスポートなど) を定義します。
- プロジェクト グループ: ユーザーがアクセスを許可されるプロジェクトとプロジェクト リソースを決定します。

新しいプロパティの実装

プロパティグループは、プロジェクトとリソースへのアクセス権を付与するカスタム プロパティを使用して実装されます。セキュリティ ロールはユーザー ディレクトリで実装されます。

このアプローチには、以下のような多くのメリットがあります。

- セキュリティ ポリシーを記述するのに必要なルールの数が減ります。
- ルールを徐々に変更できます。システムは属性を通じて構成され、ルールの変更が求められるのは、セキュリティの変更が必要なときです。
- ユーザー管理とアクセス許可のプロビジョニングがユーザー ディレクトリで管理されます。

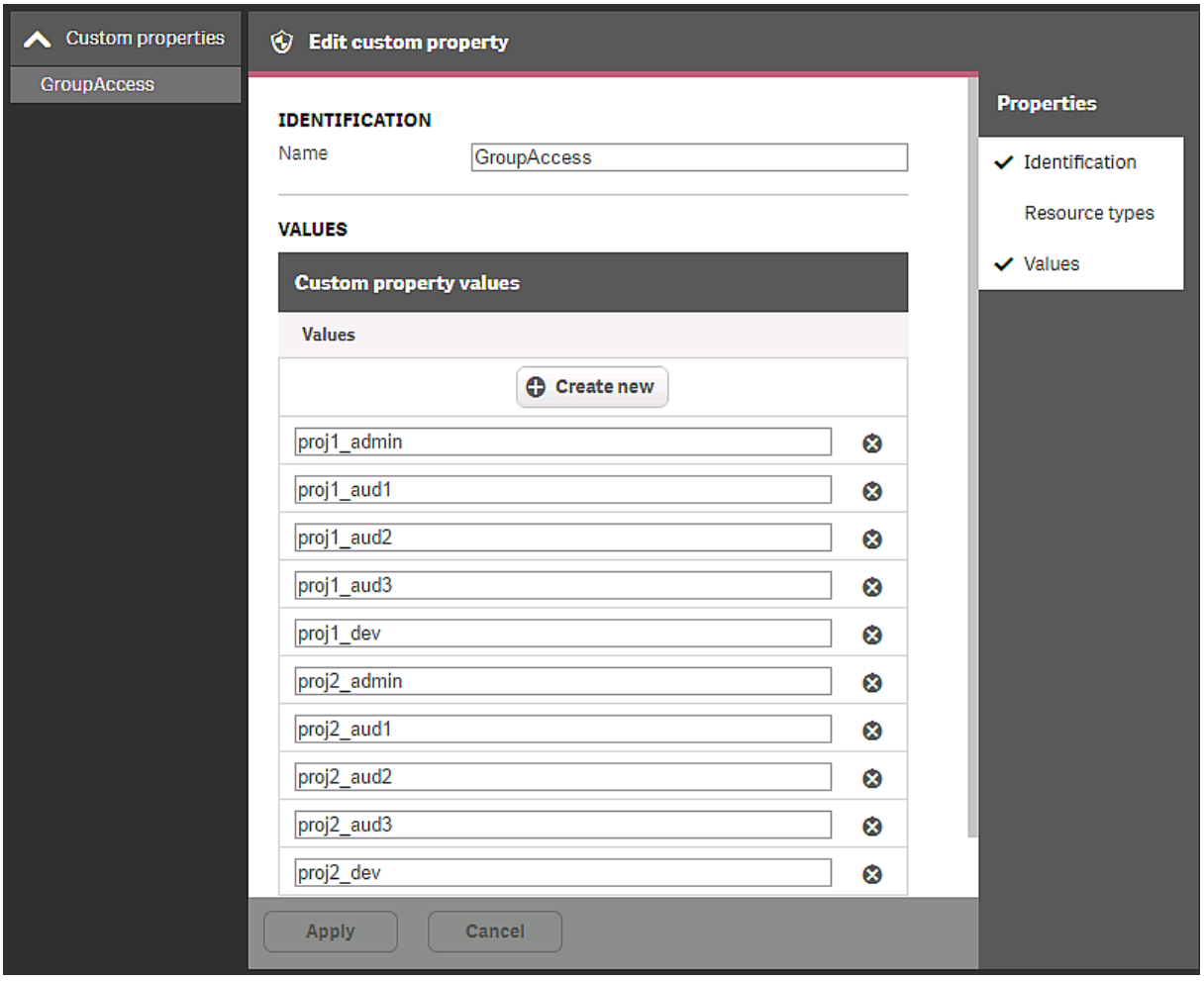
作成する必要のあるルール

リソースのアクセスには 1 つのルールが必要です。

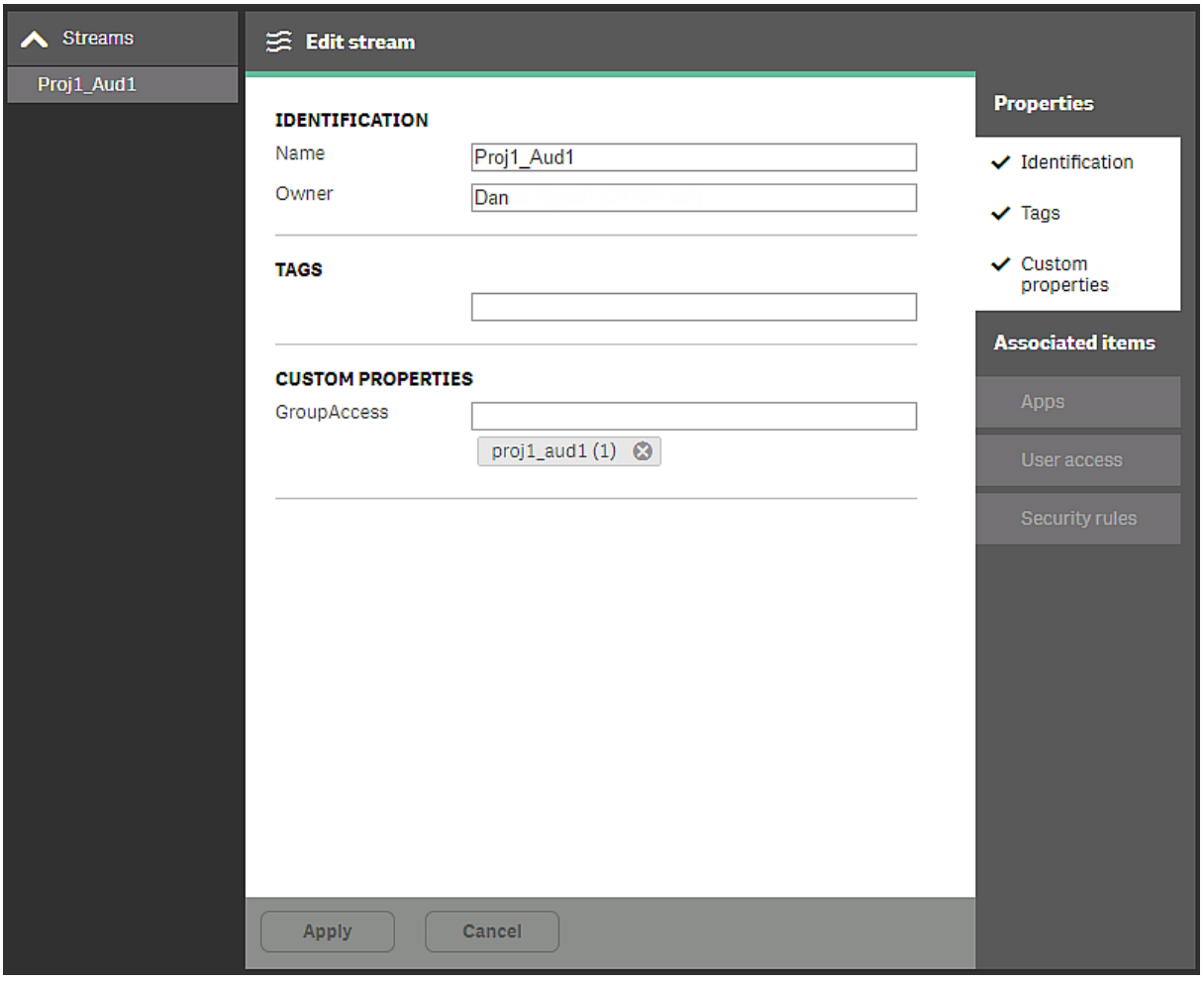
新規 リソース アクセス ルール

設定	値
名前	ResourceAccess
リソース フィルター	`Stream_*, DataConnection_*`
条件	((`user.group=resource.@GroupAccess`))
アクション	Read

このルールは、リソースのカスタム プロパティのGroupAccessにユーザーのグループ名が含まれている場合、そのユーザーにリソースへのアクセス権を付与します。これを有効にするには、すべてのユーザー グループを含んだ「GroupAccess」という名前のカスタム プロパティが必要です。



このルールはストリームとデータ接続に関連付けることができます。このルールによって、カスタム プロパティを使用して、グループのユーザーにストリームへのアクセス権を付与することが可能となります。



この例では、proj1_aud1グループが、Proj1_Aud1ストリームへのユーザー ディレクトリ アクセスに追加されました。他のグループでもアクセス許可が必要な場合、そのグループをカスタム プロパティに追加できます。

次のルールを作成して、ストリームを管理できる必要のある人を定義します。

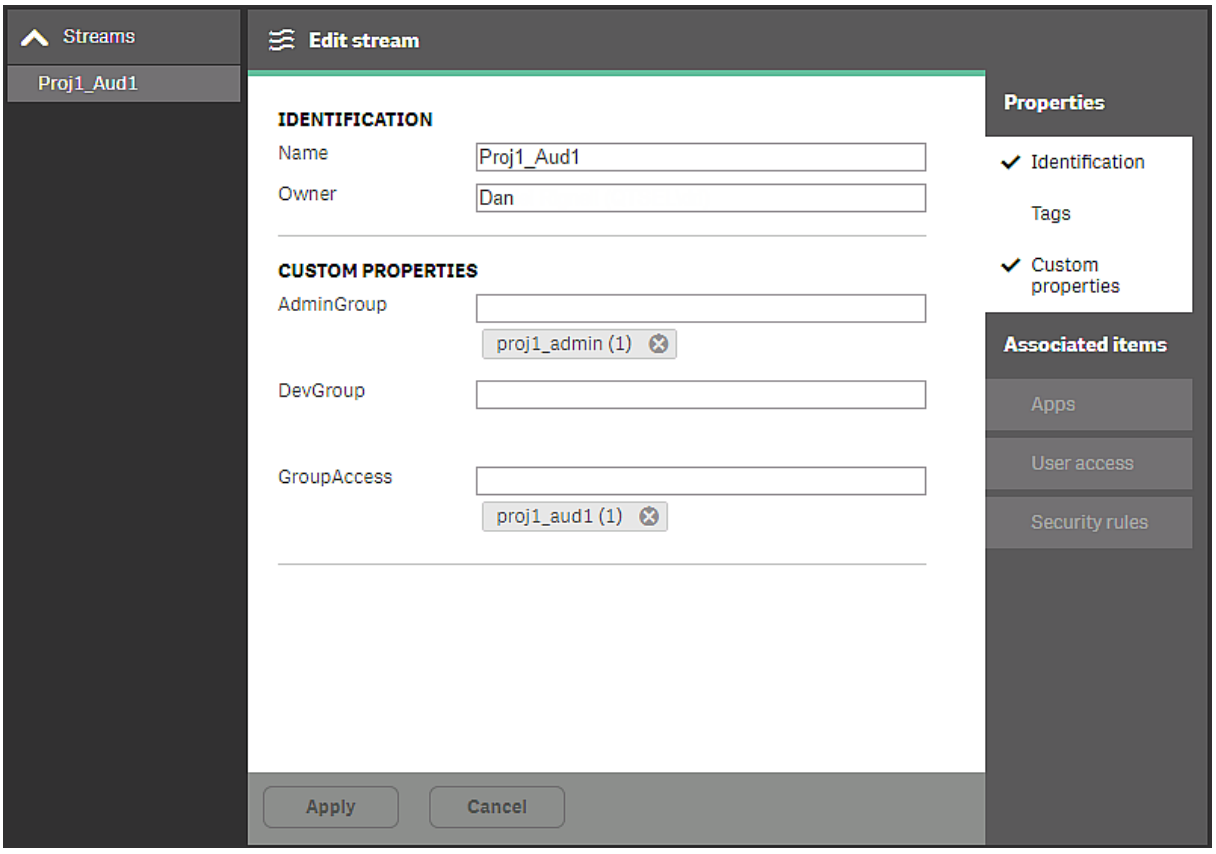
ストリーム管理ルール

設定	値
名前	TeamAdminRead
リソース フィルター	Stream*,App*,ReloadTask*,SchemaEvent*,Tag*,CompositeEvent*,ExecutionResult*,CustomProperty*,DataConnection*

条件	((resource.resourcetype="App" and user.group = resource.stream.@AdminGroup) or (resource.resourcetype="App.Object" and user.group = resource.app.stream.@AdminGroup) or (resource.resourcetype="ReloadTask" and resource.app.stream.@AdminGroup = user.group) or (resource.resourcetype="DataConnection" and resource.@AdminGroup = user.group) or resource.resourcetype ="SchemaEvent" or resource.resourcetype ="CompositeEvent" or resource.resourcetype = "Tag" or resource.resourcetype ="ExecutionResult")
アクション	Read, Update

ルールの説明: ストリームの管理グループに属しているユーザーは、そのストリームで公開されたアプリに関連するリソースを管理できます。

これを有効にするには、プロジェクトの管理者が含まれているグループの名前を含んだカスタム プロパティ AdminGroupを作成する必要があります。



この例のproj1_adminグループのユーザーには、このストリームのアプリに関連するリソースへの管理アクセス権限があります。

作成する必要のあるセキュリティロール

3 種類のセキュリティロールが定義されました。

- role_admin: 管理タスクを行える必要のあるユーザー
- role_dev: プロジェクトの開発作業を行える必要のあるユーザー
- role_ext: アプリを拡張できる必要のあるユーザー

管理者ロールには 2 つのルールが必要です。次の例では、role_adminグループのユーザーにQMCのセクションへのアクセス権を付与します。

管理者の QMC ルール

設定	値
名前	TeamAdminSections
リソース フィルター	QmcSection_App,QmcSection_DataConnection,QmcSection_ContentLibrary,QmcSection_App.Object,QmcSection_Task, QmcSection_ReloadTask, QmcSection_Event, QmcSection_SchemaEvent, QmcSection_CompositeEvent
条件	`((user.group="role_admin"))`
アクション	Read

次の例では、role_adminのユーザーに、アプリ、リロードタスク、データ接続などを作成する権限を付与します。

管理者の作成ルール

設定	値
名前	TeamAdminCreate
リソース フィルター	App*,ReloadTask*,SchemaEvent*,CompositeEvent*,ExecutionResult*,DataConnection*
条件	`((user.group="role_admin"))`
アクション	Create

role_extルールは既定のルールを微調整して作成されます。role_extグループのユーザーだけが新しいシートを使ってアプリを拡張できます。柔軟性を高めるため、新しいカスタム プロパティ(Extendable) がアプリに追加されます。Extendable がオンにされたアプリはすべてのユーザーにそのアプリへのシートの追加を許可します。

Extendableルール

設定	値
名前	CreateAppObjectsPublishedApp
リソース フィルター	QmcSection_App,QmcSection_DataConnection,QmcSection_ContentLibrary,QmcSection_App.Object,QmcSection_Task, QmcSection_ReloadTask, QmcSection_Event, QmcSection_SchemaEvent, QmcSection_CompositeEvent

条件	`!resource.App.stream.Empty() and resource.App.HasPrivilege("read") and (resource.objectType = "userstate" or resource.objectType = "sheet" or resource.objectType = "story" or resource.objectType = "bookmark" or resource.objectType = "snapshot" or resource.objectType = "embeddedsnapshot" or resource.objectType = "hiddenbookmark") and !user.IsAnonymous() and (user.group="role_dev" or user.group="role_ext" or resource.app.@Extendable="Yes")`
アクション	Create

最後は、開発者のために、もう1 つのルールを微調整して、role_devグループの開発者だけがアプリの作成を許可されるようにします。

開発者の作成ルール

設定	値
名前	CreateApp
リソース フィルター	App_*
条件	`!user.IsAnonymous() and user.group="role_dev"`
アクション	Create

概要

この設定を使い、ユーザー ディレクトリのグループを通じてQlik Senseを管理できます。また、Qlik Senseにコンテンツを追加するときに、属性の使用のみでアクセスできる必要のあるグループを定義できます。

このアプローチでは、ロールがグループから分離されており、ユーザーがさまざまなプロジェクトごとに異なるロールを持たないことを前提としています。ユーザーが異なるロールを持つ場合は、プロジェクトごとに個別のロールを作成する必要があります。

1.10 配布ポリシー - はじめに

Qlik Sense Enterprise 配布ポリシーは、オンプレミスの Qlik Sense Enterprise on Windows ノードからQlik Sense Enterprise SaaS への Qlik Sense アプリの配布方法を管理します。

マルチクラウド アクセス権を持つユーザーが使用できるよう、アプリを Qlik Sense Enterprise から実装環境に配布する必要があります。アプリをマルチクラウドに配布するには、配布ポリシーを定義する必要があります。配布ポリシーにより、配布する公開アプリ、および配布先 (Qlik Sense Enterprise SaaS) を決定します。アプリをクラウドに配布するには配布ポリシーが必要です。公開アプリが配布ポリシーの対象外である場合、その公開アプリは配布されません。

配布ポリシーは、アプリの公開時に最初に Qlik Sense Enterprise で評価されます。評価結果は、公開アプリのコピーを受け取る Qlik Sense Enterprise SaaS 上の実装環境のリストとして表示されます。配布ポリシーは、過去に公開されたアプリが変更、移動、または削除されると再評価されます。

配布ポリシーの作成

配布ポリシーの作成時に実行する手順を以下に示します。

1. ルールを適用するリソースを決めるためのリソース フィルターを設定します (App_*)。
2. ルールで許可するアクションを選択します ([配布])。
3. ルール エディターで、ルールの条件を定義します。
   公開アクションからのアプリ カスタム プロパティ名とストリーム名は、定義したルール条件をテストする際に役立ちます。
4. ルールを検証します。
5. ルールを適用します。

ハブからコレクションにアプリを公開する方法については、[] から Windows 上の Qlik Sense に関する資料の「コレクションの公開」を参照してください。

配布ポリシーの作成

配布ポリシーを使用して、Qlik Sense Enterprise から Qlik Sense Enterprise SaaS へのアプリの配布を有効化できます。配布ポリシーはセキュリティルールと似ています。いずれの場合も、ルールを適用するリソースおよび実行可能な操作を定義します。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. [**クラウド配布**] を QMC 開始ページで選択するか、[**開始**] から選択します▼ ドロップダウン メニューから選択して、概要を表示します。
3. データ マネージャーでテーブルの ⊕ 新規作成
4. [**Edit distribution policy**] (配布ポリシーを編集) ウィンドウでプロパティを編集します。

配布ポリシーの ID プロパティ

プロパティ	説明	既定値
テンプレートからルールを作成	一部の値が自動的に入力されるように、ルール用のテンプレートを選択します。 *[**テンプレートからルールを作成**] の選択を変更すると、自動的にすべての [**アクション**] がクリアされ、[**詳細設定**] セクションの [**条件**] テキスト ボックスが変更されます。*	**不特定**
無効化	ルールをアクティブにしない場合、ルールを無効化することを選択します。	オフ
名前	ルールに名前を付けます。	空
説明	オプション。ルールの説明を追加します。	空

配布ポリシーの基本プロパティ

プロパティ	説明	既定値
リソース フィルター	このリストで、ルールを適用するリソースを選択します。**App_*** は、ルールはアプリにのみ適用され、アプリオブジェクトおよびアプリシートには適用されないことを意味することに注意してください。	**App_***
アクション	ルールのアクションを選択します。	**配布**

配布ポリシーの詳細設定プロパティ

プロパティ	説明	既定値
条件	このテキストボックスは、前述のポリシー エディターで行われた変更を反映します。テキストボックスに入力して、条件を定義できます。	((subject.name=""))

[**ルールの検証**] をクリックして、構文が正しいことを確認します。

配布ポリシーのタグ プロパティ

プロパティ	説明
タグ	*利用可能な QMC タグがない場合、このプロパティグループは表示されません。* テキストボックスをクリックすると、利用可能なタグが一覧表示されます。入力を始めると、リストが少なくなります。紐付けられているタグがテキストボックスの下に表示されます。

5. 操作バーで [**適用**] をクリックし、変更内容を保存します。

ページ最下部に [**追加完了**] と表示されます。

配布ポリシー - カスタム プロパティの使用

クラウド実装環境へのアプリの配布方法を決定するための配布ポリシーを作成します。アプリを Qlik Sense Enterprise on Windows から Qlik Sense Enterprise SaaS に配布する場合は、配布ポリシーが必要です。作成されると、配布ポリシーの基準に適合するすべての公開済みアプリは定義されたターゲットに配布されます。

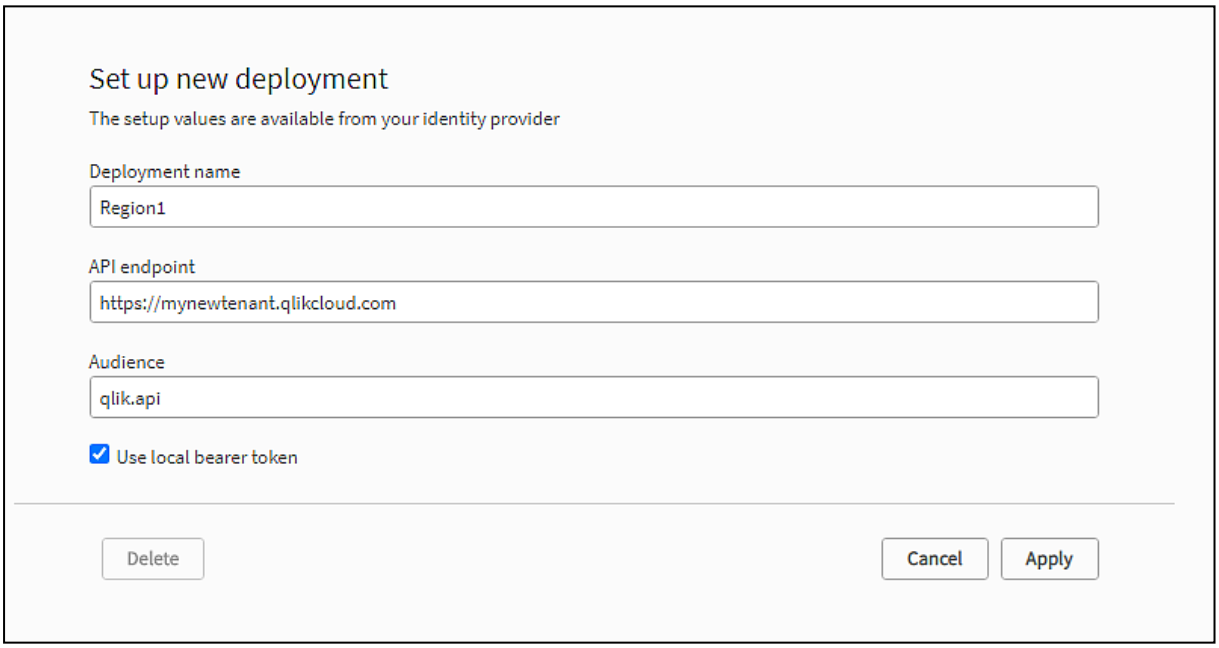
アプリが初めてクラウドに配布されると、アプリデータ(存在する場合) とメタデータ(名前、所有者、ストリーム、カスタム プロパティなど) の両方が配布されます。それ以降の配布では、最後のリロードよりも後に変更されたアプリデータのみが配布され、それ以外の場合はメタデータのみが配布されます。その際、クラウドアプリのアプリデータは変更されません。アプリコンテンツとアプリオブジェクトに加えられた変更は、アプリデータの配布をトリガーしませんが、アプリの公開またはリロードはトリガーされます。

前提条件

- マルチクラウドを含むライセンス。次のいずれか:
  - Qlik Sense Enterprise on Windows とQlik Sense Enterprise SaaS の同じ署名付きライセンスキー。
  - クラウド属性が有効になっていて、オンプレミスが署名付きライセンスを通じてアクティブ化されている、さまざまなライセンス キー。
- アプリを配布できるテナントが 2 つあること。
- テナントごとに以下を完了する必要があります。
  - *展開のセットアップ (page 626)*
  - *ID プロバイダー構成の作成 (page 627)*

これらの手順が完了したら、「*さまざまな展開にアプリを配布するための配布ポリシーの作成 (page 627)*」に進みます。

展開のセットアップ



次の手順を実行します。

1. Qlik Sense Enterprise on Windows サーバーの Qlik Management Console (QMC) で、[**クラウド配布**] を開きます。
2. [**配布ポリシー**] を選択します。
3. 画面左下で、[**Set up new**] (新規設定) をクリックします。
4. 展開名を入力します1 つ目の展開には「*Region1*」を、2 つ目の展開には「*Region2*」を使用します。これらの名前をカスタム プロパティの値として使用します。
5. **API エンドポイント**、つまりテナント アドレスを入力します。
   例: *https://my-tenant.eu.qlikcloud.com*。
6. **オーディエンス**には、*qlik.api* と入力します。

7. [**Use local bearer token**] (ローカル ベアラー トークンを使用) を選択します。

   *ローカル ベアラー トークンを使用することで、セットアップが簡略化されます。使用しない場合は、代わりに**クライアント ID**、**クライアント シークレット**、**トークン エンドポイント**を入力する必要があります。*

8. [**クリップボードにコピー**] をクリックします。
   ID プロバイダー構成でローカル ベアラー トークンが必要です。
9. [**適用**] をクリックします。

ID プロバイダー構成の作成

次の手順を実行します。

1. クラウド テナントで 管理 コンソール を開き、左側のメニューで [**ID プロバイダー**] を選択します。
2. [**新規作成**] をクリックします。
   [**ID プロバイダー構成の作成**] ウィンドウが開きます。
3. [**タイプ**] で、[*マルチクラウド*] を選択します。
4. 必要に応じて、説明を入力します。
5. [**ローカル ベアラー トークン**] ボックスに、展開設定でコピーしたトークンを貼り付けます。

さまざまな展開にアプリを配布するための配布ポリシーの作成

QMC で配布ポリシーを作成します。アプリを公開する際に、カスタム プロパティを使用してアプリの配布場所を定義できます。

まず、カスタム プロパティを作成し、次にそれを配布ポリシーで使用します。

展開に関するカスタム プロパティの作成

カスタム プロパティは展開名を値として持ちます。

次の手順を実行します。

1. QMC で [**カスタム プロパティ**] セクションを開きます。
2. データ マネージャーでテーブルの ⊕ 新規作成
3. カスタム プロパティに「*deployments*」という名前を付けます。

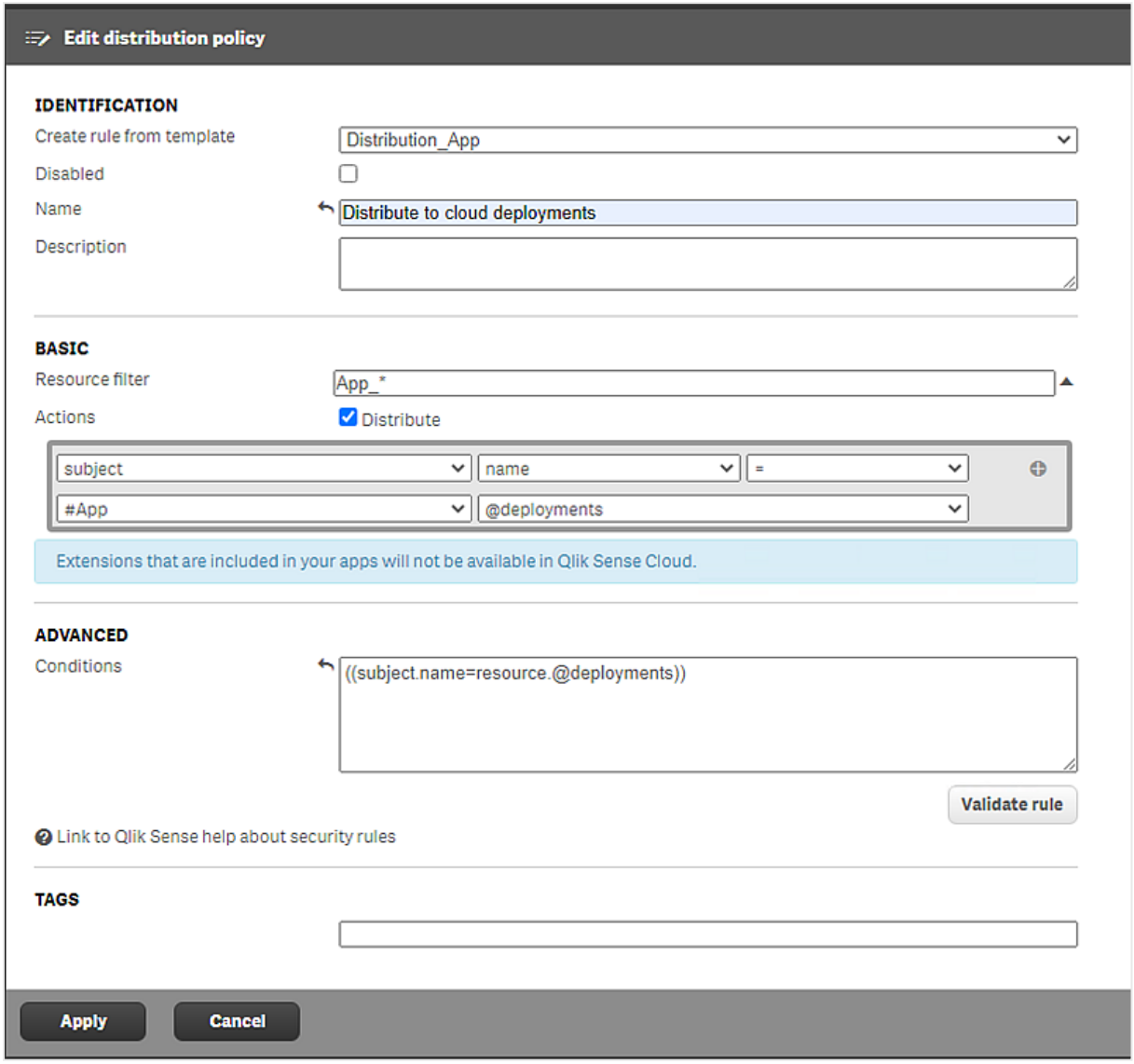
   クラウド app の詳細でタグを表示する場合は、カスタム プロパティの名前をタグの名前にする必要があります。そうすると、App の公開時にタグとして選択したカスタム プロパティの値が、クラウド app の詳細に表示されるようになります。

4. [**リソース タイプ**] で、[**アプリ**] を選択します。
5. **Values**, click ⊕ 新規作成
6. 値として「*Region1*」と入力します。
7. 同様に値「*Region2*」を追加します。
8. [**適用**] をクリックします。

配布ポリシーで使用できる2つのカスタムプロパティ値が作成されました。

配布ポリシーの作成

公開アプリをQlik Cloudの1つ以上の実装環境に配布できるかどうかは、配布ポリシーにより決定されます。公開されたアプリのみを配布できます。



次の手順を実行します。

1. QMCで、[**クラウド配布**]セクションを開き、[**配布ポリシー**]を選択します。
2. データマネージャーでテーブルの ⊕ [**新規作成**]をクリックします。
3. [**テンプレートからルールを作成 リスト**]で、[*Distribution_App*]を選択します。
4. 配布ポリシーに「*Distribute to cloud deployments*」という名前を付けます。
5. [**基本**]で、リソースフィルター値が[*App_**]になっていて、アクションに[**配布**]が選択されていることを確認します。

6. ルール エディターで、[*サブジェクト*] と[*名前*] の値をそのまま維持します。2 行目の最初のドロップダウン リストで [**#App**] を選択します。最後のフィールドで「*@deployments*」を追加します。
[**詳細**] セクションの [**条件**] ボックスには、「`((subject.name=resource.@deployments))`」という文字列が表示されます。これは、次のような意味になります。
「展開名がアプリに適用されるカスタム プロパティの値に等しい場合、アプリはその展開に配布される」
7. [**Validate rule**] (ルールの検証) をクリックします。
ルールの構文がチェックされ、有効な場合は「確認」のメッセージが表示されます。
8. [**適用**] をクリックして、ルールを保存します。

この設定によって、アプリをハブに公開したときに使用するタグに基づいて、展開のどちらか、または両方にアプリを配布することができます。

配布ポリシーの編集

配布ポリシーを使用して、Qlik Sense Enterprise から Qlik Sense Enterprise SaaS へのアプリの配布を有効化できます。配布ポリシーはセキュリティルールと似ています。いずれの場合も、ルールを適用するリソースおよび実行可能な操作を定義します。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. Select **Distribution policies** on the QMC start page or from the **Start**▼ドロップダウン メニューからリソースを選択します。
3. 編集したいポリシーを選択します。
4. アクション バーで [**編集**] をクリックします。
5. [**Edit distribution policy**] (配布ポリシーを編集) ウィンドウでプロパティを編集します。
ID

配布ポリシーの ID プロパティ

プロパティ	説明	既定値
テンプレートからルールを作成	一部の値が自動的に入力されるように、ルール用のテンプレートを選択します。 *[**テンプレートからルールを作成**] の選択を変更すると、自動的にすべての[**アクション**] がクリアされ、[**詳細設定**] セクションの[**条件**] テキスト ボックスが変更されます。*	**不特定**
無効化	ルールをアクティブにしない場合、ルールを無効化することを選択します。	オフ
名前	ルールに名前を付けます。	空
説明	オプション。ルールの説明を追加します。	空

基本

配布ポリシーの基本プロパティ

プロパティ	説明	既定値
リソース フィルター	このリストで、ルールを適用するリソースを選択します。**App_*** は、ルールはアプリにのみ適用され、アプリオブジェクトおよびアプリシートには適用されないことを意味することに注意してください。	**App_***
アクション	ルールのアクションを選択します。	**配布**

詳細設定

配布ポリシーの詳細設定プロパティ

プロパティ	説明	既定値
条件	このテキストボックスは、前述のポリシー エディターで行われた変更を反映します。テキストボックスに入力して、条件を定義できます。	((subject.name=""))

[**ルールの検証**] をクリックして、構文が正しいことを確認します。

タグ

タグ プロパティ

プロパティ	説明
タグ	*利用可能な QMC タグがない場合、このプロパティグループは表示されません。* テキストボックスをクリックすると、利用可能なタグが一覧表示されます。入力を始めると、リストが少なくなります。紐付けられているタグがテキストボックスの下に表示されます。

6. 操作バーで [**適用**] をクリックし、変更内容を保存します。

ページの最下部に [**更新完了**] と表示されます。

1.11 アクセス制御の監査

QMCには、アクセス権および関連のセキュリティルールの見直しとプレビューを行える、次の監査ツールが含まれます。[Preview (プレビュー)] ページでは、システムの稼働を中断することなく、新しいルールや編集されたルールによる影響を確認できます。

監査ツールは、既存のリソースに適用されているルールのみを表示します。たとえば、「MyApp」で始まる名前のアプリのルールを作成する場合に、Qlik Sense システムにその名前のついたアプリが実際にあると、監査ページとプレビュー ページには結果のみが表示されます。

弊社は次の部署で組織されています。財務、営業、マーケティング、開発。部門の名前に一致する値のある「Departments」というカスタム プロパティが作成され、ストリームに適用されました。最後に、QMCの [**ストリーム**] ページを使用してセキュリティルールを作成し、財務部のユーザーにQuarterly reportsストリームに対する公開および読み取り権限を付与しました。その他の部門にはすべて、読み取り権限が付与されます。次に、ルールが正しく適用されたことをチェックします。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタート ページの [**監査**] をクリックしてください。
3. [**監査**] ページで、対象のリソース リストから [**ストリーム**] を選択します。
4. 対象のリソース リストの右側で、 をクリックし、ストリーム `Quarterly reports` を選択します。
5. [**監査**] をクリックします。
   ユーザー ID とストリームがテーブルに表示されます (この例では Quarterly reports のみ)。
   グリッドには、ストリームに対する各ユーザーのアクセス権を示す文字が表示されます。
   財務のユーザーには読み取りおよび公開のアクセス権、その他すべてのユーザーには読み取りアクセス権 (カスタム プロパティ部署がある場合) が必要です。
   ユーザーのフィルタリングを指定しない場合、ストリームへのアクセス権を持つユーザーのみがグリッドに表示されます。つまり、リストに含まれていないユーザーは リソースにアクセスできません。ユーザーのフィルタリングを指定すると、そのユーザーの監査結果がグリッドに表示されます。リソースについても同様で、リソースが選択されていない場合は、監査結果のあるリソースのみがグリッドに表示されます。
6. 財務部門に属するユーザーに対応するセルをグリッドでダブルクリックします (管理者 ユーザーは クリックしないでください)。
   [**該当するルール**] ウィンドウが開きます。
   Quarterly reports ストリームに関し選択されたユーザーに適用されるセキュリティルールが表示されます。リストには以下のルールが含まれていなくてはなりません。
   - Stream_read_Quarterly reports
   - Stream_publish_Quarterly reports
7. 営業部門に属するユーザーに対応するセルをグリッドでダブルクリックします (管理者 ユーザーは クリックしないでください)。
   [**該当するルール**] ウィンドウが開きます。
   これで Quarterly reports ストリームに関し選択されたユーザーに適用されるセキュリティルールが表示されるようになりました。リストには以下のルールが含まれていなくてはなりません。
   - Stream_read_Quarterly reports

監査クエリの定義

セキュリティルールまたは負荷分散ルール、ライセンス ルールについて、クエリを行えます。

セキュリティルール クエリの定義

次の手順を実行します。

1. ターゲット リソース リストからリソースのタイプを選択します。
2. Next to the target resource list, click and select the resources to audit on.
3. To the right of **Users**, click and use the search to filter the users to audit on.
4. [**環境**] リストで、監査のコンテキストを選択します。
5. (Optional) Click if you want to simulate a certain user environment.
   例: *OS=Windows; IP=10.88.3.35; ブラウザ=Firefox;*.
6. ヘッダー バーの右側で、[**監査権限**] をクリックし、監査テーブルで表示する権限を選択します。
7. [**監査**] をクリックして、クエリを実行します。
   監査テーブルが表示されます。[**行列の入れ替え**] をクリックして、テーブルを回転させます。

負荷分散 ルール クエリを定義する

1. ヘッダー バーのドロップダウン リストから**[負荷分散ルール監査]** を選択します。
2. 監査するターゲット リソースを選択します ([**アプリ**] または [**ノード**])。
3. Next to the target resource list, click and select the resources to audit on.
4. [**環境**] リストで、監査のコンテキストを選択します。
5. (Optional) Click if you want to simulate a certain user environment.
   例: *OS=Windows; IP=10.88.3.35; ブラウザ=Firefox;*.
6. [**監査**] をクリックして、クエリを実行します。
   監査テーブルが表示されます。[**行列の入れ替え**] をクリックして、テーブルを回転させます。

ライセンス ルール クエリの定義

1. ヘッダー バーで、[**同期ルール監査**] を選択します。
   [**監査クエリ**] リソースが、自動的に [**ログイン アクセス**] に設定されます。
2. Next to the target resource list with **Login access** selected, click and use the search to filter the resources to audit on.
3. [**環境**] リストで、監査のコンテキストを選択します。
4. (Optional) Click if you want to simulate a certain user environment.
   例: *OS=Windows; IP=10.88.3.35; ブラウザ=Firefox;*.
5. [**監査**] をクリックして、クエリを実行します。
   監査テーブルが表示されます。[**行列の入れ替え**] をクリックして、テーブルを回転させます。

監査クエリ結果の表示とフィルタリング

ドロップダウン プロパティ リストを使用すると、クエリ結果のフィルタリングを実行できます。

次の手順を実行します。

1. クエリを定義して、適宜、[**監査**] をクリックします。
   クエリの結果は、テーブルに表示されます。

   非アクティブ ユーザーは表示されません。

2. [**監査の権限**] をクリックし、表示する権限を選択します。
デフォルトでは、読み取り権限が表示されます。どの権限が特定の監査で利用可能かは、選択したリソースにより異なります。次のテーブルでは、異なるセルの色が表示されます。

セルの色

色	説明
白色	アクセスを提供するルールが存在しません。
緑色	アクセスが認められています。
黄色	アクセスが無効にされています。
赤色	ルール評価が壊れています。
青	ルールを編集または新規作成する際のプレビューの色。

3. マトリクスにあるセルをダブルクリックして、[**関連ルール**] ウィンドウを開きます。
[**関連ルール**] ウィンドウには、選択したユーザー/リソースの組み合わせにアクセスを認めるセキュリティルールが表示されます。
ルールを選択して [**編集**] をクリックすると、編集ページが開きます。

> *読み取りアクセス権があるセキュリティルールのみを表示できます。*

1.12 トラブルシューティング - QMC

トラブルシューティングのトピックは、さまざまなカテゴリに分かれています。考えられる原因と、問題の解決方法を示します。

トラブルシューティング - QMC の起動

このセクションでは、QMC を起動するときに発生する可能性のある問題について説明しています。

QMCへの初回アクセス時、アクセスできない

QMC へのアクセスを初めて試みるときに、次のいずれかの問題が発生する場合があります。

証明書エラー

考えられる原因

ブラウザのセキュリティの設定が高すぎるため、Qlik Sense証明書が信頼されていません。(この証明書はインストール中に追加されます)。

提案されたアクション

このWebサイトは推奨されないという警告ですが、続行を選択します。ただし、URLが正しいことを確認してください。

サードパーティの証明書を使用すればエラーは表示されなくなります。

署名済みサーバープロキシ証明書への変更 (page 505)

ページが空白で、アドレス バーが警告を表示

考えられる原因

サードパーティの証明書が必要です。

提案されたアクション

サーバーからQMCにアクセスし、新しいサードパーティの証明書を追加します。

署名済みサーバープロキシ証明書への変更 (page 505)

ネットワーク トラフィックで表示されるエラー メッセージと401 警告

考えられる原因

Qlik Sense サイトは、信頼済みサイトの一覧に含まれていません。

提案されたアクション

ホストの完全修飾ドメイン名 (FQDN) を信頼済みサイトに追加してください。

次の手順を実行します。

1. コントロールパネルで、**インターネット オプション**を選択します。
2. [**セキュリティ**] タブを選択します。
3. [**信頼済みサイト**] を選択します。
4. [**サイト**] をクリックします。
5. [**追加**] をクリックします。
6. テキスト フィールドにホストの FQDN を入力して [**追加**] をクリックします。
7. [**閉じる**] をクリックします
8. [**OK**] をクリックします。

ホスト マシンから QMC にアクセスできない

Qlik Sense サイトをホストするマシンと同じマシンから QMC へのアクセスを試みていますが、ブラウザーに「**401.1 Access Denied**」エラーが表示されます。

考えられる原因

Windows Server のループバック セキュリティ設定により、Qlik Sense サイトをホストするマシンと同じマシンから完全修飾ドメイン名 (FQDN) を使用してアクセスすることができなくなっている可能性があります。

提案されたアクション

ローカルホストのアドレス *https://localhost/qmc* を使用して QMC にアクセスしてください。

ループ チェックを無効にすることも可能です。これについての詳細は、Microsoft サポート技術情報の記事を参照してください。

FQDN またはその CNAME エイリアスを使用してサーバーにローカルにアクセスしようとした場合のエラー メッセージ

QMC を起動すると、**[Unable to get the custom properties definitions (カスタム プロパティの定義を取得できません)]** と表示される

考えられる原因

リポジトリからカスタム プロパティの情報を取得するのに失敗しています。

提案されたアクション

QMCを更新します。

QMC を開くと、空白ページが表示される

考えられる原因

コンピュータに複数の DNS エントリーがあるため (複数のネットワークにログオンしたため)、*host.config* ファイルが誤ったホスト名を指している場合があります。

提案されたアクション

次の手順を実行します。

1. 稼働しているサービスをすべて停止します。
2. Qlik Sense のインストールに関連するすべての証明書を削除します。
3. *%ProgramData%\Qlik\Sense*フォルダを開きます。
4. *host.config* ファイルを削除します。
5. 修復を実行します。

host.config ファイルはデフォルト設定で再び作成されます。

QMCを開けない

QMC を開くと空白のページが表示されたり、別のプログラムが証明書を使用しているという警告が表示されます。SSLプロトコル エラーまたは接続が拒否されたことを伝えるメッセージが表示される場合もあります。

考えられる原因

別のプログラム (VMware、Skype、IISなど) が使用しているので、必要なポートを利用できません。

提案されたアクション

次の手順を実行します。

1. 次の場所でプロキシ システム ログを確認してください: *%ProgramData%\Qlik\Sense\Log\Proxy*。
2. プロキシが稼働中で、必要なポートを待ち受けることが可能か確認します。既定では、プロキシはポート 443 で稼働するので、このポートが利用可能になっている必要があります。
3. ポート443 を使用して、他のプログラムをすべて完全にシャットダウンし、プロキシ サービスを再起動します。また、これらのプログラムのポート設定を変更してください。

QMCを開こうとすると「ページを表示できません」と表示される

考えられる原因

Qlik Senseサービスを実行するサーバー上に存在する信頼されたルート証明書が多すぎます。

提案されたアクション

Qlik Sense Repository Service (QRS) のログを確認して、不必要な証明書はすべて削除してください。

> *システム管理者およびITセキュリティチームの確認が取れるまで、証明書は削除しないでください。*

次の手順を実行します。

1. QRSセキュリティログ ファイル (*%ProgramData%\Qlik\Sense\Log\Repository\Trace\<MachineName>_Security_Repository.txt*) に以下のメッセージが含まれていないか確認します。
   - 「Trusted root certificates on this node is uncomfortably high: <number of certificates> (このノード上には信頼されたルート証明書が多すぎます:<証明書の数>)」
   - 「This might impede SSL communication, since Windows truncates too large (300+) lists of Trusted root certificates that are sent to client during SSL handshake (このためSSL通信が妨げられる可能性があります。WindowsではSSLハンドシェーク中にクライアントに送られる信頼されたルート証明書の (300を超える) 大きすぎるリストが切り捨てられるためです)」
   - 「Please consider removing too old or otherwise invalid trusted root certificates (under <location>) (<場所> にある古い/無効な、信頼されたルート証明書の削除を検討してください)」
2. Microsoft管理コンソール (MMC) を開いて、不必要な証明書をできるだけ削除します。
   QRSセキュリティログは証明書のある場所の情報を含んでいます (ステップ1のログ メッセージの<location (場所)>を参照してください)。
3. Qlik Sense サービスを再起動します。

Qlik Sense の計画と展開

トラブルシューティング - QMC リソースの管理

このセクションでは、QMC リソースを管理するときに発生する可能性のある問題について説明しています。

エラー メッセージ: [**400 不正な要求**]

エラー メッセージ [**400 不正な要求**] が表示される場合、原因の可能性は複数あります。

QMC へのアプリのインポートに失敗

ログには、次のエラー メッセージが表示されます: Server:ImportApp_impl caught extended exception 400: Bad Request

考えられる原因

アプリに、URL が 1024 文字を超えるウェブ接続が含まれています。

提案されたアクション

1. Qlik Sense Desktop でアプリを開き、アプリに URL が 1024 文字を超えるウェブ接続が含まれているかどうか確認します。
2. bit.ly などのサービスを使用し、URL を短くします。

REST HTTP 要求が正しくありません

考えられる原因

プロキシまたはリポジトリへの REST HTTP 要求が不正に書式設定されています。

提案されたアクション

REST HTTP 要求の書式設定を修正してください。

> *完全なリクエストには、URL に ?XrfKey= <16 文字以上> が含まれている必要があります。また、同じリクエストで値と完全に同じ文字列の X-Qlik-XrfKey ヘッダーが含まれている必要があります (クロスサイトのスクリプト攻撃に抵抗するため)。*

エラー メッセージ: [**401 Unauthorized**] (401 権限がありません)

パスワードに特殊文字が含まれている場合、REST コネクターの認証は失敗します。

考えられる原因

QMC で、REST コネクタのパスワードを編集して特殊文字「%」および/または「=」および/または「;」を追加しています。

提案されたアクション

データ ロード エディターを使用してパスワードを編集します。

エラーメッセージ: [**403 Forbidden**]

考えられる原因

- コンピュータのルート証明書が多すぎる (300 以上) ため、Qlik Sense サービスの通信は認められません。
- リポジトリのルール エンジンによって、アクセスが許可されていないリソースにアクセスしようとしています。

提案されたアクション

使用されていないルート証明書を削除してください。以下の Microsoft ヘルプ ドキュメントも参照してください。
KB 931125 をインストール後の SSL/TLS 通信の問題

エラーメッセージ: [**405 Method not allowed**]

考えられる原因

URL は存在しない REST 機能を指しています。

提案されたアクション

URL を修正してください。

エラー メッセージ: [**Internal server error 500**]

エラー 500 が発生する場合、複数の原因が考えられます。

アプリのインポートに失敗しました

考えられる原因

2,500 文字を超える名前のアプリをインポートしようとしました。

提案されたアクション

アプリの名前を最大値の 2,500 文字以下にしてください。

不明なエラー

考えられる原因

不明のエラーが発生しました。

提案されたアクション

次の場所にあるシステム ログ ファイルをチェックします。

- *%ProgramData%\Qlik\Sense\Log\Proxy*
- *%ProgramData%\Qlik\Sense\Log\Repository*

エラー メッセージが繰り返し表示される場合は、Qlik Sense の担当者に連絡し、システム ログ ファイルを提供してください。

エラー メッセージ:Qlik Sense ハブに接続しようとすると[**Connection lost (接続が切断されました)**] と表示される

考えられる原因

Qlik Senseハブへのアクセス時に使用されるアドレスは、Qlik Sense Proxy Serviceのホスト許可リストに表示されません。

[**Connection lost (接続が切断されました)**] というエラー メッセージは一般的に次のようなケースで表示されます。

- Qlik Senseハブへのアクセスはホスト名「*https://myhost/hub*」やfully qualified name (FQN)「*https://myhost.company.com/hub*」ではなく「*https://192.168.0.25/hub*」などのIPアドレスを使って行われます。

- Qlik Senseハブへのアクセスはコンピュータの既定のDomain Name System (DNS) 名やFQNとして登録されているものとは違うアドレスを使って行われます。例えば、Amazon Web Service や類似の環境を使っている場合、内部に登録されているDNS 名は外部向けのアドレスと同一ではありません。

提案されたアクション

次の手順を実行します。

1. QMCから、[**仮想プロキシ**] を開きます。
2. 仮想プロキシを選択して、[**Edit (編集)**] をクリックします。
3. [**Properties (プロパティ)**] リストで、[**Advanced (詳細設定)**] をクリックします。
4. [**ホスト許可リスト**] を見付けます。
5. [**Add new value (新しい値の追加)**] をクリックして、クライアントからQlik Senseハブに接続するために使用されるアドレスを追加します。
   IPアドレス: 192.168.0.10、FQN: *myqlikserver.company.com*。
6. [**適用**] をクリックします。
   プロキシ再起動 メッセージが表示されます。
7. [**OK**] をクリックします。

許可リストにcompany.comを追加すると、ドメイン全体を許可リストにできます。これは、その他のドメイン内のアドレスをすべて許可リストにします。例: myqlikserver1.company.com、myqlikserver2.company.com。

エラー メッセージ: [**ODBC connection failed (ODBC 接続に失敗しました)**]

予定されたリロードが失敗して、エラー メッセージ [**ODBC connection failed (ODBC 接続に失敗しました)**] が表示されました。

考えられる原因

データ接続にはシングル サインオン (SSO) が採用されているため、接続が実際のユーザーによって使用されることやアプリが「SQL SELECT…」を使ってデータをロードすることが必要です。

この問題に対して考えられるソリューションは複数あります。

提案されたアクション (データ接続を変更して SSO を使わないようにする)

使用される必要のあるユーザー名とパスワードを指定してください。

提案されたアクション (手動でリロードを実行する)

データ接続への変更を行わないようにする場合、タスクを使うのではなく手動でもリロードを実行できます。

提案されたアクション (SQL からDirect Discoveryテーブルに変更する)

SSO と併用でDirect Discoveryテーブルを使用する場合、タスクを使ってアプリをリロードできます。

ユーザー アカウントで REST データ接続を使用するとユーザーがロックアウトされる

考えられる原因

REST データ接続を、AD/LDAP/ユーザー ディレクトリで利用可能なサービス アカウントではなく通常のアカウントで設定した場合、単一ユーザー アカウントの並列接続セッションの最大数 (5) が使用され、このユーザーは一時的にロック アウトされます。

提案されたアクション

ユーザー アカウントの代わりにサービス アカウントを使用し、ユーザー/プロフェッショナル/アナライザー アクセスはそのユーザー アカウントに一切割り当てないようにしてください。

タスクが実行されない

考えられる原因

タスクの状態は [**Success (成功)**] ではありません。

提案されたアクション

QMC のタスク概要ページで、状態列の ⓘ をクリックして実行 ステップの概要を表示します。

%ProgramData%\Qlik\Sense\Log\Scheduler の下にあるログ ファイルを確認します。

リロードが機能しない

リロードが機能しない場合に考えられる原因は複数あります。

リロードに失敗した

アプリで [**Reload now (すぐにリロード)**] をクリックしましたが、リロードが起動しません。

考えられる原因

タスクの状態は [**Success (成功)**] ではありません。

提案されたアクション

次の場所でログ ファイルを確認してください: *%ProgramData%\Qlik\Sense\Log\Script*。

マルチノード環境でリロードに失敗した

マルチノードの環境でアプリを選択して [**More actions (その他のアクション)**] > [**Reload now (今すぐリロード)**] をクリックしましたが、リロードは失敗し、次のメッセージが表示されました。[**タスクを実行するワーカー ノードが見つかりませんでした**]

考えられる原因

セントラル スケジューラーが [**Manager only (マネージャーのみ)**] に設定されています。

提案されたアクション

タスク実行を再トリガーします。

[**Edit scheduler (スケジューラーの編集)**] ページの [**詳細**] で、[**Type (タイプ)**] を [**マネージャーおよびワーカー**] に変更します。

スタートページで、エンジン、リポジトリ、プロキシ、スケジューラの横に数字が表示される

考えられる原因

サービスが停止しています。

提案されたアクション

次の場所にあるログ ファイルを確認します: *%ProgramData%\Qlik\Sense\Log\<サービス>*

必須の SAML 属性名が分からない

考えられる原因

必須の属性名 (userID, userDirectory、または追加された必須の属性名) は利用できません。

提案されたアクション

次の手順を実行します。

1. 属性名として任意の名前を入力します。
2. 認証を試行します。
   属性名が間違っているため、試行は失敗します。
3. Proxy Audit ログで、「Existing SAML attributes:」を含む行を探します。
   利用できるすべての属性の name か friendlyName とValue を見つけます。
4. 使用する属性名を探し、最初に入力した任意の名前の代わりにその属性名を使用します。

次はログで検索できる例です。

既存の SAML 属性: [Name='uid', Value='jod'] [Name='givenName', Value='John'] [Name='sn', Value='Davidson'] [Name='cn', Value='John Davidson'] [Name='mail', Value='john.davidson@domain.com']

ユーザーのプロパティを変更できない

考えられる原因

アクティブ ディレクトリ(AD) からインポートされたユーザープロパティは、QMC では変更できません。

提案されたアクション

AD でプロパティを変更してから再び同期します。

ユーザー ディレクトリの同期 (page 308)

ユーザー同期が動作しない

- [**ユーザー ディレクトリ コネクタ**] の概要で [**Sync all selected user directories (選択したユーザー ディレクトリをすべて同期)**] をクリックしても、ユーザーを同期できません。

- 予定したユーザー同期のタスクが成功しません。

UDC が設定されない

考えられる原因

ユーザー ディレクトリコネクタが [**設定**] されていません。

提案されたアクション

[**User directory (ユーザー ディレクトリ)**] の名前が一意のもので、空白になっていないことを確認します。

UDC が機能しない

考えられる原因

ユーザー ディレクトリコネクタが [**機能**] していません。

提案されたアクション

この場所で *UserManagement_Repository* ログを確認します: *%ProgramData%\Qlik\Sense\Log\Repository\Trace*
ユーザー ディレクトリコネクタの基になっているソース ファイルを削除すると、機能しません。

UDC のプロパティ[**Page size of search (検索のページ サイズ)**] が正しくない

考えられる原因

ユーザー ディレクトリコネクタのプロパティ[**Page size of search (検索のページ サイズ)**] が正しくありません。

提案されたアクション

ユーザー ディレクトリコネクターのプロパティ[**Page size of search (検索のページ サイズ)**] を「0」(ゼロ) に設定します。

PostgreSQL データベースでテーブル名の大文字が認識されない

考えられる原因

PostgreSQL データベースにおいて大文字または特殊文字 ("." など) を含むテーブル名は、検証時にエラーとなります。

提案されたアクション

大文字または特殊文字を含むテーブル名には引用符を使用してください。

```
"table.Name", public."Table" (または "Table"), testschema."Table"
```

拡張機能をインポートできない

考えられる原因

- 拡張機能が圧縮されていません。
- 圧縮ファイルの形式が間違っています。
- zip ファイルに無効なファイルが含まれています。
- 拡張機能のパスワードが正しくありません。
- 拡張機能が既存の拡張機能と重複しています。

提案されたアクション

- 拡張ファイルが正しく圧縮されていることを確認してください。圧縮には、zip ファイル以外の他のファイル形式は使用できません。
- zip ファイルに含まれているのが関連の拡張ファイルのみであることを確認してください。
- *QMC にすでに存在する拡張子をインポートする場合は、プロンプトが表示されたら、[**Replace**] (置き換え) をクリックして既存のファイルを新しいファイルに置き換えるか、[✕] をクリックしてキャンセルします。*

  拡張機能名 (page 266)

.lock ファイルを削除したらアプリを開けなくなった

考えられる原因

...*Sense**Apps* フォルダーの各アプリには .lock ファイルが付属しており、このファイルが削除されると、アプリを開くことができなくなります。

提案されたアクション

Qlik Sense Repository Service を再起動します。新しい .lock ファイルがアプリに生成されます。

ロックファイルは、qvf ファイルのロックを調整するために使用されます。qvf ファイルの読み取りが必要なスレッドは、書き込み中のスレッド(排他的ロックを保持) が終了するまで待機する必要があります。同様に、排他的ロックが必要なスレッドは、ファイルを読み取り中のスレッドが終了するまで待機する必要があります。

マルチノード環境のノードがオンラインにならない

QMC でノードを再作成しましたが (作成、削除して、もう一度作成)、ノードがオンラインになりません。ログには次の警告メッセージが記録されています。「ノードは無効です (最も考えられる原因はクラスタからの登録解除になります)。スタートアップを中止します...」が表示されています。

考えられる原因

削除されたノードを複数ノードの環境で再起動や再利用することはできません。

提案されたアクション

次の手順を実行します。

1. QMC でノードを削除してください。
2. ノードからソフトウェアをアンインストールします。
3. ノードでソフトウェアを再インストールします。
4. QMC でノードを再び作成します。

マルチノードサイト: ドメイン外にあるリム ノードとの通信が不可

考えられる原因

通常、Qlik Senseのマルチノードサイトにあるノードはすべて、同じ Windows のドメイン内にあります。リム ノードの 1 つがドメイン外にあり、ホスト名検索で DNS を利用できない場合、各ノードの Windows ホストファイルが更新されていない限り、ドメイン内のノードはドメイン外のノードと通信できません。

提案されたアクション

次の手順を実行します。

- ドメイン内にあるすべてのノード: ドメイン外のリム ノードを特定するための情報を用いて、Windows ホストファイル (通常は *C:\Windows\System32\drivers\etc\hosts*) を更新します。
  例: <ドメイン外にあるリム ノードの IP アドレス> <リム ノードのホスト名>
- ドメイン外にあるリム ノード:
  - ドメイン内のすべてのノードを特定するための情報を用いて、Windowsホストファイルを更新します。

    <ドメイン内にあるノード1 の IP アドレス> <完全な記述によるノード1 のドメイン名>
    <ドメイン内にあるノード2 の IP アドレス> <完全な記述によるノード2 のドメイン名>
  - リム ノード自体のホスト名に関する情報を用いて、Windowsホストファイルを更新し、リム ノードにあるQlik Senseサービス間の通信を可能にします。
    例: <ドメイン外にあるリム ノードの IP アドレス> <リム ノードのホスト名>

トラブルシューティング - QMC での移動

このセクションでは、QMC でのナビゲーション時に発生する可能性のある問題について説明しています。

QMC のアイコンが正しく表示されない

考えられる原因

Qlik Sense サイトは、信頼済みサイトの一覧に含まれていません。

提案されたアクション

QMC サイトをMicrosoft Edgeの信頼済みサイトとして追加します。

次の手順を実行します。

1. コントロールパネルで、**インターネット オプション**を選択します。
2. [**セキュリティ**] タブを選択します。
3. [**信頼済みサイト**] をクリックします。
4. [**サイト**] をクリックします。
5. テキスト ボックスに QMC の Web サイト アドレスを入力して [**追加**] をクリックします。
6. [**Close**] (閉じる) をクリックします。

アイコンが正しく表示されません。

エラー メッセージ: [信頼できないプロキシ SSL 接続/証明書]

ブラウザで、[**プロキシ SSL-接続/-証明書は信頼できません!**] と表示され、例外を作成したいのか、その認証局を信頼するのかどうかを尋ねています。

考えられる原因

Thawte や VeriSign といった有名な認証局のルート証明書でないと、ブラウザでルート証明書が認識されないことがあります。

提案されたアクション

次の手順を実行します。

1. 質問に [**はい**] と答えて、例外の作成とその認証局の信頼を承認します。
2. Qlik Sense の既定の証明書を使用できるようにするには、パブリック SSL 証明書が必要です。サーバーにインストール済みかどうかを確認してください。

プロキシ証明書の変更 (page 503)

エラーメッセージ: [404 Not found]

考えられる原因

URL が存在しないリソースを参照しています。

提案されたアクション

URL を修正してください。

トラブルシューティング - アクセス制御の設計

このセクションでは、QMC でアクセス制御を設計するときに発生する可能性のある問題について説明しています。

ユーザー ディレクトリ コネクタのセキュリティ ルールを作成できない

考えられる原因

セキュリティ ルールで [**名前**] で、ユーザー ディレクトリ コネクタの値を使用しようとしています。

提案されたアクション

セキュリティ ルールの [**ユーザー ディレクトリ**] で、ユーザー ディレクトリ コネクタの値を使用する必要があります。

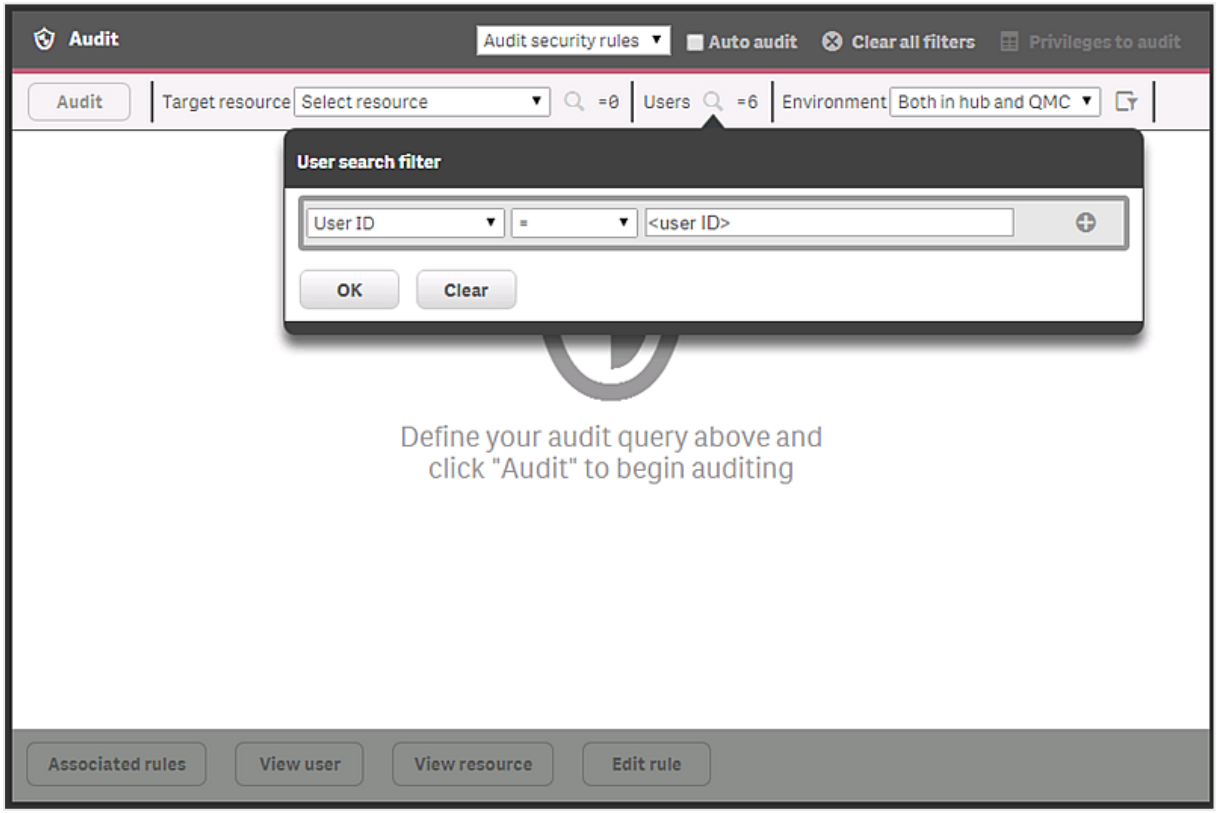
あるユーザーは、アクセスすべきでないストリームにアクセスできるようです

考えられる原因

1 つあるいはそれ以上のセキュリティ ルールに、アクセス権を要求しているユーザーの複数のアクセス権が含まれています。

提案されたアクション

以下の監査クエリーを作成して、そのユーザーがアクセスできるストリームを見つけてください。必要に応じて、セキュリティ ルールを無効にするか、編集します。



セキュリティ ルールに関連するアプリ アクセスの問題

不適切に設計されたカスタム セキュリティ ルールは、次の問題を引き起こす可能性があります。

- ユーザーは、開くことができるはずのアプリを開くことはできません。
- ユーザーは、開くことができないはずのアプリを開くことができます。

考えられる原因

1 つ以上のカスタム セキュリティルールが機能していないため、過剰なアクセス許可またはアクセス許可の欠如が発生するはずです。

提案されたアクション

ここで説明されている方法に従ってください:Qlik Sense Enterprise セキュリティルールのトラブルシューティング

トラブルシューティング - 一般

トラブルシューティング セクションは、主に QMC とは関連しない一般的な問題を扱います。

Apps の Search サブフォルダーのサイズが非常に大きい

%ProgramData%\Qlik\Sense\Apps にある Search フォルダーのサイズが非常に大きくなってしまい、サーバーのハードドライブの容量を圧迫してしまう可能性があります。

考えられる原因

Search フォルダーは、アプリ検索のキャッシュの保存に使用され、ファイルは自動的には削除されません。

提案されたアクション

Search フォルダーを削除します。

1.13 Insight Advisor の参照元機械学習

Insight Advisor は、アプリを分析し、チャートの作成に項目がどのように使用されているかを確認できます。Qlik 参照元サービスは、アプリで **Insights** が開いているときは常にアプリを分析します。このサービスは、チャート内のデータ項目とマスター アイテムの使用状況を調査します。これにより、アプリのデータ モデルに関する集計、軸、およびメジャーを作成する参照元が Insights に伝達されます。未公開アプリでは、Insights は、公開されたアプリやアプリのユーザー フィードバックから学習した参照元を使用できます。

アプリの分析では、項目に含まれるデータは調査されず、データ テーブルと項目名、およびこれらの使用方法のみが調査されます。アプリ分析は、Insight Advisor で公開されたすべてのアプリに対して有効になります。Insight Advisor にそのアプリから参照元を学習させたくない場合は、公開アプリで Insight Advisor を無効にすることができます。

1.14 Qlik Sense Enterprise on Windows での Qlik Insight Advisor Chat の構成

Qlik Insight Advisor Chat はチャットベースのインターフェースで、自然言語を使用して質問をし、データの洞察を探索することができます。これは Qlik Sense Enterprise on Windows で利用可能であり、Qlik Insight Advisor Chat を Slack や Microsoft Teams などのサードパーティツールに統合できるため、ユーザーは Qlik Sense アプリからコミュニケーションプラットフォームで直接洞察を得ること

ができます。

Qlik Insight Advisor Chat へのサブスクリプションを含む、有効な Qlik 製品ライセンスが必要です。製品ライセンスの詳細については、サイト管理者に問い合わせてください。

Qlik Insight Advisor Chat に Qlik Sense アプリを含めるには、[Insight Advisor チャットでアプリを使用可能にする] を参照してください。アプリを含めることを有効にしたら、Qlik Sense ハブから Qlik Insight Advisor Chat を使用する方法については、[会話分析を使用したアプリの探索] を参照してください。

Qlik Insight Advisor Chat のアクセス制御の作成

Qlik Sense 管理者ユーザーは、QMC でセキュリティルールを作成することにより、Qlik Insight Advisor Chat へのアクセスを制限できます。

セキュリティルールは、Qlik Sense ハブでのユーザーおよびグループアクセスにのみ適用されます。Slack や Microsoft Team などのサードパーティのコミュニケーション ツールを介したアクセスは、QMC のセキュリティルールの影響を受けません。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC スタートページから、あるいは [**スタート**] ▼ ドロップダウン メニューから [**セキュリティルール**] を選択します。
3. データ マネージャーでテーブルの **新規作成** をクリックします。
   左側に編集パネル (すべてのプロパティを保持)、右側に監査ページが配置された分割ページが表示されます。
4. [**Identification (ID)**] で、ルールに名前を付け、説明を入力します。
5. [**基本**] で、次のリソース フィルターを入力します。*IAChat_** を入力し、アクションとして [**読み取り**] を選択します。
   - すべての名前付きユーザーにアクセスを提供するには、条件 *((user.name!=""))* を入力します。
   - user1 という名前の特定のユーザーへのアクセスを制限するには、条件 *((user.userId="user1"))* を入力します。
6. [**詳細設定**] で、[**ルールの検証**] をクリックして、ルールが正しく設定されていることを確認します。

このルールは、ブラウザを更新するときに適用する必要があります。ルート管理者は常に Qlik Insight Advisor Chat にアクセスできます。

QMC でのアクセス制御とセキュリティルールの設計の詳細については、[セキュリティルールの作成] を参照してください。

外部チャネル用の Qlik Insight Advisor Chat の構成

ボット チャネル サービスを Slack や Microsoft Teams などのサードパーティ ツールに接続して、ユーザーがサードパーティのコミュニケーション ツールから直接 Qlik Sense データに関する洞察を得ることができるようにすることができます。

前提条件

- Qlik Sense ユーザーには、userId にリンクされたメール アドレスが必要です。
- Microsoft Azure ポータルにアクセスでき、Azure ボットを作成する権限があります。

  ボットとサービスは Azure でホストする必要はありませんが、Microsoft Teams ボットと Slack ボットのブローカーは Microsoft Azure を使用します。

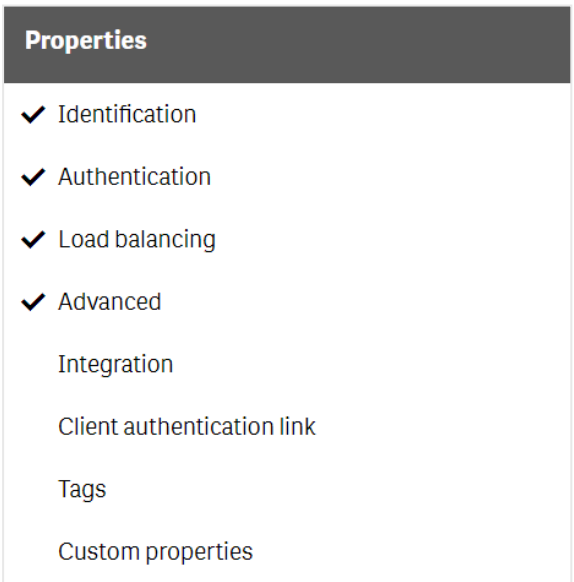
- Slack または Microsoft Teams、あるいはその両方で通信エンドポイントを構成するためのアクセス権と許可があります。

仮想プロキシの構成

外部チャネル用に Qlik Insight Advisor Chat を構成する最初のステップは、QMC に仮想プロキシを作成することです。仮想プロキシは、ボット チャネル サービスと他の Qlik サービス間の通信ネットワークを提供します。

次の手順を実行します。

1. QMC にログインします。QMC の既定のアドレスは、*https://<QPS server name>/qmc* です。
2. [**仮想プロキシ**] を選択します。
3. [**新規作成**] を選択します。
4. [**仮想プロキシの編集**] 構成ページで、右側の [**プロパティ**] メニューから [**識別**]、[**認証**]、[**負荷分散**]、[**詳細**] を選択します。



5. 次の詳細を入力します。
   識別

説明	jwt
プレフィックス	jwt
タイムアウトまでのセッション アイドル時間 (分)	30
セッション クッキー ヘッダー名	X-Qlik-Session-jwt

   認証

匿名アクセス モード	匿名ユーザーなし
認証方法	JWT
JWT 証明書	JWT 証明書を貼り付けます。

   > *%ProgramData%\Qlik\Sense\Repository\Exported Certificates\.Local Certificates\server.pem にある server.pem 証明書を使用します。*

[ユーザー ID に使用する JWT 属性]	userId
[ディレクトリに使用する JWT 属性]	userDirectory

   負荷分散
   [**負荷分散**] で、[**新しいサーバー ノードの追加**]を選択し、[**セントラル**] を選択します。

   詳細設定
   [**ホスト許可**] リストで、[**新しい値の追加**] を選択します。*localhost*、およびボット チャネル サービスに接続するその他のサーバーを追加します。

   > *他のすべての項目は空白のままにするか、既定値を選択できます。*

6. [**適用**] をクリックして、仮想プロキシ サービスを再起動することに同意します。
7. 右側の [**プロパティ**] メニューの [**関連アイテム**] で、[**プロキシ**] を選択します。
8. [**リンク**] をクリックします。
9. セントラル ノードを選択し、[**リンク**] をクリックします。

仮想プロキシの構成が完了すると、Microsoft Azure Web App Bot を作成できます。このボットは、通信プラットフォームとボット チャネル サービス間の通信を中継します。

Microsoft Azure Bot Service の作成 (page 651)

Microsoft Azure Bot Service の作成

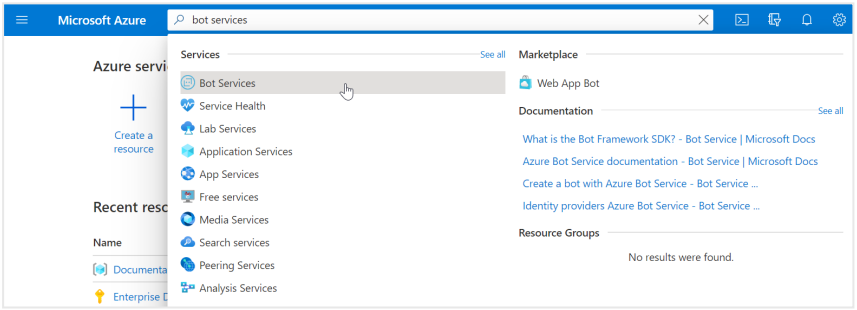
仮想プロキシを構成したら、Microsoft Azure Bot Service を作成する必要があります。Bot Service は、ユーザーと外部チャネル間の通信を提供します。

開始する前に、メモ帳を開いて、構成を完了するために必要なユーザー名、パスワード、ID、トークンを記録することをお勧めします。次のテンプレートをメモ帳にコピーします。

```
====Microsoft Azure Bot Service====
Bot handle =
MicrosoftAppId =
MicrosoftAppPassword =
===================================
===================================
```

次の手順を実行します。

1. Microsoft Azure ポータルにログインします。
2. 検索バーに「*Bot Service*」と入力します。[**サービス**] で、[**Bot Service**] を選択します。



3. [**作成**] をクリックします。
4. リストから [**Azure ボット**] を選択します。
5. [**作成**] をクリックします。
6. 次のパラメータを使用して Azure Bot を作成します。

パラメータ	**値**
Bot ハンドル	一意の名前を入力してください。
サブスクリプション	サブスクリプションを選択します。
リソース グループ	リソース グループを選択します。
データ所在地 (プレビュー)	グローバル
価格帯	適切な価格帯を選択します。
Microsoft アプリ ID	アプリのタイプ。**マルチ テナント**を選択します。 作成タイプ。[**新しい Microsoft アプリ ID を作成する**] を選択します。

終了したら、[**確認 + 作成**] をクリックします。

7. Azure ボットの検証が完了したら、[**作成**] をクリックします。
展開ページが表示されます。展開が完了するのを待ちます。

8. 左側のメニューで、[**入力**] をクリックします。
9. [**入力**] ページから、**ボット ハンドル** と**msAppId** (Microsoft アプリID) をメモ帳にコピーします。
10. [**概要**] ページに移動し、[**リソースに移動**] をクリックします。
11. 左側のメニューで [**設定**] > [**構成**] と進みます。
12. メッセージング エンドポイントを入力して [**適用**] をクリックします。
    メッセージング エンドポイントは、Qlik Sense 中央ノード サーバーへの URL です。メッセージング エンドポイントを含めます。例: *https://qliksense.domain.com/api/messages*。
13. クライアント シークレットを作成するには、**Microsoft アプリID** の横にある [**管理**] をクリックします。
    a. [**クライアント シークレット**] セクションで、[**新しいクライアント シークレット**] をクリックします。
    b. 説明を入力して有効期限を選択し、[**追加**] をクリックします。
    c. [**値**] 列で、値 (MicrosoftAppPassword) をメモ帳にコピーします。

これで、Azure Bot で通信チャネルを構成する準備が整いました。

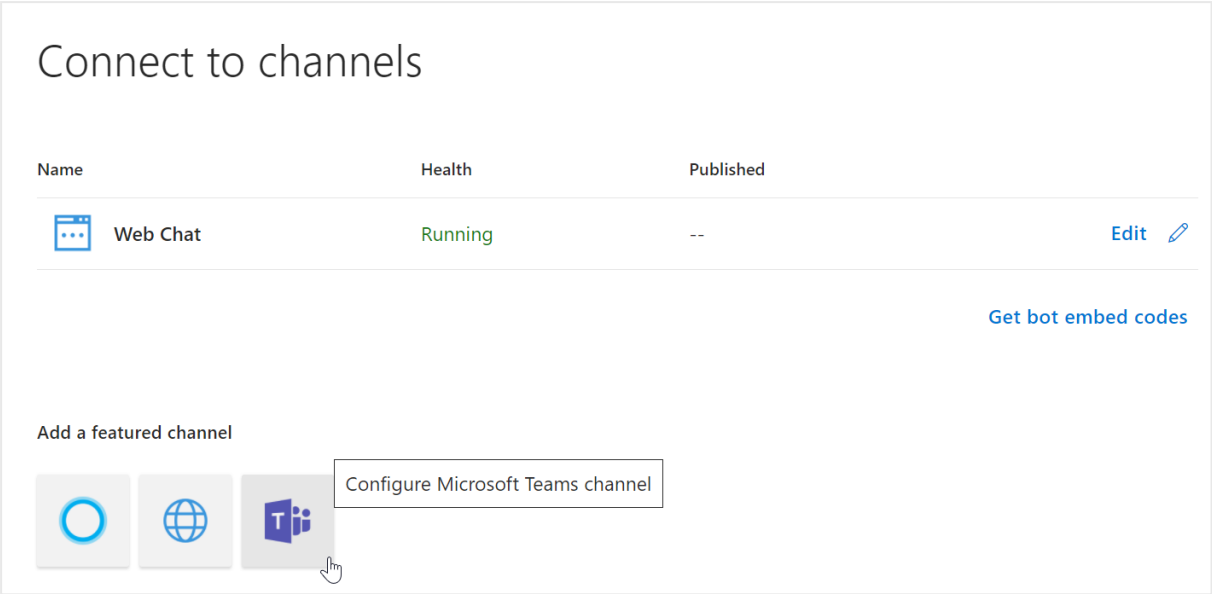
- *Slack の通信チャネルの構成 (page 653)*
- *Microsoft Teams の通信チャネルの構成 (page 652)*

Microsoft Teams の通信チャネルの構成

Microsoft Azure Bot を作成したら、Microsoft Teams チャネルを有効にできます。これにより、自然言語クエリを使用して、Microsoft Teams から直接 Qlik Sense データをクエリできます。

次の手順を実行します。

1. Microsoft Azure ポータルにログインします。
2. [**リソース グループ**] をクリックして、リソースのリストを表示します。
3. 前に作成した Azure Bot をクリックします。
4. [**ボット管理**] で、[**チャネル**] を選択します。
5. [**注目チャネルの追加**] で、[**Microsoft Teams**] を選択し、[**保存**] をクリックします。



6. 適切なメッセージング タイプを選択し、[**保存**] をクリックします。

> *続行するには、利用規約に同意する必要があります。*

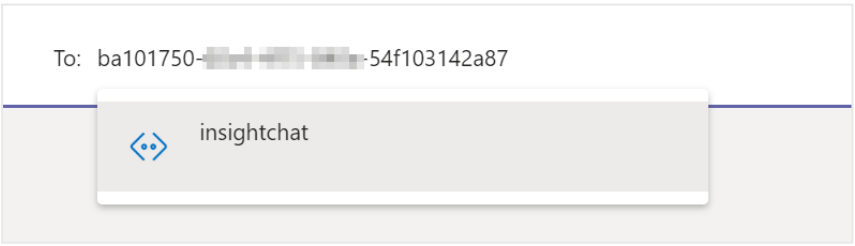
これで、Microsoft TeamsとMicrosoft Azure Bot の間に通信チャネルが できました。

MicrosoftTeams での会話の開始

通信チャネルが設定されたので、Teams を使用して Qlik Sense アプリから洞察を得ることができます。

次の手順を実行します。

1. Microsoft Teams を開きます。
2. [**新しいチャット**] をクリックします。
3. [**宛先:**] 項目に、メモ帳にコピーした **MicrosoftAppId** を入力します。



4. これで、Team チャットを使用して、Qlik Sense アプリに関するクエリを実行できます。

通信チャネルを構成したので、Bot チャネル サービスを構成できます。

Slack の通信チャネルの構成

Microsoft Azure Bot を作成したら、Slack チャネルを有効にできます。これにより、自然言語クエリを使用して Slack から直接 Qlik Sense データをクエリできます。

開始する前に、メモ帳を開いて、構成を完了するために必要なユーザー名、パスワード、ID、トークンを記録することをお勧めします。このセクションをメモ帳の下部に追加します。

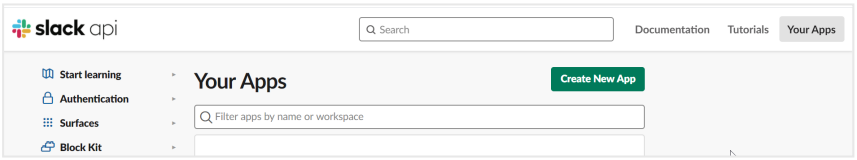
```
====Slack details====
Slack bot URL =
Bot User OAuth Access Token =
Client ID =
Client Secret =
Signing secret =
==================================
==================================
```

Slack アプリの作成

次の手順を実行します。

Slack API を使用するには、Slack 管理者権限が必要です。

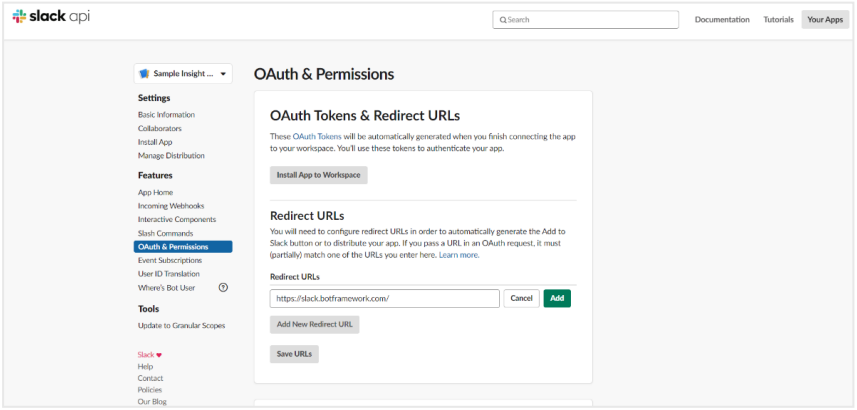
1. [Slack API] に移動します。
2. 上部のナビゲーション バーで、[**アプリ**] をクリックします。
3. [**アプリを作成**] をクリックします。



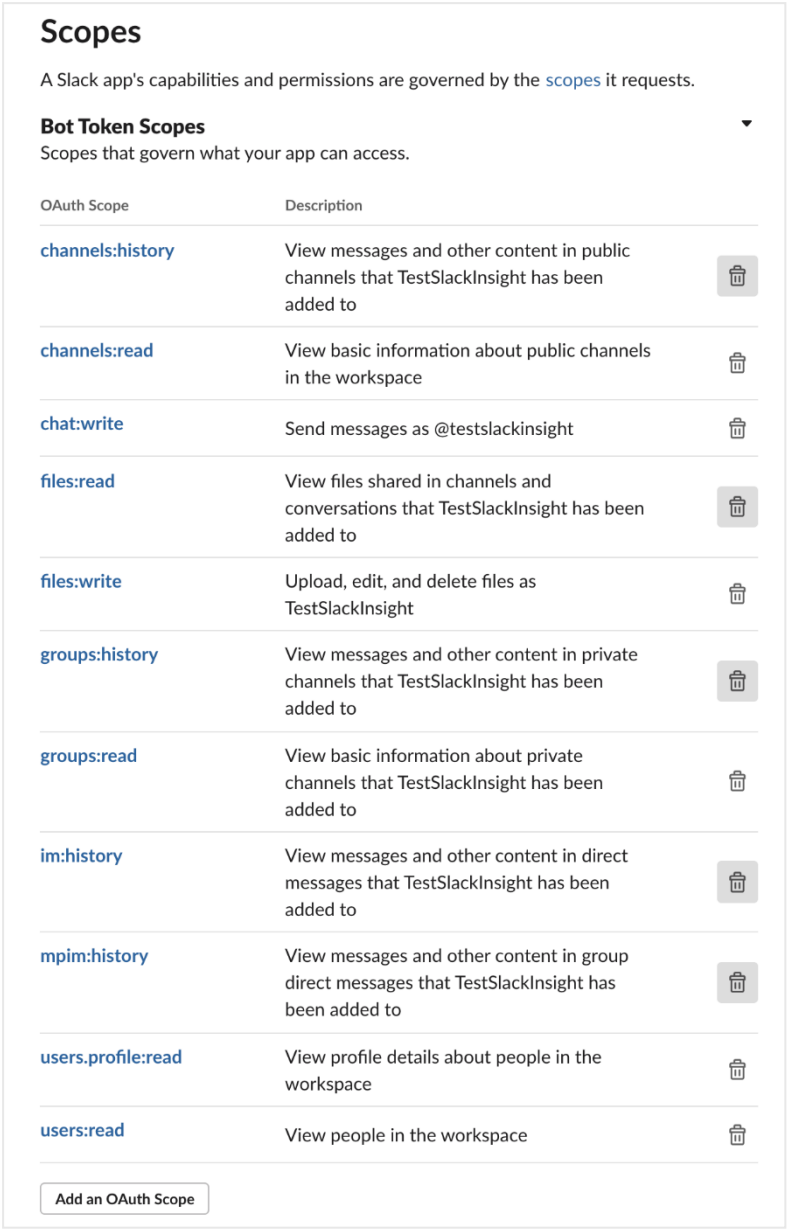
4. [**アプリ名**] を入力し、[**開発 Slack ワークスペース**] を選択して、[**アプリを作成**] をクリックします。

リダイレクト URL の追加

1. 左側のメニューの [**機能**] で、[**OAuth と権限**] を選択します。
2. [**新しいリダイレクト URL を追加**] をクリックします。
3. *https://slack.botframework.com* と入力し、[**追加**] をクリックします。

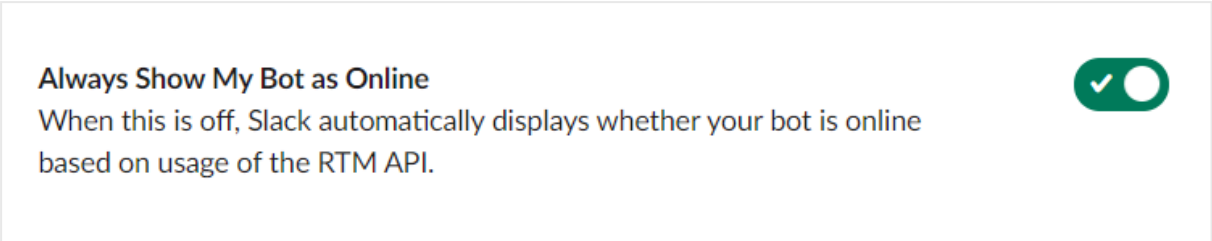


4. [**URL を保存**] をクリックします。
5. [**スコープ**] セクションまで下にスクロールします。次の [**ボット トークン スコープ**] を追加します。



Slack ボット ユーザーの作成

1. 左側のメニューの [**機能**] で、[**アプリのホーム**] をクリックします。
2. [**ボットを常にオンラインとして表示**] をオンに切り替えます。



3. スクロールダウンして、[メッセージ] タブから [**ユーザーによる Slash コマンドとメッセージの送信を許可**] を選択します。

このセクションでは、表示名と既定名を確認または編集します。

Slack ボット イベントのサブスクライブ

1. 左側のメニューの [**機能**] で、[**イベント サブスクリプション**] をクリックします。
2. [**イベントを有効化**] をオンに切り替えます。
3. [**リクエスト URL**] 項目に、メモ帳に保存した Azure Bot URL を入力します。

   URL は https://slack.botframework.com/api/Events/{Bot handle} である必要があります。ここで、{bot handle} は Azure Bot ハンドルです。

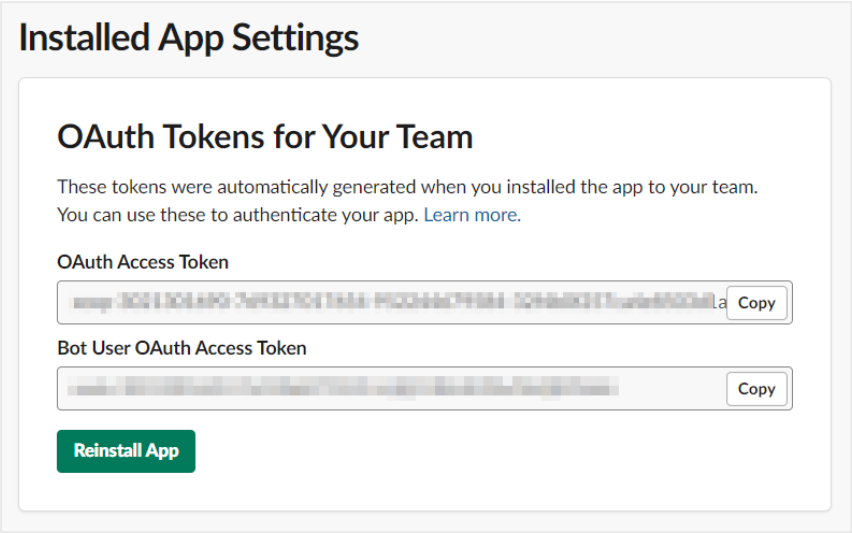
4. 下にスクロールして [**ボット イベントのサブスクライブ**] を選択し、次のユーザー イベントを追加して、[**保存**] をクリックします。
   - member_joined_channel
   - member_left_channel
   - message.channels
   - message.groups
   - message.im
   - message.mpim

インタラクティブ コンポーネントの構成

1. 左側のメニューの [**機能**] で、[**インタラクティブ コンポーネント**] を選択します。
2. [**インタラクティブ**] 機能を切り替えます。
3. [**リクエスト URL**] 項目に *https://slack.botframework.com/api/Actions* と入力し、[**変更を保存**] をクリックします。

アプリケーションのインストール

1. 左側のメニューの [**設定**] で、[**アプリのインストール**] を選択します。
2. [**アプリをワークスペースにインストール**] をクリックします。
3. 開いた権限要求ウィンドウで、[**許可**] をクリックします。
4. [**ボット ユーザーの OAuth アクセス トークン**] をコピーします。



OAuth トークンをメモ帳に保存して、後でボットチャネル構成アプリを構成するときに使用します。

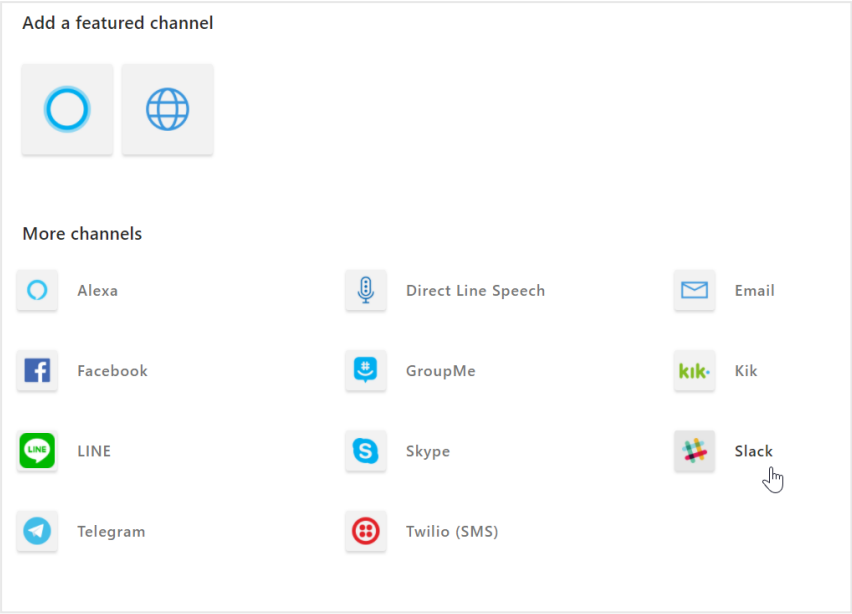
5. 左側のメニューの [**設定**] で、[**基本情報**] を選択します。
6. [**アプリの資格情報**] まで下にスクロールします。
7. [**クライアント ID**]、[**クライアント シークレット**]、[**署名シークレット**] をコピーします。

これらをメモ帳に保存します。

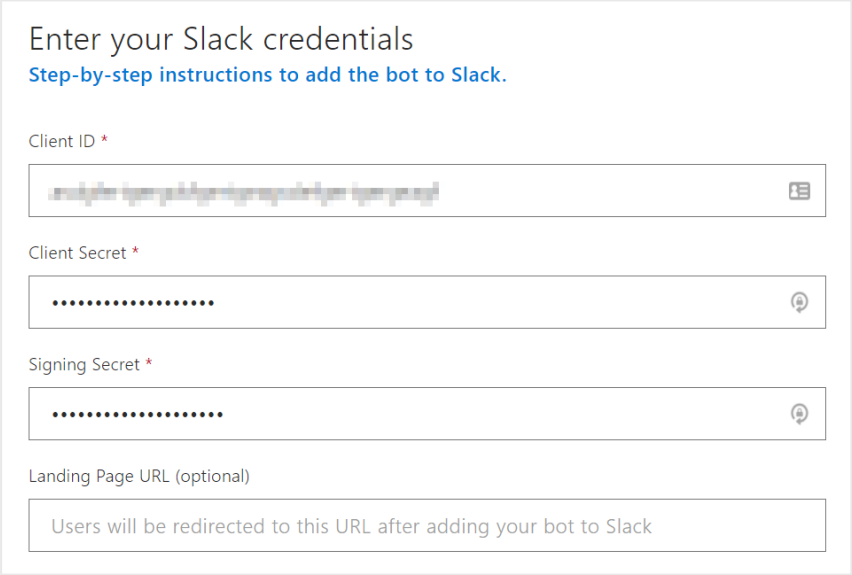
Azure での Slack ボットの構成

次の手順を実行します。

1. Microsoft Azure ポータルにログインします。
2. [**リソース グループ**] をクリックして、リソースのリストを表示します。
3. **Azure Bot** をクリックして構成します。
4. [**ボット管理**] で、[**チャネル**] を選択します。
5. [**その他のチャネル**] で、[**Slack**] を選択します。



6. [**クライアント ID**]、[**クライアント シークレット**]、[**署名シークレット**] 項目に、前に保存した値を入力し、[**保存**] をクリックします。



7. 開いた権限要求ウィンドウで、[**許可**] をクリックします。

通信チャネルを構成したので、Bot チャネル サービスを構成できます。

Bot チャネル サービスの構成

この Bot チャネル サービスは、デフォルトでは無効になっています。これを有効にするには、*services.config* ファイルでパラメーターを構成する必要があります。

Bot チャネル サービスのユーザー構成のセットアップ

1. Qlik Sense Enterprise on Windows サーバーにログオンします。
2. *%ProgramFiles%\Qlik\Sense\BotChannelService\install* に移動します。
3. *ChannelConfig.bat* ファイルを実行します。
   バッチファイル (.bat) を実行するときは、関連するチャット bot パラメーターを入力するよう求められます。

パラメーター	必須	既定値	説明
microsoftAppId	はい		Azure Web App の Bot を作成したときに生成された Microsoft App ID。
microsoftAppPassword	はい		Azure Web App の Bot を作成したときに生成された Microsoft App パスワード。
slackBotToken	いいえ	該当なし	Slack アプリの作成時の Bot ユーザー OAuth トークン。Slack に接続したくない場合は、空のままにします。
qlikRootUserId	はい		ユーザーの Qlik Sense ユーザーID。QMC の [**ユーザー**] の下にリストされています。
qlikRootUserDir	はい		ユーザーの移動元のユーザー ディレクトリ。QMC の [**ユーザー**] の下にリストされています。
virtualProxyPrefix	はい		Qlik Sense 仮想プロキシを作成したときの仮想プロキシ プレフィックス。
externalURL	いいえ	該当なし	Qlik Sense 公開 URL。URL には、仮想プロキシ プレフィックスを含めることができます (例: *insight.qlik.com/{vp_prefix}*)。 *HTTPS を URL に追加しないでください。*
disableParsingInfo	いいえ	*N*	*Y* 情報の解析を無効にする場合。
emailInAttribute	いいえ	*Y*	*N* [**Name**] または [**UserID**] プロパティでユーザーのメール アドレスが使用可能な場合。 例えば、次の画像では、John のメール アドレスは [**UserID**] にあり、Anna のメール アドレスは [**Name**] にあります。 **Name** / **User directory** / **User ID** John / UDC_BDM / john@qlik.com anna@qlik.com / UDC_BDM / anna *Y* メール アドレスが別のプロパティで定義されている場合。
emailPropertyNam	い	電	**emailInAttribute** に *N* を入力した場合は、*name* または *userid*

パラメーター	必須	既定値	説明
e	いえ	子メール	を入力して、メール アドレスが配置されるプロパティを指定します。 **emailInAttribute** に *Y* を入力した場合は、メール アドレスに使用されるプロパティ名を指定します。プロパティ名を指定しない場合は、既定値が使用されます。 例えば、Anna のメール アドレスはカスタム プロパティ**custom_field** にあります。John のメール アドレスは、既定のプロパティ**email** にあります。

User: Anna	
Property	**Value**
blacklisted	false
custom_field	qlikuser2@qlik.com
deleteProhibited	false
inactive	false
name	Anna
removedExternally	false
userDirectory	UDC_BDM
userId	qlikuser2

User: John	
Property	**Value**
blacklisted	false
deleteProhibited	false
email	qlikuser1@qlik.com
inactive	false
name	John
removedExternally	false
userDirectory	UDC_BDM
userId	qlikuser1

*完了すると、**「構成が成功しました」**というメッセージが表示されます。エラー メッセージが表示された場合は、bat ファイルを再度実行してください。*

チャット ボット サービスの有効化

マルチノード サイトでは、これはセントラル ノードで実行する必要があります。

次の手順を実行します。

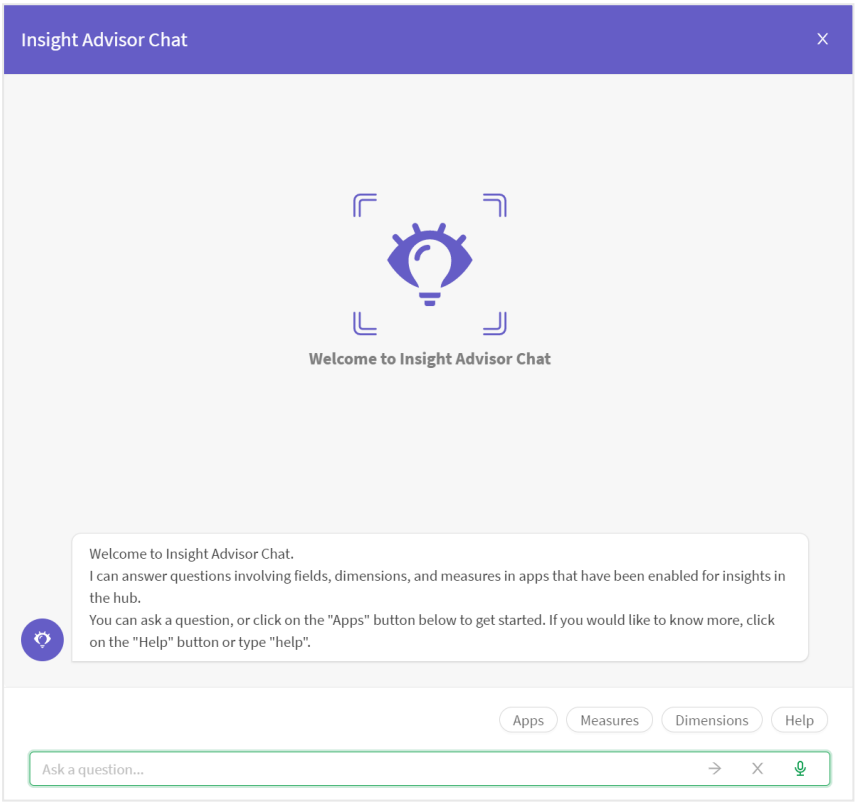
1. *%ProgramFiles%\Qlik\Sense\ServiceDispatcher* に移動します。
2. テキスト エディタで *services.config* ファイルを開きます。
3. bot-channel-service セクションを見つけて、`disabled=true parameter` をコメント アウトします。次の例のようになります。

```
[bot-channel-service]
//Disabled=true
Identity=Qlik.bot-channel-service
DisplayName=Bot Channel Service
```

```
ExePath=Node\node.exe
Script=..\BotChannelService\index.js
```

4. ファイルを保存します。
5. Qlik Sense Service Dispatcher を再起動します。
6. [**Ask Insight Advisor**] ボタンをクリックして、Insight Advisor Chat を開きます。

7. チャット機能が次のウィンドウで開いていることを確認します。



> *正常に動作しない場合、QMC でセキュリティルールが正しく設定されていることを確認します。詳細については、Qlik Sense Enterprise on Windows での Qlik Insight Advisor Chat の構成 (page 647) を参照してください。*

8. Qlik Sense Proxy Service を再起動します。

マルチノードデプロイメントのリソース使用率

マルチノード展開は、中央ノードと1 つ以上のリムノードで構成されます。マルチノード展開で Insight Advisor Chat を展開する場合、NLP ランタイムスタック(nl-parser、nl-broker、nl-app-search、data-prep) は、サービスディスパッチャの一部となり、マルチノードサイトの各ノードに展開されます。

中央ノードの Insight Advisor Chat を経由する要求は、中央ノードに展開されている NLP ランタイムスタックによって処理されます。リムノードで発生するリクエストは、同じリムノードで実行されている NLP スタックによって処理されます。NLP ランタイムスタックのロードバランシングルールがなく、ノード上で NLP スタックのいずれかの部分が無効になっている場合、そのノード上の Insight Advisor Chat を経由して来る要求は失敗します。

2 Qlik Sense Enterprise on Windows サイトの監視

Qlik Management Console (QMC) にはシステム パフォーマンスおよび Qlik Sense Enterprise on Windows サーバー ノードの使用状況を監視し、ライセンス使用状況を監視するアプリが含まれています。

Operations Monitor アプリと *License Monitor* アプリには QMC スタート ページからアクセスします。ナビゲーション パネルの **GOVERNANCE** の下にある **Monitoring apps** リンクを使用して、個別アプリを開始できる **Monitoring apps** ストリームを表示できます。

Operations Monitor アプリでは、サーバー メモリと CPU の使用率、アクティブ ユーザー数、リロード タスク アクティビティなど、ハードウェアの使用状況に関する情報が提供されます。さらに、Qlik Sense サーバー環境でのエラー、警告、ログ アクティビティに関する要約と詳細情報も提供され、トラブルシューティングに活用できます。

License Monitor アプリは、ライセンスの使用状況を追跡し、ライセンス割り当ての変更を監視するためにも活用できます。

追加の *Monitoring apps* は *%ProgramData%\Qlik\Sense\Repository\DefaultApps* からインポート可能です。「*新しい監視アプリのインポート (page 664)*」を参照してください。

追加の *Monitoring apps* には以下が含まれます。

- *Log Monitor* アプリは、使用可能なログ データをほぼすべて提示し、トレンド分析およびトラブルシューティングを有効にします。
- *Sessions Monitor* アプリは、アプリの使用方法に関するログ データを示します。
- *Reloads Monitor* アプリは、QMC およびハブで開いているアプリの両方から、リロードされたデータの詳細情報を提示します。
- *Sense System Performance Analyzer* アプリには、すべてのノードにおける Qlik Sense パフォーマンスが表示されます。
- *Sense Connector Logs Analyzer* アプリでは、特定の Qlik コネクターの使用状況とエラーに対する洞察を得ることができます。
- *App Metadata Analyzer* アプリでは、すべての Qlik Sense アプリを全体的に表示することができます (アプリのデータ モデルの詳細およびそのリソース使用率を含む)。

監視アプリは、状態の履歴およびトレンドを示すデータを提供します。リアルタイム状態は QMC 管理リソースにより提供されます。監視アプリにより明らかになった問題に対応するためのアクションは QMC でも実施可能です。

2.1 監視アプリの構成

Qlik Sense のインストールでは必ず、監視アプリをある程度構成する必要があります。

シングル ノード環境の構成

次の手順を実行します。

1. *C:\ProgramData\Qlik\Sense* を Qlik Sense の共有フォルダーの完全修飾ドメイン名 (FQDN) へのパスで置き換えてデータ接続 *ArchivedLogFolder* を更新します: *\\<FQDN>\<QlikShare>\ArchivedLogs*。

2. 接続文字列 URL および *trustedLocation* パラメーターに含まれる *localhost* を、*ノード*の FQDN で置き換え、`monitor_apps_REST_` データ接続を更新します。
3. 監視アプリでは、接続に使用する仮想プロキシ上で Windows 認証を使用する必要があります。これが既定の仮想プロキシではない場合は、*\qrs* を *\<prefix>\qrs* で置き換えます。*<prefix>* は、Windows 認証が有効になっている仮想プロキシのプレフィックスです。
参照先: *プレフィックス付きの既定の仮想プロキシ (page 664)*

マルチ *ノード*環境の構成

1. *C:\ProgramData\Qlik\Sense\Log* をセントラル *ノード*の FQDN パスである *\\<FQDN>\<UNC_Share>\Log* に置き換えて、データ接続 *ServerLogFolder* を更新します 。
2. 接続文字列 URL および *trustedLocation* パラメーターに含まれる *localhost* を、セントラル Qlik Sense repository サービス実行中の*ノード*の FQDN で置き換えて、`monitor_apps_REST_` データ接続を更新します。
3. 仮想プロキシにプレフィックスが付いている場合、`monitor_apps_REST_` データ接続を更新して付加されたプレフィックスを含める必要があります。
参照先: *プレフィックス付きの既定の仮想プロキシ (page 664)*
4. 各 rim *ノード*で Qlik Sense *ログ フォルダ* (*C:\ProgramData\Qlik\Sense\Log*) を共有します。
5. *C:\ProgramData\Qlik\Sense* を Qlik Sense の共有フォルダーの完全修飾ドメイン名 (FQDN) へのパスで置き換えてデータ接続 *ArchivedLogFolder* を更新します: *\\<FQDN>\<QlikShare>\ArchivedLogs*。
6. リム *ノード*ごとに *Log* フォルダーへの新しいデータ接続を追加します。これは、アプリを開き、データロードエディターにアクセスし、新しいデータ接続を作成することによって達成できます。rim *ノード*が 5 つある場合は、データ接続を 5 つ作成する必要があります。
例えば、rim1 のデータ接続はフォルダー *\\rim_node_1\<UNC_Share>\Log* をポイントし、rim1 と呼ばれます。
7. QMCで新しいデータ接続の名前を変更して、データ接続名に付加されている*(ユーザー名)*を削除します。例: *rim1 (user_183)*を*rim1*に変更します。
8. 手順 6 および 7 で作成されたすべての新しいデータ接続の名前を追加することにより、5 行目の *logFolderList* セクションで *Operations Monitor* のロードスクリプトを更新します。
次の手順を実行します。
    i. *Operations Monitor* アプリを QMC に複製します。
    ii. Qlik Sense ハブで複製されたアプリを開きます。
    iii. ロードスクリプトの編集: 新しいデータ接続のそれぞれの名前は、一重引用符 (') で囲み、コンマで区切る必要があります。
    例:*'ServerLogFolder'*、*'rim1'*、*'rim2' 内の各 ノードに関して*。
    iv. アプリを保存します。
    v. 重複したアプリを **Monitoring apps** ストリームに公開し、[**既存アプリの上書き**] を選択して既存 *Operations Monitor* アプリを置き換えます。
9. *License Monitor* のステップ 8 を実行します。

セントラル ノードがリロード ノードでないときに問題が発生する場合は、マルチノード環境 でリロードに失敗する監視 アプリ(page 681).

プレフィックス付きの既定の仮想プロキシ

既定の仮想プロキシでプレフィックスを使用する場合は、*Operations Monitor* と *License Monitor* を正しくリロードするために、qrs データ接続に手動でプレフィックスを追加する必要があります。既定の URL は *https://<FQDN>/qrs/app/full* です。FQDN は、リポジトリが存在するノードを参照します。仮想プロキシのプレフィックスが「qlik」の場合、URL は *https://<FQDN>/qlik/qrs/app/full* にする必要があります。

次のデータ接続を更新する必要があります。

- monitor_apps_REST_app
- monitor_apps_REST_appobject
- monitor_apps_REST_event
- monitor_apps_REST_license
- monitor_apps_REST_license_analyzer
- monitor_apps_REST_license_login
- monitor_apps_REST_license_overview
- monitor_apps_REST_license_professional
- monitor_apps_REST_license_user
- monitor_apps_REST_task
- monitor_apps_REST_user_condensed

新しい監視アプリのインポート

追加の監視アプリである、Log Monitor、Reloads Monitor、Sessions Monitor、Sense System Performance Analyzer、Sense Connector Logs Analyzer、および App Metadata Analyzer は、QMC の既定のアプリではありません。これらのアプリが QMC に表示されるようにするにはインポートが必要です。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC のスタートページで、[**アプリ**] を開きます。
3. 操作バーで [**インポート**] をクリックします。
4. [**ファイルを選択**] をクリックし、*%ProgramData%\Qlik\Sense\Repository\DefaultApps* に移動します。
5. に移動します。インポートするアプリを選択し、[**インポート**] をクリックします。
   アプリがインポートされ、*監視アプリ*のストリームに公開できるようになります。
6. 残りのアプリについて手順 2 ~ 4 を繰り返します。

Sessions Monitor、*Log Monitor*、*Reloads Monitor*、*Sense System Performance Analyzer*、*Sense Connector Logs Analyzer*、および *App Metadata Analyzer* の各アプリは、*Qlik Sense* のアップグレード時に自動的には更新されません。これらのアプリは、アップグレード後に手動でインポートする必要があります。

アプリのカスタマイズ

特定の環境で有効な場合には、ビジュアライゼーションによって監視アプリの機能を拡張することが可能です。監視アプリには、使用する軸とメジャーを示すアセットパネルが備わっています。この軸とメジャーを使用して、アプリに追加できるカスタマイズされたビジュアライゼーションを、別個のシート上に作成できます。

アセットパネルには、アプリのどのシートでも使用されないものの、特定の環境では有用な追加のビジュアライゼーションも表示されます。

Operations Monitor および License Monitor にあるデータはライブではなく、アプリのリロードの際に更新されます。リロード頻度はタスクのトリガーを編集して変更できます。

2.2 QMC からの監視アプリの起動

操作およびライセンス監視用のアプリは、QMC スタートページに移動すると起動します。監視アプリには、ナビゲーションパネルの [**ガバナンス**] の下にある [**監視アプリ**] リンクからアクセスできます。

次の手順を実行します。

1. QMC を開く: *https://<QPS サーバー名>/qmc*
2. QMC アプリを使用するユーザーにユーザーアクセスを割り当てるか、ユーザーがログインパスでアプリを使用できるグループにログインアクセスを割り当てます。
3. ナビゲーションパネルの **GOVERNANCE** の下の **Monitoring apps** リンクをクリックします。
   個別アプリを開始できる **Monitoring apps** ストリームが表示されます。

*監視アプリを初めて起動する場合は、まだリロードがされていないため表示するデータがない場合があります。License Monitor (ライセンスモニター) の場合、1 つ以上のライセンストークンが割り当てられるか、アクセスが拒否されるまでデータはありません。そのため、リロードするとデータが表示されないことがあります。次のスケジュールされたリロードの前にアプリのデータを更新するには、QMC のアプリ概要に戻り、**More actions > Reload now** ([その他のアクション] > [今すぐリロード]) の順にクリックします。*

2.3 監視アプリのアップグレード

Qlik SenseFebruary 2019 以前から Qlik SenseApril 2019 以降へのアップグレード

Qlik SenseApril 2019 では、新しい `monitor_apps_REST_user_condensed` データ接続が導入されました。新しい `monitor_apps_REST_user_condensed` データ接続が、他の `monitor_apps_REST` データ接続と同じユーザー (同じユーザー ID とパスワード) に割り当てられていることを確認してください。

また、新しい monitor_apps_REST_user_condensed データ接続の接続文字列の URL が、他の monitor_apps_REST データ接続で設定されているのと同じホスト名、および該当する場合は仮想プロキシ プレフィックスを使用するように更新されていることを確認してください。

monitor_apps_REST_データ接続に割り当てられるユーザーは、rootadmin である必要があります。

Qlik Sense 3.2.x から Qlik Sense June 2017 へのアップグレード

Qlik Sense 3.2.x から June 2017 またはそれ以降のリリースにアップグレードすると、8 つの新しい REST データ接続 (monitor_app_REST_) が導入されます。既存の qrs_ データ接続は、REST コネクターの機能が変更されたため機能しません。そのため、これらの qrs_ データ接続は削除することができます。

同期持続性から共有持続性へのアップグレード

同期持続性から共有持続性にアップグレードする場合、旧バージョンのアーカイブ ログの共有持続性 ArchivedLogs 共有への移動が必要となる場合があります。

次の手順を実行します。

1. サービス クラスターの *ArchivedLogs* フォルダーに *OlderLogs* (または任意の名前) のフォルダーを新しく作成します。このフォルダーは QMC >サービス クラスターにあります。
2. 以下に示すサブフォルダーを (旧バージョンの) *Archived Logs* から手順 1 で作成した *OlderLogs* フォルダーに移動またはコピーします。
    a. 既定の *Archived Logs* フォルダーは *c:\programdata\qlik\sense\repository\archived logs* です。
    b. 以下のフォルダーを新しい場所にコピーします。
        i. Engine
        ii. Repository
        iii. Proxy
        iv. Scheduler
        v. Printing

    上記のフォルダーを移動またはコピーするのは、他のログ フォルダー (AppMigration や Script) は監視アプリにロードされず、非常にサイズが大きくなる可能性があるためです。
3. *ArchivedLogs* フォルダー (サービス クラスター用) に、使用環境の各ノード用のフォルダーに加え、この *OlderLogs* フォルダーが存在することを確認してください。
4. QMC の *ArchivedLogsFolder* データ接続が、*ArchivedLogs* フォルダー (QMC > ServiceCluster で定義) を参照するよう更新します。
5. *c:\Programdata\Qlik\Sense\Log* にある governance*.QVD の 7 より前のバージョンは削除することができます (オプション)。
6. QMC から新しい監視アプリをリロードします。

2.4 Operations Monitor

Operations Monitor (オペレーション モニター) はサービス ログをロードし、ハードウェア使用状況、アクティブ ユーザー数、アプリ セッション数、タスク リロードの結果、エラーと警告数のパフォーマンス履歴をグラフ化します。また、*Operations Monitor* に影響する QMC の変更内容を記録します。

*シートとビジュアライゼーションの詳細については、[**ストーリー**] の下のアプリ概要ページにある、「Sessions Monitor について」というストーリーを参照してください。*

ログ ファイルは *%ProgramData%\Qlik\Sense\Log\Repository\Trace* にあります。

Operations Monitor を使用すると、システムのパフォーマンスを追跡して、悪影響を与える可能性のあるアクティビティを調査できます。たとえば、リロード タスクやセッションを分析することにより、リロードの再スケジュールやセッションの再配布によって軽減される可能性のある障壁を見つけることができます。または、**QMC Change Log** シートを使用して、システムのパフォーマンスの変化を説明可能な変化を見直すことができます。

Operations Monitor シート

Operations Monitor シートには、現在のノードにおける Qlik Sense のパフォーマンスを表示します。マルチノードに対して正しく構成してある場合 (「*マルチ ノード環境の構成 (page 663)*」参照) は、すべてのノードについての情報が含まれます。

Operations Monitor シート

24-Hour Summary	ハードウェア使用状況、アクティブ ユーザー数、アクティブ アプリ、過去 24 時間以内の リロード タスク回数が表示されます。
Performance	ユーザーはハードウェア使用状況、同時ユーザー数、同時アプリ数を表示する期間を選択できます。
Task Overview	タスク リロードの成功/失敗回数、期間に関する統計の概要を選択して表示できます。
Task Planning	ロード回数、ロードの CPU 時間、およびタスクの依存関係についての詳細情報を示します。
Task Details	期間と開始時間と終了時間の実行詳細を含む、個別のアプリ リロードの成功 / 失敗回数の詳細を表示できます。
Session Overview	選択された期間におけるアプリ、アプリ セッション、アプリ ユーザーに関する概要情報が表示され、どのユーザーがいつどのアプリを使用したかを示します。
Session Details	数値、平均期間、最終セッション日からの経過日数、開始時間と終了時間、セッションが終了した理由、アプリが実行されたクライアントのタイプなどを含む個別のユーザーおよびアプリ セッションについての詳細を表示できます。
Export Overview	どのユーザーがどのアプリ オブジェクトをいつエクスポートしたかを示す、アプリやアプリ オブジェクト、アプリ ユーザーについての概要情報を提供します。

Sheet Usage	シートにアクセスしているユーザーの概要と詳細な情報、およびアプリへのアクセスがないシートの情報を表示します。 [*未使用のシートの測定*] では、選択した期間内に使用されなかったアプリケーション内のシート数がカウントされます。たとえば、10「Unused base sheets last <=30 days」は、過去30日間に10枚のシートが未使用であることを意味します。
Apps	Qlik Sense Repository Service (QRS) に、名前、アプリオブジェクトの ID、所有者、公開、ストリームを含む、アプリの詳細を提供します。
QMC Change Log	システム パフォーマンスからユーザー アクセスまで幅広く影響する QMC での変更 (QMC リソース タイプ、特定の QMC リソース、QMC で実行したアクションのタイプ別の変更を含む) を表示します。
Export Links for Cloud	Qlik Sense SaaS にエクスポートするアプリのリンクの詳細を提供します。その後、これは汎用リンクとして Qlik Sense SaaS にインポートできます。リンクをクラウド ハブに追加したり、管理コンソールにアップロードしたりできるようにするには、まずリンクを CSV ファイルにエクスポートする必要があります。リンクを .csv ファイルにエクスポートを参照してください。
Log Details	リロードの時間、結果、エラー メッセージと警告、ログ エントリを含む *Operations Monitor* のリロードの詳細を表示できます。

Operations Monitor のデータは アプリがリロードされる際に更新されます。データは リアルタイムで更新されていません。

Operations Monitor は、エンジンのセッションログから[ProxySessionId] を使用して、Sessions Monitor のようなセッションカウントを導き出します。これにより、実質的にプロキシセッション数が算出されますが、アプリのセッション計算方法により、License Monitor および Sessions Monitor セッション数よりも若干少なくなる可能性があります。Operations Monitor は、それぞれの設計上の選択値により Sessions Monitor に登録される短いセッション(40秒未満) を除外します。

2.5 License Monitor

License Monitor (ライセンス モニター) はサービス ログをロードし、トークン割り当て、ログインとユーザー パスの使用を含むチャートとテーブル、およびエラーと警告を表示します。

*シートおよびビジュアライゼーションの詳細については、アプリ概要ページの[**ストーリー**] からアクセス可能な「License Monitor について」というストーリーを参照してください。*

ログ ファイルは %ProgramData%\Qlik\Sense\Log\Repository\Trace にあります。

プロフェッショナル アクセスおよびアナライザー アクセスを備えたユーザーベースのライセンスがある場合は、そのライセンス タイプに関連する図が表示されます。

License Monitor シート

License Monitor シートには、現在のノードにおけるQlik Sense のパフォーマンスを表示します。マルチノードに対して正しく構成してある場合 (「*マルチ ノード環境の構成 (page 663)*」参照) は、すべてのノードについての情報が含まれます。

License Monitor シート

Overview	未割り当てアクセス権とアクセス権の合計数の比率の概要、割り当て可能なAnalyzer Capacity の合計時間 (分)、過去 7 日間、28 日間、および 90 日間のログインとユーザー アクセス セッション、過去 7 日間のライセンス トークンの割り当ての変更、ライセンス使用期間の経過についての概要データが表示されます。
User Detail	ユーザーは、ユーザー アクセス パス セッション、セッションを開始したユーザー数、およびセッションを開始した個々のユーザーを表示する期間を選択できます。
Usage by App	ユーザーは、アプリで使用されたアクセス パスと、各アプリで消費されたトークンの数を表示する期間を選択できます。
Timeline	*Timeline* シートには時間の経過に伴うトークンの使用状況が表示されるため、管理者は使用状況を監視し、将来のトークン割り当てのニーズを予想することができます。
User Access History	ユーザーは、ユーザー アクセス パス セッション、セッションを開始したユーザー数、およびセッションを開始した個々のユーザーを表示する期間を選択できます。 *トークンベースのライセンスでのみ有効です。*
Login Access History	ユーザーは、ログイン パス使用状況、ログイン アクセス ユーザー数、拒否されたログイン アクセス数を表示する期間を選択できます。 *トークンベースのライセンスでのみ有効です。*
Allocation History	ログイン アクセス パスとユーザー アクセス パスへのライセンス トークンの割り当てに対する最新の変更と選択した期間の変更を表示します。
Usage Snapshot	ライセンスの割り当ておよび使用履歴のスナップショット表示を提供する概要シートです。
Unified Licensing History	Qlik Sense および QlikView のライセンス使用状況を並べて表示します。 *QlikView のライセンス使用状況を表示するには、新しい monitor_apps_qlikview_logs データ接続が、QlikView Server のログを含んでいるフォルダをポイントする必要があります。QMC でデータ接続を更新します。*
Log Details	クラスターにサーバーをリストし、サーバーのログに記入されたライセンスの使用に関する詳細を提供します。

License Monitor のデータは アプリがリロードされる際に更新されます。データは リアルタイムで更新されていません。

License Monitor は、リポジトリの AuditSecurity ログからの ProxySessionId と ObjectId の組み合わせを使用して、セッション数を取得します。同じプロキシセッションで複数のアプリを開く場合、この数は、それぞれの設計上の選択値により、他の監視アプリよりも若干多く表示されることがあります。ユーザー セッションごとに消費される実際のトークンは影響を受けません。

2.6 Log Monitor

Log Monitor は、Qlik Sense の利用可能なほぼすべてのログ データをロードし、ビジュアライゼーションします。これにより、Qlik Sense 環境における問題の傾向把握と分析、トラブル解決につなげることが可能となります。Operations Monitor と比較すると、Log Monitor はより多くのログ ファイルをロードしますが、期間は短く(既定では 7 日間) なります。

*シートとビジュアライゼーションの詳細については、[**ストーリー**] の下のアプリ概要ページにある、「Log Monitor について」というストーリーを参照してください。*

ログ ファイルは *%ProgramData%\Qlik\Sense\Log\Repository\Trace* にあります。

QMC の監視アプリへの Log Monitor アプリのインポート

Log Monitor は、既定では QMC からは利用できません。利用できるようにするには、このアプリをインポートする必要があります。

セクション *新しい監視アプリのインポート (page 664)* の説明に従ってください。

Log Monitor シート

Log Monitor シートには、現在のノードにおける Qlik Sense のパフォーマンスを表示します。マルチノードに対して正しく構成してある場合 (「*マルチ ノード環境の構成 (page 663)*」参照) は、すべてのノードについての情報が含まれます。

Log Monitor シート

Overview	直近数時間および数日のアクティビティを要約し、不規則な事象をすばやく特定することができます。
Timeline	棒グラフ Activity Timeline は、前の週のログ記録アクティビティの概要を示します。代替軸を使用して、時系列でのメジャーの変化を確認したり、調査が必要な可能性のある逸脱した値を発見したりします。
Trends	パフォーマンス (CPU および RAM)、利用状況 (アプリおよびユーザー)、エラー、リロード ステータスを示す、タイムラインのコレクションを表示します。
Errors & Warnings	エラーおよび警告の要約と詳細情報を含むタイムラインを表示します。

Filters	ログに含まれる多数のキー項目を示すフィルター パネルを格納します。項目を選択し、データからの発見につなげます。
Log Details	展開されているサーバーのエラー、警告、情報ログ エントリを表示します。

Log Monitor のデータは アプリがリロードされる際に更新されます。データは リアルタイムで更新されていません。

2.7 Reloads Monitor

Reloads Monitor は、リロードに関するログ データをロードして提示します。リロード データは、ハブでオープンされているQMC のタスクとアプリの両方から収集されます。どのアプリが更新されたか、およびアプリが更新されたタイミング、場所、頻度などの詳細を確認できます。

*シートとビジュアライゼーションの詳細については、[**ストーリー**] の下のアプリ概要ページにある、「Reloads Monitor について」というストーリーを参照してください。*

ログ ファイルは *%ProgramData%\Qlik\Sense\Log\Repository\Trace* にあります。

QMC の監視アプリへの Reloads Monitor アプリのインポート

Reloads Monitor は、既定では QMC からは利用できません。利用できるようにするには、このアプリをインポートする必要があります。

セクション *新しい監視アプリのインポート (page 664)* の説明に従ってください。

Reloads Monitor シート

Reloads Monitor シートには、現在のノードにおける Qlik Sense のパフォーマンスを表示します。マルチノードに対して正しく構成してある場合 (「*マルチ ノード環境の構成 (page 663)*」参照) は、すべてのノードについての情報が含まれます。

Reloads Monitor シート

Dashboard	リロード タスク履歴の概要を示します。棒グラフReloads by Hour およびコンボ チャートReload Count and Duration Trend で利用可能な代替軸およびメジャーを使用することで異なる表示を取得します。
Task Planning	タスクがリロードされた日時および関連付けられた期間と失敗率を表示します。このデータを使用してリロードのスケジュールを再設定し、パフォーマンスを最適化します。
Reload Summary	リロードの履歴統計および最近完了したリロードに関する詳細情報を示します。
Log Details	特定のログ イベントおよび時刻に関する詳細を示します。
Intermediate Details	Triggered、Started、Queued など、タスク リロードの中間ステートを示します。

Reloads Monitor のデータは アプリがリロードされる際に更新されます。データは リアルタイムで更新されていません。

2.8 Sessions Monitor

Sessions Monitor は、ユーザーのアプリセッションに関するログ データをロードし、表示します。

シートとビジュアライゼーションの詳細については、[ストーリー] の下のアプリ概要ページにある、「Sessions Monitor について」というストーリーを参照してください。

ログ ファイルは *%ProgramData%\Qlik\Sense\Log\Repository\Trace* にあります。

QMC の監視アプリへの Sessions Monitor アプリのインポート

Sessions Monitor は、既定では QMC からは利用できません。利用できるようにするには、このアプリをインポートする必要があります。

セクション *新しい監視アプリのインポート (page 664)* の説明に従ってください。

Sessions Monitor シート

Sessions Monitor シートには、現在のノードにおける Qlik Sense のパフォーマンスを表示します。マルチノードに対して正しく構成してある場合 (「*マルチ ノード環境の構成 (page 663)*」参照) は、すべてのノードについての情報が含まれます。

Sessions Monitor シート

Dashboard	セッション アクティビティの概要を示します。棒グラフ Sessions Over Time およびコンボ チャート User and App Count Trend で利用可能な代替軸およびメジャーを使用することで異なる表示を取得します。
Session Heatmap	セッション アクティビティが最も多い、および最も少ない時刻を示します。このデータを使用して、使用率のピーク時刻やサーバー メンテナンスに適した時刻を把握します。
Session Details	より詳細なセッション アクティビティ情報を示し、使用されていないアプリやアプリの使用頻度が高いユーザーの特定に役立てることができます。
Apps	アプリおよびアプリオブジェクトに関するメタデータを示します。
Log Details	特定のログ イベントおよび時刻に関する詳細を示します。

Sessions Monitor のデータは アプリがリロードされる際に更新されます。データは リアルタイムで更新されていません。

Sessions Monitor は、エンジンのセッションログから[ProxySessionId] を使用して、事実上のプロキシのセッション数を示す Operations Monitor のようなセッションカウントを導き出します。Sessions Monitor は、それぞれの設計上の選択値によりOperations Monitor に除外される短いセッション(40秒未満)も登録します。したがって、Sessions Monitor セッションカウントは、Operations Monitor とLicense Monitor のセッションカウントの中間になることがあります。

2.9 Sense Connector Logs Analyzer

Sense Connector Logs Analyzer アプリでは、アクティビティとエラーのパターンを調べ、コネクターのパフォーマンスのトラブルシューティングを行うことができます。

このアプリは、REST コネクター バージョン 1.7 以降とODBC コネクター バージョン 5.12 以降によって生成されるログファイルに依存しています。

古いバージョンの REST および ODBC コネクターによるログ ファイルには、ロード時に *Sense Connector Logs Analyzer* アプリが失敗する原因となる必要な列見出し名が記録されていない可能性があります。これらの古いコネクター ログ ファイルは、削除するか、または別のフォルダーに移動するようお勧めします。

*シートとビジュアライゼーションの詳細については、アプリ概要ページの [**ストーリー**] にある「 について Sense Connector Logs Analyzer」というストーリーを参照してください。*

QMC の監視アプリへの Sense Connector Logs Analyzer アプリのインポート

Sense Connector Logs Analyzer は、既定では QMC からは利用できません。利用できるようにするには、このアプリをインポートする必要があります。

セクション *新しい監視アプリのインポート(page 664)* の説明に従ってください。

一般構成

シングルノード展開では構成が不要ですが、ロード スクリプトでロードするログ履歴の日数を変更することが可能です。また、Engine、Repository、Scheduler、Proxy のログをアプリに組み込むこともできます。

構成は、ロード スクリプトの Configuration セクションで行います。

履歴の日数

履歴の日数は、ロード スクリプトで変数 **`vu_days_of_history`** として設定します。

既定値は `14` 日で、データ量が膨大になる可能性があるため、90 日以上にすることは推奨されていません。

```
SET vu_days_of_history = 14;
```

履歴データ

Sense Engine、Repository、Scheduler、Proxy のログは、アプリ設定の **vu_load_operations_monitor_qvd** 変数に含めることができます。

これにより、ServerLogFolder データ接続から Operations Monitor の履歴 QVD が取得されます。

ロードする QVD の名前は .qvd 拡張子なしで入力する必要があります。

```
SET vu_load_operations_monitor_qvd = 'governanceLogContent_7.10.2_db';
```

マルチノード展開構成

マルチノード環境では、各ノードの **\\FQDN\CustomData** などの共有フォルダーへの新規データ接続を作成する必要があります。データ接続はその後、ロードスクリプトの **vu_data_connection_list** 変数で定義されます。

構成は、ロードスクリプトの Configuration セクションで行います。

1. 各ノードで C:\ProgramData\Qlik フォルダーを共有します。

   共有フォルダーに Custom Data と名付けます。
2. リムノードごとに新しいデータ接続を追加します。各ノードの完全修飾ドメイン名 (FQDN) を使用します。

   フォルダー \\rim_node_2\Custom Data\ を指し示す connector_logs_rim2 という名前のデータ接続を作成します。
3. QMC > Data Connection セクションで、前のステップで作成した新しいデータ接続の名前を変更して、データ接続名に付加されているユーザー名を削除します。

   connector_logs_rim2 (my_domain\my_user1) の名前は connector_logs_rim2 に変更する必要があります。
4. QMC > データ接続セクションで、[ID] タブにある **monitor_apps_connector_logs** データ接続の接続文字列をアップデートし、FQDN のセントラルノードを使用するようにします。

   \\central_node_name\Custom Data

> *共有フォルダーにユーザーのアクセス権限がセットされていた場合は、それに応じてユーザー ID およびパスワードの項目を定義する必要があります。そうでなければ、未定義のままとしてください。*

5. ロードスクリプトを更新して、前のステップで作成して名前を変更したデータ接続を追加します。
   データ接続は、**vu_data_connection_list** 変数で定義されます。各データ接続は、既存の一重引用符で囲み、コンマで区切ります。

```
SET vu_data_connection_list = 'monitor_apps_connector_logs,connector_logs_
rim2,connector_logs_rim3';
```

6. 更新したアプリを保存します。
7. アプリをリロードする。
   アプリは、QMC またはデータロードエディターからロードできます。

Sense Connector Logs Analyzer シート

Sense Connector Logs Analyzer シートには、すべてのノードにおける Qlik コネクターの使用状況とエラーが表示されます。

シートの詳細については、アプリ概要ページの [**ストーリー**] にある「*について Sense Connector Logs Analyzer*」というストーリーを参照してください。

> *Sense Connector Logs Analyzer のデータはアプリがリロードされる際に更新されます。データはリアルタイムで更新されていません。*

2.10 App Metadata Analyzer

App Metadata Analyzer アプリには、Qlik Sense Enterprise 展開で Qlik Sense アプリケーションのメタデータを分析するダッシュボードが備えられています。これには、アプリのデータモデルの詳細およびそのリソース使用率を含めて、すべての Qlik Sense アプリが全体的に表示されています。

> *このアプリには Qlik Sense バージョン June 2018 以降が必要です。*

> *シートとビジュアライゼーションの詳細については、アプリ概要ページの [**ストーリー**] にある「App Metadata Analyzer」というストーリーを参照してください。*

このアプリでは、データを次のアプリケーションレベルのメタデータエンドポイントから取得します: **http(s)://{server}/api/v1/apps/{GUID}/data/metadata**。

ここで、`{server}` はユーザーの Qlik Sense Enterprise サーバー、`{GUID}` はアプリケーション ID です。

QMC の監視アプリへの App Metadata Analyzer アプリのインポート

App Metadata Analyzer は、既定では QMC からは利用できません。利用できるようにするには、このアプリをインポートする必要があります。

セクション *新しい監視アプリのインポート (page 664)* の説明に従ってください。

一般構成

ロードスクリプトで必要な構成が 2 つあります。セントラル ノードのホスト名および仮想プロキシのプレフィックス (Windows 認証仮想プロキシにプレフィックスが含まれている場合) の定義です。

構成は、ロードスクリプトの Configuration セクションで行います。

セントラル ノードのホスト名

セントラル ノードのホスト名は、ロードスクリプトで変数 **vu_central_node_host_name** として設定されます。

既定値は `localhost` です。

```
SET vu_central_node_host_name = 'my_central_node.domain.com';
```

仮想プロキシのプレフィックス

仮想プロキシのプレフィックスも、ロードスクリプトで変数 **vu_virtual_proxy_prefix** として設定されます。

```
SET vu_virtual_proxy_prefix = 'my_virtual_proxy_prefix';
```

仮想プロキシのプレフィックスを使用していない場合は、空白にしておきます。

```
SET vu_virtual_proxy_prefix = '';
```

オプションでのしきい値の設定

オプションで、既定のしきい値を変更することができます。この設定は、ロードスクリプトの Thresholds セクションで行います。

```
// Optional Configuration (No need to change these unless you desire) SET vu_months_in_reload_
interval = 3; // Width of app last reload date for grouping apps in this app // Visual
Thresholds - change these if you want to highlight specific apps based on these attributes SET
vAppDiskSizeThreshold = 524288000; // 500 MB SET vAppRAMSizeThreshold = 1073751824; // 1 GB
SET vRAMToFileSizeRatioThreshold = 6; // RAM / File Size is typically between 4-6x SET
vAppRecordCountThreshold = 10000000; // Number of records in an app SET
vTableRecordCountThreshold = 10000000; // Number of records in a table SET
vFieldValueCountThreshold = 10000000; // Number of field records SET
vFieldCardinalityThreshold = 1000000; // Number of distinct field values SET vNoOfFields =
```

```
150; // Number of Distinct Fields SET vReloadCPUTimeThreshold = 1800000; // CPU Time spent on
last reload (milliseconds); default = 1,800,000 = 30 Minutes
```

App Metadata Analyzer シート

シートの詳細については、アプリ概要ページの [**ストーリー**] にある「*App Metadata Analyzer について*」というストーリーを参照してください。

App Metadata Analyzer のデータは アプリがリロードされる際に更新されます。データは リアルタイムで更新されていません。

2.11 トラブルシューティング: Qlik Senseサイトの監視

このセクションでは、Qlik Senseサイトを監視するときに発生する可能性のある問題について説明しています。

監視アプリが適切にバックアップされていない

Qlik Sense をアップグレードすると、監視アプリが正しくバックアップされません。

通常、Qlik Sense をアップグレードすると、監視アプリの既存のバージョン番号は、アプリ名に付加される対応するバージョン番号と置き換えられます。その後、[**アプリ**] でも最新の監視アプリが利用できるようになります。

考えられる原因

監視アプリのアップグレードプロセスが失敗しています。

提案されたアクション

*%ProgramData%\Qlik\Sense\Repository\DefaultApps*から最新のアプリを手動でインポートしてください。

次の手順を実行します。

1. QMCで、 **[Apps (アプリ)]** を開きます。
2. **[Import (インポート)]** をクリックして、*%ProgramData%\Qlik\Sense\Repository\DefaultApps*のLicense Monitor.qvfを選択します。
   表示が出ても、アプリの名前は変更しないでください。
3. 新しくインポートされた License Monitor を Monitoring apps ストリームに公開し、既存の License Monitor を置き換えます。
4. Operations Monitor.qvfのためにステップ2を繰り返します。

5. 新しくインポートされた Operations Monitor を Monitoring apps ストリームに公開し、既存の Operations Monitor を置き換えます。
6. Log Monitor、Reloads Monitor、および Sessions Monitor に関してステップ 2 とステップ 3 を繰り返します。

間違って監視アプリを削除してしまった

間違って監視アプリを削除してしまい、QMC の中に監視用アプリが見当たりません。

考えられる原因

監視アプリの偶発的または意図的な削除。

提案されたアクション

次の手順を実行します。

1. QMCで、 **[Apps (アプリ)]** を開きます。
2. **[Import (インポート)]** をクリックして、*%ProgramData%\Qlik\Sense\Repository\DefaultApps*のLicense Monitor.qvfを選択します。
   表示が出ても、アプリの名前は変更しないでください。
3. 新しくインポートされた License Monitorアプリを Monitoring appsストリームに公開します。
4. 影響を受ける監視アプリすべてに関してステップ 2 とステップ 3 を繰り返します。

監視アプリが破損した

監視アプリが破損して機能しなくなりました。

考えられる原因

技術的エラー。

提案されたアクション

次の手順を実行します。

1. QMCで、 **[Apps (アプリ)]** を開きます。
2. **[Import (インポート)]** をクリックして、*%ProgramData%\Qlik\Sense\Repository\DefaultApps*のLicense Monitor.qvfを選択します。
   表示が出ても、アプリの名前は変更しないでください。
3. 新しくインポートされたLicense Monitorを Monitoring appsストリームに公開し、既存の破損した License Monitorを置き換えます。
4. Operations Monitor.qvfのためにステップ2を繰り返します。
5. 新しくインポートされたOperations Monitorを Monitoring appsストリームに公開し、既存の破損した Operations Monitorを置き換えます。

監視アプリのリロードに失敗した

リロードが失敗する場合に考えられる原因は複数あります。

QMC における管理者権限の不足

考えられる原因

Qlik Sense サービスを実行するサービス アカウントには、QMC で必要とされる RootAdmin ロールがありません。

提案されたアクション

監視アプリがデータをすべて問題なく取得するためには、Qlik Sense サービスを実行しているサービス アカウントに十分な権限が必要です。これを達成するためのもっとも簡単なのは、QMC でそのサービス アカウントに RootAdmin の役割を付与する方法です。あるいは、異なるアカウント/ユーザー (つまり、RootAdmin) を使用するようにデータ接続を変更することもできます。

リム ノードでリロードが実行される

考えられる原因

負荷分散ルール *ResourcesOnNonCentralNodes* が原因で、リム ノードでのリロードに失敗します。

提案されたアクション

負荷分散ルール *ResourcesOnNonCentralNodes* を編集してください。

次の手順を実行します。

1. QMC のスタート ページで、[**負荷分散ルール**] を開きます。
2. *ResourcesOnNonCentralNodes* を選択し、[**編集**] をクリックします。
3. [**拡張**] で、[**条件**] を次のように編集します。
   ```
   ((node.iscentral="false"))
   ```
4. [**適用**] をクリックします。

メッセージ:「Error: HTTP protocol error 403 (Forbidden): The server refused to fulfill the request」

考えられる原因

monitor_apps_REST_license_overview データ接続で構成されているユーザーには、そのライセンスとアクセス タイプのエンティティへの読み取りアクセス権がありません。

提案されたアクション

次の手順を実行します。

1. QMC で [**データ接続**] 概要ページを開きます。
2. *monitor_apps_REST_license_overview* データ接続を選択し、[**編集**] をクリックして、適切なアクセス権を持っているユーザーのユーザー ID とパスワードの資格情報を入力します。
3. 変更内容を保存します。

メッセージ:「Error: Field not found...」(項目が見つかりません...)

考えられる原因

監視アプリに使用されていた一部の項目がログ ファイルからなくなってしまっています。

提案されたアクション

2.1.1以降にアップグレードしてください。

メッセージ:「Error: Table 'tempDateTimeList' not found...」(テーブル 'tempDateTimeList' が見つかりません...)

このエラーは、アップグレード後に発生する可能性があります。特に、環境を同期持続性から共有持続性に変更した場合や、Archived Logs が保存されている Qlik Sense クラスター共有が変更された場合に発生する可能性があります。

考えられる原因

ArchivedLogsFolder のデータ接続が正しくないために、アプリがログ ファイル内のライセンス履歴データを検出できません。

提案されたアクション

正しいフォルダーの場所を示すように、*ArchivedLogsFolder* のデータ接続を修正します。

メッセージ:「Error: QVX_UNEXPECTED_END_OF_DATA...」

このエラーについては、複数の原因が考えられます。

カスタマイズされたプロキシ ポート

考えられる原因

プロキシの HTTPS ポートは変更されています。

提案されたアクション

すべての `monitor_apps_REST_` データ接続を変更して好みのポート番号を使用します。

CUSTOM CONNECT TO「*provider=QvRestConnector.exe;url=https://localhost:4443/qrs...*」。

影響を受けるデータ接続は、次の通りです。

- `monitor_apps_REST_app`
- `monitor_apps_REST_appobject`
- `monitor_apps_REST_event`
- `monitor_apps_REST_license_access`
- `monitor_apps_REST_license_login`
- `monitor_apps_REST_task`
- `monitor_apps_REST_user (this connection is now obsolete)`

- monitor_apps_REST_user_condensed
- monitor_apps_REST_license_user

Qlik Sense サービスを実行中のユーザー アカウントに行われた変更

エラー メッセージ: **エラー: QVX_UNEXPECTED_END_OF_DATA: HTTP protocol error 401 (Unauthorized): Requested resource requires authentication.**

考えられる原因

インストール中に、Qlik Sense サービスを実行するユーザー アカウントが作成されます。Qlik Sense サービスに関するアカウントの変更または異なるアカウントの認証情報を選択して実行する場合、それに応じてデータ接続を更新する必要があります。

提案されたアクション

次の手順を実行します。

1. QMC で [**データ接続**] 概要ページを開きます。
2. それぞれの monitor_apps_REST_ データ接続に関して、[**編集**] をクリックし、新しい [**ユーザー ID**] および [**パスワード**] の認証情報を入力します。
3. 変更内容を保存します。

License Monitor、Operations Monitor、または Session Monitor のリロードに失敗する

エラー メッセージ: **エラー: QVX_UNEXPECTED_END_OF_DATA: HTTP protocol error 500 (Internal Server Error): 「System.OutOfMemoryException」タイプの例外がスローされました。**

考えられる原因

ユーザーとユーザー属性の数が多すぎます。

提案されたアクション

次の手順を実行します。

- ユーザー リストを消去してサイズを縮減してください。
- QMC のユーザー ディレクトリ コネクター設定で、[**既存のユーザーのユーザー データの同期**] を選択したままにして、大量のユーザーおよびユーザー属性が同期されるのを防止してください。

マルチノード環境でリロードに失敗する監視アプリ

リロードが失敗する場合に考えられる原因は複数あり1ます。

セントラル ノードがリロード ノードではない

既定の monitor_apps_REST_ データ接続文字列を持つ監視アプリは、セントラル ノードがリロード ノードでないマルチ ノード環境では、リロードに失敗する場合があります。

考えられる原因

監視アプリがリロードされるリロード ノードにはプロキシは設定されません。

提案されたアクション

すべての monitor_apps_REST_ データ接続を変更して セントラル ノードの fully qualified domain name (FQDN) を指すようにします。これは、接続文字列 URL の *localhost* および *trustedLocation* パラメーターをセントラル ノードの FQDN に置き換えることで可能です。

CUSTOM CONNECT TO「*provider=QvRestConnector.exe;url=https://centralnodeserver.company.com/qrs...*」。

影響を受けるデータ接続は、次の通りです。

- monitor_apps_REST_app
- monitor_apps_REST_appobject
- monitor_apps_REST_event
- monitor_apps_REST_license_access
- monitor_apps_REST_license_login
- monitor_apps_REST_task
- monitor_apps_REST_user (this connection is now obsolete)
- monitor_apps_REST_user_condensed
- monitor_apps_REST_license_user

リポジトリデータベースが別のマシン上にある

考えられる原因

REST データ接続が指しているのは Qlik Sense Repository Database の FQDN であり、Qlik Sense Repository Service ではありません。

提案されたアクション

マルチノードまたは「リモート」の Qlik Sense Repository Database の状況では、Qlik Sense Repository Database が実際にどこに存在するかに関係なく、REST データ接続が Qlik Sense Repository Service の FQDNを指すようにする必要があります。

データベース ログをオフにした後、Operations Monitor アプリでリロードが失敗する

データベース ログをオフにした後、Operations Monitor のリロード タスクが失敗します。

次のエラー メッセージが表示されます。

エラー: Table 'time_range_working' not found (テーブル 'time_range_working' が見つかりません)

考えられる原因

監視アプリはデータベース内の最新のログのチェックを続行し、最後のログ メッセージがデータベースに書き込まれた後、これらのログを約 10 時間使用します。データベース ログをオフにした場合、ロード スクリプトの新しいログが見つけられなくなるため、リロードプロセスが失敗する原因となる可能性があります。

提案されたアクション

Operations Monitor アプリのロード スクリプトを手動で更新すると、リロードの失敗を回避できます。

1. ファイル ログが有効になっていることを確認します。
2. Operations Monitor アプリのロード スクリプトを更新します。これは公開済みのアプリであるため、先にこれを複製する必要があります。
   次の手順を実行します。
   i. QMC で Operations Monitor アプリを複製します。
   ii. Qlik Sense ハブで複製されたアプリを開きます。
   iii. 次のように変数 `db_v_file_override` を 0 (既定値) から 1 に変更して、ロード スクリプトの 9 行目を更新します。
   ```
   SET db_v_file_override = 1
   ```
   この変数を 1 に設定すると、スクリプトはデータベース ログのログ エントリをチェックしません。
   iv. アプリを保存します。
   v. 複製したアプリを [監視アプリ] ストリームに公開し、[**既存のアプリを置き換え**] を選択して、既存の Operations Monitor アプリを置き換えます。
3. Operations Monitor を起動して、再度タスクをリロードします。すぐに機能しない場合は、数分待ってから再度リロードします。

この手順に従うことで、データベース ログを安全にオフにすることができます。

Qlik RESTコネクタ経由でのQRSへの接続に失敗した

この問題はQlik RESTコネクタを使用するアプリがあるときにだけ発生します。

Qlik RESTコネクタ経由でのQRSへの接続に問題があるというエラー メッセージが表示されます。

考えられる原因

そのQlik RESTコネクタはアンインストールされたか破損しているため利用できません。

提案されたアクション

リロード中にこのエラー メッセージが表示されたら、Qlik Senseインストールが正常に動作しているか確認する必要があります。Qlik Sense の修理またはのアップグレードを検討してください。

3 ログを使用した Qlik Sense Enterprise on Windows のトラブルシューティング

Qlik Sense Enterprise on Windows が予想通りに動作しない場合 (さらに調査が必要なエラー メッセージがシステムから返される場合や、エラー発生時にまったく応答しない場合など) は、トラブルシューティングが必要になることがあります。

Qlik Sense システムが生成するログ メッセージは、セキュリティに関わる出来事、運用上の問題、ポリシー侵害などの検出に使用される重要な情報を提供します。

ログを使用して Qlik Sense のトラブルシューティングを行う方法の説明は、「使用例」に基づいています。各使用例は、アプリを開くやタスクの停止など、通常のユーザーやシステム アクションに対応しています。

それぞれの使用例は、次の表にあるセクションで説明します。

使用例

セクション	説明
手順	このセクションには、使用例を実行する際に Qlik Sense によって実行 (および記録) されるアクションが一覧表示されます。
成功	このセクションには、成功した場合に Qlik Sense がログ エントリを書き込むログ ファイルが一覧表示されます。
エラー	このセクションには、使用例を実行した場合に発生する可能性のあるエラーが一覧表示されます。 *<MachineName>_Service_<Service>.txt* ファイルにはエラーが発生した場合にすべてのエラーが記録されますので、このファイルをチェックすることをお勧めします。各エラー セクションには、エラーの場合に実行するアクションの説明も含まれます。 *一部の使用例には、エラー セクションがありません。エラーに関する情報は、Qlik Sense マニュアルの今後のリリースに追加される予定です。*

3.1 表記規則

以下の表記規則は、Qlik Sense のマニュアルで使用されます。

コーディング スタイル

- メニュー コマンドおよびダイアログは、[**太字**] で記載されています。
- ファイル名およびパスは、*斜体* で記載されています。
- サンプル コードは `Lucida Console` で表示されます。

環境変数

Qlik Sense のマニュアルで使用されているパスは、環境変数を使っている場合があります。Microsoft Windows オペレーティング システムの変数および同等パスは以下のとおりです。

環境変数

環境変数	Microsoft Windows
%LocalAppData%	*C:\Users\<username>\AppData\Local*
%ProgramData%	*C:\ProgramData*
%ProgramFiles%	*C:\Program Files*
%UserProfile%	*C:\Users\<ユーザー名>*

3.2 Qlik Sense Repository Service

このセクションでは、Qlik Sense のログを使用して Qlik Sense Repository Service (QRS) に関連する問題をトラブルシューティングする方法について説明します。

ユーザーの更新

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS が、ユーザーが更新できるサービス アカウントが、更新によって無効になっていないことを確認します。
3. QRS がユーザーを更新します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Repository.txt*

ユーザーの削除

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS が、削除されるユーザーがサービス アカウントではなく、ルート管理者アクセス権を持つ最後のユーザーでもないことを確認します。
3. QRS がユーザーを削除します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Repository.txt*

アプリを開く

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS は、アプリが存在することを確認します。
3. QRS が、ユーザーがアプリを開くことができることを確認します。
4. QRS は Qlik Sense Engine Service (QES) にリクエストを送信します。
5. QES が、アプリのデータセットへのアクセス権を確認します。
6. QES がアプリをロードして返します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*
- *<MachineName>_AuditActivity_Engine.txt*

エラー

アカウントが無効になっています

アカウントが無効になっていますエラー

説明	Command=Open app;Result=403;ResultText=Error: セキュリティ
メッセージ	アカウントが無効になっています。有効にするには、管理者にお問い合わせください。(HTTP コード: 403)
アクション	適切なアクセス権を取得するには、Qlik Sense のシステム管理者にお問い合わせください。

アプリの追加

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS が、ユーザーがアプリを作成できることを確認します。
3. QRS は Qlik Sense Engine Service (QES) にリクエストを送信します。
4. QES がアプリを作成します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

エラー

拒否

拒否エラー

説明	Command=Create app;Result=403;ResultText=Error: セキュリティ
メッセージ	拒否 (HTTP コード: 403)
アクション	ユーザーはアプリを作成できません。

アプリの削除

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS が、リポジトリデータベースのアプリに削除のマークを設定します。
3. QRS が、Qlik Sense Engine Service (QES) にディスクからアプリを削除するように要求します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*
- *<MachineName>_AuditActivity_Engine.txt*

エラー

削除操作に失敗しました

削除操作に失敗しましたエラー

説明	Command=Delete app;Result=400;ResultText=Error: PersistenceFailed
メッセージ	削除操作に失敗しました (HTTP コード: 400)
アクション	エラーの考えられる原因: アプリは存在しません。

アプリの公開

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS がアプリをストリームにリンクします。
3. QRS が、公開済みのアプリの名前が変更されたかどうかを確認します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

アプリのエクスポート

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS が、Qlik Sense Engine Service (QES) にアプリを見つけるのに必要な情報を提供します。
3. アプリID が QES からクライアントにダウンロードされます。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*
- *<MachineName>_AuditActivity_Engine.txt*

エラー

Resource not found(リソースが見つかりません)

リソースが見つかりませんエラー

説明	Command=Export app;Result=9003;ResultText=Error: EngineQix
メッセージ	リソースが見つかりません。パラメータ: QVF ヘッダー エラー (読み取り) (HTTP コード: 400)
アクション	次の手順に従います。 1. リソースが Qlik Management Console (QMC) に存在していることを確認します。 2. Qlik Sense ハブでアプリを開くことができるかを確認します。 3. QVF ファイルがセントラル ノード、または Qlik Sense サイトのリム ノードにあるかどうかチェックします。

アプリのインポート

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. アプリが作成された Qlik Sense システムへのアクセス権を持っている場合は、次の操作が実行されます。
    a. QRS がリポジトリデータベースにメタデータを保存します。
    b. QRS が Qlik Sense Engine Service (QES) にコンタクトします。
    c. アプリが移行されます (必要に応じて)。
3. QES がアプリ(オブジェクトを含む) をインポートし、これを保持します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*
- *<MachineName>_AuditActivity_Engine.txt*

エラー

データが壊れています

データが壊れていますエラー

説明	Command=Import app;Result=11;ResultText=Error: EngineQix
メッセージ	データが壊れています。パラメータ: QVF ファイルが壊れています (HTTP コード: 500)
アクション	アプリの形式が無効なため、インポートできません。

書き込みに失敗しました

書き込みに失敗しましたエラー

説明	Command=Import app;Result=9000;ResultText=Error: EngineQix
メッセージ	書き込みに失敗しました。パラメータ: REST クライアント応答エラー (HTTP コード: 500)
アクション	次の手順に従います。 1. 要求がタイムアウトしている場合は、Qlik Sense Engine Service (QES) が稼働しているかを確認します。 2. Qlik Sense で作成されたアプリを開くことができるか確認します。 3. データ ロード エディタでアプリ データをロードし、Qlik Management Console (QMC) でアプリをリロードできるか確認します。 4. アプリのリロードの履歴を確認します。

Resource not found(リソースが見つかりません)

リソースが見つかりませんエラー

説明	Command=Import app;Result=2;ResultText=Error: EngineQix
メッセージ	リソースが見つかりません。パラメータ: QVF オブジェクト エラー (HTTP コード: 500)
アクション	インポート用の QVF 作業ファイルを指定します。

アプリのリロード

アプリ内のデータは、次のようにさまざまな方法でリロードできます。

- ユーザーが、手動で Qlik Management Console (QMC) のアプリ データをリロードする。
- アプリ データが、リポジトリ データベース内のスケジュールされたタスクによってリロードされる。

- ユーザーが、データ ロード エディタにデータを手動でロードする。このようなリロードに関する情報は、*<MachineName>_AuditActivity_Engine.txt* に記録されます。
  アプリのリロード(page 728)

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS が Qlik Sense Engine Service (QSS) にコンタクトします。
3. QSS がリロード タスクを開始します。
4. QSS が Qlik Sense Engine Service (QES) に接続し、アプリのリロードを開始します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*
- *<MachineName>_AuditActivity_Engine.txt*
- *<MachineName>_AuditActivity_Scheduler.txt*

アプリの複製

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS は、アプリが存在することを確認します。
3. QRS が、ユーザーがアプリを複製できることを確認します。
4. QRS は Qlik Sense Engine Service (QES) にリクエストを送信します。
5. QES がアプリのコピーを作成します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*
- *<MachineName>_AuditActivity_Engine.txt*

エラー

Resource not found(リソースが見つかりません)

リソースが見つかりませんエラー

説明	Command=Duplicate app;Result=-2146233074;ResultText=Error: リソースが見つかりません [LOCERR_PERSISTENCE_NOT_FOUND]:リソースが見つかりません (QVF ヘッダー エラー(読み取り))

メッセージ	複製に失敗しました。アプリ'Test' が 'Test (1)' に複製されました。追加情報: 'リソースが見つかりません [LOCERR_PERSISTENCE_NOT_FOUND]:リソースが見つかりません (QVF ヘッダー エラー (読み取り))'
アクション	エラーの考えられる原因: アプリがディスクから削除されました。再度アプリのインポートを試してみてください。

アプリオブジェクトの追加

手順

Qlik Sense は以下の手順を実行します。

1. Qlik Sense Engine Service (QES) は Qlik Sense Repository Service (QRS) にコンタクトします。
2. アプリオブジェクトが、一括操作でリポジトリデータベースに追加されます。
3. QES がアプリオブジェクトを保持します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

アプリオブジェクトの更新

手順

Qlik Sense は以下の手順を実行します。

1. Qlik Sense Engine Service (QES) は Qlik Sense Repository Service (QRS) にコンタクトします。
2. アプリオブジェクトは、一括操作でリポジトリデータベースで更新されます。
3. QES は永続的アプリオブジェクトを更新します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

アプリオブジェクトの削除

手順

Qlik Sense は以下の手順を実行します。

1. Qlik Sense Engine Service (QES) は Qlik Sense Repository Service (QRS) にコンタクトします。
2. アプリオブジェクトは、一括操作によってリポジトリデータベースから削除されるように設定されています。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

アプリオブジェクトの公開

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS が、リポジトリデータベースで公開するようにアプリオブジェクトを設定します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

アプリオブジェクトの公開中止

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS が、リポジトリデータベースで公開中止するようにアプリオブジェクトを設定します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

拡張機能の追加

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS が拡張機能を追加します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

拡張機能の作成

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS が拡張機能を作成します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

拡張機能のアップロード

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS が拡張機能をアップロードします。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

エラー

プロセスはファイルにアクセスできません

プロセスはファイルにアクセスできませんエラー

説明	Command=Upload extension;Result=500;ResultText=Error: IO
メッセージ	ファイルが別のプロセスで使用されているため、プロセスはファイル '<Filename>' にアクセスできません。(HTTP コード: 500)
アクション	次の手段を試してください。 • Qlik Management Console (QMC) で進行中のプロセスの終了を待ってから、拡張機能を再度アップロードします。 • QRS を再起動します。

拡張機能の削除

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS が拡張機能を削除します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

拡張コンテンツの追加

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS が拡張コンテンツを追加します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

拡張コンテンツの削除

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS が拡張コンテンツを削除します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

コンテンツ ライブラリの追加

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS がコンテンツ ライブラリを追加します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

コンテンツ ライブラリの削除

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS がコンテンツ ライブラリを削除します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

コンテンツ ライブラリのコンテンツのアップロード

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS が、コンテンツ ライブラリのコンテンツをアップロードします。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

エラー

'Qlik.Sense.Common.Exceptions.ConflictException' タイプの例外がスローされました

'Qlik.Sense.Common.Exceptions.ConflictException' タイプの例外がスローされましたエラー

説明	Command=Upload content library content;Result=409;ResultText=Error: 競合
メッセージ	'Qlik.Sense.Common.Exceptions.ConflictException' タイプの例外がスローされました。(HTTP コード: 409)
アクション	ライブラリのコンテンツは既に存在しています。名前を変更するか、別のライブラリのコンテンツに置き換えてください。

コンテンツ ライブラリのコンテンツの削除

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS が、コンテンツ ライブラリのコンテンツを削除します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

ユーザー アクセスの追加

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRSが、アクセスを追加可能なことを確認します。
3. QRSがアクセスを追加します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Repository.txt*

エラー

検証に失敗しました

検証に失敗しましたエラー

説明	Command=Add User Access;Result=400;ResultText=Error: 不正な要求
メッセージ	<BrokenRules>
アクション	アクセスを追加できることを確認します。

ユーザー アクセスの更新

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRSが、アクセスを更新可能なことを確認します。
3. QRSがアクセスを更新します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Repository.txt*

ユーザー アクセスの削除

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRSが、アクセスを削除できることを確認します。

3. QRSがアクセスを削除します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Repository.txt*

ユーザー アクセス リクエストの許可

手順

Qlik Sense は以下の手順を実行します。

- Qlik Senseが、ユーザーが有効なアクセス パスを持っていることを確認します。これは、ユーザーがリソース (アプリなど) へのアクセスを要求するたびに実行されます。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Repository.txt*

ユーザー アクセスの許可

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) が、Qlik Sense ライセンスを確認し、ユーザーにアクセス パスを付与できるかどうかを判断します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Repository.txt*

エラー

ログイン アクセスが拒否されました

ログイン アクセスが拒否されましたエラー

説明	Command=License user access;Result=403;ResultText=Error: アクセスが拒否されました
メッセージ	SessionID のログイン アクセスが拒否されました: 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx', Hostname: "xx.xx.xx.xx", OperationType: 'UsageDenied'
アクション	適切なアクセス権を取得するには、Qlik Sense のシステム管理者にお問い合わせください。

ライセンスからのユーザー アクセスの追加

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS が、ユーザー アクセスを追加できることを確認します。
3. QRS がユーザー アクセスを認識します。
4. QRS がユーザー アクセスを追加します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Repository.txt*

エラー

ユーザー アクセスを追加できません

ユーザー アクセスを追加できませんエラー

説明	Command=Add user access from license;Result=400;ResultText=Error: 不正な要求
メッセージ	<BrokenRules>
アクション	次のことを確認してください。 • ライセンスの有効期限が切れていないこと • ライセンスが拒否リストに記載されていないこと • Qlik Sense ライセンスに利用可能な十分なトークンがあること

アプリの権限の追加

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) が、アプリの権限を該当するユーザー グループに追加します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Repository.txt*.

証明書のエクスポート

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) が証明書をエクスポートします。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Repository.txt*

ライセンスのダウンロード

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) がライセンスを検証してダウンロードします。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Repository.txt*

エラー

ライセンス: シリアル番号またはコントロール番号が無効です

ライセンス: シリアル番号またはコントロール番号が無効ですエラー

説明	Command=Download license;Result=400;ResultText=Error: ValidationFailed
メッセージ	ライセンス: 無効なシリアル番号または制御番号です (HTTP コード: 400)
アクション	有効な Qlik Sense ライセンスを指定します。

ライセンスの追加

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) は、ユーザーが指定したライセンスを追加します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Repository.txt*

エラー

ライセンス: シリアル番号またはコントロール番号が無効です

ライセンス: シリアル番号またはコントロール番号が無効ですエラー

説明	Command=Update license;Result=400;ResultText=Error: ValidationFailed

メッセージ	ライセンス: 無効なシリアル番号または制御番号です (HTTP コード: 400)
アクション	有効な Qlik Sense ライセンスを指定します。

Update license (ライセンスの更新)

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) は、ユーザーが指定したライセンスを追加します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Repository.txt*

エラー

ライセンス: シリアル番号またはコントロール番号が無効です

ライセンス: シリアル番号またはコントロール番号が無効ですエラー

説明	Command=Update license;Result=400;ResultText=Error: ValidationFailed
メッセージ	ライセンス: 無効なシリアル番号または制御番号です (HTTP コード: 400)
アクション	有効な Qlik Sense ライセンスを指定します。

ライセンスの削除

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) はライセンスを削除します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

ルールの追加

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS がルールを追加します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

ルールの更新

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS がルールを更新します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

ルールの削除

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS がルールを削除します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

ストリームの追加

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS がストリームを追加します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

ストリームの削除

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS がストリームを削除します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

サーバー ノード登録

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) が、指定したサーバー アドレスへの接続を確立します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

エラー

証明書の配布時に次のリモート ホストに接続できません

証明書の配布時に次のリモート ホストに接続できませんエラー

説明	Command=Server node registration;Result=400;ResultText=Error: REST
メッセージ	証明書の配布時に次のリモート ホストに接続できません: http://<ServerAddress>:4444/setup/certificateDistribution (HTTP コード: 400)
アクション	有効なサーバー アドレスを指定します。

サーバー ノード構成

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) がサーバー ノードの構成を更新します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

タスクの作成

手順

Qlik Sense は以下の手順を実行します。

1. Qlik Sense Repository Service (QRS) がタスクを作成し、これをリポジトリデータベースに保存します。
2. タスク情報は、QRS によってリム ノードに同期されます。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

タスクの更新

手順

Qlik Sense は以下の手順を実行します。

1. Qlik Sense Repository Service (QRS) がタスクを更新し、これをリポジトリデータベースに保存します。
2. 更新されたタスク情報が、QRS によってリム ノードに同期されます。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

タスクの削除

手順

Qlik Sense は以下の手順を実行します。

1. Qlik Sense Repository Service (QRS) がタスクを削除し、これをリポジトリデータベースから削除します。
2. タスクの削除は、QRS によってリム ノードに同期されます。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

タスクの開始

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) が、Qlik Sense Engine Service (QSS) にタスクを実行するように要求します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

エラー

Resource not found(リソースが見つかりません)

リソースが見つかりませんエラー

説明	Command=Start task;Result=-1;ResultText=Error: -----System.Net.WebException: Unable to connect to the remote server ---> System.Net.Sockets.SocketException: No connection could be made because the target machine actively refused it 127.0.0.1:5050 at System.Net.Sockets.Socket.EndConnect(IAsyncResult asyncResult) at System.Net.ServicePoint.ConnectSocketInternal(Boolean connectFailure, Socket s4, Socket s6, Socket& socket, IPAddress& address, ConnectSocketState state, IAsyncResult asyncResult, Exception& exception) --- End of inner exception stack trace --- at System.Net.HttpWebRequest.EndGetRequestStream(IAsyncResult asyncResult, TransportContext& context) at System.Net.HttpWebRequest.EndGetRequestStream(IAsyncResult asyncResult) at System.Net.WebClient.UploadBitsRequestCallback(IAsyncResult result)-----
メッセージ	Trailing task exception in SchedulerClient.StartTask('1xx1111x-111x-111x-1xx1-111xxx1x1x11'): '↓-----↓System.Net.WebException: Unable to connect to the remote server ---> System.Net.Sockets.SocketException: No connection could be made because the target machine actively refused it 127.0.0.1:5050↵↓ at System.Net.Sockets.Socket.EndConnect(IAsyncResult asyncResult)↵↓ at System.Net.ServicePoint.ConnectSocketInternal(Boolean connectFailure, Socket s4, Socket s6, Socket& socket, IPAddress& address, ConnectSocketState state, IAsyncResult asyncResult, Exception& exception)↵↓ --- End of inner exception stack trace ---↵↓ at System.Net.HttpWebRequest.EndGetRequestStream(IAsyncResult asyncResult, TransportContext& context)↵↓ at System.Net.HttpWebRequest.EndGetRequestStream(IAsyncResult asyncResult)↵↓ at System.Net.WebClient.UploadBitsRequestCallback(IAsyncResult result)↓-----'
アクション	Qlik Sense Engine Service (QSS) が稼働しているか確認します。

タスクの停止

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) が、Qlik Sense Engine Service (QSS) にタスクの実行を停止するように要求します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

ユーザーディレクトリの同期

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) がユーザー ディレクトリを同期します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*

リポジトリの開始

手順

Qlik Sense は以下の手順を実行します。

1. QRS のコマンド ライン パラメータを検証します。
2. QRS がログ フレームワークをロードします。
3. QRS が証明書を検証します。
4. QRS が Qlik Sense Repository Database (QRD) への接続を確立します。
5. 必要に応じて、QRS が、リポジトリデータベース スキーマの移行ステップを実行します。
6. ハードウェア情報が収集されます。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_Service_Repository.txt*

エラー

証明書は正しくインストールされていません

証明書は正しくインストールされていませんエラー

説明	Command=Start Repository;Result=-1;ResultText=Certificates are not correctly installed
メッセージ	証明書を初期化しています。
アクション	エラーは無効な証明書に関連しています。証明書に関するサポートについては、システム管理者にお問い合わせください。

リポジトリの停止

手順

Qlik Sense は以下の手順を実行します。

1. 内部サービスが停止します。
2. バックグラウンド スレッドが停止します。
3. Qlik Sense Repository Database (QRD) を除くすべての Qlik Sense サービスが停止します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_Service_Repository.txt*

サービスの状態のチェック

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) が、指定した Qlik Sense サービスとの通信が機能していることを確認します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_Service_Repository.txt*

エラー

次のサービス アカウントは存在しません

次のサービス アカウントは存在しませんエラー

説明	Command=Check service status;Result=403;ResultText=Error: セキュリティ
メッセージ	次のサービス アカウントは存在しません: <Service.Name> (HTTP コード: 403)
アクション	指定した Qlik Sense サービスを再起動します。

プラグインのロード

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) が、インストール中に指定したプラグインをロードします。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_Service_Repository.txt*

ルールの監査

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) が、指定されたルールをリポジトリデータベースから取得します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Repository.txt*

セキュリティの監査

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) が、指定されたセキュリティルールをリポジトリデータベースから取得します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Repository.txt*

ライセンスの監査

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) スレッドは、バックグラウンドで実行されます。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Repository.txt*

ライセンス ルールの監査

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) スレッドがバックグラウンドで実行され、ライセンス使用状況を監視します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Repository.txt*

ライセンスのメンテナンス

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) スレッドは、バックグラウンドで実行されます。
  以下に示す目的で、スレッドは、ライセンスにリンクされているプロキシ セッションを継続的に確認します。

- ユーザーがライセンス トークンを過剰に使用することを防ぐ
- ライセンスに関連する変更が原因で、ユーザーがログイン パスを使用できなくなっていないかどうか確認する
- そのアクセス パスのプロキシ セッションがタイムアウトしているかどうか確認する

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Repository.txt*

証明書の配布

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Repository Service (QRS) が、リム ノードに証明書を配布します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_Service_Repository.txt*

エラー

証明書の配布に失敗しました

証明書の配布に失敗しましたエラー

説明	Command=Distribute certificate;Result=-2146233088;ResultText=Error: 証明書の配布時に次のリモート ホストに接続できません: http://<ServerAddress>:4444/setup/certificateDistribution
メッセージ	証明書の配布に失敗しました
アクション	有効なサーバー アドレスを指定します。

3.3 Qlik Sense Proxy Service

このセクションでは、Qlik Sense のログを使用して Qlik Sense Proxy Service (QPS) に関連する問題をトラブルシューティングする方法について説明します。

プロキシの開始

手順

Qlik Sense は以下の手順を実行します。

1. Qlik Sense Proxy Service (QPS) がプロキシを作成します。
2. QPS がプロキシを開始します。

3. ハードウェア情報が収集されます。
4. QPS がハードウェア情報をログに書き込みます。
5. QPS が証明書をインストールします。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Proxy.txt*
- *<MachineName>_Service_Proxy.txt*

エラー

ハードウェア情報の取得中にエラーが発生しました

ハードウェア情報の取得中にエラーが発生しましたエラー

説明	Command=Start proxy;Result= -1;ResultText=Error occurred while retrieving hardware information
メッセージ	メッセージは異なる場合があります。
アクション	レジストリ設定を確認します。

プロキシはポート '443' をリッスンしません

プロキシはポート '443' をリッスンしませんエラー

説明	QPS の起動時に内部サービスが開始されると、ポートの競合が発生する場合があります。 Command=Start internal service;Result=-2147467259;ResultText=Error: Only one usage of each socket address
メッセージ	プロキシはポート '443' をリッスンしません (別のプロセスにバインドされている可能性があります)
アクション	次の手順に従います。 1. ポート 443 が Qlik Sense で利用できることを確認します。 2. Qlik Sense サービスを再起動します。

プロキシの停止

手順

Qlik Sense は以下の手順を実行します。

1. Qlik Sense Proxy Service (QPS) が Qlik Sense Repository Service (QRS) を通知します。
2. QPS 設定と通知の呼び出しスレッドが停止します。
3. QPS が、QRS に証明書がインストールされていることを確認します。
4. 内部サービスが停止します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_Service_Proxy.txt*

接続を開く

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Engine Service (QES) へのソケットを開きます。これは、ユーザーが Qlik Sense でアプリを開くたびに発生します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Proxy.txt*
- *<MachineName>_Service_Proxy.txt*

エラー

Web ソケット接続を開けませんでした

Web ソケット接続を開けませんでしたエラー

説明	Command=Open connection;Result=400;ResultText=Error: Web ソケット接続を開けませんでした
メッセージ	接続 '<ID of connection>' は、1 つのエラー メッセージを送信するためにストリーム ステートに転送されました
アクション	次の手順に従います。 1. QES が稼働しているかを確認します。稼働していない場合は、QES を起動します。 2. QES に接続できることを確認します。

Web 例外: プロトコル エラー: 応答ストリームが存在します

Web 例外: プロトコル エラー: 応答ストリームが存在しますエラー

説明	Command=Open connection;Result=400;ResultText=<different from zero>;ResultText=Error: <error message>
メッセージ	Web 例外: プロトコル エラー: 応答ストリームが存在します。リモート エンドポイント '{0}' + さまざまな例外メッセージ
アクション	次のことを確認してください。 • QES が稼働中であること。 • サーバーのポート 4747 でローカルに QES に接続できること。

Web 例外: プロトコル エラー: 応答ストリームが存在しません

Web 例外: プロトコル エラー: 応答ストリームが存在しませんエラー

説明	Command=Open connection;Result=400;ResultText=<different from zero>;ResultText=Error: <error message>
メッセージ	Web 例外: プロトコル エラー: '{0}' への接続中に応答ストリームが存在しません ' + さまざまな例外メッセージ
アクション	次のことを確認してください。 • QES が稼働中であること。 • サーバーのポート 4747 でローカルに QES に接続できること。

サービス URI の接続中の Web 例外

サービス URI の接続中の Web 例外エラー

説明	Command=Open connection;Result=400;ResultText=<different from zero>;ResultText=Error: <error message>
メッセージ	サービス URI {0} への接続中に Web 例外が発生しました ' + さまざまな例外メッセージ
アクション	URI のサービスが利用できることを確認します。

接続は、1 つのエラー メッセージを送信するためにストリーム ステートに転送されました

接続は、1 つのエラー メッセージを送信するためにストリーム ステートに転送されましたエラー

説明	Command=Open connection;Result=400;ResultText=<different from zero>;ResultText=Error: <error message>
メッセージ	接続 '{0}' は、1 つのエラー メッセージを送信するためにストリーム ステートに転送されました + さまざまな例外メッセージ
アクション	次のことを確認してください。 • QES が稼働中であること。 • サーバーのポート 4747 でローカルに QES に接続できること。

Web ソケット接続を開けませんでした

Web ソケット接続を開けませんでしたエラー

説明	Command=Open connection;Result=400;ResultText=<different from zero>;ResultText=Error: <error message>
メッセージ	Web ソケット接続を開けませんでした

アクション	次のことを確認してください。 • QES が稼働中であること。 • サーバーのポート 4747 でローカルに QES に接続できること。

接続の終了

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Engine Service (QES) へのソケットを閉じます。これは、ユーザーがアプリを閉じるたびに発生します (ブラウザでタブを閉じる場合など)。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Proxy.txt*

エラー

Web ソケット接続を開けませんでした

Web ソケット接続を開けませんでしたエラー

説明	Command=Open connection;Result=400;ResultText=Error: Web ソケット接続を開けませんでした
メッセージ	接続 '<ID of connection>' は、1 つのエラー メッセージを送信するためにストリーム ステートに転送されました
アクション	次の手順に従います。 1. QES が稼働しているかを確認します。稼働していない場合は、QES を起動します。 2. QES に接続できることを確認します。

Command=Open connection;Result=<different from zero>

Command=Open connection;Result=<different from zero>

説明	Command=Open connection;Result=<different from zero>;ResultText=Error: <error message>
メッセージ	接続の終了に関連するログ メッセージがないか検索します。 上記のようなログ エントリが見つかった場合は、メッセージ フィールドの情報の内容を確認します。
アクション	次の手順に従います。 1. メモリ消費を分析し、netstat (無効なステートの TCP ソケット) を実行します。問題が発生した場合は、接続 (QES への Web ソケット) は Qlik Sense Proxy Service (QPS) によって配置されていることから、QPS を再起動します。 2. 問題が解決しない場合は、QES が稼働しているかを確認します。 3. Qlik のサポートにお問い合わせください。

セッションの開始

手順

Qlik Sense は以下の手順を実行します。

- ユーザーが Qlik Sense にアクセスすると、新しいプロキシ セッションが開始します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Proxy.txt*

エラー

セッションを開始できません

セッションを開始できませんエラー

説明	ユーザーが新しいプロキシ セッションを開始できない場合は、次に関連している可能性があります。 • Qlik Sense Proxy Service (QPS) の構成 • インストール固有の問題 次の情報を含むログ メッセージを検索します。 Command=Start session;Result=<different from zero>;ResultText=Error: <error message>
メッセージ	上記のようなログ エントリが見つかった場合は、メッセージ フィールドの情報の内容を確認します。
アクション	セッションの開始のログ エントリがない場合は、プロキシの開始コマンドのログ エントリを調べて QPS の構成を確認します。

セッションの停止

手順

Qlik Sense は以下の手順を実行します。

- ユーザーがログアウトするか、プロキシ セッションがタイムアウトすると、プロキシ セッションは停止します。セッションが実行されているブラウザをユーザーが閉じると、ブラウザが閉じられた瞬間から計算された [*タイムアウトまでのセッション アイドル時間 (分)*] 設定を超えたときにプロキシ セッションが停止します。[*タイムアウトまでのセッション アイドル時間 (分)*] は、仮想プロキシで定義されます。[仮想プロキシ] を参照してください。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Proxy.txt*

エラー

セッションを停止できません

セッションを停止できませんエラー

説明	次の情報を含むログ メッセージを検索します。 Command=Stop session;Result=<different from zero>;ResultText=Error: <error message>
メッセージ	上記のようなログ エントリが見つかった場合は、メッセージ フィールドの情報の内容を確認します。
アクション	セッションの停止のログ エントリがない場合は、プロキシの開始コマンドのログ エントリを調べて Qlik Sense Proxy Service (QPS) の構成を確認します。 最後の手段として、QPS を再起動します。

ログアウト

手順

Qlik Sense は以下の手順を実行します。

- プロキシ セッションがタイム アウトした場合、自分でログアウトした場合に、ユーザーはログアウトします。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Proxy.txt*

エラー

Command=Logout;Result=<return code not zero>

Command=Logous;Result=<return code not zero> エラー

説明	Command=Logout;Result=<return code not zero>;ResultText=Error: <error message>
メッセージ	上記のようなログ エントリが見つかった場合は、メッセージ フィールドの情報の内容を確認します。
アクション	ログアウト時に問題が繰り返し発生する場合は、次の手順に従います。 1. Qlik Sense Proxy Service (QPS) を再起動します。 2. netstat を実行してソケットのステータスを分析し、CLOSE_WAIT、SYN_SENT、FIN_WAIT_2 ステートのソケットを分析します。

ログイン

手順

Qlik Sense は以下の手順を実行します。

1. ユーザーが有効なユーザー ディレクトリにリンクしているかどうかを確認します。
2. ユーザーがリポジトリデータベースに存在しているか確認します。
3. ユーザーが Qlik Sense へのアクセス権を持っているかどうかを確認します。
4. ユーザーがライセンスに関連するアクセス権を持っているかどうかを確認します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Proxy.txt*

エラー

ログオンに失敗しました

ログオンに失敗しましたエラー

説明	Command=Login;ResultCode=403;ResultText=Error: アクセスが拒否されました
メッセージ	ユーザー '<username>' のログインが失敗しました。資格情報を確認します。
アクション	次の手順に従います。 • ユーザーがリポジトリデータベースに存在しているかを確認します。 • ユーザーがライセンスに関連する Qlik Sense へのアクセス件を持っていることを確認します。 • ユーザーがブロックされていないかを確認します。

証明書のインストール

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Proxy Service (QPS) は、証明書がリポジトリデータベースにインストールされるのを待機します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditSecurity_Proxy.txt*

3.4 Qlik Sense Engine Service

このセクションでは、Qlik Sense のログを使用して Qlik Sense Engine Service (QSS) に関連する問題をトラブルシューティングする方法について説明します。

タスクの開始

手順

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. セントラル ノードのマネージャー Qlik Sense Engine Service (QSS) が各ワーカー QSS と通信して、タスクを実行できるワーカーを確認します。
3. タスクは、負荷分散ルールに従って、現在使用可能なワーカーQSSのうちで負荷が最も少ないものに割り当てられます。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Scheduler.txt*
- *<MachineName>_AuditActivity_Repository.txt*

エラー

タスクが見つかりません

タスクが見つかりませんエラー

説明	Command=Start task;Result=5;ResultText=Error: 失敗
メッセージ	タスクが見つかりません
アクション	次の手段を試してください。 • リポジトリデータベースにアクセスできる場合は、データベースでタスクを検索します。 • タスクがリム ノードに正常に同期されているかを確認します。 • 同一のタスクを新たに作成し、動作することを確認します。

スケジューラがライセンスされていません

スケジューラがライセンスされていませんエラー

説明	Command=Start task;Result=10;ResultText=Error: 失敗
メッセージ	スケジューラがライセンスされていません。タスクの実行が許可されていません
アクション	有効な Qlik Sense ライセンスを指定します。

スケジューラーはマネージャーではありません

スケジューラーはマネージャーではありませんエラー

説明	Command=Start task;Result=15;ResultText=Error: 失敗
メッセージ	スケジューラーはマネージャーではありません。タスクの実行が許可されていません
アクション	セントラル ノードの QSS が「マネージャー」または「マネージャーとワーカー」であることを確認してください。

タスクのアクティブ セッションが見つかりました

タスクのアクティブ セッションが見つかりましたエラー

説明	Command=Start task;Result=20;ResultText=Error: 失敗
メッセージ	タスクのアクティブ セッションが見つかりました。タスクが開始されていません
アクション	次の手段を試してください。 • タスクが完了するまで待機します。 • タスクを停止します。 • QSS を再起動します。

タスクが無効になりました

タスクが無効になりましたエラー

説明	Command=Start task;Result=25;ResultText=Error: 失敗
メッセージ	タスクが無効になりました
アクション	タスクを有効にします。

TaskExecutionSession が既に存在しています

TaskExecutionSession が既に存在していますエラー

説明	Command=Start task;Result=30;ResultText=Error: 失敗
メッセージ	TaskExecutionSession が既にアプリ<App.Name> に存在しています
アクション	次の手段を試してください。 • アプリをリロードしているタスクが完了するまで待機します。 • アプリをリロードしているタスクを停止します。 • QSS を再起動します。

タスクを実行するワーカー ノードが見つかりませんでした

タスクを実行するワーカー ノードが見つかりませんでしたエラー

説明	Command=Start task;Result=40;ResultText=Error: 失敗
メッセージ	タスクを実行するワーカー ノードが見つかりませんでした: <Task.Name>
アクション	次の手順に従います。 1. ワーカー ノードのステータスを確認してリロードを実行できるかどうかを判断します。 2. リロードするアプリがワーカー ノードに存在することを確認します。

TaskExecutionSession を作成できません

TaskExecutionSession を作成できませんエラー

説明	Command=Start task;Result=45;ResultText=Error: 失敗

メッセージ	TaskExecutionSession を作成できません
アクション	QSS を再起動します。

タスク開始時の予期しない例外です

タスク開始時の予期しない例外ですエラー

説明	Command=Start task;Result=50;ResultText=Error: 失敗
メッセージ	タスク開始時の予期しない例外です。例外メッセージ: <Exception.Message>
アクション	QSS を再起動します。

タスクの開始を試みるときの予期しない例外です

タスクの開始を試みるときの予期しない例外ですエラー

説明	Command=Start task;Result=55;ResultText=Error: 失敗
メッセージ	タスクの開始を試みるときの予期しない例外です。例外メッセージ: <Exception.Message>
アクション	QSS を再起動します。

タスクの再試行回数が最大値に達しました

タスクの再試行回数が最大値に達しましたエラー

説明	Command=Start task;Result=80;ResultText=Error: 失敗
メッセージ	タスク(ID/名前) <Task.ID>/<Task.Name> の再試行回数が最大値 (<Amount>) に達しました
アクション	QSS を再起動します。

再試行を開始できません

再試行を開始できませんエラー

説明	Command=Start task;Result=90;ResultText=Error: 失敗
メッセージ	再試行を開始できません。TaskExecutionSession が null です
アクション	QSS を再起動します。

タスクの終了

手順

Qlik Sense は以下の手順を実行します。

- タスクを実行したワーカー ノードの Qlik Sense Engine Service (QSS) が、マネージャーの QSS に結果を送信します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Scheduler.txt*
- *<MachineName>_AuditActivity_Repository.txt*

エラー

TaskCompletedFail で失敗しました

TaskCompletedFail で失敗しましたエラー

説明	Command=Finished task;Result=60;ResultText=Error: 失敗
メッセージ	TaskCompletedFail で失敗しました。タスクを強制的にエラーにします
アクション	タスクがリム ノードに正常に同期されているかを確認します。

ステート<State> でタスクを完了しました

ステート<State> でタスクを完了しましたエラー

説明	Command=Finished task;Result=65;ResultText=Error: 失敗
メッセージ	ステート<State> でタスクを完了しました
アクション	タスクがリム ノードに正常に同期されているかを確認します。

セッションの削除に失敗しました

セッションの削除に失敗しましたエラー

説明	Command=Finished task;Result=70;ResultText=Error: 失敗
メッセージ	タスク ID <Task.ID> の ID <Session.ID> のセッションの削除に失敗しました
アクション	QSS を再起動します。

TaskCompletedSuccess の予期しない例外です

TaskCompletedSuccess の予期しない例外ですエラー

説明	Command=Finished task;Result=50;ResultText=Error: 失敗
メッセージ	TaskCompletedSuccess の予期しない例外です。例外 メッセージ: <Message>
アクション	QSS を再起動します。

TaskCompletedFail の予期しない例外です

TaskCompletedFail の予期しない例外ですエラー

説明	Command=Finished task;Result=50;ResultText=Error: 失敗
メッセージ	TaskCompletedFail の予期しない例外です。例外 メッセージ: <Message>
アクション	QSS を再起動します。

タスクが失敗しました

タスクが失敗しましたエラー

説明	Command=Finished task;Result=0;ResultText=Error: 失敗
メッセージ	タスクが失敗しました
アクション	タスクが失敗した原因を確認します。 そのタスクがリロードタスクの場合は、リロードに失敗した原因を示すエンジンログとスクリプトログを確認します。

タスクの実行

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Engine Service (QSS) が、タスクの実行中に、タスク実行チェーンのさまざまなステートを記録します。

成功

成功した場合は、ログエントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Scheduler.txt*

エラー

タスク ID をステートに設定しようとしています

タスク ID をステートに設定しようとしていますエラー

説明	Command=Task execution;Result=55;ResultText=Error: 失敗
メッセージ	タスク (ID) <Task.ID> を <State> に設定しようとしています。許可されていません。ステートの変更は行われません。
アクション	次の手順に従います。 1. タスクを再実行します。 2. QSS を再起動します。

TaskExecutionSession を null にすることはできません

TaskExecutionSession を null にすることはできませんエラー

説明	Command=Task execution;Result=90;ResultText=Error: 失敗
メッセージ	TaskExecutionSession を null にすることはできません。提案されたステート <State> のタスクが削除されたため、ステートの変更を続行できません。

アクション	次の手順に従います。 1. タスクを再実行します。 2. QSS を再起動します。

ステートの変更が抑制されました

ステートの変更が抑制されましたエラー

説明	Command=Task execution;Result=85;ResultText=Error: 失敗
メッセージ	ID <Task.ID> の <Task.Name> に対して <State> へのステートの変更が抑制されました。
アクション	必要なアクションはありません。タスクが停止したときにステートが抑制されました。

<Task.Name> を取得できません

<Task.Name> を取得できませんエラー

説明	Command=Task execution;Result=5, 75;ResultText=Error: 失敗
メッセージ	AuditActivityLog の ID <Task.ID> の <Task.Name> は取得できません。アプリではなくタスクの ID と名前のみを記録します。
アクション	次の手順に従います。 1. タスクを再実行します。 2. QSS を再起動します。

マネージャーの開始

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Engine Service (QSS) がセントラル ノードで起動すると、マネージャー スケジューラが開始します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_Service_Scheduler.txt*

ワーカーの開始

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Engine Service (QSS) が起動すると、ワーカー スケジューラが開始します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_Service_Scheduler.txt*

マネージャーの再開

手順

Qlik Sense は以下の手順を実行します。

- 一時停止中のマネージャー Qlik Sense Engine Service (QSS) を再開します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_Service_Scheduler.txt*

ワーカーの再開

手順

Qlik Sense は以下の手順を実行します。

- 一時停止中のワーカー Qlik Sense Engine Service (QSS) を再開します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_Service_Scheduler.txt*

初期設定の読み取り

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Engine Service (QSS) が起動時に初期設定を読み取ります。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_Service_Scheduler.txt*

サービス起動時のハードウェア情報の記録

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Engine Service (QSS) のサービス起動時のハードウェア情報を記録します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_Service_Scheduler.txt*

エラー

ハードウェア情報の記録に失敗しました

ハードウェア情報の記録に失敗しましたエラー

説明	Command=Start scheduler;Result=50;ResultText=Error: 失敗
メッセージ	ハードウェア情報の記録に失敗しました
アクション	QSS を再起動します。

マネージャーの停止

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Engine Service (QSS) がセントラル ノードでシャットダウンすると、マネージャー スケジューラが停止します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_Service_Scheduler.txt*

ワーカーの停止

手順

Qlik Sense は以下の手順を実行します。

- Qlik Sense Engine Service (QSS) がシャットダウンすると、ワーカー スケジューラが停止します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_Service_Scheduler.txt*

マネージャーの一時停止

手順

Qlik Sense は以下の手順を実行します。

- 実行中のマネージャー Qlik Sense Engine Service (QSS) を一時停止します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_Service_Scheduler.txt*

ワーカーの一時停止

手順

Qlik Sense は以下の手順を実行します。

- 実行中のワーカー Qlik Sense Engine Service (QSS) を一時停止します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_Service_Scheduler.txt*

ワーカーの設定の変更

手順

Qlik Sense は以下の手順を実行します。

- ワーカー Qlik Sense Engine Service (QSS) の設定の変更を記録します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Scheduler.txt*

3.5 Qlik Sense Engine Service

このセクションでは、Qlik Sense のログを使用して Qlik Sense Engine Service (QES) に関連する問題をトラブルシューティングする方法について説明します。

アプリを開く

手順

Qlik Sense は以下の手順を実行します。

1. アプリが既に開いているかどうかを確認します。
2. 開いていない場合は、QVF ファイルをロードします。
3. ファイルからアプリのプロパティを読み取ります。
4. ファイルからスクリプトを読み取ります。
5. アプリを開きます。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Engine.txt*

エラー

異なるモードで既に開いています

異なるモードで既に開いていますエラー

説明	Command=Open app;Result=1009;ResultText=Error: アプリは異なるモードで既に開いています
メッセージ	<AppId>
アクション	データのあるアプリを開くときにデータのないアプリを開いていないか (または その逆) を確認します。

既に開いています

既に開いていますエラー

説明	Command=Open app;Result=1002;ResultText=Error: アプリは すでに開いています
メッセージ	<AppId>
アクション	アプリが既に開いていないか確認します。

無効なパスです

無効なパスですエラー

説明	Command=Open app;Result=4;ResultText=Error: 無効なパスです
メッセージ	パラメータの形式が正しくありません
アクション	アプリ名、パスワード、ユーザー名、シリアル番号が UTF-8 でエンコードされた文字列であることを確認します。

Resource not found(リソースが見つかりません)

リソースが見つかりませんエラー

説明	Command=Open app;Result=9003;ResultText=Error: リソースが見つかりません
メッセージ	QVF ヘッダー エラー (読み取り)
アクション	エラーの考えられる原因: アプリがディスクから削除されました。再度 アプリのインポートを試してみてください。

アプリの追加

手順

Qlik Sense は以下の手順を実行します。

1. アプリ名が有効かどうかを確認します。
2. アプリを作成します。

3. QVF ファイルを保存します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Engine.txt*

エラー

無効な名前です

無効な名前ですエラー

説明	Command=Create app;Result=3001;ResultText=Error: アプリの保存に失敗しました。
メッセージ	<AppName>
アクション	次の文字列がアプリ名に含まれていないことを確認します。 • 特殊文字: <>:\"/|?* • Microsoft Windows で予約されているデバイス名 (“COM1”、“LPT1” など)

アプリの削除

手順

Qlik Sense は以下の手順を実行します。

1. アプリのすべてのアプリ インスタンスをアンロードします。
2. QVF ファイルを削除します。
3. Qlik Sense Repository Service (QRS) にファイルを削除するように要求します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Engine.txt*

エラー

削除に失敗しました

削除に失敗しましたエラー

説明	Command=Delete app;Result=9002;ResultText=Error: 削除に失敗しました
メッセージ	<REST client response error>
アクション	QRS から応答がないため、実行を停止しているかどうか、またはリクエストを処理できないかどうかを確認します。

アプリのエクスポート

手順

Qlik Sense は以下の手順を実行します。

1. QVF ファイルを開きます。
2. 新しい QVF ファイルにコピーします。
3. アプリのコンテンツをエクスポートします。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Engine.txt*

エラー

ディスクがいっぱいです

ディスクがいっぱいですエラー

説明	Command=Export app;Result=9009;ResultText=Error: ディスクでスペースが不足しています
メッセージ	CopyQvfFile
アクション	ディスクの空き容量を増やします。

ファイルが壊れています

ファイルが壊れていますエラー

説明	Command=Export app;Result=3002;ResultText=Error: ファイルは破損しています
メッセージ	CopyQvfFile
アクション	エクスポートしたファイルに書き込みできるかを確認します。

アプリのインポート

手順

Qlik Sense は以下の手順を実行します。

1. 現在のバージョンの Qlik Sense にアプリを移行できるかどうかを確認します (必要な場合)。
2. インポートするアプリのコピーを開きます。
3. コピーから不要なオブジェクト (接続など) を削除します。
4. Qlik Sense Repository Service (QRS) にアプリを保存するように要求します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Engine.txt*

エラー

ファイルが壊れています

ファイルが壊れていますエラー

説明	Command=Import app;Result=9008;ResultText=Error: アプリがより新しい製品バージョンで作成されました。
メッセージ	移行
アクション	アプリが新しいバージョンの Qlik Sense で作成されたのではないことを確認します。

内部エラーです

内部エラーですエラー

説明	Command=Import app;Result=10;ResultText=Error: 内部エラーです
メッセージ	ファイル (ImportApp) をインポートできませんでした
アクション	インポート時には、最初に QVF ファイルがローカルの *\App* フォルダにコピーされます。これが失敗する場合、フォルダが書き込み禁止になっている可能性があります。フォルダが書き込み禁止になっていないかを確認します。

アプリのリロード

手順

Qlik Sense は以下の手順を実行します。

- リロードスクリプトを実行します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Engine.txt*

アプリの複製

手順

Qlik Sense は以下の手順を実行します。

1. ソース アプリとターゲット アプリのアプリ ID を比較します。
2. Qlik Sense Repository Service (QRS) にアプリを開くように要求します。
3. QVF ファイルをコピーします。
4. ファイルのコピーをインポートします。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Engine.txt*

エラー

複製に失敗しました

複製に失敗しましたエラー

説明	Command=Duplicate app;Result=8;ResultText=Error: Invalid parameters (パラメータが無効です)
メッセージ	ファイルをコピーできませんでした。SrcAppId とTargetAppId が同じです
アクション	ソース ID とターゲット ID が同じでないことを確認します。

アプリの公開

手順

Qlik Sense は以下の手順を実行します。

1. アプリがセッション アプリかどうかを確認します。セッション アプリの場合、公開には対応していません。セッション アプリは Qlik Sense Engine Service (QES) メモリにのみ存在し、どのファイルにもリンクしていません。
2. オブジェクトをリポジトリデータベースに保存します。
3. Qlik Sense Repository Service (QRS) にアプリを公開するように要求します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Engine.txt*

エラー

アクセス拒否

アクセス拒否 エラー

説明	Command=Publish app;Result=8;ResultText=Error: アクセスが拒否されました
メッセージ	オブジェクトを保存できませんでした
アクション	アプリを公開する前に、公開操作で必要なオブジェクトをフラッシュできなかった場合は、ディスクが書き込み禁止になっていないかを確認します。

REST 接続に失敗しました

REST 接続に失敗しましたエラー

説明	Command=Publish app;Result=18;ResultText=Error: Rest 接続に失敗しました
メッセージ	REST クライアント応答エラー
アクション	QRS から応答がないため、実行を停止しているかどうか、またはリクエストを処理できないかどうかを確認します。

アプリの公開中止

手順

Qlik Sense は以下の手順を実行します。

1. アプリがセッション アプリかどうかを確認します。セッション アプリの場合、公開には対応していません。セッション アプリは Qlik Sense Engine Service (QES) メモリにのみ存在し、どのファイルにもリンクしていません。
2. オブジェクトをリポジトリデータベースに保存します。
3. Qlik Sense Repository Service (QRS) にアプリの公開を取り消すように要求します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Engine.txt*

エラー

アクセス拒否

アクセス拒否エラー

説明	Command=Unpublish app;Result=8;ResultText=Error: アクセスが拒否されました
メッセージ	オブジェクトを保存できませんでした
アクション	アプリを公開中止する前に、公開操作で必要なオブジェクトをフラッシュできなかった場合は、ディスクが書き込み禁止になっていないかを確認します。

REST 接続に失敗しました

REST 接続に失敗しましたエラー

説明	Command=Unpublish app;Result=18;ResultText=Error: Rest 接続に失敗しました
メッセージ	REST クライアント応答エラー
アクション	QRS から応答がないため、実行を停止しているかどうか、またはリクエストを処理できないかどうかを確認します。

アプリの置換

Qlik Sense は以下の手順を実行します。

1. リクエストが Qlik Sense Repository Service (QRS) に送信されます。
2. QRS がリポジトリデータベースを更新します。
3. QRS が Qlik Sense Engine Service (QES) にコンタクトします。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_AuditActivity_Repository.txt*
- *<MachineName>_AuditActivity_Engine.txt*

エンジンの開始

手順

Qlik Sense は以下の手順を実行します。

1. Qlik Sense Engine Service (QES) が、現在の実行モード (サーバーまたはデスクトップ) を設定します。
2. QES がコマンド ライン引数を解析します。
3. QES がログの記録を構成します。
4. QES がオペレーティング システムとバージョンを検出します。
5. QES が照合とメモリの構造を初期化します。
6. QES が終了ハンドラを設定し、内部スレッドを開始し、ライセンスを確認します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_Service_Engine.txt*

エラー

登録に失敗しました

登録に失敗しましたエラー

説明	Command=Start engine;Result=-1;ResultText=Error:Server crash
メッセージ	登録時にサーバーがクラッシュしました
アクション	次の手順に従います。 1. 既定の *\App* フォルダーが存在するか確認します。 2. ネットワーク コントローラーの状態を確認します。 3. ネットワーク ポートの状態を確認します。

エンジンの停止

手順

Qlik Sense は以下の手順を実行します。

1. Qlik Sense Engine Service (QES) がキャッシュトリマを停止します。
2. QES がキャッシュをクリアします。
3. QES がプロセス ハンドラを終了します。
4. QES がスレッドを終了します。

成功

成功した場合は、ログ エントリが手順全体で次のファイルに書き込まれます。

- *<MachineName>_Service_Engine.txt*

エラー

キャッシュトリマが停止しません

キャッシュトリマが停止しませんエラー

説明	Command=Stop engine;Result=-1;ResultText=Warning
メッセージ	キャッシュトリマが停止しません
アクション	Qlik のサポートにお問い合わせください。