QlikView の展開

QlikView®
May 2024

Contents

1 はじめに

このガイドでは、インストール時のアドバイスなど、QlikView の計画と実装方法に関する情報について解説します。

QlikView Server は、QlikView の情報をホストし、インターネットやイントラネットを通して共有するプラットフォームを提供します。QlikView Server は、複数のユーザーやクライアント、ドキュメント、オブジェクトへのセキュアな接続を実現します。

QlikView Publisher はコンテンツとアクセス、配信を管理します。またデータを限定して、各ユーザーにカスタマイズした情報のみを表示させることもできます。QlikView Publisher サービスとユーザー インターフェイスは、QlikView Server とQlikView 管理コンソール (QMC) に完全に統合されています。

1.1 計画とインストール

展開の計画

ここではアーキテクチャ、展開シナリオ、セキュリティ面、ロギング、およびライセンス契約に関して QlikView サイトに必要なものを確認し、QlikView サイトの展開を計画する方法について学びます。

QlikView Server をインストールする

QlikView サイトが機能するようにインストールする方法については、このセクションをご覧ください。

1.2 バックアップとアップグレード

QlikView をバックアップおよび復元する

このセクションでは、QlikView Server インストールの完全なバックアップを作成する方法について確認できます。ここには、証明書をバックアップして復元する方法についての専用ドキュメントが記載されています。

インストールをアップグレードして移行する

このセクションでは、QlikView Server を最新リリースにアップグレードする方法についての情報を確認できます。ここでは、QlikView Server 展開を異なるコンピュータまたはコンピュータのクラスターに移行する方法についての情報を確認できます。

1　　のシステム要件 QlikView Server

このセクションでは、QlikView Server を正常にインストールし稼働させるために、対象システムが満たす必要がある要件を記載しています。

システム要件

コンポーネント	要件
プラットフォーム *	• Microsoft Windows Server 2016 • Microsoft Windows Server 2019 • Microsoft Windows Server 2022 開発およびテスト専用: • Microsoft Windows 10 Anniversary Update (ビルド1607) 以降 • Microsoft Windows 11
プロセッサ (CPU)	Multi-core x64 と互換性のあるプロセッサ
メモリ	最小 4 GB。データ容量によってはさらに大きなメモリが必要な場合があります。QlikView はインメモリ分析技術であり、QlikView 製品のメモリ要件は、分析されるデータ量に直接関係しています。
ディスク空き容量	インストールには計 900 MB が必要
セキュリティ	• Microsoft Active Directory (NTLM または Kerberos) • ローカル Windows ユーザー アカウント (NTLM) • サードパーティ製セキュリティ (QlikView Server Enterprise Edition が必要)
Web サーバー	• QlikView Web サーバー • Microsoft IIS 8、8.5 または 10
.NET フレームワーク	4.8 以上
インターネットプロトコル	• IPv4 • IPv6 • デュアル スタック (IPv4 および IPv6)
Qlik Sense 互換性	QlikView Server は、Qlik Sense Enterprise がインストール済みのコンピュータにはインストールできません。 QlikView アプリは Qlik Sense Enterprise SaaS にパブリッシュすることができます。

* プラットフォームに標準製造元サポートがある場合。

ライセンス アクティブ化により、Qlik Licensing Service へのアクセスが要求されています。ポート 443 を開いて、license.qlikcloud.com への発信を許可します。
プロキシの使用がサポートされています。Windows でプロキシ サービスを設定する詳しい方法については、「QlikView Server で Qlik License Service 通信用にプロキシを構成する」を参照してください。

1.3　QlikView Publisher

QlikView Publisher は QlikView Server の追加ライセンスを必要とするモジュールです。これらは、QlikView Server にライセンスを適用することによって、インストールされます。

Publisher 要件

コンポーネント	要件
リポジトリデータベース	• ネイティブ XML • SQL Server (Microsoft によってサポートされている任意のバージョン)

1.4　QlikView Workbench

QlikView Workbench は QlikView Server の追加ライセンスを必要とするモジュールです。これらは、QlikView Server にライセンスを適用することによって、インストールされます。QlikViewWorkbench では QlikView ServerEnterprise Edition が必要です。

QlikView Workbench は、これらの項目を使用するメモリ内のデータ項目とオブジェクト向けにのみサポートされています。

Workbench 要件

コンポーネント	要件
開発用ツール	• Microsoft Visual Studio 2015 • Microsoft Visual Studio 2017 • Microsoft Visual Studio 2019
コンテンツ管理システムの統合	• Microsoft SharePoint 2013 • Microsoft SharePoint 2016 • Microsoft SharePoint 2019

1.5　Qlik NPrinting 互換性

QlikView 2023 年 5 月 IR は、Qlik NPrinting May 2023 IR 以降の IR とのみ互換性があります。

QlikView Desktop は、QlikView とQlik NPrinting との接続に必要であり、各 Qlik NPrinting Engine コンピュータにインストールする必要があります。

サーバーまたはクラスター接続を使用している場合、QlikView Server および QlikView Desktop は同じバージョンである必要があります。

詳細については、Qlik NPrinting を QlikView に接続するを参照してください。

1.6　ブラウザ サポート

ブラウザ サポート

ブラウザ	AccessPoint QlikView ポータル	QlikView プラグイン	QlikView Ajax クライアント	QlikView 管理コンソール
Microsoft Edge (Microsoft Windows 用の最新版)	√	√ (IE モードで実行)	√	√
Microsoft Edge (iOS デバイス用と Android デバイス用の最新版)	√	X	√	X
Mozilla Firefox (最新バージョン)	√	X	√	√
Apple Safari 15, Apple Safari 16	√	X	√	X
Apple Mobile Safari (iOS 15 および iOS 16 デバイス)	√	X	√	X
Google Chrome (Microsoft Windows、Apple Mac、および Android デバイス用の最新版)	√	X	√	√

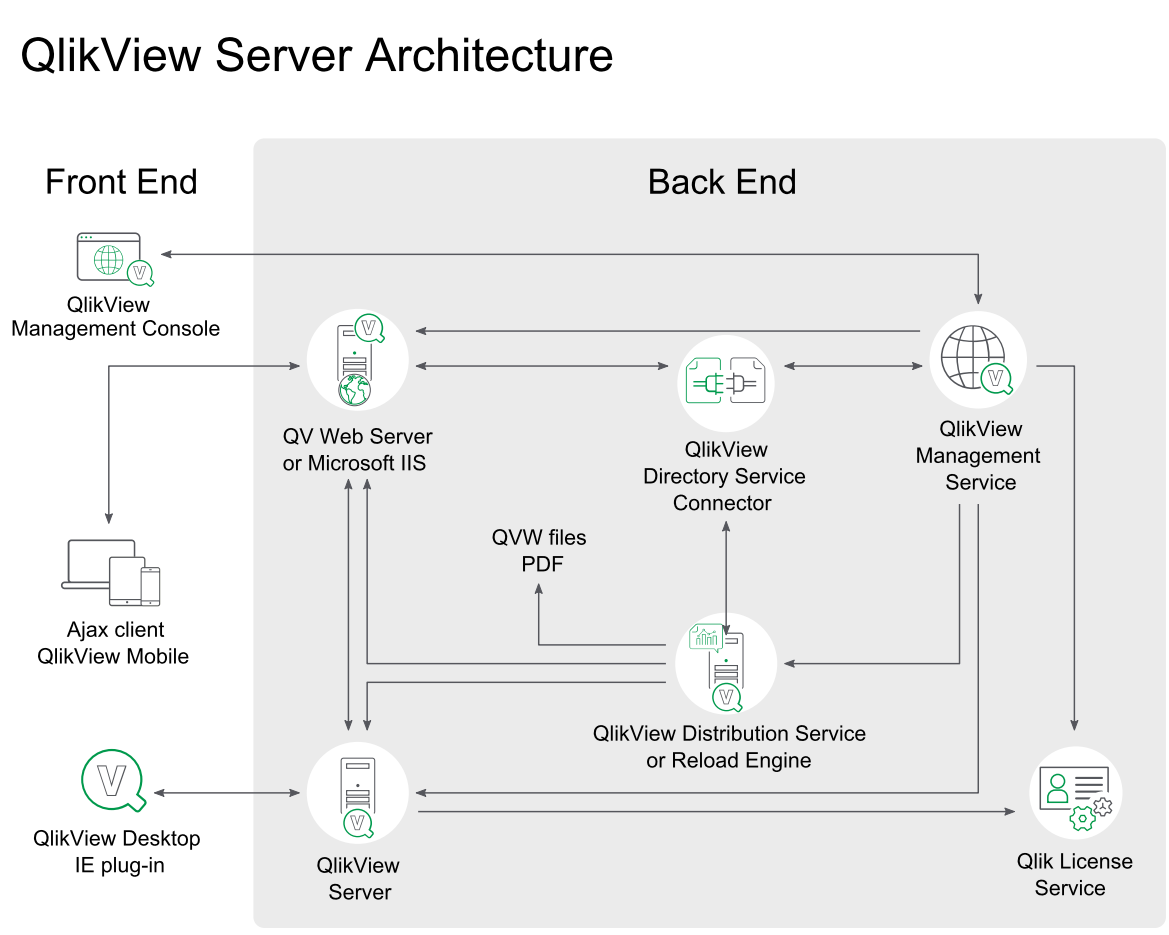
2 QlikView の展開の計画

このセクションでは QlikView のアーキテクチャ、展開、セキュリティ、ログ記録、ライセンス契約などについて説明します。

> *Microsoft IIS をウェブ サーバーとして使用する場合は、QlikView Server より前にインストールしてください。*

2.1 アーキテクチャ

QlikView インストールの全体的な構造は、いくつかの役割に分割されています。



各サービスのインスタンスが 1 つある QlikView Server アーキテクチャ

フロント エンド

フロント エンドとは、エンド ユーザーが QlikView Server を介して閲覧できるドキュメントやデータを操作する場所です。フロント エンドには、バックエンドの QlikView Publisher (Publisher ライセンスを有する QlikView Distribution Service) で作成する QlikView ユーザー ドキュメントが含まれています。クライアントとサーバー間

のすべての通信はここで行われ、QlikView Server がクライアントの認可を実行します。

フロントエンドは基盤リソース (クラスタ化用の Windows ベースのファイル共有など) に依存しています。

QlikView Server は現在、Windows ファイル共有のみ適合しています。つまり、Windows オペレーティング システムのインスタンスでストレージを所有、管理、共有する必要があります (通常は \\<servername>\<share> のようなパスを使ってアクセスします)。

QlikView では、Windows Distributed File System (DFS) をサポートしていません。

エンドユーザーの許可 (内蔵されているカスタム ユーザーは例外) は QlikView の外で行われます。

バック エンド

バック エンドとは、QlikView Developer で作成した QlikView ソース ドキュメントがある場所です。これらのリソース ファイルには、多用なデータ ソース (データ ウェアハウスや Microsoft Excel® ファイル、SAP®、Salesforce.com® など) から抽出されたデータ スクリプトが含まれています。データの抽出には、中間ファイル (QVD ファイル) が含まれる場合があります。QlikView の主要なコンポーネントは、バック エンドでファイルのロードと配信を実行する QlikView Distribution Service です。

バック エンドでは、クラスタ化用の基盤リソース (Windows ベースのファイル共有など) とともに、SMTP サーバーやディレクトリ カタログといったリソースも使用します。

QlikView Server は現在、Windows ファイル共有のみに適合しています。つまり、Windows オペレーティング システムのインスタンスでストレージを所有、管理、共有する必要があります (通常は \\<servername>\<share> のようなパスを使ってアクセスします)。

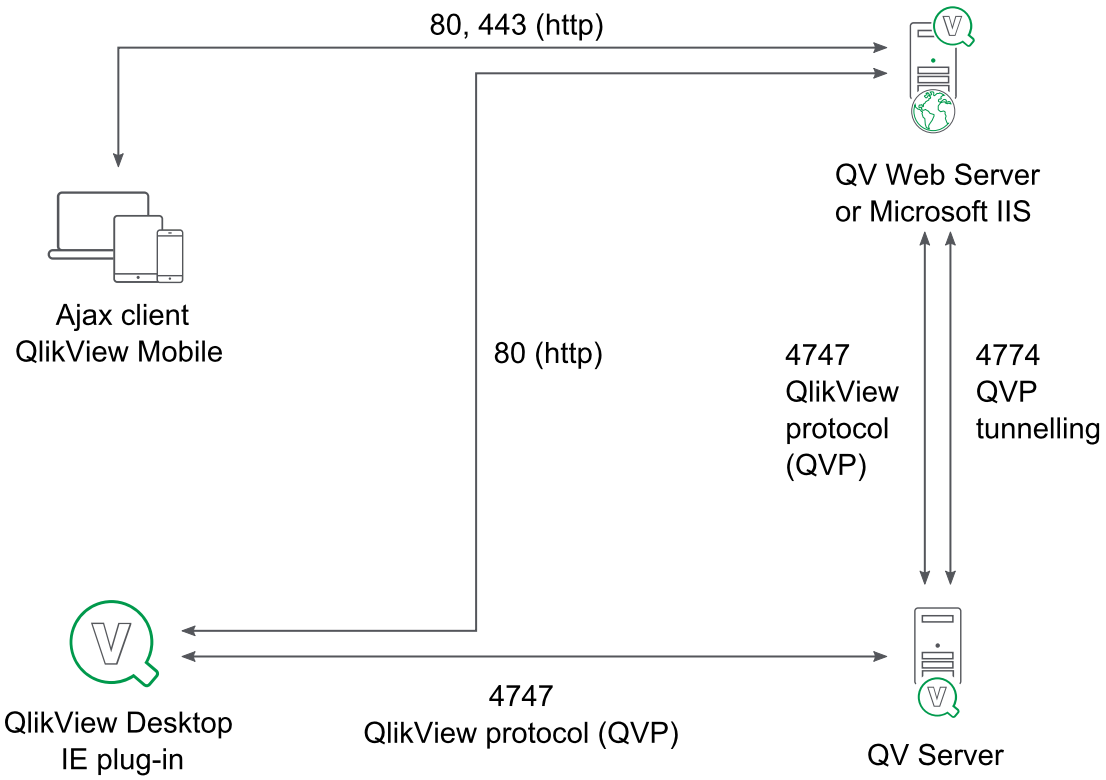
QlikView では、Windows Distributed File System (DFS) をサポートしていません。

QlikView Server

インストールされるサーバーの数は (クラスター化に関係なく)、ライセンスによってのみ制限されます。但し、ひとつのサーバー (物理/仮想) で複数の QlikView Server (QVS) プロセスを起動させることはできません。QlikView Server はどのようなリソースでも利用できるよう設計されています。応答時間を最小限に抑えるために、QlikView Server はメモリにできるだけ多くの計算結果を保存します。

QlikView Server - クライアントの通信

QlikView Server クライアントの通信構造は 3 つの主要なプロセスを必要とし、整合性があり安全性の高い方法でそれぞれと通信可能である必要があります。この相互作用は、他の従属的なプロセスと同様、潜在的に多数のコンピュータと多数のネットワーク接続を使用することができます。



QlikView Server - クライアントの通信

3 つの主要なプロセスは以下の通りです。

クライアントの通信処理

プロセス	説明
QlikView Server (QVS)	クライアントに QlikView の機能性を提供します。このサービスのホストとして機能しているマシンは、Microsoft Windows オペレーティング システム上で動作している必要があります。
クライアント	Web ブラウザやアプリケーション シェルで動作し、クライアント コード用のコンテナを提供します。クライアントは、QlikView のインターフェースと機能性をエンド ユーザーに提供するために、直接もしくはウェブ サーバーを通して QlikView Server と通信します。
Web サーバー	ウェブ サーバーは、クライアントに HTML ウェブ ページを供給するために使用できる HTTP サーバーを起動し、ユーザーの許可を支援して、クライアントと QlikView Server 間の通信を可能にします。

カスタム ユーザーは例外で、クライアント ユーザーの許可は Windows 許可を使用するといったように、QlikView 外で実施されます。

QlikView Server を使ったクライアント通信のプロトコル定義は以下の通りです。

クライアントの通信プロトコル

プロトコル	説明
QlikView Protocol (QVP)	暗号化、バイナリ、TCP ベース。ポート 4747 で QVS と直接通信します。
QVPX	XML ベース。ウェブ サーバーを経由して http/https を使用して QVS と通信します。

Windows クライアント (*.exe*/*.ocx*) はポート 4747 の QVP を使用して QlikView Server と直接通信します。これらのクライアントには、QlikView Server との通信を構築、維持するためのウェブ サーバーは必要ありません。

AJAX クライアントとモバイル クライアントは直接 QlikView Server と通信しません。QlikView Web Server (QVWS) や Microsoft IIS のようなウェブ サーバーを通して QVPX プロトコルを使用した通信を確立、管理する必要があります。これは、通常ポート 80 (http) を通して行われます。また、ウェブ サーバーでは、ポート 4747 の QVPX2 プロトコルを使用して QVS と通信します。

QVS のデフォルトのインストール設定では、Microsoft IIS ではなくQVWS を使用します。QVWS は、Windows 7 以降および Windows Server 2008 以降で、IIS とポート 80 を共有しています。

QlikView Server のユーザー ドキュメントへのアクセス

ユーザーがドキュメントを開くには、次が必要です。

- ユーザー用の Client Access License (CAL)
- ドキュメントへのアクセス権

ユーザー ドキュメントを読み込むのは QlikView Server (QVS) なので、実質的には QVS を起動するアカウントに対してのみ読み取り可能である必要があります。アクセス権限は、ドキュメントの ACL リスト (QVS が NTFS モードで起動している場合) あるいは *.META* ファイル (QVS が Document Metadata Service (DMS) モードで起動している場合) にいずれかに保存されます。これらの設定は、バック エンドからの配信の一部に含まれます。

エンド ユーザーが作成した各アイテム (レイアウト、レポート、ブックマーク、ノート、入力項目値など) は、共有ファイルに保存されます。共有ファイルはバック エンドからの配信で置き換えられません。

QlikView ウェブ サーバー

QlikView Web Server (QVWS) は QlikView Server のインストールに含まれます。QlikView ウェブ サーバーはスタンドアロン サービスとして動作し、QlikView Server インストールにかかるニーズを満たします。

QlikView Server の代替オプションとして、より高い柔軟性とさらなる許可スキーム、アプリケーション用のウェブ サービスを提供する Microsoft IIS ソリューションを展開することが可能です。Microsoft IIS を使用すると、設定を管理する特別なサービスである QlikView Settings Service がインストールされます。

QVS 環境で他のウェブ サービスを使用することができますが、QVS に到達するトラフィックのいずれかの地点で、QVWS あるいは IIS の専用 ASPX ページを経由する必要があります。

QlikView Web Server のコンポーネント (QVWS と IIS ベースの両方) は次のような複数のタスクを実行します。

- AccessPoint バック エンドの処理
- ステートレス http と QVS とのセッション ベースの通信間のトラフィックの変換やルート設定

- QVS クラスターのロードバランス処理
- 静的コンテンツの提供 (オプション)
- Windows認証ユーザーの認証処理
- カスタム ユーザーを使用した認証処理 (オプション)
- Windows や Directory Service Connector (DSC) を使用したグループへの配信 (オプション)

QlikView Server トンネル

QVS 通信ポート (4747) がネットワークのファイアウォールによってブロックされた場合、Windows クライアントは、ポート 80 (http) を経由する通信を試行します。QVS トンネル通信を確立するには、接続パスに QVWS を含むか、Microsoft IIS にインストールする必要があります。

QlikView Directory Service Connector

Directory Service Connector (DSC) は、アクティブ ディレクトリや LDAP、ODBC、カスタム ユーザーといったさまざまなソース (これらに限定されるものではありません) からエンドユーザーに関連するユーザー情報を取得します。

ウェブ サーバーは DSC を使用してグループ配信を行い、QlikView Distribution Service は DSC を使って配信中にメール アドレスや UID の検索を行います。また Management Service では、管理者がユーザーやグループの検索に使用します。

QlikView Management Service

QlikView Management Service は QlikView Management Console および QlikView API の双方における、すべての管理のエントリポイントです。

QlikView Management Service (QMS) は、自身のデータベースである QVPR の設定を保持します。デフォルトでは、QVPR は XML ファイル形式で保存され、SQL データベースとして設定を保存する方法もあります。

> *すべての QlikView サーバーは、同じ地域設定である必要があります。地域設定が異なると、QlikView XML 参照ファイルのロード時にエラーが発生する場合があります。*

インストールはアクティブな QMS の単一インスタンスでのみを可能です。冗長に対しては、アクティブ/パッシブなフェイルオーバーを使用する必要があります。QMS が起動するために、他のサービスは不要です。

QlikView [Distribution Service] (配布サービス)

QlikView Distribution Service を使用する QlikView インストールでは、バック エンドおよびフロント エンドは両方とも、開発およびテスト、展開に活用されます。

QlikView Distribution Service は次のようなソース ドキュメントを使用します。

- ユーザー ドキュメント
- フォルダへの配信やメールを経由する配信用の *.qvw* ファイル
- フォルダへの配信やメールを経由する配信用の *.pdf* ドキュメント

最終配信先に到達するまでの一連のイベントには、次のようなタスクが 1 つ、あるいは複数含まれます。

- 1 つあるいは複数のデータ ソース (QVD を含む) から1 つあるいは複数の *.qvw* や *.qvd* ファイルにデータをロードする。
- ドキュメントを1 つあるいは複数のサイズの小さなドキュメントに縮小/分割する。
- 属性および使用規則を追加する (QVS に配信する場合にのみ適用)。

QlikView Distribution Service は、定義済みのスケジュールに従い、あるいはイベントに対する処理としてタスクを実行します。

QlikView Distribution Service なしの QlikView 構造

QlikView Distribution Service がないと、QlikView の機能構造は制限的になります。配信および分割機能は、データをユーザー ドキュメントにリロードすることで削除や置換を行います。QlikView Distribution Service がないので、開発者はバックエンド サーバーから手動で *.qvw* ファイルを展開する必要があります。

Reload Engine

Publisher ライセンスが QlikView Distribution Service に接続されていない場合、Reload Engine が Publisher の配信サービスを代行します。Reload Engine がリロードするのはユーザー ドキュメントのみで、設定はユーザー ドキュメントで直接定義されます。

> *Reload Engine を機能させるには、すべての QlikView サービスを同一のマシン上で実行する必要があります。サービスを複数のマシンにインストールする場合は (例えば、あるマシンには QMC、DSC、QDS をインストールし、別のマシンには QVS と QVWS をインストール)、Reload Engine が機能しません。*

Qlik License Service

Qlik License Service は QlikView April 2019 以降のリリースに組み込まれており、QlikView Server が署名付きキー ライセンスを使用して有効化されている場合に使用されます。Qlik License Service にはライセンスに関する情報が保管され、製品の有効化と権利の管理の際に Qlik によってホストされている License Back-end Service と通信します。License Back-end Service へのアクセスとライセンス情報の取得にはポート 443 が使用されます。

マルチノード展開の場合は、Qlik License Service は QlikView Management Service (QMS) が実行されているマシンにインストールされます。Qlik License Service のステータスは、Windows マシンで実行中のサービスのリストにある Qlik Service Dispatcher を起動して停止することによって管理できます。

ドキュメント、データ、タスク

ユーザー ドキュメント

ユーザー ドキュメントとは、QlikView Server (QVS) にあり、エンド ユーザーがアクセスして閲覧する文書です。ユーザー ドキュメントを完全に識別するには、QVS サーバー/クラスターおよびサーバーへの相対パスが必要です。実質的に、ユーザー ドキュメントは次の 3 つのファイルで構成されています。

- QlikView ドキュメント ファイル (*.qvf* または *.qvw*)。データとレイアウトが含まれます。
- *.META* ファイル。内容は次の通りです。

    - AccessPoint 属性
    - 事前ロードオプション
    - 許可 (Document Metadata Service (DMS) モードのみ)
- 共有ファイル (*.Shared* または *.TShared*、以下を参照)

> *ユーザードキュメントが QlikView Distribution Service によって配信される場合、QlikView ドキュメントファイルおよび .META ファイルのデータは上書きされます。*

ユーザードキュメントへのアクセスは、QlikView Server が管理します。

共有ファイル

ユーザーは次のようないくつかのオブジェクトで QlikView Server を通して共有やコラボレーションを行うことができます。

- ブックマーク
- チャートを含むシートオブジェクト
- レポート
- ノート

これらのオブジェクトは、アクセスの方法や場所に関わらず、認証ユーザーが利用できるユーザーオブジェクトとして定義する、または、QlikView Server を通してドキュメントのすべてのユーザーが利用できる共有オブジェクトとして定義することができます。

オブジェクトは QlikView マネージメントコンソール (QMC) を使って設定および管理されます。

QVS でサーバーオブジェクトが有効になり、QVS オブジェクト設定のいずれかのチェックボックスがオンに設定され、ドキュメントが QVS 上で開かれると、専用のデータベースファイルが作成され、QlikView ドキュメントと同じ場所に保存されます。ファイルは QlikView ドキュメントと同じ名前になりますが、共有ファイルの拡張子 (*.Shared* または *.TShared*) が付けられます。

- QlikView ドキュメント:*Presidents.qvw*
- QVS 共有ファイル:*Presidents.qvw.TShared*

QlikView ドキュメントの名前が変更されている場合には、QVS でそのドキュメントを開く前に、ドキュメント名を一致させるために必ず手動で共有ファイルの名前を更新しておく必要があります。これによって、ドキュメントに付随する共有オブジェクトを維持できます。

サーバーオブジェクトやレポート、ブックマーク、入力項目データの更新中は、ファイルは排他的にロックされています。選択を行ったり、単にオブジェクトをアクティブにしている場合は、ファイルがロックされることはなく、多数のサーバーから同時にファイルを読み取ることができます。部分的にロックすることも可能なので、ファイルの異なるセクションをクラスター内の別のサーバーから同時に更新することもできます。

サーバーからドキュメントを開いた際に一度読み込まれたファイルは、変更が生じるまで再度読み込まれることはありません。セッションはどれも、その共有ファイルの同一の内部コピーを共有します (つまり、セッションを開く場合にディスクからファイルを読み込む必要がありません)。

サーバー オブジェクトは QMC で **[ドキュメント (Documents)] > [ユーザー ドキュメント (User Documents)] > [サーバー (Server)] > [サーバー オブジェクト (Server Objects)]** タブの順で選択して、管理できます (例: 所有権の変更や削除)。

ソース データ

ソース データは QlikView ドキュメント ファイルにデータを投入するために使用される外部データです。ソース データはリロード中に QlikView ドキュメント ファイルに次のいずれかの方法でロードされます。

1. QlikView Distribution Service を介してロード
2. Reload Engine を介してロード
3. 開発者が手動でロード

QlikView ドキュメント ファイルがロードされたら、エンド ユーザーはソース データにアクセスするのではなく、QVS から QlikView ドキュメントを使用できます。

[Source Documents] (ソース ドキュメント)

ソース ドキュメントは、Publisher ライセンスがある場合に限り利用できます。ソース ドキュメントの大半は開発者から提供されるもので、QlikView Distribution Service が配信プロセスの一部として作成したドキュメントもあります。QlikView Data (QVD) ファイルもまた、配信の中間処理の一部として作成されます。QVD ファイルは、QlikView による読み取り時間が最適化されるようデータ テーブル形式で保存されます。

ソース ドキュメントへのアクセスは、NTFS が管理します。

タスク

タスクは多用な操作を実行するために使用され、任意のパターンで連結されています。タスクを説明するには、まずソース ドキュメントをユーザードキュメントに変換するところから始めます。

ソース ドキュメントをユーザードキュメントに変換する

ひとつのソース ドキュメントを変換して複数のユーザー ドキュメントを作成することができます。

ソース
タスクは常にソース ドキュメントと連結しているため、ソースが提供されます。

レイアウト
ソース ドキュメントにはレイアウトが含まれており、ユーザー ドキュメントにそのままコピーされます。サーバー側のレイアウトはユーザー ドキュメントと関連付けられており、これもまた変更できません。

リロード
次のデータ操作が可能です。

- ドキュメントに保存された状態での使用 (リロードなし)
- ソースから部分的にリロード (スクリプト準備が必要)
- ソースから完全にリロード、古いデータは削除
- 「Script Parameters」の使用に関連するリロード (スクリプト準備が必要)

サイズ縮小や分割

リロードされたドキュメントはサイズ縮小や分割ができます。つまり、サイズの小さな 1 つのドキュメントに縮小する (単純な縮小)、もしくは複数の小さなドキュメントに分割する (ループと分割) の両方が可能です。

サイズ縮小や分割は、QMC で直接あるいはブックマークを使って選択を行い、実行します。

配信

配信には QlikView Publisher ライセンスが必要です。

配信先は次のように定義します。

- QlikView Server のユーザー リストとフォルダ
- ファイル システムのユーザー リストとフォルダ
- ユーザー リスト (メール アドレスなどが一般的)

> *異なるユーザーに異なるコンテンツを配信する場合は、「ループと分割」を使用してください。そうでないと、同一のドキュメントが全員に配信されてしまいます。*

情報 (Information)

情報は、サーバーへの配信の一部としてドキュメントに関連付けることができます。ドキュメントを別のロケーションに配信したとしても、情報は配信されません。情報は QlikView AccessPoint が使用します。

ドキュメントに関連付けられる情報は次の通りです。

- 説明
- カテゴリ
- 任意の名前と値

サーバーの設定

ドキュメントに対する設定はサーバーに配信されます。ドキュメントを別のロケーションに配信したとしても、設定は配信されません。設定は QlikView Server で行います。

サーバーによる許可は次の通りです (すべてのサーバー)

- サーバー オブジェクトを作成するユーザーの許可
- ドキュメントをダウンロードするユーザーの許可
- ドキュメントの印刷および Microsoft Excel へのエクスポートを行うユーザーの許可

QlikView AccessPoint による設定は次の通りです (すべてのサーバー)

- QlikView プラグイン推奨
- モバイル クライアント推奨
- AJAX クライアント推奨

サーバーによる操作は次の通りです (すべてのサーバー)

- 監査ログ
- オープン セッションの最大化

- ドキュメントのタイムアウト
- セッションのタイムアウト

利用設定 (サーバーごと)

- なし
- オンデマンド
- 事前ロード

ポート

QlikView は、Web ブラウザー (ユーザー) とサーバー間、およびシングル/マルチ ノードの展開での異なるサービス間の通信にポートを使用します。

下の表に、QlikView 展開で使用されるポートの概要を示します。

QlikViewポート

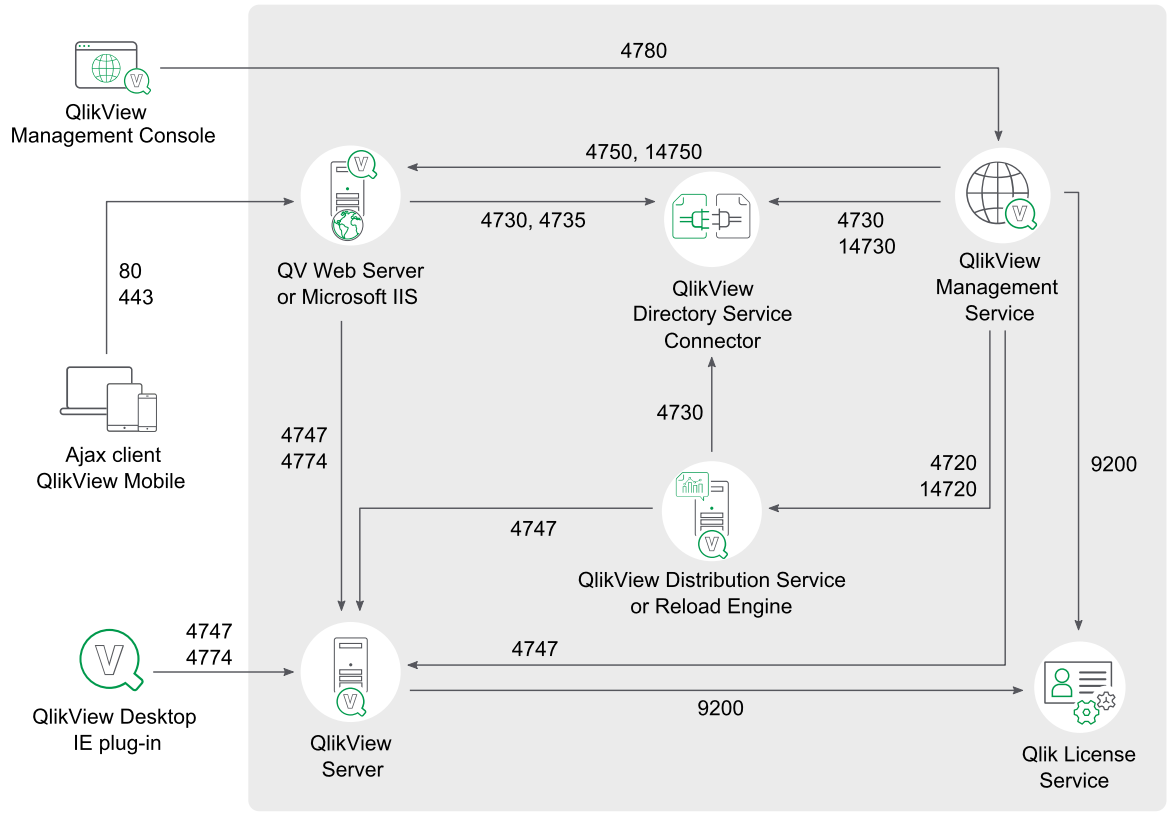
-	コンポーネント	着信	発信
	QlikView Server (QVS)	4747 (QVP:QlikView プロトコル) 4774 (QVP トンネリング) 14747 (クラスターは SOAP API を使用) 4749 (SSL)	14747 (クラスター ブロードキャスト)
	QlikView Web Server (QVWS)	80 (HTTP) 443 (HTTPS) 4750 (SOAP API) 14750 (証明書)	4730 (DSC SOAP API) 4735 (DSC カスタム ユーザー SOAP API) 4747 (QVS QVP) 4774 (QVS QVP トンネリング)
	QlikView Distribution Service (QDS)	4720 (SOAP API) 14720 (証明書)	4730 (DSC SOAP API) 4747 (QVS QVP)
	QlikView Directory Service Connector (DSC)	4730 (SOAP API) 14730 (証明書) 4735 (カスタム ユーザー SOAP API)	-

-	コンポーネント	着信	発信
	QlikView Management Service (QMS)	4780 (HTTP) 4799 (SOAP API)	4747 (QVS QVP) 4750 (QVWS SOAP API) 14750 (QVWS 証明書) 4720 (QDS SOAP API) 14720 (QDS 証明書) 4730 (DSC SOAP API) 14730 (DSC 証明書) 4735 (DSC カスタム ユーザー) 4799 (Remote QMS SOAP API)
	Qlik License Service	9200	443 (HTTPS)

下の表に、異なる QlikView サービスへの接続に使用されるポートの例を示します。QlikView の展開では、これらのサービスをみな同じサーバーにインストールできます (単一ノードの展開)。また代わりに、異なるサービスを異なるサーバーにインストールするマルチノードの展開にすることもできます。QlikView のアーキテクチャ(構成) と展開の詳細については、「*アーキテクチャ(page 10)*」および「*配置 (page 49)*」ページを参照してください。

次の図は、QlikView Server 展開 (QV:QlikView).

QlikView Server Ports Communication



では、

この章では、QlikView Server/Publisher の各コンポーネントについて詳しく説明します。

> *QlikView サービスの実行に使用するアカウントには、ローカル管理者権限が必要です。*

QlikView サービスの設定方法については、「設定」を参照してください。

QlikView Server のロードシェアリング (クラスタリング)

概要

クラスタリングの概要

実行可能ファイル	*%ProgramFiles%\QlikView\Server\QVS.exe*
データ	*%ProgramData%\QlikTech\QlikViewServer*
リッスン ポート	QVP: 4747; QVP (トネリング): 4774; ブロードキャスト: 14747; SNMP: 161
使用/コントロール	-
利用者	QDS、QMS、QVWS、QlikView Desktop/QlikView プラグイン/OCX

ファイル

設定と構成

構成ファイル

ファイル	説明
Settings.ini	QlikView Server (QVS) 設定を保存します。このファイルを手動で変更するには QVS の再起動が必要です。このファイルは常に「データ(Data)」フォルダに保存されます。

クラスター

QVS はクラスターの調整に *.pgo* ファイルを使用します。ファイルは「データ(Data)」フォルダーに格納されています。

クラスター ファイル

ファイル	説明
BorrowedCalData.pgo	借用された Client Access Licenses (CAL) を追跡します。
CalData.pgo	CAL を追跡します。
IniData.pgo	*Settings.ini* の調整済みバージョン。
ServerCounters.pgo	統計を追跡します。
TicketData.pgo	チケットを追跡します。

ログ

ログはクラスター内のノードごとに保存されます。ログ ファイルは既定で Data フォルダに格納されます。

ログ ファイル

ファイル	説明
Events_<computer_name>.log	イベントのログ。
Performance_<computer_name>.log	パフォーマンスのログ。
Sessions_<computer_name>.log	セッションのログ。

特別なフォルダ

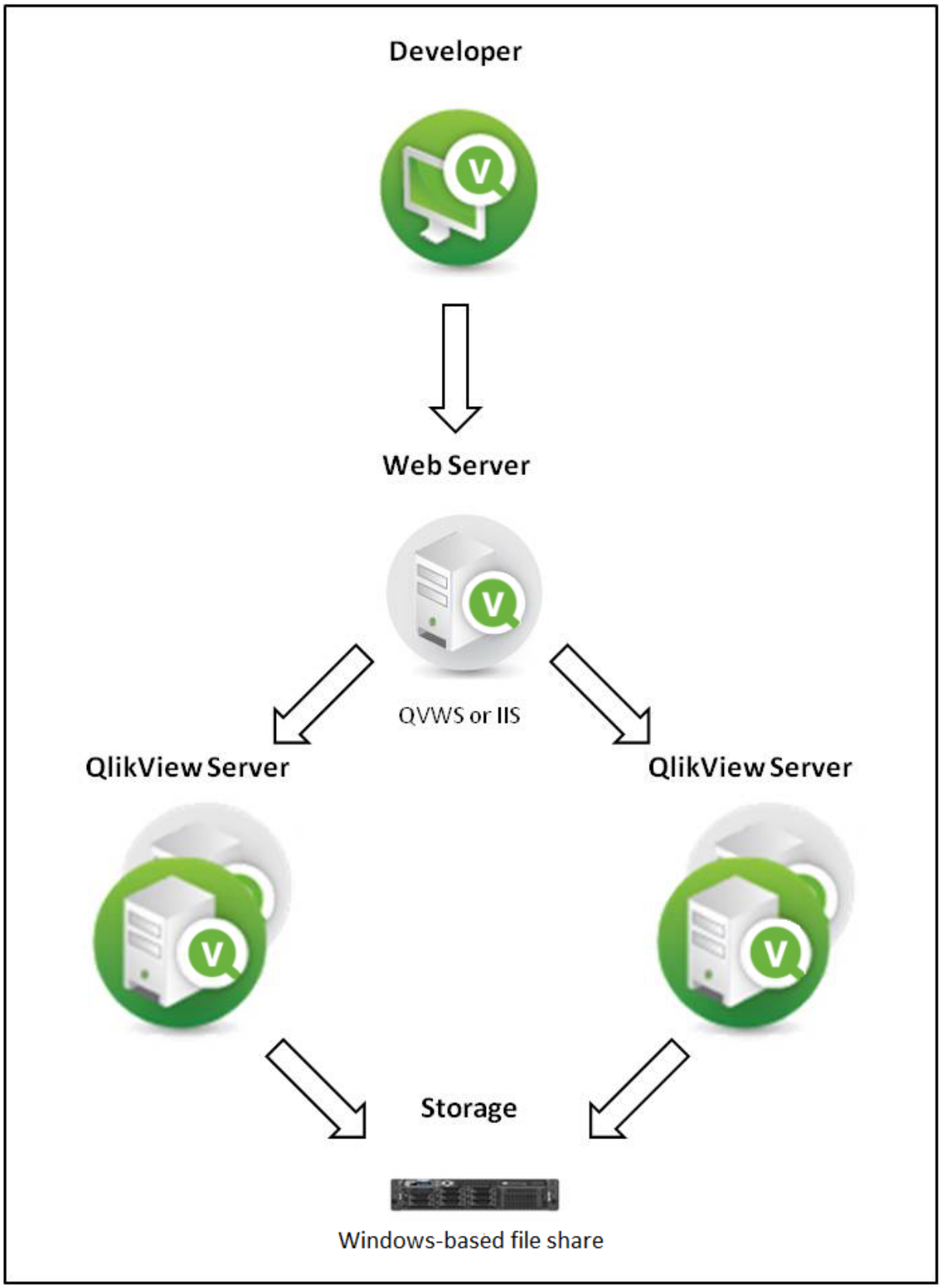
特別なフォルダは Deta フォルダに格納されます。

特別なフォルダ

フォルダ	説明
Extensions	*Extensions フォルダーは手動で作成する必要があります。* デフォルトでは、QVS はこのフォルダー内の拡張機能を検索するよう設定されています。Extension オブジェクトは *Extensions|Objects* に、ドキュメント拡張機能は *Extensions|Document* に格納されています。クラスターですべての拡張機能を単一の場所で管理するには、QlikView Management Console (QMC) を使用します。
Temp	デフォルトでは、QVS はこのフォルダーに一時ファイルを作成するよう設定されています (たとえば AJAX クライアントを用いてエクスポートする場合、このフォルダーに一時ファイルが作成されます)。

ロードシェアリング (クラスタリング)

すべてのクラスタリングには、クラスタが有効化された QlikView Server ライセンスが必要です。QlikView Server は、複数のマシンをまたいだドキュメントのロードシェアリングをサポートします。この共有には、サーバー オブジェクト情報、ドキュメントの自動ロード、またユーザー ライセンス CAL をリアル タイムで共有する機能が含まれます。同じライセンス ナンバーを共有する複数のサーバー インスタンスを有効にするには、特別なライセンスを利用します。



QlikView Web Server を使用したロードシェアリング

複数の QVS 間でロードシェアリングを使用するには、すべてのドキュメントとサポートファイルがサーバー間で共有されている必要があります。つまり、すべてのサーバーはファイルのために同じ物理的な場所を示す必要があります。QVS はロードシェアリング データを格納するための追加ファイルを作成し、保持します。これらのファイルは Persistent Group Object (*.pgo*) ファイル タイプの拡張子で「データ (Data)」フォルダに格納されています。これらのファイルは QVS 実行時はロックされます。それぞれの *.pgo* ファイルには借用中の CAL、使用中の CAL、サーバー設定、チケットデータに関する情報が含まれます。

オペレーティング システムのロードバランスまたはフェールオーバー設定は、QVS ロードシェアリング設定に含まれないため、QVS はこれらのシステムを制御できません。

サーバーの構成設定は、すべてのクラスター化された QVS で共有され、クラスター化された QVS に接続する QMC で管理できます。特定の QVS システムのパフォーマンスをそのシステムに接続された QMC でモニターすることが可能です。負荷分散設定、つまりクライアントがどの QVS に送られるかどうかの設定は、QlikView Web Server (QVWS) に保存されます。

ドキュメント関連のメタデータは、*.meta* ファイルを通じて共有されます (ドキュメントごとにファイル 1 点)。このデータは通常、Document Metadata Service (DMS) データとして参照されます。DMS データが QVS 内で共有されるため、自動化されたドキュメントのロードはすべてのサーバーで行われます。DMS 許可もクラスター化されたすべての QVS で共有されます。

QlikView Distribution Service

概要

QlikView Distribution Service の概要

実行可能ファイル	*%ProgramFiles%\QlikView\Distribution Service\QVDistributionService.exe*
データ	*%ProgramData%\QlikTech\DistributionService*
リッスン ポート	HTTP: 4720、SNMP: 4721
使用/コントロール	DSC、QVS、QVB
利用者	QMS

マシンを再起動すると、Windows のイベント ログには QlikView Distribution Service (QDS) が正常に起動していても、すぐに起動できなかったというメッセージが記載されます。これは、Windows のタイムアウト期間 (デフォルトは 30 秒) より QDS の初期化に時間がかかることが原因です。このイベント ログ メッセージを回避するには、Windows のタイムアウト期間を変更するか、QDS の設定を別の開始が遅いサービスに応じて、ビジー期間外で QDS が起動するよう変更します。

ファイル

QlikView Distribution Service (QDS) ファイルは、主な目的ごとに 3 つのグループに分けられます。*DistributionGroupDefinition.xml* を除くすべてのファイルは QDS の「Data」フォルダーに保存されます。

クラスター化された設定では、すべての QDS が同じプログラム フォルダを共有する必要があります。これを解決するには、プログラム データ パスを含む *config_<サーバー名>.xml* ファイルを使用します。

QDS Data フォルダには、以下にリストされていないファイルが表示される可能性があります。以下にリストされていないファイルは、システムでのみ使用されます。変更したり、削除したりしないでください。

設定と構成

下記のファイル リストは、QVPR に保存されている情報のローカル コピーです。

ファイルの設定と構成

ファイル	**説明**
service_key.txt	QMS API の呼び出しに使用されるサービス キー。
Config_servername.xml	このファイルには、*QVDistributionService.exe.config* ファイルの既定構成に加えられたすべての変更がリストされます。 このファイルは、QDS クラスター環境内の各 ノードに存在します。
Configuration.xml	サービスの構成ファイル。
Tasks\Task_<GUID>.xml	実際のタスク。 削除されたタスクは (サポート上の問題解析のため) 自動的には削除されませんので注意が必要です。
Triggers\Triggers_<GUID>.xml	実際のトリガー。 削除されたトリガーは (サポート上の問題解析のため) 自動的には削除されませんので注意が必要です。
MasterConfigurationNotification.xml	構成通知ファイルのリスト。 QDS の同期を維持し、QDS ノードに構成の変更を通知するために使用します。
MasterTaskNotification.xml	タスク通知ファイルのリスト。 QDS の同期を維持し、QDS ノードにタスクの変更を通知するために使用します。
MasterTaskExecutionNotification.xml	タスク実行通知ファイルのリスト。 QDS の同期を維持し、QDS ノードにタスクの実行変更を通知するために使用します。
MasterTriggerNotification.xml	トリガー通知ファイルのリスト。 QDS の同期を維持し、QDS ノードにトリガー イベントの変更を通知するために使用します。
TaskDetails.xml	*Tasks* フォルダで利用可能なタスクのリスト。 ファイルを QVPR の同フォルダと同期させるために使用します。

TriggerDetails.xml	*Triggers* フォルダで利用可能なトリガーのリスト。 ファイルを QVPR の同フォルダと同期させるために使用します。
DistributionGroupDefinition.xml	配布グループの構成ファイル。 場所: *%ProgramData%\QlikTech\ManagementService\DistributionGroups*

クラスター

クラスター ファイル

ファイル	説明
LoadBalancer.xml	(クラスター内の) どのノードにタスクを実行させるかを決定するために QDS が使用します。
NodeInformation.xml	ロード バランサーで使用されない他のすべての QDS ノードのデータが記録されます。

ログ

ログ ファイル

ファイル	説明
TaskResults\TaskResult_<GUID>.xml	GUID により識別されたタスクの最新の結果。
TaskLogIndex\TaskLogIndex_<GUID>.xml	これは検証用 (タスクごとに 1 ファイル) で、実際のログです。
EdxResults\EdxResult_<GUID>.xml	タスクが完了するまで、このファイルには EDX タスクの現在のステータスが記録されます。タスクの実行が完了すると、結果 (成功/失敗) および (あれば) 結果として開始されたタスクが記録されます。
<node-nr>\Log\<Date>.txt	一般的な QDS イベントおよびエラー ログ。
<node-nr>\Log\Cluster_<Date>.txt	同期化ログ。
<node-nr>\Log\LoadBalancer_<Date>.txt	ロード バランスのログ。
<node-nr>\Log\Root_<Date>.txt	QDS イベント ログ。
<node-nr>\Log\WebService_<Date>.txt	QDS イベント ログ。
<node-nr>\Log\Workorder_<Date>.txt	QDS イベント ログ。

<node-nr>\Log\<date>\<time> - <task name>\Tasklog.txt	QDS タスク ログ。
<node-nr>\Log\<date>\<time> - <task name>\DistributionReport.xml	タスクに関連する配信 (配信タスクがある場合にのみ)。

ログ ファイル保存期間の変更

デフォルトでは、ログ ファイルは 30 日間保存された後に Application Data Folder (既定のパスは *C:\ProgramData\QlikTech\DistributionService*) から削除されるよう設定されています。

ログ ファイルの保存期間は *QVDistributionService.exe.config* ファイル内で変更できます。

> *QVDistributionService.exe.config を編集する前に QVDistributionService.exe.config のバックアップを作成しておくことをお勧めします。*

次の手順を実行します。

1. Windows Services を開きます。
2. QlikView Distribution Service を右クリックして **停止** をクリックし、このサービスを停止します。
3. Windows Services を閉じます。
4. *C:\Program Files\QlikView\DistributionService* に移動し、テキスト編集プログラムで QVDistributionService.exe.config ファイルを開きます。
5. `<add key="NbrOfDaysToKeepQDSLogs" value="30" />` を検出し、レポートの保存期間となる日数値を編集します。
6. 設定を保存し、ファイルを閉じます。
7. Windows Services を開きます。
8. QlikView Distribution Service を右クリックして [開始] をクリックし、このサービスを起動します。
9. Windows Services を閉じます。

QlikView Batch

概要

QlikView Batch の概要

実行可能ファイル	*%ProgramFiles%\QlikView\Distribution Service\qvb.exe*
データ	-
リッスン ポート	COM
使用/コントロール	-
利用者	QDS

QlikView Batch (QVB) はグラフィカル オブジェクトやユーザー入力オブジェクトに対応していません。このため、QVB はユーザー入力の必要なスクリプトなどを含むドキュメントをリロードできません。

ファイル

設定と構成

ファイルの設定と構成

ファイル	説明
Settings.ini	保存設定に使用。

ログ

ログ ファイル

ファイル	説明
<document_name>.log	リロード ログは リロードされたドキュメントとともに保存されます。

QlikView Publisher のリポジトリ

概要

Publisher のリポジトリの概要

実行可能ファイル	-
データ	*%ProgramData%\QlikTech\ManagementService\QVPR*
リッスン ポート	-
使用/コントロール	-
利用者	QMS

ファイル

デフォルトでは、QlikView Publisher Repository (QVPR) は XML ファイルのセットです。このファイルは、*.zip* ファイルとして *%ProgramData%\QlikTech\ManagementService\QVPR\Backups* にバックアップされます。

「セキュリティグループ」

QlikView Server/Publisher をインストールすると、2 つのセキュリティグループが作成されます。

QlikView Server/Publisher のサービスは、QlikView Administrators セキュリティグループに属するアカウントで実行する必要があります。QMC に接続するユーザーはこのグループに属している必要があります。リモートサービスに接続するユーザーも QlikView Administrators に属している必要があります。

API を介して接続するユーザーは、QlikView Management API セキュリティグループに属している必要があります。グループはインストールにより作成されないため、手動で追加およびデータの投入 (QlikView Administrators グループのメンバーなど) を実行する必要があります。別の QlikView Server/Publisher からタスクをインポートするには、このグループのメンバーシップが必要です。

QlikView EDX セキュリティグループはインストールにより作成されないため、ユーザーが EDX タスクを実行するには手動で追加 (およびデータを投入) する必要があります。

ドキュメント管理者

QlikView Administrators グループに属さないユーザーにタスク作成の責任を委譲する場合、ユーザーをドキュメント管理者に指定できます。ドキュメント管理者に指定されたユーザーは、ユーザー ドキュメントまたはソース ドキュメントのいずれかに関連する QMC のタブにのみアクセスできます。

ドキュメント管理者機能を使用するには QlikView Publisher ライセンスが必要です。

ドキュメント管理者の指定に関する詳細は、QMC オンライン ヘルプを参照してください。

設定ファイル

このセクションで説明されているパラメータを設定するには QMC を使用します。設定ファイルを直接変更すると、問題の原因になる可能性があるためです。

QlikView Management Service – QVManagementService.exe.config

このファイルは、デフォルトでは *%ProgramFiles%\QlikView\Management Service* にインストールされます。このファイルには自動生成された修正不可のタグが多数含まれますが、次の設定は修正可能です。

QlikView Management Service 設定

構成	説明
ApplicationDataFolder	ログ フォルダやその他のすべてのファイル/フォルダが作成されるフォルダ。既定値は *%ProgramData%\QlikTech\ManagementService* です。このフォルダには、XML 版の QVPR と LEF 情報が保存されます。
UseHTTPS	True に設定すると、https を介して通信が行われます。この設定を有効化するには、ウェブ サイトの証明書が必要です。
Trace	デバッグのログ取得に使用されます。
QMSBackendListenPort	バックエンドで Management Service が通信を行うポート。既定値は 4799 です。
QMSFrontendWebServicePort	フロント エンドで Management Service が通信を行うポート。既定値は 4780 です。
MaxLogRecords	そのタスクで取得されるべきログの最大レコード数。
EnableAuditLogging	True に設定すると、a) システム内で行われるタスクおよび設定の変更、b) 変更の実行者、c) 変更の実行日を記録します。
AuditLogFolder	監査ログを保存するフォルダへのパス。
AuditLogKeepMaxDays	それぞれのログが保存される最大日数。

構成	説明
ServiceFailureAlertEmailAddresses	セミコロンで区切られたメール アドレスのリスト。サービス障害が発生した場合、リストされた受信者にメールを送信します。ServiceFailureAlertEmailAddresses タグにメール アドレスを追加すると、機能が有効になります。変更を適用するには、Management Service を再起動する必要があります。この機能には、QMC 内で構成されたメール サーバーが必要です。詳細は、「メール サーバー設定」を参照してください。 メールの件名と本文は、ServiceFailureAlertEmailSubject と ServiceFailureAlertEmailBody を使用してカスタマイズできます。
ServiceFailureAlertEmailBody	サービス障害の場合に送信されるメールの本文 (プレーン テキスト)。
ServiceFailureAlertEmailSubject	サービス障害の場合に送信されるメールの件名。

QlikView Distribution Service – QVDistributionService.exe.config

このファイルは、デフォルトでは *%ProgramFiles%\QlikView\Distribution Service* にインストールされます。appSettings は修正可能なタグです。設定ファイルの設定内容を以下に記載します。

QlikView Distribution Service 設定

構成	説明
ApplicationDataFolder	ログ フォルダやその他のすべてのファイル/フォルダが作成されるフォルダ。既定値は *%ProgramData%\QlikTech\DistributionService* です。このフォルダには、XML 版の QVPR と LEF 情報が保存されます。
WebservicePort	QlikView Distribution Service が通信に使用するポート。既定値は 4720 です。
UseHTTPS	`True` に設定すると、https を介して通信が行われます。
DSCAddress	Directory Service Connector サービスが通信に使用するポート。既定値は 4730 です。値を変更する場合は、*QVDirectoryServiceConnector.exe.config* ファイル内の「DSCAddress」タグも同様に変更する必要があります。
DSCTimeoutSeconds	Directory Service Connector の呼び出しのタイムアウト。
DSCCacheSeconds	Directory Service Connector からの応答をサービスがキャッシュする時間。
QlikViewEngineQuarantineTimeInms	許可される QlikView Engine の起動頻度 (ミリ秒単位)。
OpenDocumentAttempts	配信時にドキュメントを開く試行回数。これを過ぎるとエラーとして記録されます。

構成	説明
DebugLog	True に設定すると、「Error」ログでメモリ使用量やスタックトレースのログが有効になります。
Trace	True に設定するとデバッグのログが有効になります。
EnableBatchMode	この設定を有効にすると、バッチが QlikView Distribution Service を呼び出すよう設定できます。
ServiceStopGracetimeInSeconds	QMC から QDS に停止要求が出されたときに、QlikView Distribution Service (QDS) で実行中のタスクを完了させるための猶予時間 (秒)。 既定値は 1800 です。

Directory Service Connector – QVDirectoryServiceConnector.exe.config

このファイルは、デフォルトでは *%ProgramFiles%\QlikView\Directory Service Connector\QVDirectoryServiceConnector.exe.config* に格納されています。最も一般的に変更される設定は以下の通りです。

Directory Service Connector 設定

構成	説明
ApplicationDataFolder	ログ フォルダやその他のすべてのファイル/フォルダが作成されるフォルダ。既定値は *%ProgramData%\QlikTech\DirectoryServiceConnector* です。
WebservicePort	Directory Service Connector サービスが通信に使用するポート。既定値は 4730 です。値を変更する場合は、*QVDistributionService.exe.config* ファイル内の「DSCAddress」タグも同様に変更する必要があります。
UseHTTPS	True に設定するとhttp ではなくSSL/TSL を介して通信が行われます。この設定を有効化するには、ウェブ サイトの証明書が必要です。
PluginPath	Directory Service Connector が利用可能な DSP プラグインを探すためのパス。既定値は *%ProgramFiles%\QlikView\Directory Service Connector\DSPlugins* です。
Trace	True に設定するとデバッグのログが有効になります。
DisableCompress	この設定を有効にすると、http 通信の圧縮が無効化されます。

QlikView Web Server

ウェブ サーバーは、QlikView Web Server (QVWS) または Microsoft IIS に組み込むことができます。QVWS は、QlikView Server の初期設定である完全なインストールによって Windows のサービスとしてインストールされます。IIS を使用すると、ASPX ページ セットと特別なサポート サービス QlikView Setting Service (QSS) により同一の機能が提供されます。QSS は ASPX ページで使用する設定の管理用インターフェースとしての役割を果たします。

概要

QlikView Web Server

QlikView Web Server プロパティ

Property	
実行可能ファイル	*%ProgramFiles%\QlikView\Server\Web Server\QVWebServer.exe*
データ	*%ProgramData%\QlikTech\WebServer*
リッスン ポート	HTTP: 80; HTTP: 4750; SNMP: 4751
使用/コントロール	DSC
利用者	ウェブ ブラウザ クライアントとモバイル クライアント

QlikView 設定サービス

QlikView 設定サービス プロパティ

Property	
実行可能ファイル	*%ProgramFiles%\QlikView\Server\Web Server Settings\QVWebServerSettingsService.exe*
データ	*%ProgramData%\QlikTech\WebServer*
リッスン ポート	HTTP: 4750
利用者	QMS

ファイル

設定と構成

構成ファイル

ファイル	**説明**
Config.xml	サービスの構成ファイル。

ログ

ログ ファイル

ファイル	**説明**
Log\<date>.txt	イベントおよびエラー ログ。

QlikView Web サービスの設定

QlikView 管理コンソール のいずれかを使用して Web サーバーを構成できます。追加の構成は下記の場所に保存されている *config.xml* ファイルを編集することで実行できます。

C:\ProgramData\QlikTech\WebServer

config.xml ファイルには、次に示すように、一般的であってもデフォルトとしては設定されていないオプションの使用を簡易化するために、コメント アウトされたセクションが含まれます。

```
<Config>
<DefaultUrl>http://_/</DefaultUrl>
<DefaultQvs>local</DefaultQvs>
<ConfigUrl>http://_:4750/qvws.asmx</ConfigUrl>
<TunnelUrl>/scripts/QVSTunnel.dll</TunnelUrl>
<QvsStatusUrl>/QvAjaxZfc/QvsStatus.aspx</QvsStatusUrl>
<LogLevel>Information</LogLevel>
<UseCompression>True</UseCompression>
<InstallationPath>C:\Program Files\QlikView\Server\Web Server</InstallationPath>
<QvsAuthenticationProt>Negotiate</QvsAuthenticationProt>
<QvpPort>-1</QvpPort>
<AddCluster>
<Name>local</Name>
<LoadBalancing>Random</LoadBalancing>
<AlwaysTunnel>False</AlwaysTunnel>
<AddQvs>
<Machine>localhost</Machine>
<Port>4747</Port>
<LinkMachineName>RD-CENTEST1</LinkMachineName>
<Weight>1</Weight>
</AddQvs>
</AddCluster>
<AddDSCCluster>
<CustomUserPort>-1</CustomUserPort>
<DirectoryServiceConnectorSettings>
<ID>17da91ee-c4a6-4cdb-a2fb-ab472ece659f</ID>
<Url>http://rd-centest1:4730/qtds.asmx</Url>
<Name>Default DSC</Name>
<Username>DxdCGMWfOwU=</Username>
<Password>DxdCGMWfOwU=</Password>
<LogLevel>Normal</LogLevel>
</DirectoryServiceConnectorSettings>
</AddDSCCluster>
<Authentication>
<AuthenticationLevel>Always</AuthenticationLevel>
<LoginAddress>/qlikview/login.htm</LoginAddress>
<LogoutAddress>logout.htm</LogoutAddress>
<GetTicket url="/QvAjaxZfc/GetTicket.aspx" />
<HttpAuthentication url="https://_/scripts/GetTicket.asp" scheme="Basic" />
<HttpAuthentication url="/QvAJAXZfc/Authenticate.aspx" scheme="Ntlm" />
</Authentication>
<AccessPoint>
<Path>/QvAJAXZfc/AccessPoint.aspx</Path>
<AjaxClientPath>/QvAJAXZfc/opendoc.htm</AjaxClientPath>
<PluginClientPath>/QvPlugin/opendoc.htm</PluginClientPath>
<DefaultPreferedClient>Ajax</DefaultPreferedClient>
<DefaultView>Thumbnails</DefaultView>
<DefaultPagesizeDetails>40</DefaultPagesizeDetails>
<DefaultPagesizeThumbnails>4</DefaultPagesizeThumbnails>
<HighlightNotExecutedJobs>False</HighlightNotExecutedJobs>
<HighlightThresholdMinutes>60</HighlightThresholdMinutes>
<AllowCmdUrl>False</AllowCmdUrl>
<Target />
<RespectBrowsable>True</RespectBrowsable>
</AccessPoint>
<Ajax>
<Path>/QvAJAXZfc/QvsViewClient.aspx</Path>
<Path>/QvAJAXZfc/QvsViewClient.asp</Path>
<NoCrypto>False</NoCrypto>
```

```
<ProhibitMachineId>False</ProhibitMachineId>
<Recording>False</Recording>
<AllowCmdUrl>True</AllowCmdUrl>
</Ajax>
<Web>
<Folders>
<Folder>
<Name>QlikView</Name>
<Path>C:\Program Files\QlikView\Web</Path>
</Folder>
<Folder>
<Name>QvClients</Name>
<Path>C:\ProgramFiles\QlikView\Server\QvClients</Path>
</Folder>
<Folder>
<Name>QvAJAXZfc</Name>
<Path>C:\ProgramFiles\QlikView\Server\QvClients\QvAjaxZfc</Path>
</Folder>
<Folder>
<Name>QvDesktop</Name>
<Path>C:\Program Files\QlikView\Server\QlikViewClients\QlikViewDesktop</Path>
<Folder>
<Folder>
<Name>QvPlugin</Name>
<Path>C:\Program Files\QlikView\Server\QvClients\QvPlugin</Path>
</Folder>
</Folders>
<Types>
<Type>
<Extension>.css</Extension>
<Content>text/css</Content>
</Type>
<Type>
<Extension>.htm</Extension>
<Content>text/html</Content>
</Type>
<Type>
<Extension>.html</Extension>
<Content>text/html</Content>
</Type>
<Type>
<Extension>.jpg</Extension>
<Content>image/jpg</Content>
</Type>
<Type>
<Extension>.gif</Extension>
<Content>image/gif</Content>
</Type>
<Type>
<Extension>.jar</Extension>
<Content>application/octet-stream</Content>
</Type>
<Type>
<Extension>.png</Extension>
<Content>image/png</Content>
</Type>
<Type>
<Extension>.exe</Extension>
<Content>application/octet-stream</Content>
```

```
</Type>
<Type>
<Extension>.msi</Extension>
</Type>
<Type>
<Extension>.htc</Extension>
<Content>text/xml</Content>
</Type>
<Type>
<Extension>.js</Extension>
<Content>text/javascript</Content>
</Type>
<Type>
<Extension>.xslt</Extension>
<Content>text/xml</Content>
</Type>
<Type>
<Extension>.xml</Extension>
<Content>text/xml</Content>
</Type>
<Type>
<Extension>.xls</Extension>
<Content>application/vnd.ms-excel</Content>
</Type>
<Type>
<Extension>.csv</Extension>
<Content>application/octet-stream</Content>
</Type>
<Type>
<Extension>.pdf</Extension>
<Content>application/pdf</Content>
</Type>
</Types>
</Web>
</Config>
```

次の表には、一例として挙げられたタグについて説明しています。

タグの例

Tag	説明
DefaultURL	QlikView Server の URL。
ConfigUrl	これは QlikView Web Server と通信するために QMC で使用される URL です。
TunnelUrl	トネリングに使用される URL。
QvsStatusUrl	QlikView Server のステータスページへの URL。
LogLevel	ログ記録のレベルを設定します。使用できる設定には Information (高)、Warning (中)、Error (低) があります。

Tag	説明
UseCompression	送信された情報を圧縮するかどうかを設定します。
InstallationPath	QlikView Web Server のインストール用パス。
QvsAuthenticationProt	QlikView Server の認証。Negotiate、Kerberos、または NTLM に設定します。
AddCluster - Name	クラスターの名前。
AddCluster - LoadBalancing	ロードバランスの計算方法。使用できる値は、クライアントが QVS にランダムに誘導される場合は Random で、最低平均 CPU をレポートする QVS が選択される場合は CpuUsage、あるいは、クライアントがリクエストしたドキュメントが既にロードされている QVS に直接誘導される場合は LoadedDocument になります。
AddCluster - AddQvs - AlwaysTunnel	QlikView Server への通信を常にトンネルするには、true に設定します。
AddCluster - AddQvs - Machine	QlikView Server が実行中のコンピュータの名前。
AddCluster - AddQvs - Port	QlikView Server がリッスンしているポート。
AddCluster - AddQvs - LinkMachineName	QlikView Server の外部名で、QlikView Plug-in クライアントによって使用されます。
AddCluster - AddQvs - Weight	ランダム ロードバランシングの使用時、QlikView Server がより頻繁に選択されるようにするには、高めの値を設定します。
AddDSCCluster - CustomUserPort	Directory Service Connector のポート。
AddDSCCluster - DirectoryServiceConnectorSettings - Url	Directory Service Connector の場所。
AddDSCCluster - DirectoryServiceConnectorSettings - Name	クラスター名。

Tag	説明
AddDSCCluster - DirectoryServiceConnectorSettings - Username	Directory Service Connector への接続に必要であれば、ユーザー名を入力します。
AddDSCCluster - DirectoryServiceConnectorSettings - Password	Directory Service Connector への接続に必要であれば、パスワードを入力します。
Authentication - AuthenticationLevel	クライアントが AccessPoint へどのようにアクセスするかを指定します。使用できる値は Always、Login、Never です。
Authentication - LoginAddress	カスタム ユーザー用の代替ログイン ページへのパス。
Authentication - LogoutAddress	カスタム ユーザー用の代替ログアウト ページへのパス。
Authentication - GetTicket	クライアント用にサーバーからチケットを取得するために使用される URL と認証。
Authentication - HttpAuthentication	SSL/TSL 使用時、クライアント用にサーバーからチケットを取得するために使用される URL と認証。
AccessPoint - Path	Access Point がインストールされている場所。
AccessPoint - AjaxClientPath	Ajax クライアントへの相対パス。
AccessPoint - PluginClientPath	QlikView プラグイン クライアントへの相対パス。
AccessPoint - DefaultPreferredClient	ユーザーが AccessPoint へ最初にアクセスする際、クライアント用に優先クライアントとして設定するかを指定します。
AccessPoint - DefaultView	AccessPoint 内でのドキュメントのデフォルト ビュー (詳細またはサムネイル)。
AccessPoint - DefaultPagesizeDetails	詳細 ビューを使用中の、AccessPoint の行数。
AccessPoint - DefaultPagesizeThumbnails	サムネイル ビューを使用中の、AccessPoint の行数。

Tag	説明
AccessPoint - RespectBrowsable	True に設定している場合は、Browsable として設定されているもののみをマウントし、QVS が AccessPoint に表示されます。
Ajax - Path	*QvsViewClient.aspx* へのパス。パスの変更は可能ですが、設定を機能させるためには、ファイル名の変更は行わないでください。
Ajax - NoCrypto	QlikView Web Server と QlikView Server の間で暗号化の使用を禁止します。
Ajax - ProhibitMachineID	マシン ID の送信を禁止します。これで匿名のブックマークの使用を効果的に排除することができます。
Ajax - Recording	True に設定した場合、AJAX zero footprint クライアントはログに記録されます。
SafeForwardList	*Authenticate.aspx* を通じてリダイレクトがリクエストされると、DNS の検索は、このタグに指定されているパスの IP アドレスを取得するために実行されます。IP アドレスがリダイレクト リクエストと一致したら、リダイレクトが許可されます。
StrictSafeForwardList	*Authenticate.aspx* を通じてリダイレクトがリクエストされると、このタグに指定されたパスのホスト名は、着信 リダイレクト パスのホスト名と比較されます。一致した場合 (大文字と小文字の区別なし) は、リダイレクトが許可されます。
Web - Folders	QlikView Web Server の様々な仮想フォルダへのパスです。既定以外のフォルダにファイルをインストールした場合、名前とパスを変更します。

Tag	説明
`Web - Types`	Access Point/QlikView Web Server からクライアントがダウンロードすることを許されているファイル拡張子を指定します。

ロードバランス

QVWS はウェブページをホストし、AccessPoint に対しファイル リストを準備し、また各種 QlikView Server (QVS) のロードバランスを管理します。

AccessPoint は QVWS でホストされるドキュメント用のウェブ ポータルです。AccessPoint のページは、初期設定では *%ProgramFiles%\QlikView\Web* にあります。QVWS はまた、エンドユーザーがアクセスする AJAX ページのウェブ サーバーとしての役割も果たします。

QVWS のロードバランスは、Web サーバーのロードバランスとは異なります。これは、操作内容とリソース消費は各ユーザーにとってほとんど同じであり、エンドユーザーがどのサーバーに接続するかは問題ではないためです。

ロードバランスのスキームは以下の通りです。

ロードバランス スキーム

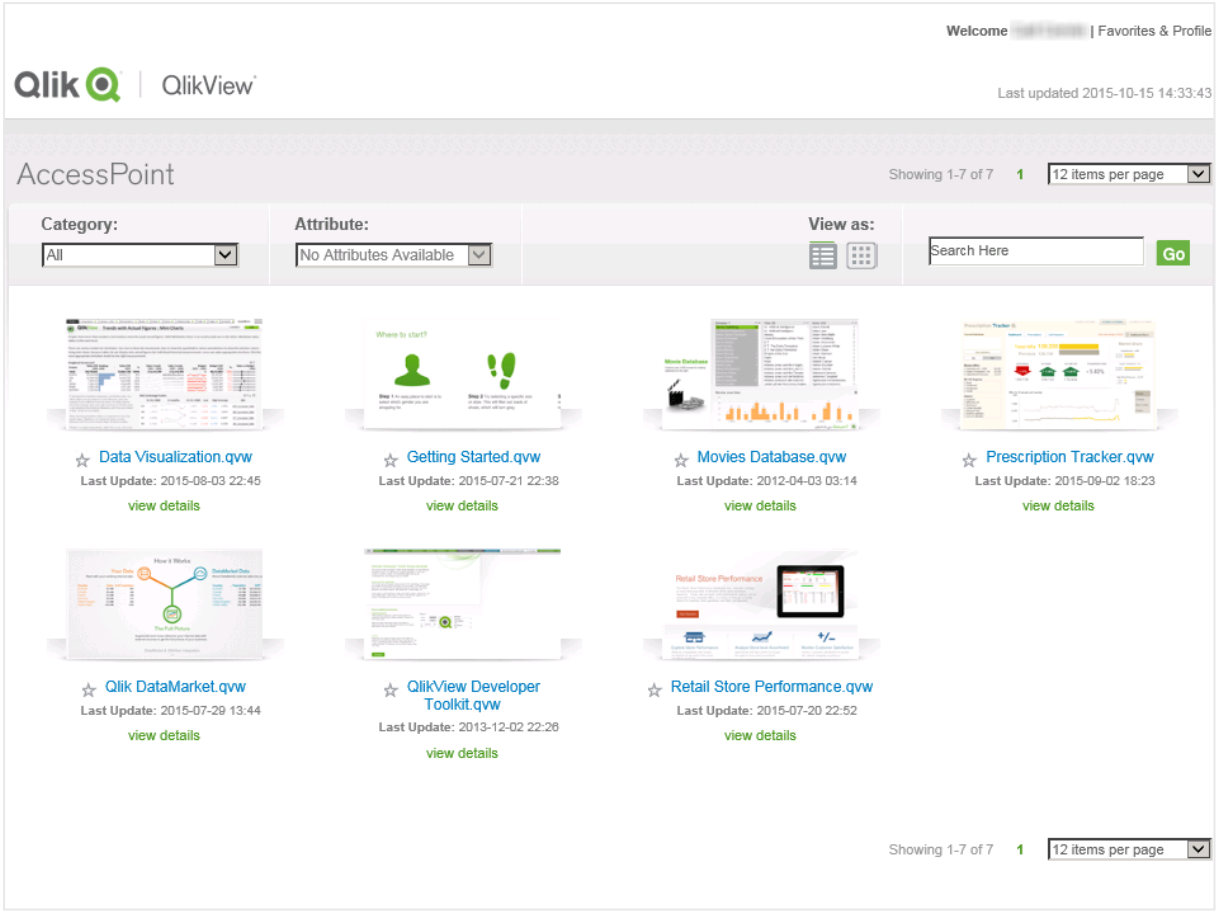
スキーム	説明
ランダム (Random)	デフォルトのロードバランス スキーム。ユーザーが指定したドキュメントがロードされているかどうかに関わらず、ユーザーはランダムなサーバーに送信されます。
ロード済みドキュメント (Loaded Document)	指定ドキュメントがロードされている QVS が 1 つの場合、ユーザーをその QVS に送信します。指定ドキュメントがロードされている QVS が 2 つ以上ある場合、ユーザーは RAM の空き容量が最も大きな QVS に送信されます。
CPU の RAM オーバーロード (CPU with RAM Overload)	ユーザーは、ビジー度が最も低い QVS に送られます。

ロードバランスの設定は QMC で行います。

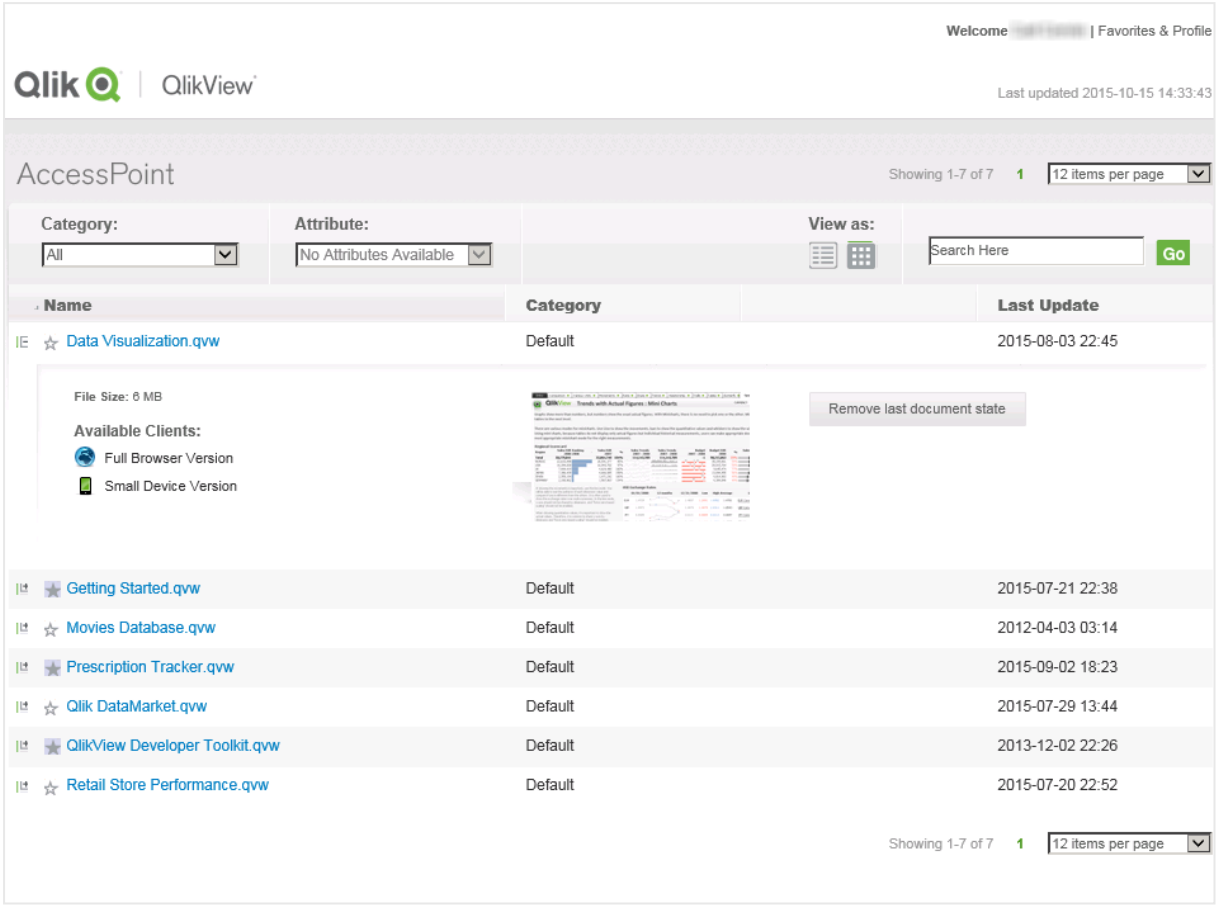
QlikView AccessPoint

QlikView AccessPoint は、各ユーザーがアクセスするドキュメントをリストする Web ポータルです。AccessPoint は各ドキュメントとリンクするだけで、ドキュメントをホストするわけではありません。ホスティングは QlikView により行われます。

ドキュメントはサムネイルまたは詳細リストとして表示可能です。



AccessPoint でのサムネイル ビュー



AccessPoint での詳細 ビュー

AccessPoint で利用可能な設定は以下の通りです。

AccessPoint 設定

構成	説明
カテゴリ	ドキュメントのカテゴリグループ。カテゴリの管理は QMC の **[ドキュメント (Documents)] > [ユーザー ドキュメント (User Documents)] > [ドキュメント情報 (Document Information)]** で行います。
属性	ドキュメントの属性 グループ。属性の管理は QMC の **[ドキュメント (Documents)] > [ユーザー ドキュメント (User Documents)] > [ドキュメント情報 (Document Information)]** で行います。
表示形式	ドキュメントの表示タイプ、**詳細 (Detailed)** ビューまたは**サムネイル** (Thumbnails) ビュー。 詳細表示ではドキュメントを名前 (Name)、カテゴリ(Category)、最終更新日 (Last Update) 別にソートできます。

サムネイル ビューで **[詳細を表示 (view details)]** をクリックするか、または詳細 ビューでドキュメント名の左側にあるプラス記号 **(+)** をクリックすると、ドキュメントの追加情報が表示されます (下記を参照)。

追加のドキュメント情報

項目/ボタン	説明
最終更新日 (Last Update)	ドキュメントが最後に更新された日。 *これはサムネイル ビューでのみ表示されます。*
次回更新日 (Next Update)	ドキュメントが次回更新される日。 *これはドキュメントがスキーマのあるタスクの一部である場合にのみ表示されます。*
ファイル サイズ (File Size)	ドキュメントのサイズ。
対象クライアント (Available Clients)	クライアントをクリックするとそのクライアントでドキュメントが開きます。
ドキュメントの最後の状態を削除 (Remove last document state)	このボタンをクリックするとドキュメントの最後の状態が削除されます。

*QlikView 管理者が QMC で **[最終更新時間が (分) よりも古い場合に警告を表示]** 設定を有効化している場合は、最終更新日項目の横にアイコンが表示されます。✔ は、定義期間内にドキュメントが更新されていることを表します。⚠ は、定義期間内にドキュメントが更新されていないことを表しします。*

サムネイルまたは詳細 ビューでドキュメント名の横にあるスター アイコンをクリックすると、ドキュメントの設定を変更できます。

ドキュメント基本設定

構成	説明
クライアントを選択して開く (Open with)	デフォルトとなるクライアントを選択し、そのクライアントでドキュメントを開きます。
お気に入りに追加 (Add to favorites)	お気に入りにドキュメントを追加するにはこのリンクをクリックします。お気に入りを表示するには AccessPoint で **[カテゴリ (Category)] > [お気に入り (Favorites)]** の順に選択します。

Ajax クライアントのモーダル ダイヤログの変更

[Print] **(印刷)**, **[Export] (エクスポート)**、**[Server Connection Lost] (サーバー接続の切断)** などのモーダル ダイアログは、*customTranslations*.

C:\Program Files\QlikView\Server\QlikViewClients\QlikViewAjax\htc\customFiles に. ここにある *customConfig ファイル* と *customTranslations ファイル* は空ですが、*customConfigExample ファイル* と *customTranslationsExample ファイル* は編集方法を示すサンプルです。

customTranslations ファイルへの *編集を有効にするには*、その前提として、`TranslationEvents` TranslationEvents を `true` に設定しておく*必要*があります。

変更内容を反映するには、サーバーを停止して再起動してください。

Directory Service Connector

概要

Directory Service Connector の概要

実行可能ファイル	*%ProgramFiles%\QlikView\Directory Service Connector\QVDirectoryServiceConnector.exe*
データ	*%ProgramData%\QlikTech\DirectoryServiceConnector*
リッスン ポート	HTTP: 4730、SNMP: 4731
使用/コントロール	-
利用者	QDS、QMS、QVWS

ファイル

設定と構成

設定内容は QVPR に基づきます。

ファイルの設定と構成

ファイル	**説明**
Config.xml	サービスの構成ファイル。
Resources/<id>.xml	DSP の構成。

ログ

ログ ファイル

ファイル	**説明**
Log\<date>.txt	イベントおよびエラー ログ。

DSP インターフェース

専有の Directory Service Provider (DSP) を開発する理由は、QlikView がデフォルトではサポートされていないディレクトリサービス上のユーザーにドキュメントを配信することと、ウェブ サーバー上のグループへの配信を可能にするためです。

DirectoryServiceProvider

DirectoryServiceProvider は、フレームワークにプラグインするクラスのインターフェースです。インターフェースのメンバーは以下にリストされている通りです。

Directory Service Provider インターフェース メンバー

メンバー	説明
`LogMessage LogMessageEvent { set; get; }`	構成後、この項目はだたちにインスタンスを作成し、加工されていないログ機能の提供を行います。
`string ProviderName { get; }`	自由に記述可能な、任意のコンポーネントの名称を設定します。
`string ProviderType { get; }`	フレームワークによって内部的に使用されるコンポーネントの一意の ID を記述します。すでにプロバイダによって使用されている ID は、`AD` と `NT`、`Local`、`Custom` です。
`void SetupPath (string _path, string _username, string _password);`	指定したパスにおいて対応する Directory Service ノードを表すノードを作成します。不具合が発生したら、例外がスローされます。
`IList<string>GetKnownRootPaths ();`	返されたリストには、ここにリストされたメソッドように 1 つ以上の実行可能なパスを含める必要があります。
`void ClearCache ();`	(あれば) キャッシュをクリアにします。
`string DomainName { get; }`	パスに関連付けられた「domain name」が設定されます。異なるプロバイダのノードを分けるための修飾子として使用されます (たとえば、実装されたアクティブディレクトリプロバイダはドメイン名として `NetBIOSName` を使用します)。
`IDictionary<string, string> GetSettings ();`	サポートされている設定のディクショナリには、`key` として設定名、`value` として種類の名前があります。
`void SetSetting (string _name, string _value);`	プロバイダは構文解析を実施する必要があります。
`IList<IDSObject> Search (string [] _pattern, eSearchType _type, string _otherattribute);`	与えられたいずれかのパターンに合致する属性でノードを検索します。属性は、`type` パラメータで指定され、これは一覧にある 1 つ以上の値です。`type` が「other」の場合、最後のパラメータには属性名を指定します。検索タイプ「legacyid」は、以前のバージョンとの互換用に使用されます。検索は、任意の種類の 0 個以上の文字と合致するワイルドカード「*」を含むパターンをサポートします。
`void Dispose ();`	プロバイダがオブジェクトをリリースすると直ちにコールされます。
`IDSObject`	Directory Service 内のいずれのタイプのノードにも使用されるシンプルなインターフェース。
`string ID { get; }`	インスタンスのパス内で一意のノード ID で、すべての実行において一致します。
`string DisplayName { get; }`	Directory Service 内のノードの共通の名前。
`string AccountName { get; }`	(あれば) ノードに関連付けられたアカウントの名前。
`eDSObjectType ObjectType { get; }`	オブジェクトの基本的な種類。
`IList<IContainer> MemberOf ();`	ノードがメンバーとなっているすべてのグループのリスト。

メンバー	説明
`string GetCustomProperty (string _name);`	本来インターフェースでサポートされていない他のプロパティ。存在しない場合、NULL が返されます。
`string Email { get; }`	ノードに関連付けられた主要なメールI アドレス(存在する場合)。

QlikView Management Service

概要

QlikView Management Service の概要

実行可能ファイル	*%ProgramFiles%\QlikView\Management Service\QVManagementService.exe*
データ	*%ProgramData%\QlikTech\ManagementService*
リッスン ポート	HTTP: 4780 (ウェブ)、HTTP: 4799 (API)、SNMP: 4781
使用/コントロール	DSC、QDS、QVS、QVWS
利用者	Web ブラウザ/API クライアント

ファイル

設定と構成

QlikView Management Service (QMS) は QVPR のグローバル ビュー設定を保持します。

ファイルの設定と構成

ファイル	説明
Config.xml	サービスの構成ファイル。

ログ

ファイルの設定と構成

ファイル	説明
Log\<date>.txt	イベントおよびエラー ログ。

SNMP

QlikView は すべてのサービスに対し SNMP エージェントを提供します。

> *QlikView は iReasoning MIB ブラウザを使った SNMP エージェントからのデータ取得をサポートしてします。*

この実装はまだ初期段階にあり変更される可能性があるため、デフォルトではこの設定は無効になっています。書き込みの際は、エージェントからの読み込み操作が有効になります。次のメッセージがサポートされています。

- `GetRequest`
- `GetResponse`

- GetNextRequest

すべてのサービスは標準 SNMP クエリに結果を返します (下記を参照)。

標準 SNNP クエリ

識別子	クエリ	説明
1.3.6.1.2.1.1.1	sysDescr	サービス/製品の説明。 例: `sysDescr.0:Qlikview Publisher Commandcenterservice version 8.50.600`
1.3.6.1.2.1.1.2	sysObjectID	ユニットの種類。 例: `sysObjectID.0:iso.org.dod.internet.private.enterprises.qliktech.products.publisher.Distributionservice`
1.3.6.1.2.1.1.3	sysUpTime	システム使用可能時間。 例: `sysUpTime.0:0 hours, 12 minutes, 15 seconds`
1.3.6.1.2.1.1.4	sysContact	設定ファイルで設定可能。 例: `sysContact.0:Unspecified System contact`
1.3.6.1.2.1.1.5	sysName	設定ファイルで設定可能。 例: `sysName.0:Unspecified name`
1.3.6.1.2.1.1.6	sysLocation	設定ファイルで設定可能。 例: `sysLocation.0:Unspecified location`
1.3.6.1.2.1.1.7	sysService	定数、72 はアプリケーションサーバーを指します。 例: `sysServices.0:72`

QlikView Distribution Service はさらなるクエリに結果を返すことができます。下記の内容は MIB ファイルで指定されます。

各サービスには設定ファイルがあり、これはインストール フォルダ内の該当サービスのサブフォルダに格納されています。たとえば、QlikView Distribution Service の設定ファイルは *QlikViewdistributionService.exe.config* です。

SNMP 設定は、設定ファイルの `SNMP SETTINGS` の部分で調整できます。SNMP のデフォルト設定はすべてのサービスでオフになっているため、有効にする必要があります。

SNMP 設定

構成	説明
EnableSNMP	SNMP リスナーを有効にします。この値の既定値は `false` です。
SNMPPort	Publisher Service 用に使用するポートを設定します。各サービスのデフォルト設定は以下を参照してください。
SNMPsysContact	管理ノードを担当する人物の連絡先情報。この値の既定値は `Unspecified System contact` です。
SNMPsysName	管理ノードの管理者により割り当てられた名前。規則では、これはノードの完全なドメイン名です。名前が不明な場合、値は長さが 0 の文字列です。空白のままにすると、現在のマシン名となります。この値の既定値は `Unspecified name` です。
SNMPsysLocation	ノードの物理的な場所 (例:「3 階の電話室」)。この値の既定値は `Unspecified location` です。
DebugSNMP	SNMP リスナー用の拡張デバッグ ログを有効にします。この値の既定値は `false` です。

サービスのデフォルト ポート設定は以下の通りです。

デフォルトのポート設定

Service	デフォルトのポート設定
QlikView Management Service	4781
Directory Service Connector	4731
QlikView [Distribution Service] (配布サービス)	4721 (デフォルトの SNMP ポート)
QlikView Server	161
QlikView Web Server	4751

ポートはすべて設定可能です。サービスが異なるマシンにインストールされている場合、すべて同じポートを使用して実行することができます。実装が実験的な SNMP 領域から Qlik の割り当てた領域に変わると、ポートが変わります。

MIB ファイル

MIB ファイルは QlikView の配布に含まれているため、SNMP 管理者は QlikView Distribution Service からの追加の応答を解釈できます。ただし、MIB ファイルは変更される可能性があります。ファイルは *.\QlikView\Support Tools* にインストールされます。サポート ツールはカスタム インストールする必要があります。

QlikView Distribution Service は、上記に記したもの以外に、次のクエリの結果を返すことができます。

その他のクエリ

識別子	クエリ
1.3.6.1.4.1.30764.1.2.2.1	QDSTaskExecuteStatusTable
1.3.6.1.4.1.30764.1.2.2.1.1	QDSTaskExecuteStatusEntry
1.3.6.1.4.1.30764.1.2.2.1.1.1	QDSTaskID (タスク ID 番号)
1.3.6.1.4.1.30764.1.2.2.1.1.2	QDSTaskName (タスク名)
1.3.6.1.4.1.30764.1.2.2.1.1.3	QDSTaskExecuteStatus (タスク ステータス): • 待機中 (Waiting) • 実行中 (Running) • 中断中 (Aborting) • 失敗 (Failed) • 警告 (Warning)
1.3.6.1.4.1.30764.1.2.2.1.1.4	QDSTaskNextExecutionAt (次回いつタスクが実行されるか)
1.3.6.1.4.1.30764.1.2.2.1.1.5	QDSTaskLastExecutedAt (前回いつタスクが実行されたか)
1.3.6.1.4.1.30764.1.2.2.1.1.6	QDSTaskCurrentWork (現在タスクが何を実行中か)
1.3.6.1.4.1.30764.1.2.2.1.1.7	

参照先:

- Simple Network Management Protocol
- Simple Network Management Protocol (ウィキペディア)

2.2 配置

QlikView アーキテクチャはサイトのコンセプトに基づいています。QlikView サイトは共通の論理リポジトリまたは中央ノードに接続された 1 つ以上のノード (つまり、サーバー マシン) のコレクションです。

QlikView はさまざまな方法で展開できます。このセクションではさまざまな展開シナリオについて説明します。

ファームの構築

サーバー ファームの方が 1 つのロケーションにあるサーバーより、パフォーマンスや冗長性、セキュリティにおいて優れた機能性を提供します。

計画

実際のインストールを開始する前に、計画を立てることが必要です。考慮すべき項目は、以下の通りです。

- 信頼性のメカニズム
- ウェブ サーバー (QlikView Web Server もしくは Microsoft IIS)
- 冗長性レベル
- サービスを実行するアカウント

- QVPR 形式 (XML もしくは SQL)
- ユーザー ディレクトリ
- ユーザー許可
- ファイアウォール

信頼性のメカニズム

信頼性のメカニズムは Windows グループもしくは証明書によって実現できます。

Windows グループは、すべてのサービスが単一のアクティブ ディレクトリ(AD) にあれば、実装が容易です。暗号化された通信が必要な場合は、手動で追加できます。

証明書は、ドメインを超えた環境で信頼性メカニズムとともに、SSL/TSL 暗号化も提供します。

ウェブ サーバー

QlikView Web Server は、QlikView 以外の目的でウェブ サーバーを必要としない場合に使用されます。ライトウェイトで管理が容易ですが、QlikView インストールに必要なタスクを同時にサポートするには限界があります。

Microsoft IIS をホストするウェブ サーバーが推奨されるのは、次のような場合です。

- より柔軟性の高い、あるいは高度なチューニングが必要な場合
- QlikView より他のタスクでウェブ サーバーを使用する頻度が高い場合
- 初期設定で必要な許可スキームが使用できない場合

冗長性レベル

冗長性レベルは、クラスター化もしくは同一のサービスを複数のマシンで実行する場合に問題となります。QlikView Management Service (QMS) 以外のすべてのサービスは、複数のマシンにインストール可能です。さらに、クラスター化が可能なのは QlikView Server (QVS)、QlikView Distribution Service (QDS)、Directory Service Connector (DSC) です。

サービスを実行するアカウント

QlikView サービスを管理するには、専用アカウントを作成する必要があります。アカウントにはインストール中、正しい権限を割り当てる必要があります。

すべてのサービスに同一のアカウントを使用することをお薦めします。

QVPR 形式

QVPR 形式の選択は、QlikView 製品以外の理由 (バックアップや利用設定など) に基づきます。インストールは、通常 XML モードで開始されます。

ユーザー ディレクトリ

Windows ユーザーの場合、デフォルトは QlikView です (NTFS モード)。Windows ユーザー以外にアクセス権を付与する場合 (匿名以外) は、Document Metadata Service (DMS) モードで QlikView Server が起動している必要があります。

ユーザー許可

QlikView は複数の許可スキームをサポートしています。ASPX 開発およびウェブ サービスで Microsoft IIS を使用する場合には追加スキームが必要な場合があります。

ファイアウォール

(ファイアウォールで適切なポートが開いているなど) サービスの通信が可能であることを確認してください。

では、(page 21)

ルートと最初のインストール

まず、適切なサービス アカウント (複数の場合もあり) が設定され、サービスがインストールされているマシンが利用可能であることを確認してください。

すべてのインストールは単一の QMS 上に存在する必要があり、まず最初に QMS をインストールしなければなりません。QMS が続いてインストールされるサービスすべてと通信できることを確認してください。

同一サーバーで実行するサービスが複数ある場合は、それらを同時にインストールすることができます。

他のマシンにサービスを追加する

次の手順は、他のサーバーに他のサービスをインストールすることです。同一サーバーで実行するサービスが複数ある場合は、それらを同時にインストールすることができます。サービスを追加する順序は重要ではありません。

サービスをインストールしたら、QlikView Management Console (QMC) に戻りサービスを設定します。これは、[システム (System)] タブで設定します。最初のステップとしてサービスを追加します。クラスターの構築と新しいクラスターの作成の違いには注意が必要です。

クラスタリング

このセクションでは、QlikView Server クラスターの作成方法について概説します。

QlikView Server

QlikView Server クラスターが適切に動作するには、**[システム (System)] > [設定 (Setup)] > [QVS リソース (QVS resource)] > [フォルダ (Folders)] > [ルート フォルダ (Root Folder)]** の順で選択し、共通の共有フォルダを設定することが重要です。さらに、**[代替の一時ファイル フォルダ パス (Alternate Temporary Files Folder Path)]** を共通の共有フォルダに設定する必要があります (ルート フォルダとは別)。

拡張機能を使用している場合は、共通の共有フォルダに **[代替拡張パス (Alternate Extension Path)]** を設定することで管理が容易になります。

共通のロケーションに対し **[システム (System)] > [設定 (Setup)] > [QVS リソース (QVS resource)] > [ログ (Logging)] > [ログ フォルダ (Log Folder)]** の順で選択して設定を行うのは共通ですが、必須ではありません。

> *ルート フォルダは、クラスター ファイル (.pgo ファイル) およびユーザー ドキュメント以外には使用しないでください。*

QlikView Distribution Service

QDS クラスターの場合、**[システム (System)] > [設定 (Setup)] > [基本設定 (General)]** の順で選択し、共通の共有フォルダに **[アプリケーション データ フォルダ (Application Data Folder)]** を設定する必要があります。さらに、**[ソース フォルダ (Source Folders)]** を共通の共有フォルダに設定してください。

Directory Service Connector

DSC クラスターに特別な設定は不要です。クラスター化された DSC とクラスター化されていない DSC の違いは設定が共有か否かという点です。

QlikView Web Server

複数のウェブ サーバーを設定することは可能ですが、設定は個別に行います (つまり、クラスター化はされません)。複数のウェブ サーバーで QlikView Web Server (QVWS) と複数の Microsoft IIS を起動させることは一般的ではありませんが、技術的な観点からは可能な設定です。

Microsoft IIS を使ったトンネリング

トンネリングは、Windows ネイティブ クライアント (QlikView Desktop、OEM OCX、QlikView プラグイン) が使用するとともに、クライアントが ポート 4747 を使って QlikView Server と通信できない場合に必要です (たいていはファイアウォールがトラフィックをブロックしていることが原因)。

- QVWS: 追加の設定は不要です。
- Microsoft IIS: *QVSTunnel.dll* ファイルを ISAPI フィルタに追加する必要があります。

Microsoft IIS 7 でトンネリングを設定するには次の手順を実行します。

1. Internet Information Services Manager を開きます。
2. IIS トップ ノードを選択します。
3. ISAPI および CGI の制限ダイアログを開きます。
4. 操作 (Action) パネルで **[追加 (Add)]** を選択して、*QVSTunnel.dll* を検索します。
5. インスタンスの説明を入力して、**[拡張パスの実行を許可する (Allow extension path to execute)]** ボックスをオンにします。
6. QlikView Server および Publisher ページをホストするサイトを開いて、**[スクリプト (Scripts)]** をクリックします。
7. [ハンドラー マッピング (Handler Mappings)] ダイアログを開きます。
8. ISAPI dll を検索し、操作 (Action) パネルの **[機能のアクセス許可の編集 (Edit Features Permission)]** を選択します。
9. 開いたダイアログで **[実行 (Execute)]** をクリックします。

QVS および Microsoft IIS が異なるコンピュータ上にある場合は、レジストリで以下のエントリが必要です。

```
[HKEY_LOCAL_MACHINE\SOFTWARE\QlikTech\QlikTunnel]
```

- “QVSPort”=dword:000012a6
- “QVSServer”=“QvsHost”

レジストリにすでにエントリが存在する場合、手動で追加する必要があります。

クライアントのブラウザ ウィンドウに次の URL を入力して QlikView Server トンネルをテストできます。

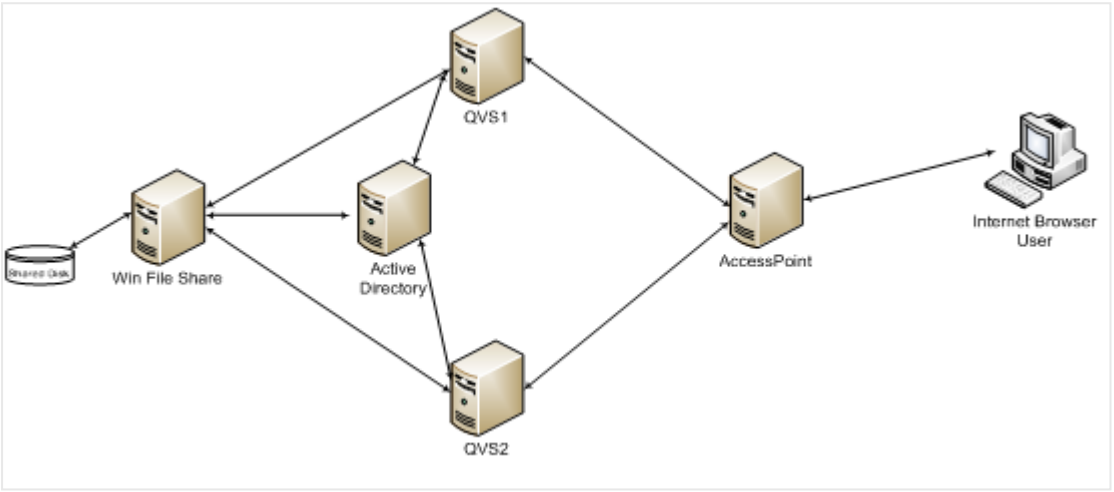
http://<Servername>/scripts/qvstunnel.dll?test

Servername はウェブ サーバーです。トンネルを正しく設定したら、ウェブ パージにトンネリングが使用可能になったというメッセージとQlikView Server のバージョン番号が表示されます。

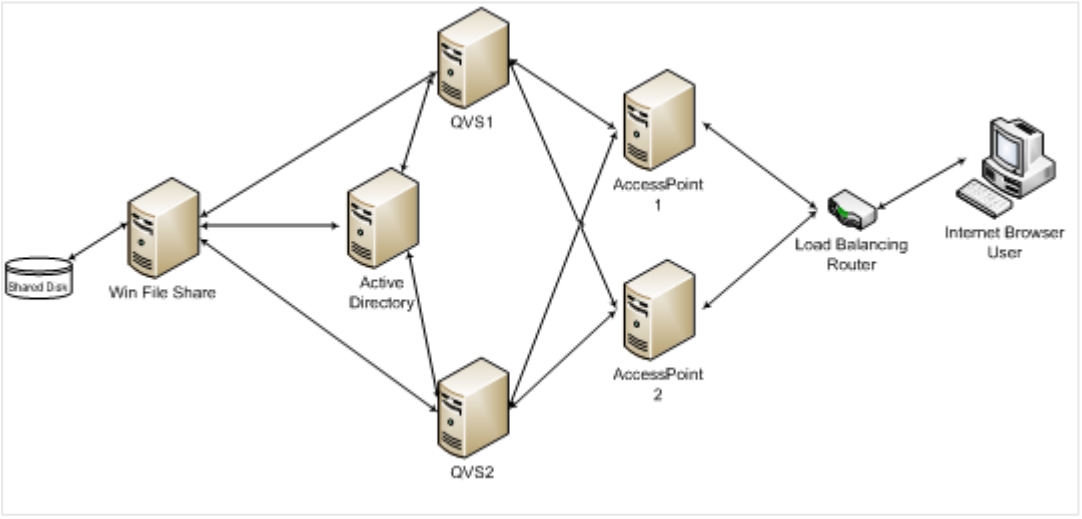
QlikView Server のクラスター化

本章では、クラスター化された障害への適応力のあるQlikView Server の構成を構築するためのアーキテクチャおよびインストール要件とオプションについて説明します。

次の図は、クラスター化および負荷分散化されたQlikView Server の構成を示しています。



次の図は、障害への適応力のある、クラスター化され負荷分散化されたQlikView Server の構成を示しています。ここでは AccessPoint ロード バランスが使用されています。



QlikView Server のロード バランス機能は QlikView Web ポータルの AccessPoint に含まれています。本章では、適宜、ネットワーク ロード バランスを使用して、このコンポーネントに障害への適応力をつける方法を説明します。

QlikView Server をクラスター化する理由

QlikView Server をクラスタ化ーすることにより、以下の目標を達成できます。

水平ユーザー スケーラビリティ

単一の QlikView Server によって提供できるよりも多くのリソースが必要な場合は、サーバーを追加することができます。たとえば、サーバーが 100 人の同時ユーザーに対応できるのに対し、200 人の同時ユーザーをサポートしなければならない状況においては、サーバーを追加できます。この場合、最初の 100 人のユーザーをサーバー A、次の 100 人をサーバー B に割り当てることができます。また、障害への適応力を提供できるようサーバーをクラスター化することも可能です。

障害への適応力

ユーザー数が増えると、QlikView へのユーザーの障害適応力も高まります。QlikView Server をクラスター化すると、構成に障害への適応力を組み込むことができます。単一のサーバーでは 100 人のユーザーをサポートできる上記の例の場合、障害への適応力を構成に組み込むために、3 台のサーバーが使用されます。これにより、1 台のサーバーを使えなくなっても (ハードウェアの故障などにより)、システムはまだ 200 人のユーザーに対応できます。3 台のサーバーすべてがアクティブなノードであれば、すべてのサーバーをフル稼働しなくても応答時間を短縮することができます。また、ノードが失われた場合でも影響されるユーザー数を少なくできます。

QlikView ではセッション復元のオプションが一切提供されていません。実際には、QlikView クラスターのノードが失われるとユーザーが実行していた分析も失われ、クラスターに再接続して作業を再開することになります。ただしこれは、QlikView アプリケーション内のデータが失われてリロードが必要になるということではありません。データはファイル システムの QlikView ドキュメント ファイルに保存されています。アプリケーションで何を選択してあったのかが失われてしまうのみです。

負荷分散

QlikView の構成では、QVS クラスター内にあるすべてのマシンの能力をフル活用するために、負荷分散アルゴリズムを採用しています。どの QVS を使うかは、AccessPoint が稼働する Web サーバーにより決定されます。QVS の負荷分散方法には、3 つのオプションがあります。参照 : *QVS の負荷分散オプション (page 56)*。

クラスタ化ーされた QlikView 構成の要件

クラスター化された QlikView 構成の構築には、3 つの高レベルの必要条件があります。

- クラスター化された QlikView Server のライセンス キー
- ルートフォルダー用の共有ストレージ領域
- 同じビルド番号

クラスター化された QlikView Server のライセンス キー

クラスター化された環境では、QlikView Server マシンは同じライセンス キーを使ってインストールされます。これはクラスター化できるよう有効にしておかなくてはなりません。ライセンス認証ファイル (LEF) で以下のエントリを調べると確認できます。

```
NUMBER_OF_CLUSTER_NODES; 2 (クラスタ内のノード数)
```

クラスター化された QlikView Server は共有ストレージを介して構成とライセンス情報をサーバー間で共有するため、構成およびライセンス管理はすべてのノードで QlikView 管理コンソール (QMC) から 1 回だけ実行する必要があります。

サーバーは同じネットワーク サブネット上にインストールし、ルート ドキュメント ディレクトリを共有しなくてはなりません。これは共有ネットワーク ストレージの要件になります。構成情報は Persistent Global Objects (*.pgo*) ファイルに保存されます。

10 分たってもサーバーを起動または リセットできない場合は、上記の LEF エントリをチェックしてください。これは通常、許可されている数よりも多くのマシンに QlikView Server がインストールされていることを示しています。

共有ネットワークストレージ

QlikView では、QlikView Server クラスターでアクセスする必要がある QlikView ドキュメントを保存するために、共有ネットワークストレージが必要です。共有ネットワークストレージは、*.pgo* (Persistent Global Objects) ファイル、*.meta* ファイル、および共有ファイル (*.Shared* または *.TShared*) の保存にも使用されます。共有ネットワークストレージを構成すると、クラスターのノード全体で共有する協同オブジェクトも有効になります (.shared ファイルを使用)。

QlikView Server 内の共有ネットワークストレージの要件は次のとおりです。

- ネットワークストレージは、Windows ベースのファイル共有でホストする必要があります。
- QlikView Server (QVS) は、Windows Server 2008 R2 (またはそれ以降) にマウントされ、そのサーバーから共有される SAN (NetApp、EMCなど) の使用をサポートします。
- ファイル共有サーバーに接続するには、クラスター内の QlikView Server ノードのネットワーク遅延が 4 ミリ秒未満である必要があります。そうでない場合、パフォーマンスが低下する可能性があります。
- ファイル共有への帯域幅は、サイトのトラフィック量に適切である必要があります。リロード後に保存され、メモリに開かれるドキュメントの頻度とサイズによって、この要件が決まります。1 ギガビット ネットワーキングをお勧めします。
- 次の共有ストレージ オプションはサポートされていません。
    - Linux OS ベースの共有ストレージ システムはサポートされていません。これには、SMB ファイル共有プロトコルまたは NTFS ディスク ドライブ フォーマットをサポートするシステムが含まれます。
    - CIFS ファイル共有プロトコルに依存する Windows ベースの共有ストレージ システムはサポートされていません。
    - QlikView は Windows Distributed File System (DFS) をサポートしていません。

> *サポートされていないシステムのタイプでファイルをホストすると、不安定な QVS クラスターが作成され、CAL が消失して QVS が止まる可能性があります。*

> *QlikView Server 11.20 から QlikView Server 12.10 以降にアップグレードするときに、バックエンドファイル システムが原因でインストールに各種の問題が発生する場合があります。QlikView Server 12.10 以降のバージョンではディスクをより集中的に使用するので、QlikView 11.20 より大規模なファイル サーバーを必要とします。QlikView 展開を計画する場合には、ストレージの種類およびリソース容量に留意することが重要です。詳細については、次の Qlik サポートの記事を参照してください。「QlikView and its backend File Share System」(QlikView とそのバックエンド ファイル共有システム)*

> *QlikView では、Windows Distributed File System (DFS) をサポートしていません。*

厳密に必要ではありませんが、次の操作も適切です。

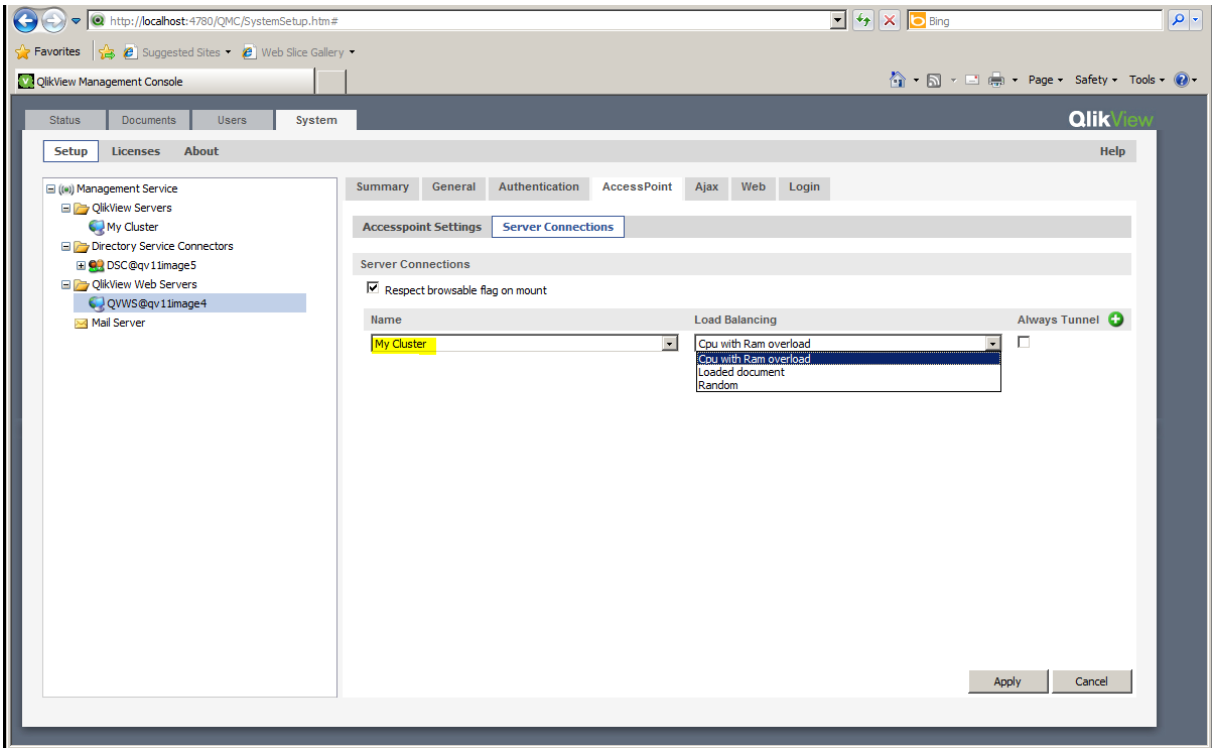
- クラスター内のすべての QlikView Server が到達可能な共有の共有フォルダーへの一時ファイルの代替パスを設定します。
- 拡張機能を使用している場合は、共通の共有フォルダーへの代替拡張パスを設定します。
- 共通の共有フォルダーへのログ フォルダーを設定します。

QVS の負荷分散オプション

QVS は 3 つの負荷分散戦略をサポートしています。

- Random (ランダム) (既定設定): ラウンド ロビン タイプの戦略で、セッションがクラスターのノード全体で配布されるため、ほとんどのユーザーに適しています。
- Loaded document (ロード済みドキュメント): 同じドキュメントのセッションが同じサーバーにルーティングされている場合に使用されます。この戦略は、クラスター内の単一のノードよりも多いドキュメントを取り扱うことができる構成向けです。AccessPoint は、ドキュメントがすでにロードされているかどうか、またサーバー上で利用できる RAM の容量に基づいて決定を下します。
- RAM がオーバーロードしているCPU (CPU with RAM overload): QlikView Web Server (QVWS) は、(1) RAM と (2) CPU 使用率という2 つの要素に基づいてトラフィックをルーティングできます。ノードは以下の基準を使用して選ばれます。
  - すべての利用可能なノードで RAM をすでに利用 (低レベル) できる場合は、最低 CPU 使用率のノードを選択します。
  - 利用可能なあらゆるノードで RAM の使用量が中程度の場合は、利用可能な RAM が最も多いノードを選びます。

QVS 負荷分散戦略を設定するには、QMC で **[System]** (システム) > **[Setup]** (設定) > **[QlikView Web Servers]** の順に選択してください。**[AccessPoint]** タブで Web サーバーを選択します。



負荷分散オプションの場所。

Web Server の負荷分散

ネットワーク ロード バランサーは AccessPoint の障害への適応力を提供し、利用可能な AccessPoint サーバーにセッションをルーティングします。この機能はサードパーティのソフトウェアとハードウェアによるものです。

ロード バランサーに関してはいくつかの要件があります。

- セッションの持続性/スティッキー セッションのサポート: 通常、クッキーを使用することでユーザー セッションをクラスター内の同じノードで存続できるようにします。
- Availability (可用性): ロード バランサーは AccessPoint のウェブ サーバーとQlikView サーバーの可用性をチェックします。
- ロード バランス アルゴリズムの何らかの形で、どのサーバーのロードが最も少ないか判定します。

セッションの持続性

ユーザーのセッションを一貫して同じサーバーにルーティングすることが要件になっています。これを行う方法はデバイスによって異なります。利用可能なオプションについては、ロード バランサー文書を参照してください。

可用性のチェック

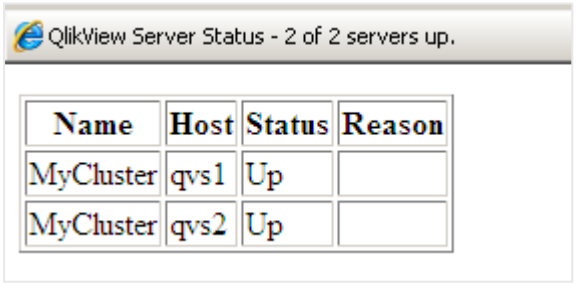
AccessPoint の特別な Web ページでは、システムのステータスを自動的にチェックできます。

http://myAccessPoint/QvAjaxZfc/QvsStatus.aspx

AccessPoint とクラスター内の少なくとも 1 つの QlikView Server が応答する場合、このページは 200 の http ステータス コードを戻します。このページが返すその他のステータス コードは、エラーとみなされます。このページの一般的なエラーには以下のようなものがあります。

- 404: The AccessPoint is unable to respond. Check the web server. (404: AccessPoint は応答できません。Web サーバーの設定を確認してください。)
- 503: No QlikView Servers responded to the AccessPoint and therefore it cannot service user requests. (503: QlikView Server は AccessPoint に応答しないため、ユーザーのリクエストに対応できません。)

QlikView Server クラスターのステータスも Web ページに表示されます。

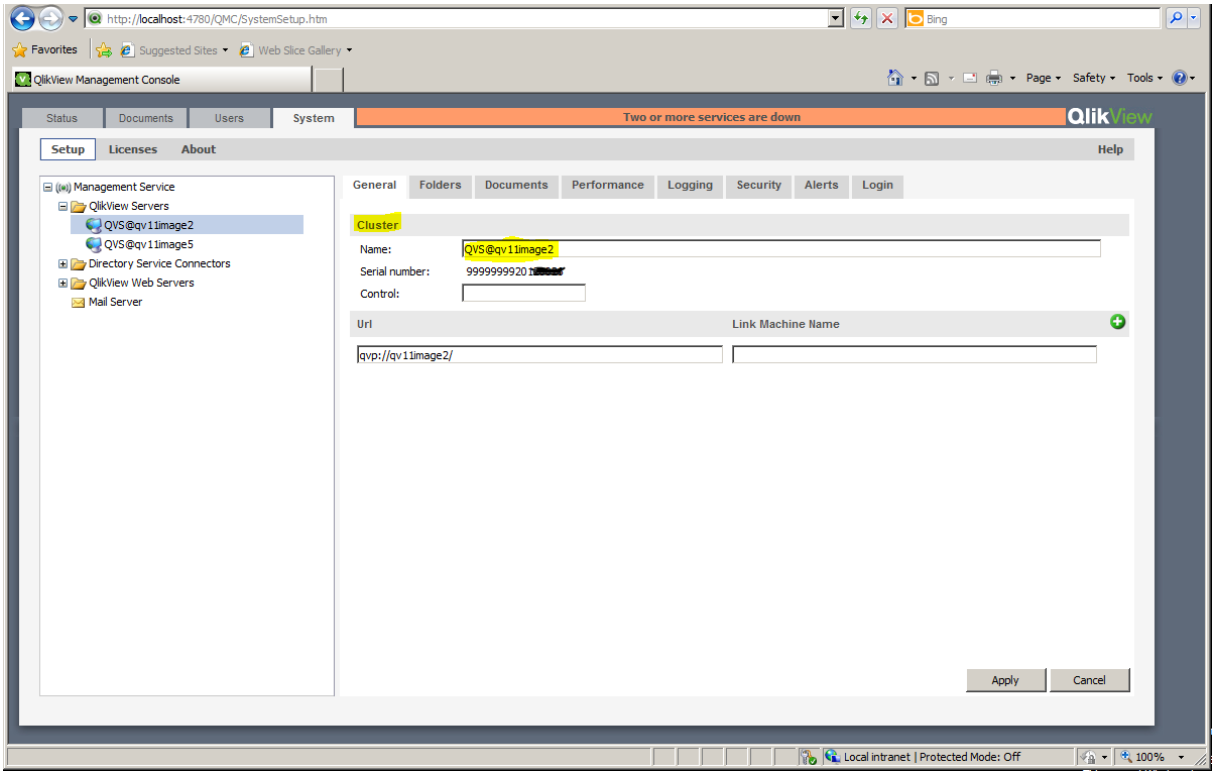


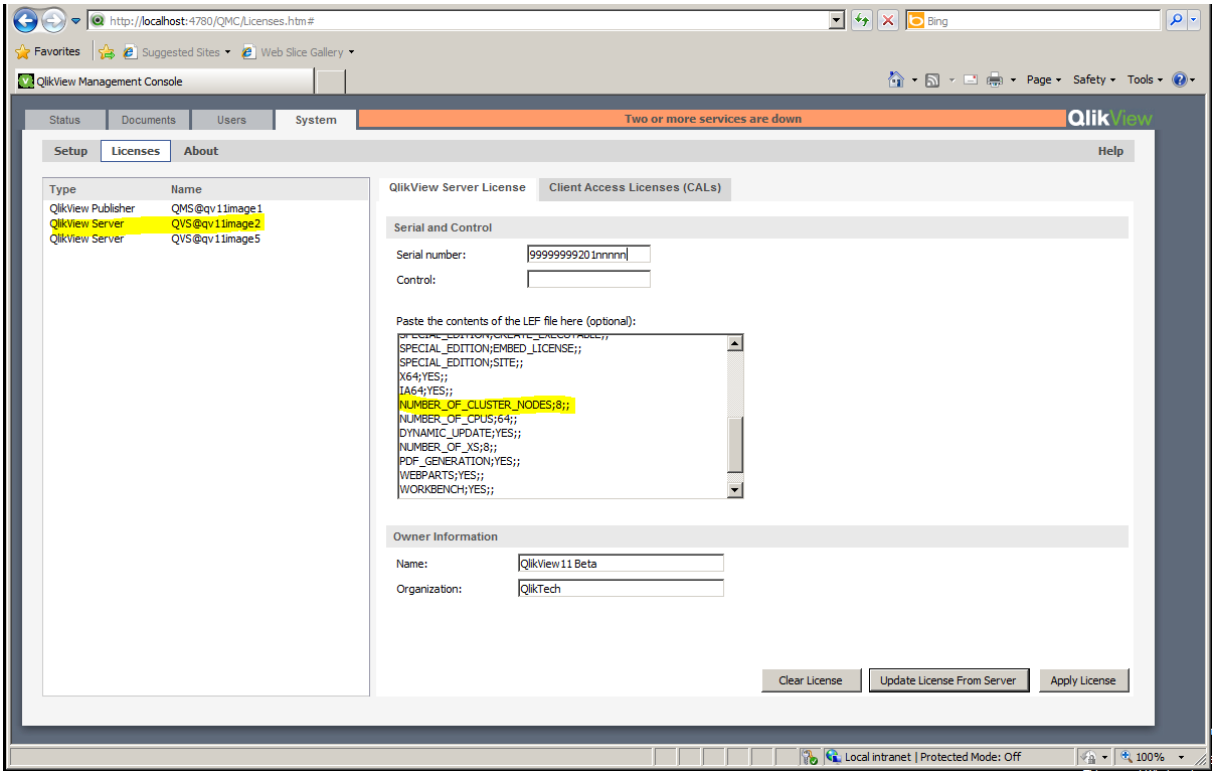
QlikView Server ステータス画面。

QlikView クラスターの構築とインストール

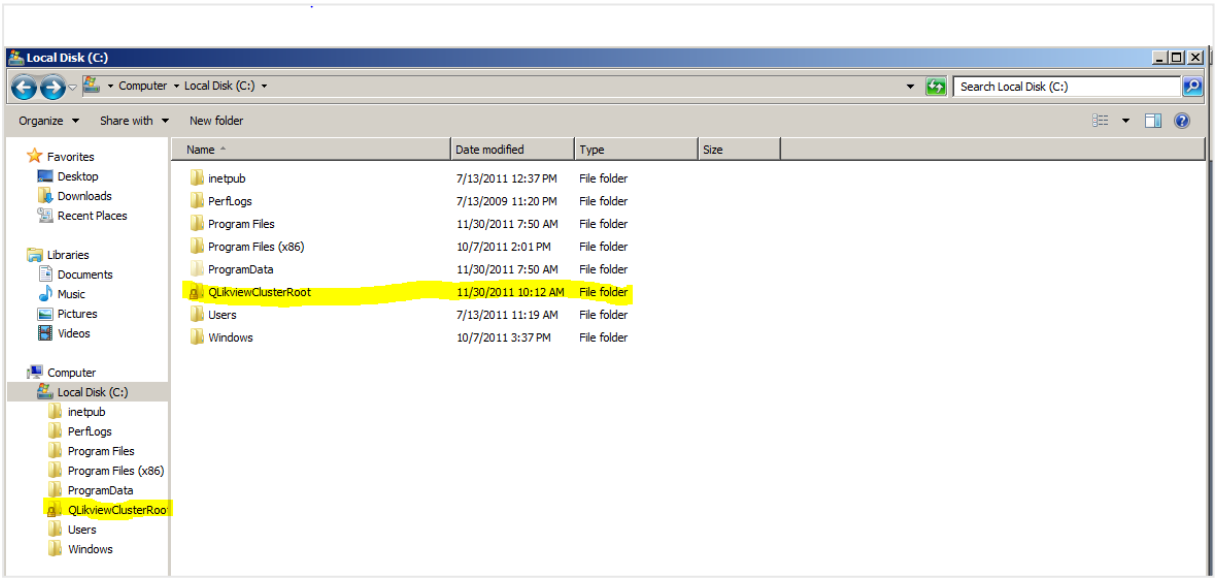
QMC を使用して QlikView Server クラスターを構成、有効化するには、以下の手順に従ってください。

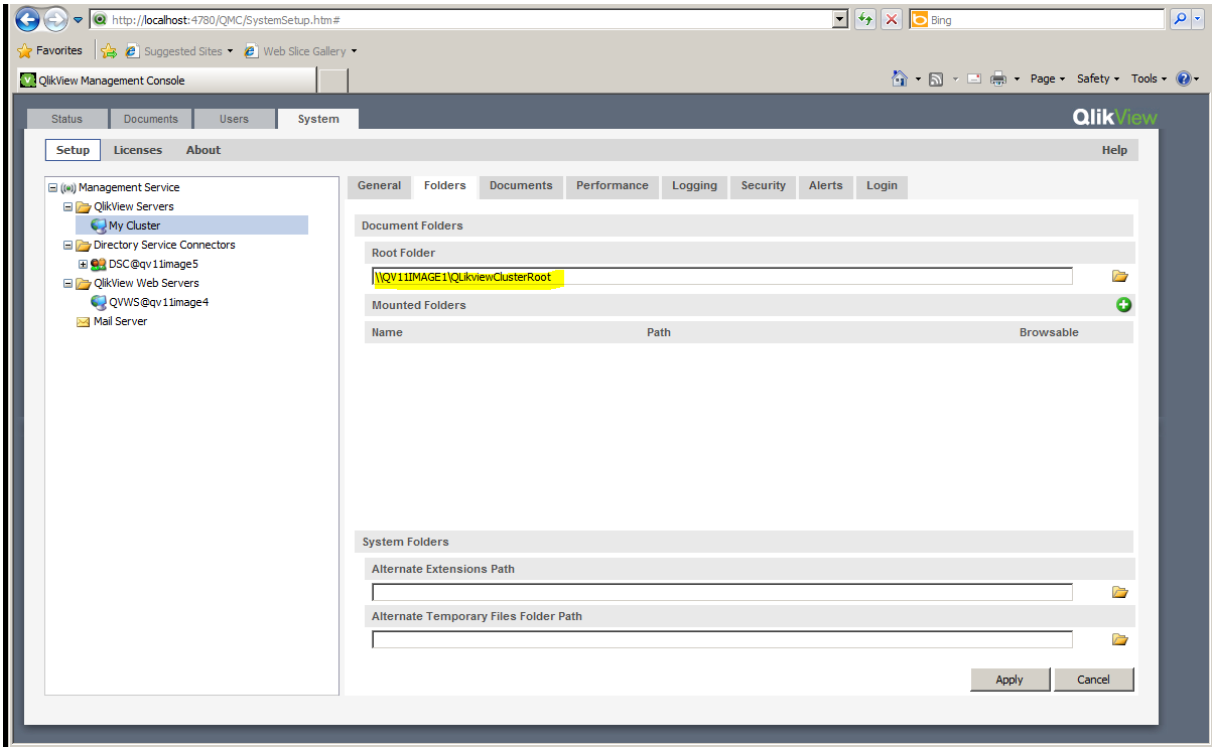
1. クラスターに最初の QlikView Server をインストールしてライセンスを授与します。これは QlikView Server の最初のコピーです。



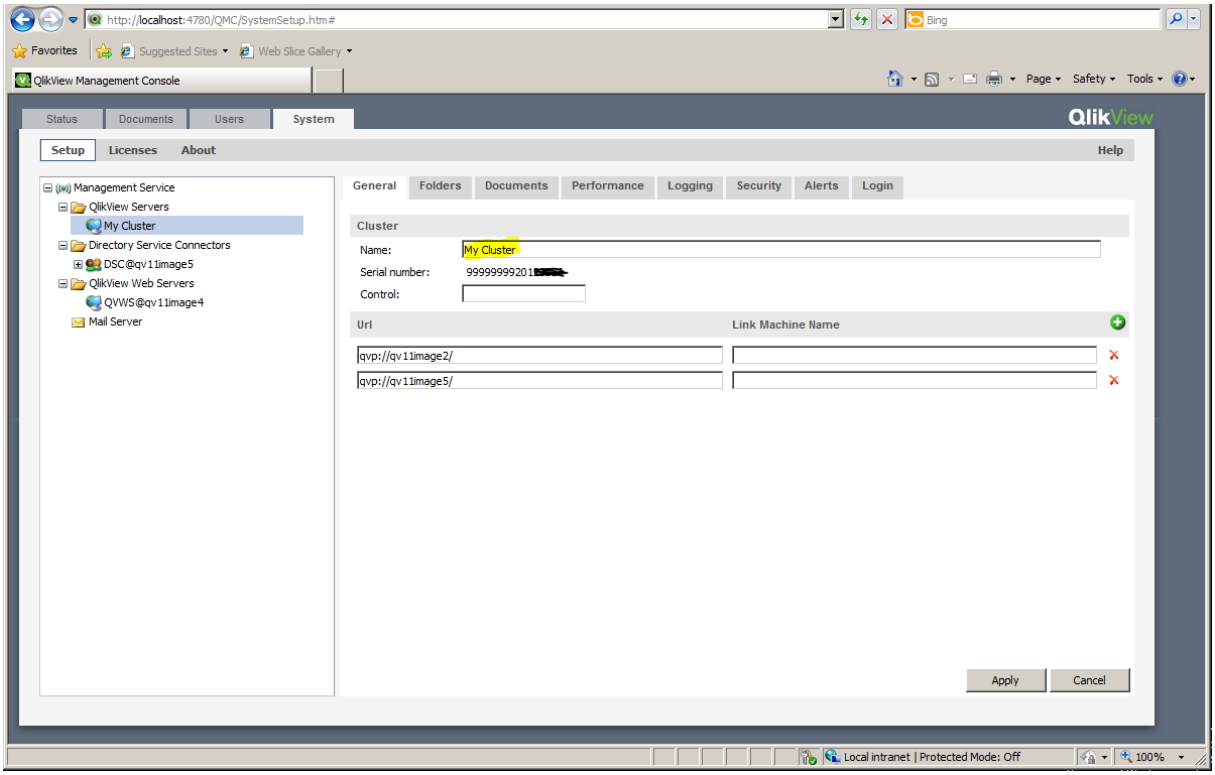


2. クラスター内のすべての QlikView Server がアクセスできるファイル システム上のフォルダーを指すよう、ドキュメント フォルダーを構成します。

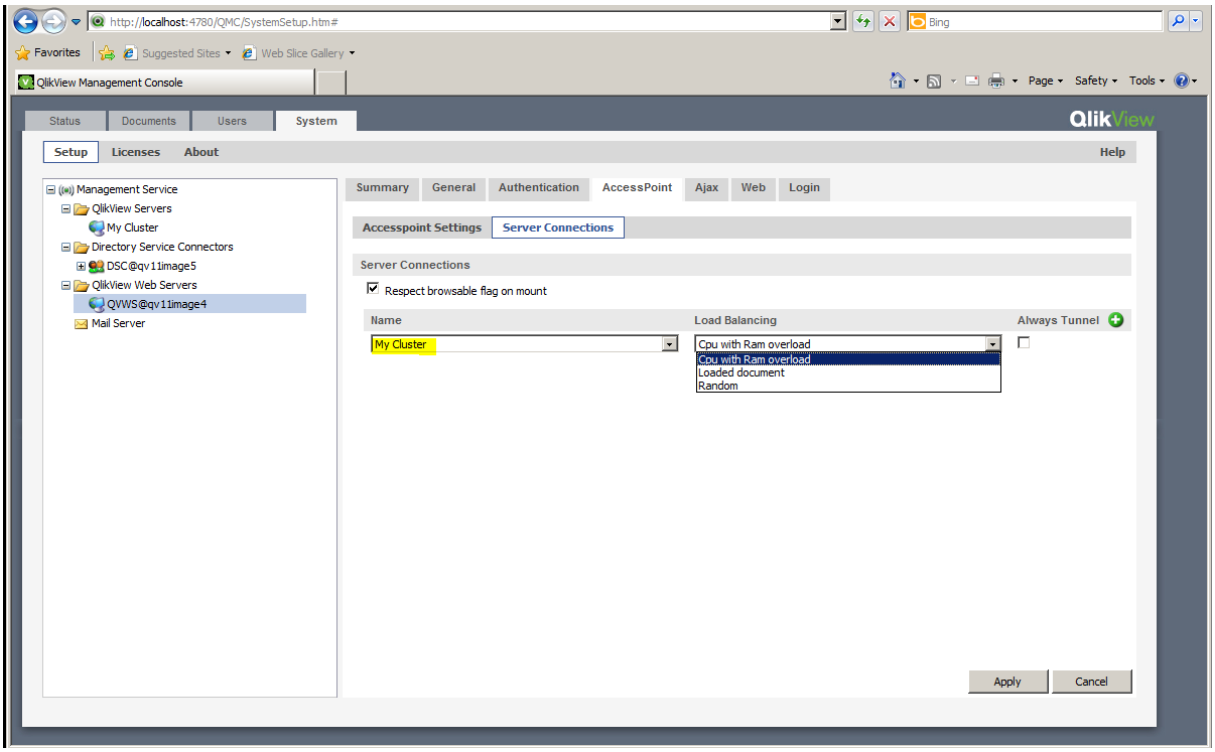




3. クラスターに次の QlikView Server をインストールします。
4. すべての QlikView サービスがローカル管理者として実行され、「QlikView Administrators」ローカル グループのメンバーであることを確認します。
5. QMC で **[システム (System)]** > **[設定 (Setup)]** を開き、サーバーを選択します。その後、**[General (基本設定)]** タブに進み、ライセンスのコントロール番号と、クラスターの 2 番目の QlikView Server へのアドレスを入力します。
6. クラスターの名前を適切な名前に変更します。
7. クラスターの QlikView Server ノードでステップ 3 ~ 5 を繰り返します。



8. AccessPoint の設定で、クラスターが **[Server Connections (サーバー接続)]** で選択されていることを確認します。



9. これでクラスターの設定は終了し、使用準備が整いました。

QlikView Server クラスターからのノードの削除

次の手順を実行します。

1. QMC の [**システム**] タブに移動し、[**QlikView Server**] を選択します。
2. QVS クラスターを強調表示して削除するノードを特定し、 を選択します。
3. ライセンス コントロール キーを入力し、[**適用**] を選択します。
4. QlikView Server サービス (QVS) を再始動します。

不均衡な QVS クラスタリング

デフォルトで、QlikView Server (QVS) クラスターでは CPU、コア、および RAM についてすべてのノードが平等である必要があります。ただし、ハードウェア仕様が異なるノードを使用することはできます。不均衡なクラスターの設定は、性能の異なるコンピュータをクラスター化する必要がある場合や、サイズが異なるドキュメントを処理する必要がある場合に有用です。

QVS 不均衡クラスタリングを有効化するには、*ActivateUnbalancedCluster* 構成を変更します。*ActivateUnbalancedCluster* を有効化することにより、QlikView 管理コンソール (QMC) で CPU affinity とワーキング セットを設定することはできなくなります。代わりに、クラスターの各ノードで QlikView Server (QVS) *Settings.ini* ファイルを編集することにより、クラスターの設定を管理します。

この機能を使用する場合、完全な **CPU Affinity** のみがサポートされます (コアの 100%)。

不均衡なクラスターを設定する際は、負荷分散アルゴリズムをアクティブ化する必要があります。これは、特定のニーズに合わせて構成できます。次を参照してください: *負荷分散アルゴリズムのカスタマイズ (page 63)*。

> *不均衡な QVS クラスターを設定することにした場合、不均衡なノードをクラスターに追加する前に、以下の初期設定を完了することが推奨されます。*

QVS 不均衡クラスターの設定

QVS 不均衡クラスターの設定手順は、クラスターが QlikView Web Service (QVWS) とMicrosoft IIS (QV 設定サービス) のどちらを使用しているかによって異なります。

QVWS を使用した不均衡 QVS クラスタリング

次の手順を実行してください。

1. *QVManagementService.exe.config* ファイルで、*ActivateUnbalancedCluster* 構成を *true* に設定します。デフォルトで、ファイルは *C:\Program Files\QlikView\Management Service* に入っています。
2. *QVWebServer.exe.config* ファイルで、*UnbalancedClusterLoadBalancer* 構成パラメータを *true* に設定します。デフォルトで、ファイルは *C:\Program Files\QlikView\Server\Web Server* に入っています。
3. QlikView 管理コンソール で、[**システム**] メニューに進み、[**セットアップ**] を選択し、サービスのリストから [**QlikView Web Servers**] を選択し、[**AccessPoint**] タブ、[**サーバー接続**] に進んで、[**負荷分散**] 項目で [**CPU の RAM オーバーロード**] オプションを選択して、不均衡クラスター環境のアルゴリズムを利用します。

過去にロードされたドキュメントに重みを付与するよう負荷分散アルゴリズムををカスタマイズする場合、*UnbalancedClusterLoadBalancerLoadedDocWeight* を *UnbalancedClusterLoadBalancerCpuWeight* と *UnbalancedClusterLoadBalancerRamWeight* より高い値に設定します。
UnbalancedClusterLoadBalancerLoadedDocWeight の値の設定方法については、「*負荷分散アルゴリズムのカスタマイズ (page 63)*」を参照してください。

Microsoft IIS を使用した不均衡 QVS クラスタリング
Microsoft IIS を使用している場合、Internet Information Services (IIS) Manager を使用して IIS 設定に次のパラメータを追加する必要があります。

次の手順を実行してください。

1. *QVManagementService.exe.config* ファイルで、*ActivateUnbalancedCluster* 構成を *true* に設定します。デフォルトで、ファイルは *C:\Program Files\QlikView\Management Service* に入っています。
2. Internet Information Services (IIS) Manager を起動します。
3. 左側のナビゲーション メニューで、QlikView サービスをインストールするサイトをクリックします。インストールの設定により、**デフォルト ウェブ サイト** または別のカスタム サイトです。
4. 中央ペインの [**ASP.NET**] セクションで、[**アプリケーション設定**] をクリックします。
5. 右側の [**アクション**] ペインで、[**追加...**] をクリックすると、[**アプリケーション設定の追加**] ウィンドウが開きます。[**名前:**] の下に *UnbalancedClusterLoadBalancer* を入力し、[**値:**] の下には *true* と入力します。[**OK**] をクリックしてアクションを確認します。
6. 右側の [**アクション**] ペインで、もう一度 [**追加...**] をクリックします。[**アプリケーション設定の追加**] ウィンドウで、[**名前:**] の下には *UnbalancedClusterLoadBalancerCpuWeight* を、[**値:**] の下には *5* を入力します。[**OK**] をクリックしてアクションを確認します。
7. 右側の [**アクション**] ペインで、もう一度 [**追加...**] をクリックします。[**アプリケーション設定の追加**] ウィンドウで、[**名前:**] の下には *UnbalancedClusterLoadBalancerRamWeight* を、[**値:**] の下には *3* を入力します。[**OK**] をクリックしてアクションを確認します。
8. 右側の [**アクション**] ペインで、もう一度 [**追加...**] をクリックします。[**アプリケーション設定の追加**] ウィンドウで、[**名前:**] の下には *UnbalancedClusterLoadBalancerLoadedDocWeight* を、[**値:**] の下には *3* を入力します。[**OK**] をクリックしてアクションを確認します。
9. QlikView 管理コンソール で、[**システム**] メニューに進み、[**セットアップ**] を選択し、サービスのリストから [**QlikView Web Servers**] を選択し、[**AccessPoint**] タブ、[**サーバー接続**] に進んで、[**負荷分散**] 項目で [**CPU の RAM オーバーロード**] オプションを選択して、不均衡クラスター環境のアルゴリズムを利用します。
過去にロードされたドキュメントに重みを付与するよう負荷分散アルゴリズムををカスタマイズする場合、*UnbalancedClusterLoadBalancerLoadedDocWeight* を *UnbalancedClusterLoadBalancerCpuWeight* と *UnbalancedClusterLoadBalancerRamWeight* より高い値に設定します。
UnbalancedClusterLoadBalancerLoadedDocWeight の値の設定方法については、「*負荷分散アルゴリズムのカスタマイズ (page 63)*」を参照してください。

負荷分散アルゴリズムのカスタマイズ

必要に応じて負荷分散アルゴリズムの重みをカスタマイズできます。手順は、クラスターが QlikView Web Service (QVWS) と Microsoft IIS (QV 設定サービス) のどちらを使用しているかによって異なります。

QVWS の負荷分散アルゴリズムをカスタマイズする

インストールで QVWS を使用している場合、*QVWebServer.exe.config* ファイル (*C:\Program Files\QlikView\Server\Web Server*) で次の設定を編集します。この手順では、QVS *Settings.ini* ファイルも変更する必要があります。

1. *UnbalancedClusterLoadBalancerCpuWeight* を 0 ~ 10 の値に設定します。高い値は、負荷分散アルゴリズムでどの QVS クラスター ノードを使ってドキュメントを開くかを決定する際に、処理能力により重みを付与する必要があることを示します。
2. *UnbalancedClusterLoadBalancerRamWeight* を 0 ~ 10 の値に設定します。高い値は、負荷分散アルゴリズムでどの QVS クラスター ノードを使ってドキュメントを開くかを決定する際に、RAM パフォーマンスにより重みを付与する必要があることを示します。
3. *UnbalancedClusterLoadBalancerLoadedDocWeight* を 0 ~ 10 の値に設定します。高い値は、負荷分散アルゴリズムでどの QVS クラスター ノードを使ってドキュメントを開くかを決定する際に、QVS クラスター ノードにロードされたドキュメントの数により重みを付与する必要があることを示します。
4. ローカル ノードの QVS *Settings.ini* ファイルに、CPU Affinity 設定がないことを確認してください。デフォルトで、このファイルは *C:\ProgramData\QlikTech\QlikViewServer* にあります。
   次が存在する場合は削除します:
   ```
   MaxCoreMask
   MaxCoreMaskHi
   MaxCoreMaskGrp1
   MaxCoreMaskGrp1Hi
   MaxCoreMaskGrp2
   MaxCoreMaskGrp2Hi
   MaxCoreMaskGrp3
   MaxCoreMaskGrp3Hi
   ```
5. ワーキング セットの下限と上限は、デフォルトでそれぞれ 70 と90 に設定されています (RAM 使用率 %)。必要に応じて古い設定を削除するか、ローカル ノード QVS *Settings.ini* ファイルでカスタマイズされたレベルに変更します。
   ```
   WorkingSetSizeLoPct=nn
   WorkingSetSizeHiPct=nn
   ```
6. 関与するすべてのシステムを再起動します。

Microsoft IIS の負荷分散アルゴリズムをカスタマイズする

Microsoft IIS をウェブ サーバーとして使用するインストールの負荷分散アルゴリズムをカスタマイズするには、Internet Information Services (IIS) Manager を使用することにより次の設定を編集します。

1. Internet Information Services (IIS) Manager を起動します。
2. 左側のナビゲーション メニューで、QlikView サービスをインストールするサイトをクリックします。インストールの設定により、**デフォルト ウェブ サイト** または別のカスタム サイトです。
3. 中央ペインの [**ASP.NET**] セクションで、[**アプリケーション設定**] をクリックします。
4. *UnbalancedClusterLoadBalancerCpuWeight* 設定を選択します。右側の [**アクション**] ペインで、[**編集...**] をクリックすると、[**アプリケーション設定の編集**] ウィンドウが開きます。[**値:**] お下に、0 ~ 10 の値を入力します。高い値は、負荷分散アルゴリズムでどの QVS クラスター ノードを使ってドキュメントを開くかを決定する際に、処理能力により重みを付与する必要があることを示します。[**OK**] をクリックしてアクションを確認します。

5. *UnbalancedClusterLoadBalancerRamWeight* 設定を選択します。右側の [**アクション**] ペインで、[**編集...**] をクリックすると、[**アプリケーション設定の編集**] ウィンドウが開きます。[**値:**] お下に、0 ~ 10 の値を入力します。高い値は、負荷分散アルゴリズムでどの QVS クラスター ノードを使ってドキュメントを開くかを決定する際に、RAM パフォーマンスにより重みを付与する必要があることを示します。[**OK**] をクリックしてアクションを確認します。
6. *UnbalancedClusterLoadBalancerLoadedDocWeight* 設定を選択します。右側の [**アクション**] ペインで、[**編集...**] をクリックすると、[**アプリケーション設定の編集**] ウィンドウが開きます。[**値:**] お下に、0 ~ 10 の値を入力します。高い値は、負荷分散アルゴリズムでどの QVS クラスター ノードを使ってドキュメントを開くかを決定する際に、QVS クラスター ノードにロードされたドキュメントの数により重みを付与する必要があることを示します。[**OK**] をクリックしてアクションを確認します。
7. 関与するすべてのシステムを再起動します。

QlikView Publisher のクラスタリング

本章では、QlikView Publisher の概要と、スケーラビリティ、障害への適応力、または双方のクラスター化された構成でこれを使用する方法について説明します。また、本章ではアーキテクチャとインストール要件のほか、クラスター化された障害への適応力のある QlikView Publisher の構成を構築するオプションについても取り扱います。

はじめに

QlikView Publisher は QlikView Server のモジュール オプションで、QlikView の分析、アプリケーション、レポートの単一のコントロール ポイントを提供するスケジュール、管理、マネジメント ツールです。管理者は、企業全体で QlikView アプリケーションおよびレポートのセキュリティとアクセスをスケジュール、配信、管理することができます。

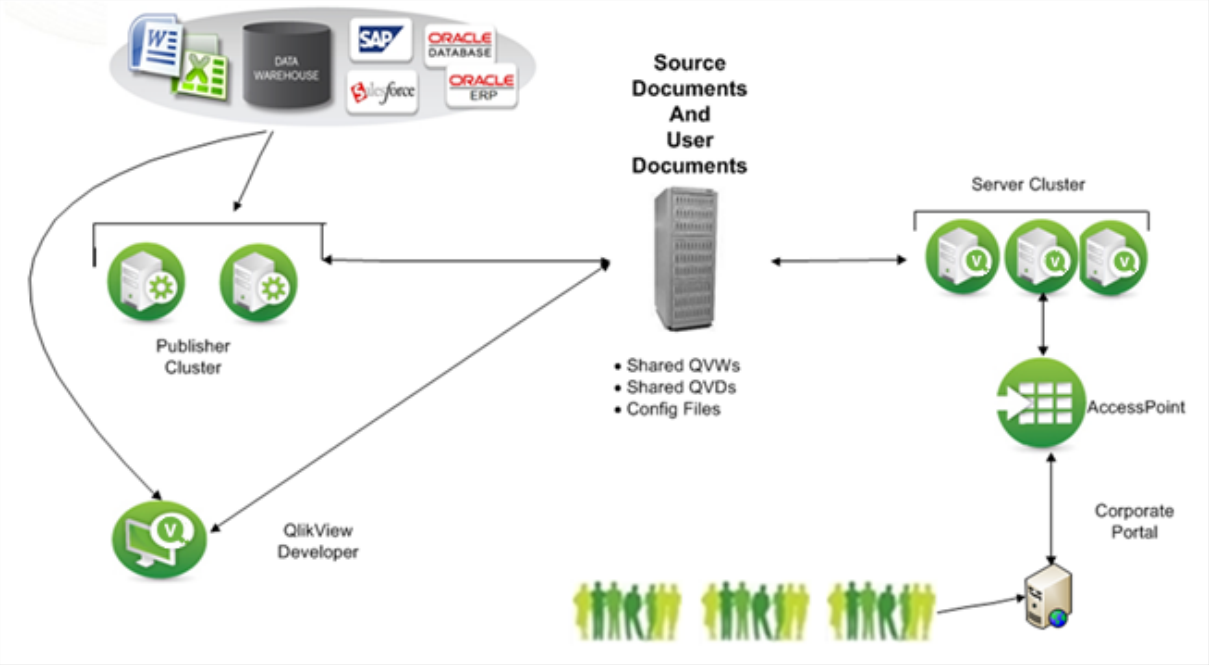
QlikView Publisher は以下の主な機能を実行します。

- ソース QlikView ドキュメント ファイルの接続文字列で定義されたデータ ソースから直接データをロードします。
- これは、さまざまなルール (ユーザー認証やデータ アクセスなど) に基づいてソース QlikView ドキュメント ファイルからのデータとアプリケーションを「分割」し、これらの新規作成ドキュメントを適切な QlikView Server に、またはメールを介した静的レポートとして分散するための配布サービスとして使用されます。
- QlikView Publisher を使用する際は、Publisher のみがデータのロードと配信用のソース ドキュメント フォルダとデータ ソースにアクセスできます。QlikView ユーザーはソース ドキュメントとデータにアクセスできません。

クラスター化されたアーキテクチャを配置することにより、QlikView Publisher はウェブ サービス技術を使用してスケーラビリティや障害への適応力を達成します。管理者はサービスをクラスター化して、ロード バランスを提供することができます。SNMP のネイティブ サポートは、ツールをモニタリングするエンタープライズ システムとの統合を有効にします。外部エンタープライズ スケジューリング ツールはウェブ サービスの呼び出しを使用して Publisher のタスクをトリガーできます。タスクは、QlikView 管理者がオンデマンドでスケジュールして実行することもできます。

以下の図は、異なるタスクとロード バランスを処理するように構成された 2 サーバーのクラスター化 QlikView Publisher を示しています。また、この図にはロード バランスで QlikView AccessPoint を使用する 3 サーバーの

クラスター化 QlikView Server も含まれています。QlikView Developer によって作成されたドキュメントはソース ドキュメント フォルダに保存されます。QlikView Publisher タスクはデータを取得して、その結果をユーザー ドキュメント フォルダに保存するために使用します。



負荷が不均衡なサービス クラスターを設定する方法については、「*不均衡 QlikView Publisher クラスタリング (page 76)*」を参照してください。

[Source Documents] (ソース ドキュメント)

ソース ドキュメントには、a) さまざまなデータ ソース (データ ウェアハウス、Microsoft Excel ファイル、SAP、Salesforce.com など) からデータを抽出するための QlikView ドキュメント ファイル内のスクリプト、b) *.qvd* ファイル内の実際のバイナリデータ抽出、c) コードの 1 行でデータ モデルを継承した別の QlikView ドキュメント ファイルからのバイナリデータが含まれています。

QlikView Developer を使用して作成した QlikView ソース ドキュメントは以下のフォルダにあります。

- Windows Server 2008以降: *\ProgramData\QlikTech\SourceDocuments*. これは Windows Server 2008 以降の QlikView のデフォルトの場所です。

ユーザー ドキュメント

ユーザー ドキュメント フォルダは、QlikView Server で使用するリポジトリです。フォルダは以下の場所にあります:

- Windows Server 2008以降: *\ProgramData\QlikTech\Documents*。これは Windows Server 2008 以降の QlikView のデフォルトの場所です。

タスク

タスクは、データの配信およびデータのリロード用に管理者によって作成されます。タスクは、XML ファイルのコレクションとして QlikView Publisher リポジトリ、または SQL Server データベースに保存されます。タスクを実行すると、QlikView Publisher は QlikView Batch (QVB) を呼び出します。これはユーザー インターフェースのない

QlikView Desktop に類似しています。

> *QlikView Batch (QVB) はグラフィカル オブジェクトやユーザー入力オブジェクトに対応していません。このため、QVB はユーザー入力の必要なスクリプトなどを含むドキュメントをリロードできません。*

QVB は、ソース ドキュメント フォルダに保存されているドキュメントをリロードし、連想型 QlikView データベースを作成します。これは各ドキュメント内に保存されます。QVB はデータ ソースからロード スクリプトによって説明されているデータを取得することによりリロードを実行します。QlikView Publisher は、暗号化された QVP プロトコルを使用して QlikView Server のユーザー ドキュメント フォルダにドキュメントを配信し、クラウド環境、メール サーバーやファイル フォルダにも配信します。QlikView Publisher は Directory Service Connector (DSC) を使用して、ドキュメントを配信する場所と宛先を判定することができます。

QlikView Publisher をクラスター化する理由

QlikView における Publisher の役割は、QlikView 管理者が設定した基準に従ってデータを配信、更新することです。これを行うため、Publisher はスケジュールどおり、またはオンデマンドで多くのタスクを実行します。Publisher のタスクは、クラスターで配信できる最小のエンティティです。単一のタスクを分割して複数のクラスター ノードで並行して実行することはできません。複数のサーバー上で Publisher サービスをクラスター化すると、管理者は Publisher ロード バランス アルゴリズムを使用して並行して作動している複数のサーバーに複数のタスクを配信できます。つまり、Publisher クラスターはデータの分散配信とリロードのスケーラビリティ、利用設定、サービス性を向上させるために使用できます。

さらに、Publisher クラスター ライセンスは クラスターにおける Publisher サービスおよび独立した Publisher サービスの構成を有効にします。たとえば、Publisher クラスターは、大量のデータおよびタスクを取り扱うために企業のオフィスで使用できます。また、単一の Publisher サービスは、Publisher が製造データ ソースを使用してドキュメントの配信のみを行う関連製造工場で使用できます。

QlikView Publisher をクラスター化すると、以下の目標を満たすことができます。

- 水平スケーラビリティ
- 障害への適応力

水平スケーラビリティ

ハードウェアを水平に拡張すると、QlikView の構成のリソースを増やすことができます。ハードウェア サーバーを追加すると、QlikView Publisher のワークロードを増やせます。クラスター化された Publisher サーバーはその後、QlikView タスクの負荷を分散するように構成できます。

たとえば、特定のハードウェア サーバーでは、QlikView Publisher は 8 件のタスクを同時に処理できます。リソースを増やす必要がある場合、QlikView Publisher サービスは必要に応じて拡張できます。新しいハードウェア サーバーで QlikView Publisher サービスを追加すると、Publisher クラスターの構成で追加サーバーを設定して最高 16 件のタスクを取り扱うことができます。このシナリオでは、最初の 8 件のタスクがサーバー A、次の 8 件のタスクがサーバー B に割り当てられています。また、サーバーがクラスター化されている場合は、2 つのサーバーでタスクの負荷を分散することもできます。

障害への適応力

構成に含まれているタスクの数が増えると、タスクを時間通りに完了する期間がますます重要になります。QlikView 配信サービスをクラスター化すると、構成で障害への適応力を得られます。上記の場合は、単一のサーバーが 100 件の同時タスクをサポートでき、構成に障害への適応力をつけるために追加サーバーを構成で

きます (サーバーは合計 3 台)。サーバーが失われた場合でも (ハードウェアの故障やネットワーク接続の問題など)、障害許容クラスターは最高 200 件のタスクをサポートします。3 台のサーバーすべてがアクティブなノードであれば、すべてのサーバーをフル稼働しなくても応答時間を短縮することができます。また、ノードが失われた場合は、タスクとタスクチェーンの数を限定します。

クラスター化された QlikView Publisher 構成の要件

クラスター化された QlikView Publisher の構成では、以下の高レベルの要件を満たす必要があります。

- クラスター化された QlikView Publisher のライセンス キー
- 共有ネットワーク ストレージ
- ロード バランス戦略

クラスター化された QlikView Publisher のライセンス キー

クラスター化された環境では、QlikView Publisher サーバーは同じライセンス キーでインストールされます。これは、ライセンス認証ファイル (LEF) で以下のエントリを調べると確認できます。

PRODUCTLEVEL;30;; (30 は QlikView Publisher のコード)

NUMBER_OF_XS;N;; (N は許可されている QlikView Distribution Services の数)

クラスター化された QlikView Publisher 構成のサーバーは、共有ストレージを介して相互に構成とライセンス情報を共有します。このため、構成およびライセンス管理は、すべてのノードについて QMC で 1 回だけ行う必要があります。

共有ネットワーク ストレージ

QlikView の共有ネットワーク ストレージは、QlikView Publisher クラスターでアクセスする必要のあるソース (.qvf または .qvw) およびクラスター ファイル (通知、タスク、トリガー、ログなど) を格納するために使用できます。

QlikView Publisher クラスター内の共有ネットワーク ストレージの要件は次のとおりです。

- ネットワーク ストレージは、Windows ベースのファイル共有でホストする必要があります。
- QlikView Publisher は、Windows Server 2008 R2 (またはそれ以降) にマウントされ、そのサーバーから共有される SAN (NetApp、EMCなど) の使用をサポートします。SAN を介してサーバーに示されるストレージは、ローカルで接続されたストレージとして表示されます。SAN ストレージが Publisher で使用される場合、QlikView Server によってアクセスされる配信データは SAN ストレージ上にはありません。
- ファイル共有サーバーに接続するには、クラスター内の QlikView Publisher ノードのネットワーク遅延が 4 ミリ秒未満である必要があります。そうでない場合、パフォーマンスが低下する可能性があります。
- QlikView Publisher クラスター内の最大 2 つのノードが同じ共有ストレージを共有できます。3 つ以上の QlikView Publisher ノードが必要な場合は、追加のクラスターに追加の Publisher ノードを展開することをお勧めします。QlikView 管理コンソールは複数の Publisher クラスターを管理できます。
- ファイル共有への帯域幅は、サイトのトラフィック量に適切である必要があります。リロード後に保存され、メモリに開かれるドキュメントの頻度とサイズによって、この要件が決まります。1 ギガビット ネットワーキングをお勧めします。
- 次の共有ストレージ オプションはサポートされていません。
    - Linux OS ベースの共有ストレージ システムはサポートされていません。これには、SMB ファイル共有プロトコルまたは NTFS ディスク ドライブ フォーマットをサポートするシステムが含まれます。

- CIFS ファイル共有プロトコルに依存する Windows ベースの共有ストレージ システムはサポートされていません。
- QlikView は Windows Distributed File System (DFS) をサポートしていません。

ロード バランス戦略

ロード バランス

ロード バランスは メモリ使用量とCPU 使用率に基づき、内部のランキング システムによって決定されます。Qlik では、広範にテストされているデフォルトの設定を使用するよう推奨しています。

デフォルトの設定を変更するには、*QlikViewDistributionService.exe.config* という構成ファイルを編集します。キーは JavaScript で記述されています。

```
<add key="LoadBalancingFormule" value="(AverageCPULoad*400) + ((MemoryUsage / TotalMemory) *
300) + ((NumberOfQlikViewEngines / MaxQlikViewEngines)*200) + (NumberOfRunningTasks*100)"/>
```

ここではそれぞれ以下に該当します。

- `AverageCPULoad`: 起動しているすべての QVB の平均 CPU 負荷。
- `MemoryUsage`: アプリケーション全体の合計 メモリ使用量。
- `TotalMemory`: サーバーのメモリ量の合計。
- `NumberOfQlikViewEngines`: 現在使用されている QlikView エンジンの数。
- `MaxQlikViewEngines`: QlikView エンジンの最大数として設定された値。
- `NumberOfRunningTasks`: 現在実行中のタスクの数。

同時タスク

デフォルトで、4 つの QlikView タスクを単一のノード上で同時に実行できます。推奨される最大数は、ノード当たり8 件の同時タスクです。10 件以上のタスクを単一のノードで同時に実行する必要がある場合は、Windows レジストリで修正を行い、さらに多くの同時タスクを実行できるようにデスクトップのヒープ サイズを変更する必要があります。

> *10 件以上の同時タスクを実行するには、大規模なサーバーが必要です。また、Publisher タスク向けにサーバーをさらに追加することもできます。*

同時に実行できるタスクの数を変更するには、以下の手順を実行してください。

1. Windows Server レジストリをバックアップします。
2. 以下の Windows Server レジストリ設定を見つけます。

   ```
   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session\Manager\SubSystems\Windows
   %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
   SharedSection=1024,3072,512 Windows=On SubSystemType=Windows
   ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3
   ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off
   MaxRequestThreads=16
   ```

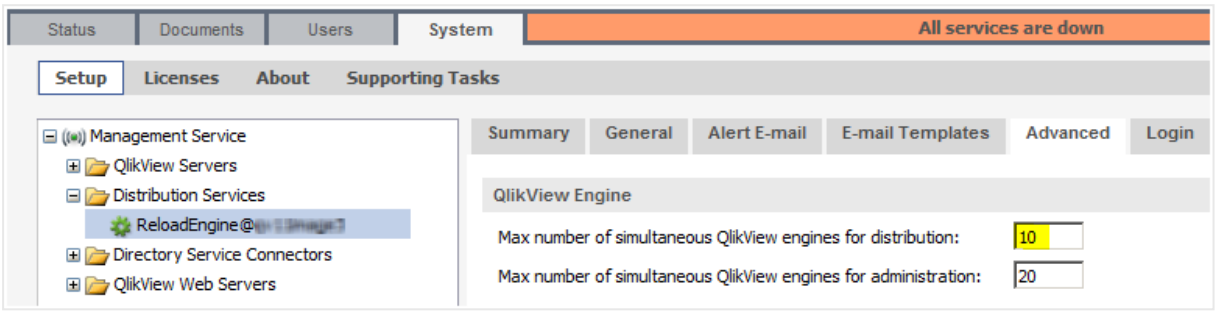
   `SharedSection` の既定値は 64 ビット (x64) では 1024,20480,768 です。

3. `SharedSection` を 1024,20480,2048 に設定し、デスクトップのヒープ サイズを変更します。

   ```
   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session\Manager\SubSystems\Windows
   %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
   SharedSection=1024,20480,2048 Windows=On SubSystemType=Windows
   ```

```
ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3
ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off
MaxRequestThreads=16
```

4. レジストリの変更を保存し、コンピュータを再起動します。
5. QMC の **[配信用同時 QlikView エンジンの最大数 (Max number of simultaneous QlikView engines for distribution)]** 設定を必要なエンジン数に変更します。

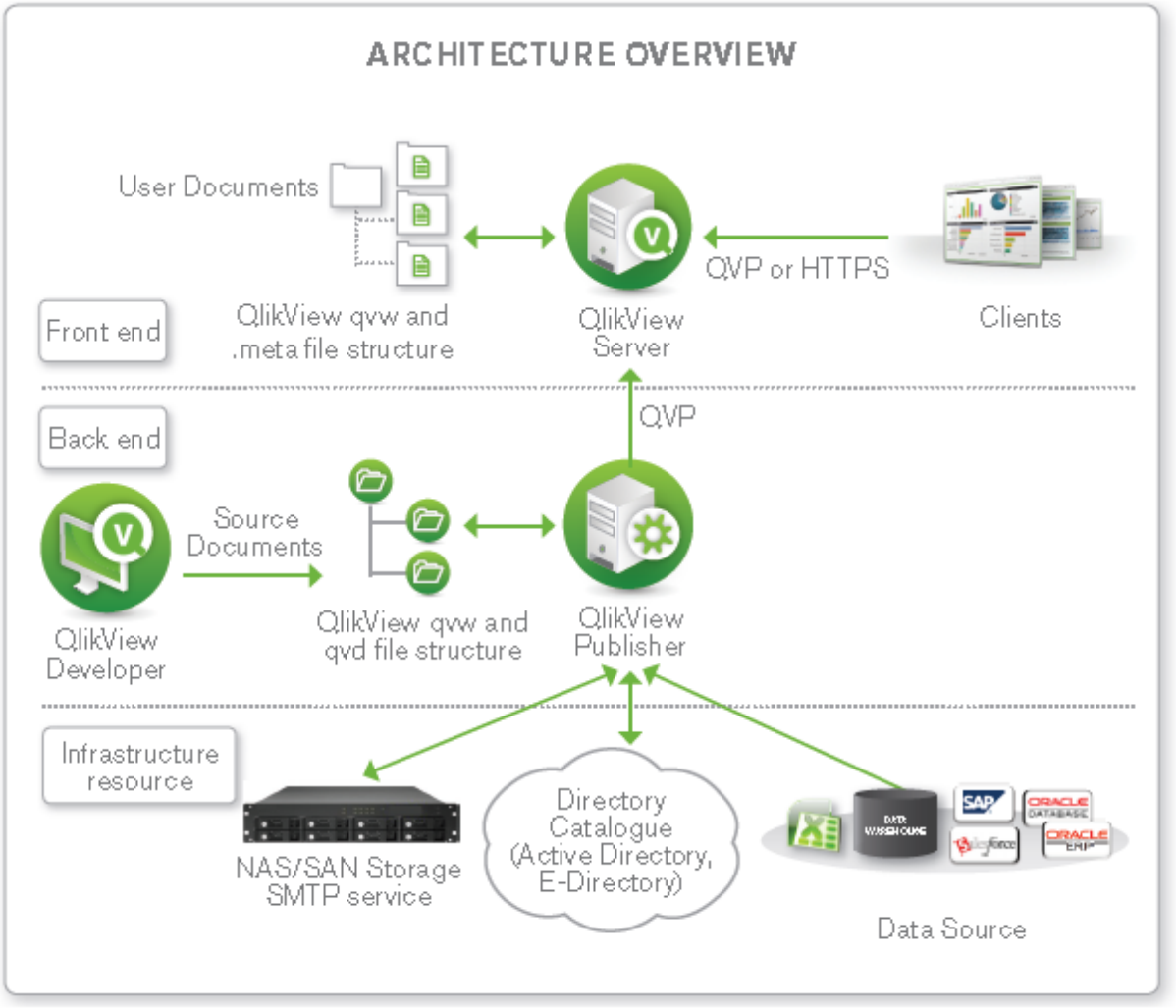


セキュリティ

QlikView Publisher は QlikView アプリケーションおよびデータへのアクセスを提供します。このため、QlikView Server の標準的なセキュリティ機能に加えて、QlikView Publisher をエンタープライズ セキュリティ ソリューションに統合することが重要になります。

QlikView Publisher は QlikView ソリューション内でバックエンドプロセスとして表示されます。セキュリティの観点から、フロントエンドにバックエンドへのオープン ポートがないことを理解しなくてはなりません。フロントエンドはバックエンドのデータ ソースにクエリを送信せず、ユーザー ドキュメント (`.qvf` または `.qvw` ファイル) にはバックエンドにあるデータ ソースへの接続文字列は含まれていません。エンドユーザーはフロントエンドにある QlikView ドキュメントにのみアクセスできます。バック エンド内では、Windows ファイル システムが常に許可を行っています。QlikView はアクセス権限を管理しません。

以下の図は、QlikView 製品とデータおよびアプリケーションを含む標準的な QlikView の構成を簡素化したものです。



ディレクトリサービス

QlikView ドキュメント向けのセキュリティを提供するために、QlikView Publisher を外部ディレクトリサービス (Active Directory、LDAP、データベース、その他のサインオン ソリューションなど) に接続することができます。外部ディレクトリサービスは、QlikView が信頼関係を築いている認証ソースです。

QlikView は内蔵ディレクトリサービス プロバイダ (DSP) を備えており、QlikView 管理者は Active Directory のユーザー権限を QlikView ドキュメントやその一部に割り当てることができます。QlikView Publisher はこの内蔵プロバイダを活用して、Active Directory との直接的な統合を提供するとともに、これをサポートしています。

QlikView は他のディレクトリサービス向けに構成可能な LDAP を作成する手段も提供しています。構成可能な LDAP を使用すると、QlikView 管理者は Active Directory 以外の認証システムによって認証されているユーザーに権限を授与できます。

QlikView Server の許可モード

QlikView Server は、QlikView ドキュメントへのアクセスを許可するための相互に排他的な 2 つのオプションを提供します。QlikView Server (NTFS または DMS) の許可モードに応じて、Publisher はドキュメントへの権限

を割り当てる際、適切な Access Control List (ACL) に表示します。NTFS 許可の場合、Publisher はドキュメントを QlikView Server に送信する際、標準的な NTFS ACL を表示します。DMS 許可では、Publisher はアプリケーションに関連する *.meta* ファイル内に含まれている ACL を表示します。

静的データ削除

データ分割は、行レベルのセキュリティ設定に基づいて QlikView アプリケーションからアプリケーション データを削除できるセキュリティのメカニズムです。QlikView Publisher は該当するセキュリティのシナリオとは関係なくデータ分割を自動化できます。ただし、Publisher では、管理者はカスタムまたは Active Directory DSP を介して利用できる外部認証ソース内で定義されたユーザーあるいはグループに基づいてデータ分割を構成できます。Publisher は、QlikView で「ループと分割 (Loop&Reduce)」機能を使用してデータ分割を行います。Publisher データ分割は、Section Access に関連している動的データ分割と混同しないでください。

QlikView Publisher クラスター化の構成

このセクションの手順は、Windows Server 2008 R2以降で有効です。

要件

QDS クラスター構成を開始する前に以下の要件を満たす必要があります。

- 複数の QDS をサポートする QlikView Publisher ライセンス。Publisher LEF には NUMBER_OF_XS;N;; のエントリを含める。ここで N は 2 以上。
- QlikView AccessPoint (QlikView Web Server または Microsoft IIS ベース)、QlikView Management Service (QMS)、QlikView Server (QVS)、DSC がすでにネットワーク内の QlikView システムにインストールされている。
- 各コンピュータで QlikView サービスを実行するドメイン・ユーザーを使用できる。
- 共有ストレージ デバイスとして、Qlik では Windows ベースのファイル共有としてマウントされた共有デバイスを推奨。

  すべての QDS クラスター ノードでは、以下の中央に保存されたデータへの読み取り・書き込みアクセスが必要。

  - QlikView Publisher ステータス、構成、ログ ファイル
  - QlikView ソース ドキュメント

段階的な手順

共有ストレージ デバイスの準備

各 Publisher クラスター ノードでアクセスされるファイル用のフォルダを作成します。

- \\<*server1*>*ProgramData**QlikTech**DistributionService* (application folder)
- \\<*server1*>*ProgramData**QlikTech**SourceDocuments* (source documents folder)

クラスター化 ノードの準備

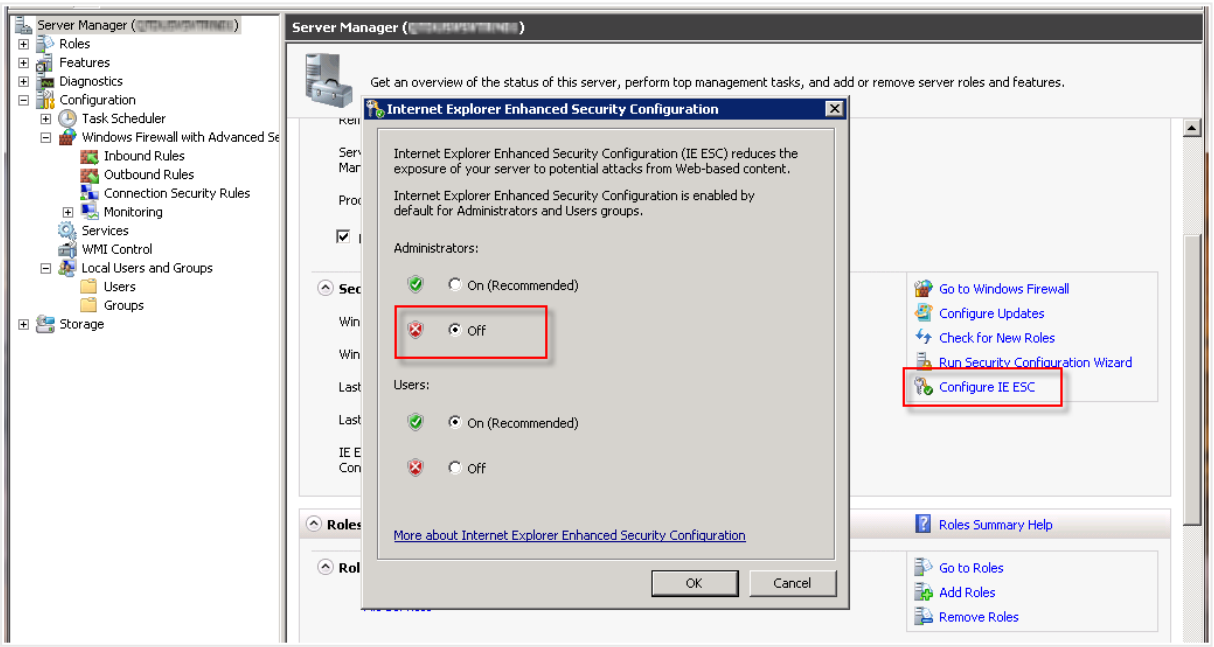
予定されている各 QDS クラスター ノードで以下の手順に従います。

1. 管理者としてログインします。
2. QlikView ソリューションを保護するためにファイアウォールを構成します。QlikView サービスでは、以下のテーブルに含まれているポートを開いておく必要があります。

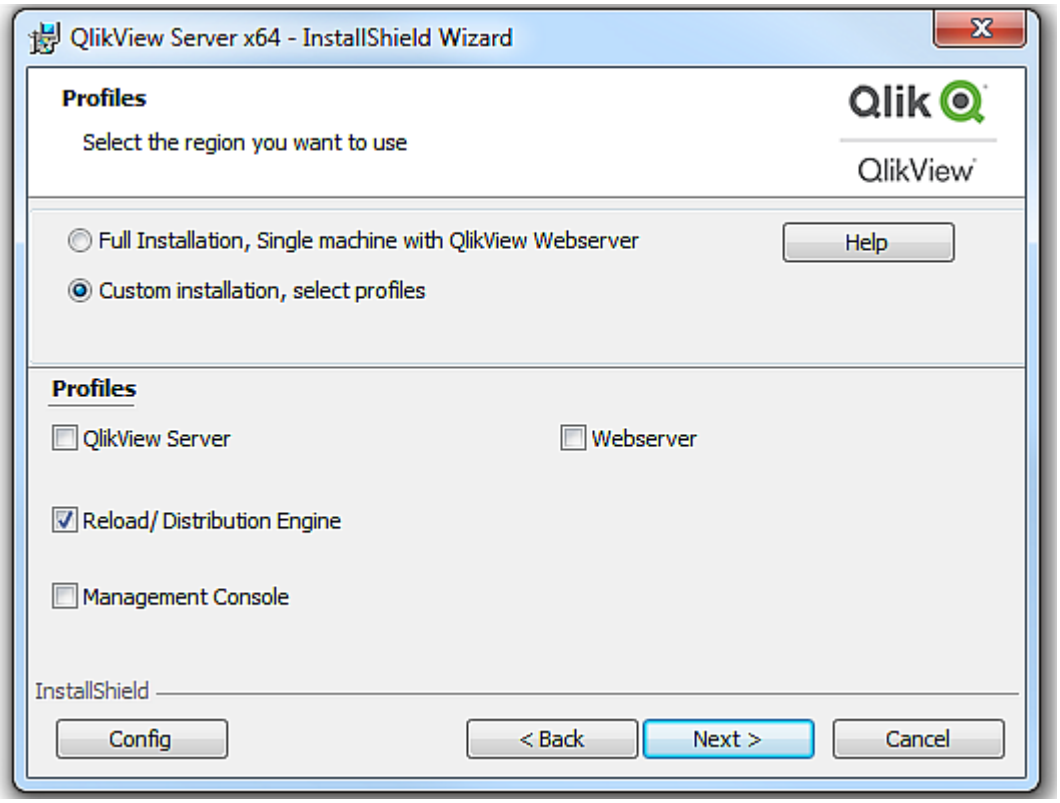
開く必要のあるポート

Service	ポート
QDS (Publisher) (Publisher で必要)	4720/TCP
DSC (Publisher で必要)	4730/TCP
QMS (Publisher で必要)	4780/TCP
QlikView Web Server/Microsoft IIS 構成	4750/TCP
QVS 構成	4749/TCP
QVP 通信	4747/TCP
QMS (EDX 呼び出し) (Publisher で必要)	4799/TCP

3. 管理者用の Internet Explorer Enhanced Security Configuration を非アクティブにします。デフォルトで、Windows Server 2008以降はこの構成が有効にされた状態で発送されます。これは基本的にロックダウンされたバージョンで、ウェブ参照用にサーバーにわずかながらセキュリティを追加します。構成を有効にすると、QMC とサービス コンテンツの表示で問題が発生する可能性があります。Internet Explorer Enhanced Security Configuration はオンのままにしておけますが、問題が発生した場合は Administrators グループでこの機能をオフにしてください。



4. QlikView サービスの実行に使われるドメイン ユーザーを Local Administrators Group に追加します。
5. QlikView 64-bit (x64) サーバー設定を起動し、**[カスタム インストール (Custom installation)]** を選択してからプロファイルを選びます。その後、**[リロード/配信エンジン (Reload/Distribution Engine)]** 機能を選択し、Publisher がある各ノードでこれをインストールします。

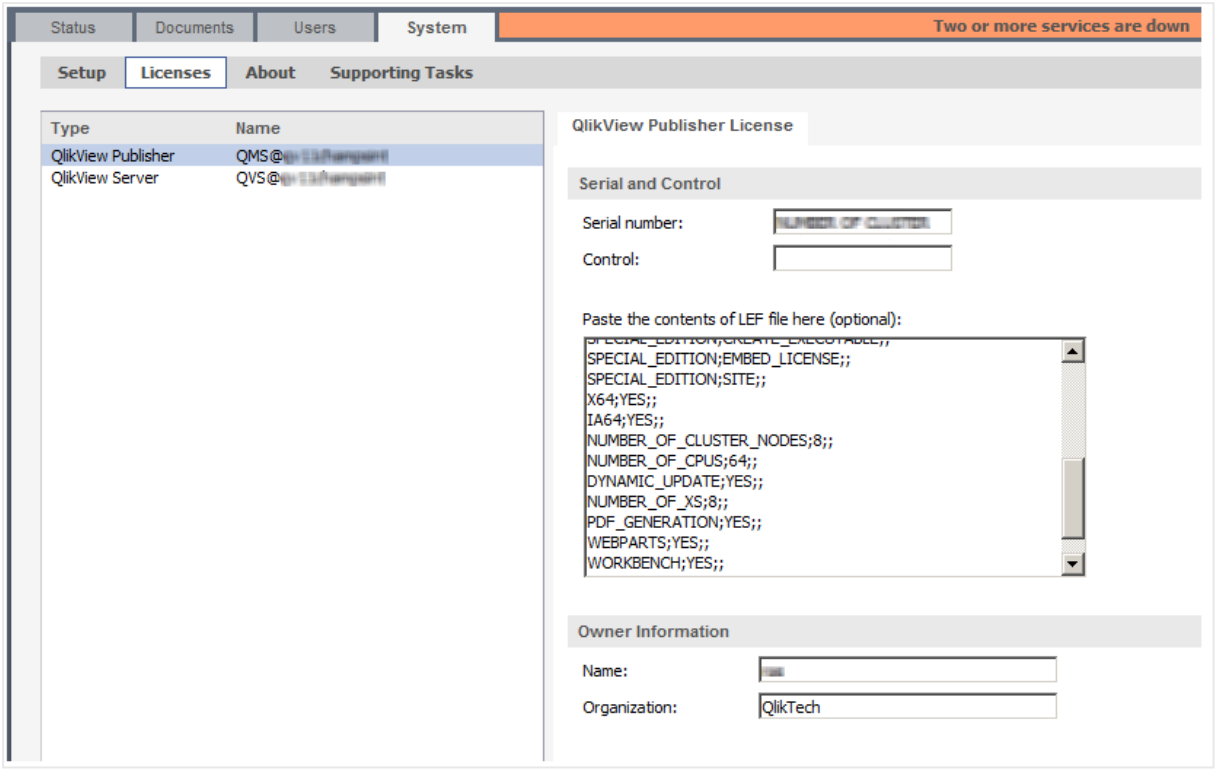


6. QlikView サービス アカウントの資格情報を入力します。
7. 設定を終了してシステムをすぐに再起動します。

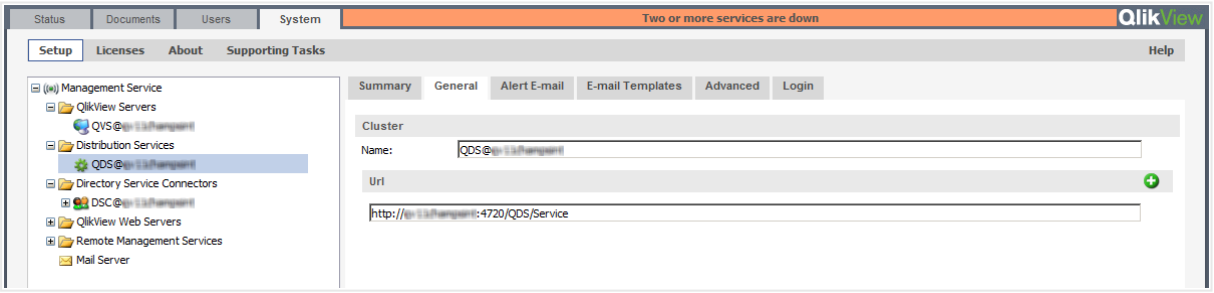
QMC での QDS クラスターの構成

QMC で QDS クラスターを構成するには以下の手順に従ってください。

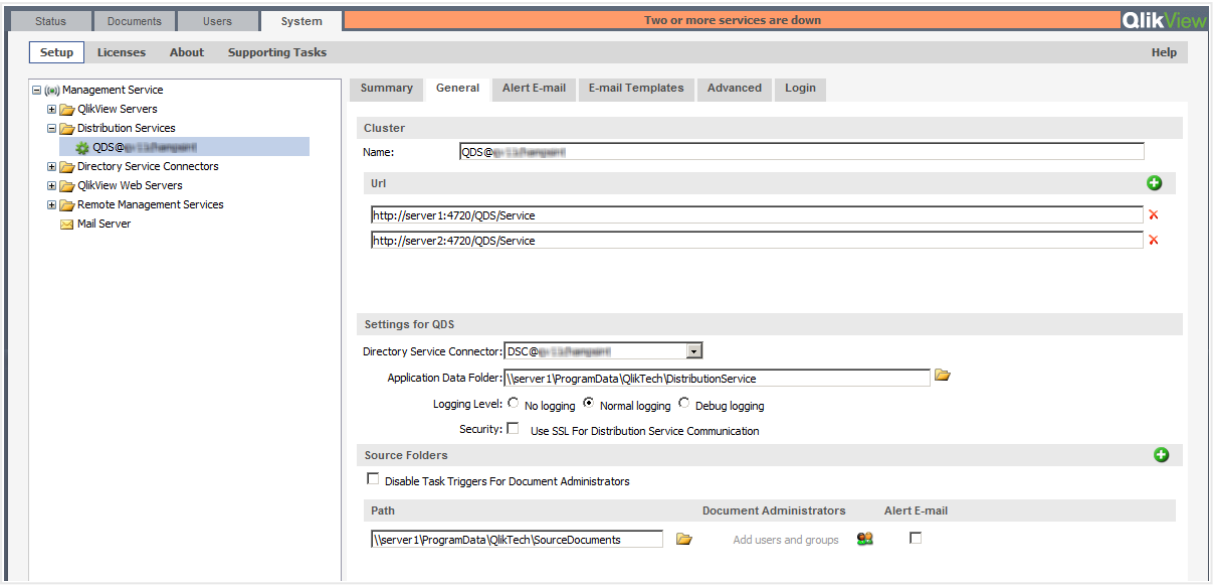
1. QMC を開き、アクティブにしたクラスター モデルを使って QlikView Publisher ライセンスを登録します。



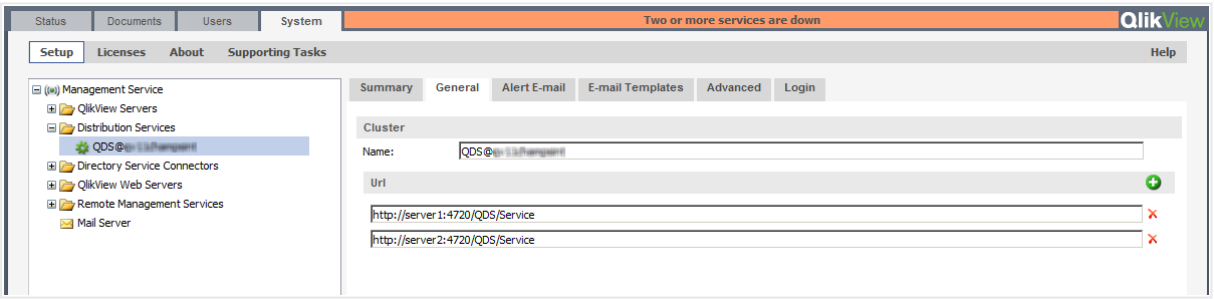
2. **[システム (System)]** > **[設定 (Setup)]** タブで **[配信サービス (Distribution Services)]** に最初の QDS クラスター ノードを追加します。



3. UNC 構文を使い、**[アプリケーション データ フォルダ (Application Data Folder)]** と **[ソース フォルダ (Source Folders)]** を共有デバイス フォルダ パスに切り替えます。



4. **[適用 (Apply)]** をクリックして、QDS を手動で再起動します。
5. 各追加 QDS クラスター ノードを URL 形式で追加します。



6. **[適用 (Apply)]** をクリックして、あらゆるノードで QDS を手動で再起動します。

不均衡 QlikView Publisher クラスタリング

本章では、クラスター化された不均衡な QlikView Distribution Service (QDS) の展開を構築するための要件とオプションについて説明します。既定では、QlikView Distribution Service クラスターにおいてはすべてのノードが CPU、コア、および RAM に関して均等であることが必要です。

クラスターを設定するには QlikView Publisher のライセンスが必要です。QlikView Publisher の詳細については、「*QlikView Publisher のクラスタリング (page 65)*」ページを参照してください。

QlikView の負荷分散機能は QlikView Management Console に含まれています。本章では、配布グループを使用してこのコンポーネントを効率化する方法についても取り上げます。

QDS Publisher グループとは?

Publisher グループは QDS クラスターのサブセットです。各 Publisher グループには、一意の名前と、そのグループに含まれる QDS ノードセット (1 つまたは複数) が付与されます。ノードが属する Publisher グループ数に制限はありません (ゼロでも複数でも可能)。

タスクはそれぞれ、Publisher グループのいずれかのグループに割り当てられているか、まったく割り当てられていないかのどちらかです。Publisher グループに割り当てられているタスクは、Dedicated Task (専用タスク) と呼ばれ、そのグループに属するいずれかの QDS ノードのみで実行できます。どの Publisher グループにも割り当てられていないタスクは、Regular Task (通常タスク) と呼ばれ、どの QDS ノードでも実行できます (ただし、特定の条件下にある Publisher グループの QDS では実行できないこともあります)。

QDS クラスターは、この機能をアクティブ化する前に設定して機能するようにしておく必要があります。

この機能をアクティブ化するには、*DistributionGroupDefinition.Template* のコピーを *C:\ProgramData\QlikTech\ManagementService\DistributionGroups* に作成し、名前を *DistributionGroupDefinition.xml* に設定します。QDS クラスター ノードの QMS サービスを手動で再起動してください。

QDS Publisher グループの構成

配布グループは *DistributionGroupDefinition.xml* ファイルの次の設定を使用して構成できます。

```
<DistributionGroupDefinition>   <QDSSettings>     <QDS QDIdentifier = "d033930c-0000-e6ec-
1519-f3c628a443ae">       <MaxSimultaneousQvbs>4</MaxSimultaneousQvbs>
<MaxSimultaneousReaderQvbs>2</MaxSimultaneousReaderQvbs>
<DedicatedQvbs>1</DedicatedQvbs>       <RunDedicatedTaskAlone>True</RunDedicatedTaskAlone>
  <GraceTimeMinutes>30</GraceTimeMinutes>       <DistributionGroups>          <Group>Group
A</Group>          <Group>Group B</Group>       </DistributionGroups>     </QDS>
</QDSSettings> </DistributionGroupDefinition>
```

Publisher グループの各 QDS について次の構成を行う必要があります。

- *MaxSimultaneousQvbs* - QlikView Batch インスタンスの同時最大数 (既定値は 4)。
- *MaxSimultaneousReaderQvbs* - QlikView Batch リーダーの同時最大数 (既定値は 20)。
- *DedicatedDistributionQvbs* - 専用の QlikView Batch インスタンス数 (既定値は 0)。
- *RunDedicatedTaskAlone* - 専用タスクを単独で実行するか否か (既定値は false)。
- *GraceTimeMinutes* - *RunDedicatedTaskAlone* が *True* に設定されている場合、次の専用タスクが始まるまでの待ち時間として設定されている時間枠に入ると、QDS 内で通常タスクを起動できないことになります (既定値は 0)。

MaxSimultaneousQvbs が *4* で *DedicatedQvbs* が *2* に設定されている場合に、その時点で実行中の専用タスク数に基づいて起動可能な通常タスクと専用タスクの数を次の表に示します。

タスクの数

実行中の専用タスクの数	起動可能な新しい専用タスクの数	起動可能な通常タスクの数
0	4	2
1	3	2
2	2	2
3	1	1
4	0	0

RunDedicatedTaskAlone オプションが *True* に設定されている場合、QVB では専用タスクは常に利用可能となります。*MaxSimultaneousQvbs* が *4*、*DedicatedQvbs* が *2*、そして *RunDedicatedTaskAlone*が *True* に設定されている場合に、その時点で実行中の専用タスク数に基づいて起動可能な通常タスクと専用タスクの数を次の表に示します。

タスクの数

実行中の専用タスクの数	起動可能な新しい専用タスクの数	起動可能な通常タスクの数
0	4	2
1	3	0
2	2	0
3	1	0
4	0	0

タスクの構成

Publisher グループを作成すると機能がアクティブ化され、既存の各タスクは通常タスクとみなされます。タスクを新規作成する場合や既存のタスクを編集する場合は、ソース ドキュメントの [General] (基本設定) タブの [**Publisher Groups**] (Publisher グループ) ドロップダウン リストを使用します。

このドロップダウン リストにはすべての Publisher グループ名が表示されます。ドキュメントに Publisher グループが割り当てられると、そのドキュメントに関連付けられたタスクはすべて専用タスクとなります。ドキュメントに関連付けられたタスクを通常タスクにするには、[Publisher Groups] (Publisher グループ) ドロップダウン リストから **<any>** (<任意>) を選択します。通常タスクはどのノードでも実行できます。

QlikView Server Extension

QlikView Server への Extension の追加

QlikView Server で QlikView Extension を実行するには、*Extensions* フォルダのコンテンツが *%UserProfile%\AppData\Local\QlikTech\QlikView\Extensions\Objects* からサーバー上の *%ProgramData%\QlikTech\QlikViewServer\Extensions\Objects* フォルダにコピーされている必要があります。

Extension へのパスを変更した場合 (クラスター内のすべてのサーバーに共通のロケーションへの変更など) は、そのパスを使用する必要があります。パスのセットは、*%UserProfile%\AppData\Local\QlikTech\QlikView\Extensions* に対応している (つまり *\Objects* を含まない) 点に注意してください。

カスタム ユーザー用 IIS の設定

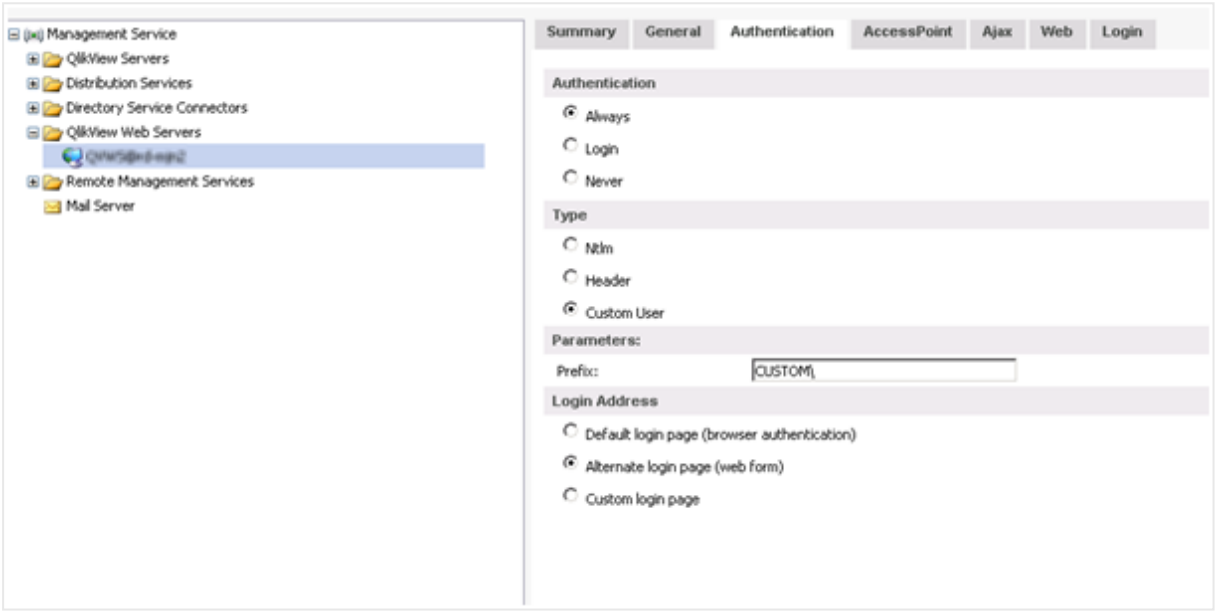
Microsoft IIS をカスタム ユーザー用のウェブ サーバーとして使用するには、設定が必要です。

カスタム ユーザー用の IIS 設定手順は次の通りです。

1. QlikView Management Console で、**[システム (System)]** > **[設定 (Setup)]** > **[認証 (Authentication)]** の順で選択し、次のようにパラメータを変更します。

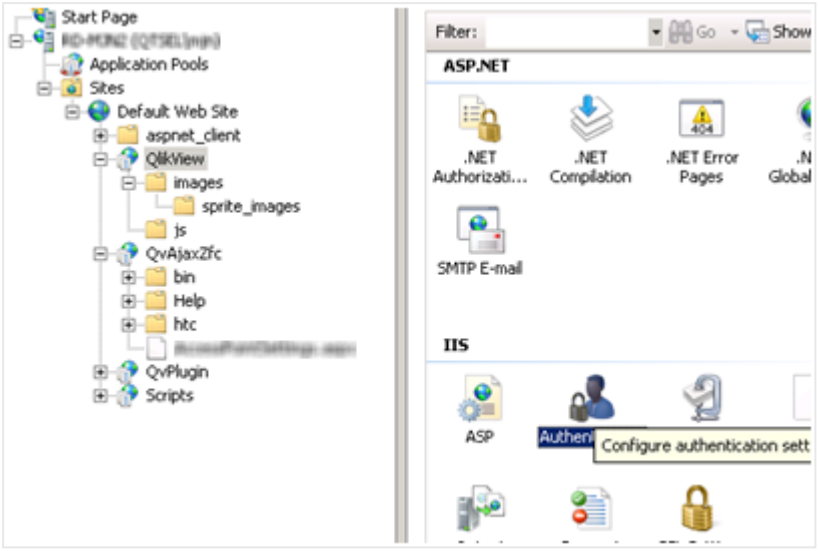
QlikView Management Console パラメータ

パラメータ	変更
認証	常に表示
タイプ	Custom User
パラメータ (Parameters)	CUSTOM\
ログイン アドレス (Login Address)	代替ログイン ページ (ウェブフォーム)



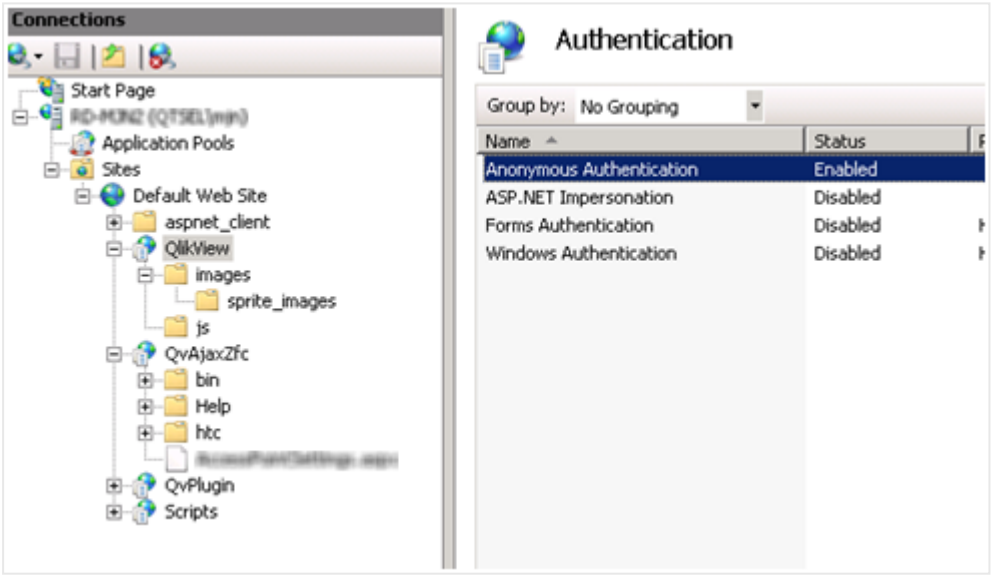
認証 (Authentication) タブ

2. QlikView 仮想フォルダから、**[認証 (Authentication)]** を選択します。



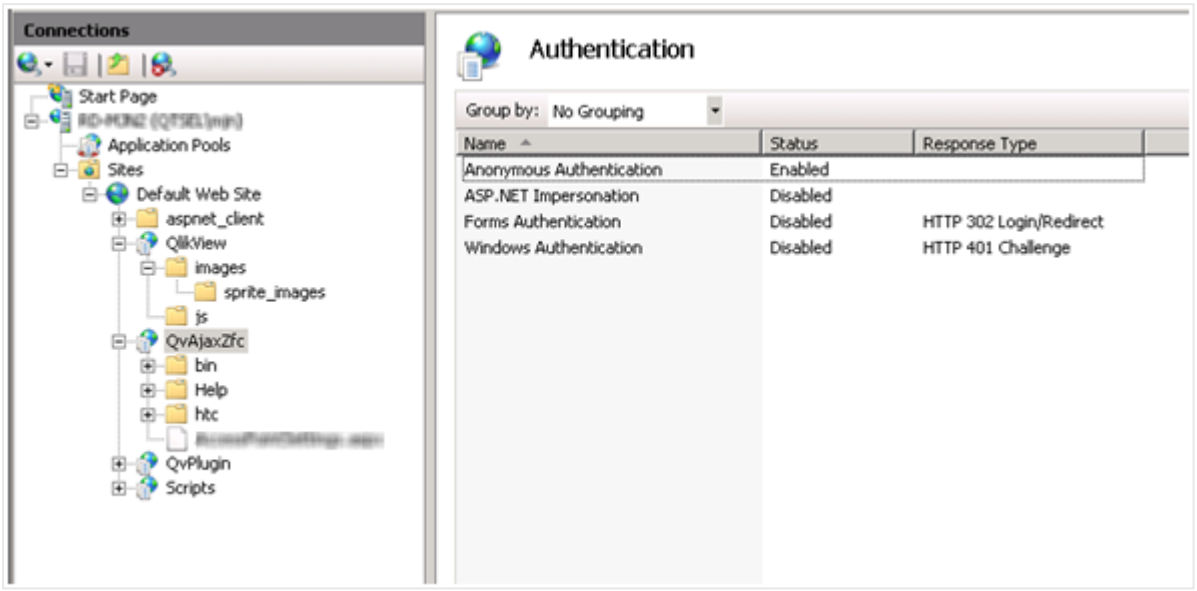
認証を選択する

3. **[Windows 認証 (Windows Authentication)]** を無効にし、**[匿名認証 (Anonymous Authentication)]** を有効にします。



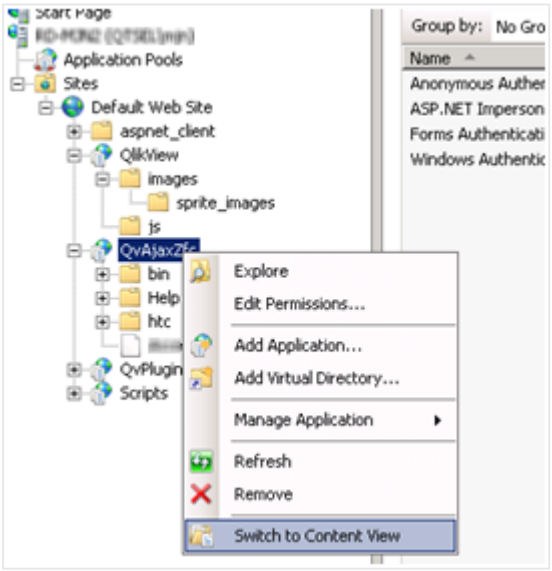
QlikView 仮想フォルダの匿名認証を有効にする

4. QvAjaxZfc フォルダから、**[認証 (Authentication)]** を選択します。
5. **[Windows 認証 (Windows Authentication)]** を無効にし、**[匿名認証 (Anonymous Authentication)]** を有効にします。



QvAjaxZfc フォルダの匿名認証を有効にする

6. QvAjaxZfc を右クリックして **[コンテンツ ビューに切り替え (Switch to Content View)]** を選択します。



コンテンツ ビューに切り替えを選択する

7. カスタム ユーザー用 Microsoft IIS の設定が完了しました。

QlikView EDX が有効化されたタスクのトリガー

QlikView Event Driven Execution (EDX) により、外部イベントをトリガーとして使用して QlikView Publisher でタスクを開始することができます。

EDX タスクを設定するには、QlikView Management Service API (QMS API) を使用する必要があります。リクエスト呼び出しを実行するユーザーは、QlikView Administrators ローカル グループか QlikView EDX ローカル グループのメンバーでなければなりません。QlikView Administrators グループは QlikView Server のインストール時に作成されますが、QlikView EDX グループは [**Computer Management**] (コンピュータの管理) で手動作成する必要があります。EDX が有効なタスクをトリガーできるのは、QlikView EDX グループのメンバーのみです。

QlikView EDX グループの作成

次の手順を実行します。

1. [**Computer Management**] (コンピュータの管理) で [**Local Users and Groups**] (ローカル ユーザーとグループ) を開きます。
2. グループ セクションを展開し、ツールバーで [**Action**] (アクション) > [**New Group...**] (新しいグループ) を選択します。
3. グループ名を「QlikView EDX」と入力し、[**Create**] (作成) を選択します。

EDX タスクの作成

EDX タスクを作成するには、次の署名を使用します。

```
TriggerEDXTaskResult TriggerEDXTask(Guid guid, string taskNameOrId,
                                    string password, string variableName,
                                    List<string> variableValues)
```

EDX タスク パラメータ

パラメータ	目的
guid	タスクが定義される QlikView Distribution Service (QDS) の ID。
taskNameOrId	タスクの名前またはタスクの ID (文字列)。
password	パスワード (タスクで必要となる場合)。
variableName	変数名 (タスクで必要となる場合)。
variableValues	変数の値のリスト。

返される結果には、タスクが問題なく開始されたかどうかに関する情報が含まれます。

下記の例は、タスクをトリガーした後、これが終了するまで、あるいは一定の期間が経過するまで待機するプロセスを説明したものです。

```
        using System;         using System.Collections.Generic;         using System.Linq;
    using System.Threading;         using QMSAPI;                    class Program         {
        static void Main(string[] args)                {                        try                        {
create a QMS API client                                 IQMS apiClient = new QMSClient();
retrieve a time limited service key                             ServiceKeyClientMessageInspector.ServiceKey =
```

```
                    apiClient.GetTimeLimitedServiceKey();
                    {                                          //Trigger the task
                    apiClient.TriggerEDXTask(qdsService.ID, "PauseEDX", "edx", "", new List<string>());
                                                               EDXStatus executionStatus = null;
is completed or 60 seconds has passed.                         SpinWait.SpinUntil(() =>
                                                   System.Threading.Thread.Sleep(1000);
task...");                                                     //Get the current state of the task.
executionStatus =                                              apieClient.GetEDXTaskStatus(qdsServic
                                                                                                //Ret
executionStatus !=                                             null && executionStatus..TaskStatus =
TaskStatusValue.Completed;                                     }, 60 * 1000);
result                                             if (executionStatus != null)
(executionStatus.TaskStatus);                             }                    }                    catch
                {                                  Console.WriteLine("An exception occurred: " + ex.Message);
                //wait for user to press any key               Console.ReadLine();             }
```

この例は、QlikView マネージメント コンソール (QMC) の一部としてインストールされる QMS API ドキュメントから生成したものです。これには、利用可能な手法および QMS API の開始方法に関する詳細情報が含まれます。

共有ファイルのクリーンアップと変換

QlikView 共有ファイル クリーンアップ ツールは、システム管理者が共有ファイルを確認 (分析) および削除 (修復) するために使用するコマンド ライン ツールです。このツールはまた、異なる形式の共有ファイルを変換するためにも使用できます。「共有ファイルの変換」を参照してください。このツールを呼び出すには、QlikView Server 実行可能ファイル (QVS.exe) を特別なパラメーターで実行します。

クリーンアップ ツールで使用可能なモードは 2 つあり、それぞれ異なるコマンドライン パラメーターで指定します。

確認モード

-v パラメーターを使用して、コマンドラインで指定した共有ファイルを分析します。分析中に、クリーンアップ ツールは 1 つ以上の無効または破損したオブジェクトのエントリがあるかどうかを検出します。次に QVS は無効なエントリに関してできる限り多くの情報をログに書き込みます。

削除モード

-p パラメーターを使用して共有ファイルを確認し、その後破損したエントリを削除して新しい共有ファイルを作成します。クリーンアップ バージョンは、オリジナルと同じフォルダーに配置されます。新しいファイルでは、サフィックス *_clean* が *.Shared* または *.Tshared* の形式の後に使用されます。オリジナルの共有ファイルは上書きされません。この後、オリジナルの共有ファイルをクリーンアップ バージョンに置き換えることもできます。

共有ファイルの変換

共有ファイルを作成する場合は、オリジナルの形式またはトランザクション形式で保存できます。オリジナルの形式は末尾が *.Shared* で、トランザクション形式の共有ファイルは末尾が *.TShared* になっていることで識別できます。*.TShared* を使用したトランザクション形式の共有ファイルの方が、ネットワーク エラー、停電、ディスク容量不足などの障害の場合でも安定性が高くなります。*.TShared* 形式は 16 EB (エクサバイト) までのサイズをこなせるため、2 GB を超える場合にはこの形式を使用することをお勧めします。

オリジナルとトランザクションの 2 つの異なる形式は、同じサーバー上の異なるアプリケーションに同時に使用することができます。ただし、ひとつのアプリケーションの中ではどちらか一方 (*.Shared* または *.TShared*) しか使用できません。新規の共有ファイルを作成する時点で、*Settings.ini* ファイル内で規定してください。QlikView Server の場合、*Settings.ini* ファイルは *C:\ProgramData\QlikTech\QlikViewServer* にあります。

ファイル形式の設定:

`DefaultBlobDbType=0`
この設定の場合、新しい共有ファイルは *.Shared* 形式で作成されます。

`DefaultBlobDbType=1`
この設定の場合、新しい共有ファイルは *.TShared* 形式で作成されます。

共有ファイルの変換は、QlikView 共有ファイルのクリーンアップ コマンドでも実行できます (下のタブ、およびページ下の 例 セクションの例 n.4 を参照してください)。

共有ファイル内容の所有者の設定および変更

QMC でサーバー オブジェクトの所有者を変更することができますが、一部のオブジェクト タイプの場合 (「DocumentContent」、「InputFieldValues」および「ObjectContent」)、この方法で所有者を変更することはできません。この場合に所有者を変更するには、クリーンアップ ツールで -so (所有者を設定) または -ro (所有者を置き換え) パラメーターを使用する必要があります。これらのパラメーターは削除 モードで使用することをお勧めします。

クリーンアップ ツールのコマンドの形式

クリーンアップ ツールのコマンドの形式は次のとおりです。

```
"<QVS_executable_path>" -x "<Shared_file_path>" <Cleaning_tool_mode> <Output format>
<Ownership> <Delete_user_entries> [-l "<Log_folder_path>"] [-rBM <BM_size>]   [-o "<Shared_
file_save_path>"]
```

次の表は、それぞれのコマンド パラメーターについて説明しています。

クリーンアップ ツールのコマンド パラメーター

パラメータ	説明
`QVS_executable_path`	QVS 実行可能ファイル (QVS.exe) を含んでいるシステム フォルダーへのフル パス。
`-x`	`-x` パラメーターは、QVS にクリーンアップ ツールのみを実行するように指示します。
`Shared_file_path`	クリーンアップする共有ファイルへのパス。 ディレクトリへのパスまたはファイルへのパスを受け入れます。 • フォルダーへのパスで呼び出された場合、操作はフォルダー内のすべての共有ファイルに適用されます。 • 1 つのファイルを指定した場合、操作はこのアイテムのみに適用されます。

パラメータ	説明
Cleaning_tool_mode	• -p は削除モードに使用 • -v は確認モードに使用
Output format	[オプション] -f (出力形式を指定) パラメータは、クリーニング ツールによる共有ファイル形式間の変換を可能にします。 形式は、same、orig または tx (例: -f tx) のように指定することができます。 • same 入力ファイルのファイル形式が使用されます • orig の元の *.TShared* 形式が出力形式に使用されます • tx *.TShared* (トランザクション ファイル) 形式が出力形式に使用されます 形式 (-f パラメータ) を指定していない場合、既定値の same が使用されます。
Ownership	• -so user は所有者の設定に使用 • -ro from_user to_user は所有者の置き換えに使用
Delete_user_entries	• -du0 ユーザーはユーザーから非共有エントリを削除 • -du1 ユーザーはユーザーからすべてのエントリを削除 複数のユーザーを削除する必要がある場合、この項目ではファイルへのパスを受け入れます • -df0 file.txt は file.txt ファイルのリストにあるユーザーから非共有エントリを削除します • -df1 file.txt は file.txt ファイルのリストにあるユーザーからすべてのエントリを削除します QlikView Server にアクセスしたことのあるユーザーのリストを取得するには、Governance Dashboard アプリケーションを使用します。Qlik Community から無償で入手できます (ここ で関連ドキュメントを参照してください)。 ユーザーの一覧は、ガバナンスダッシュボードの [操作/セッション] サブタブにある ListBox の [*Athenticated User*] を csv 形式にエクスポートすることで簡単に抽出することができます。その後、リストを編集し (共有ファイルから削除するユーザーのみを維持します)、クリーンアップ ツールに入力として渡すことができます。
-l Log_folder_path	[オプション] 生成されたログ ファイルの場所を変更する場合は、-l を使用してログ フォルダーのパスを指定します。

パラメータ	説明
-rBM BM_size	[オプション] -rBM パラメーターを使用して、大きなブックマークを共有ファイルから削除します。<BM_size> (バイト単位) より大きいすべてのブックマークが削除されます。
-o Shared_file_save_path	[オプション] -o パラメーターを使用して、共有ファイルが保存されている場所へのパスを変更します。

共有ファイル クリーンアップ ツールの使用

共有ファイル クリーンアップ ツールは、管理者モードで Windows コマンドプロンプトを使用して実行します。次の手順を実行します。

%ProgramData%Qliktech\Documents とは異なる (一時) フォルダーにある QVS.exe のコピーおよび共有ファイルと一緒にクリーンアップ ツールを実行するようお勧めします。%ProgramData%Qliktech\Documents folder のパスに保存されているクリーンアップ ツールを実行するには管理者権限が必要です。

このクリーンアッププロセスでは共有ファイルが完全に再生成されます。これによりファイルの断片化に関する問題が解決するとともに、サイズとアクセス時間も縮減できる場合があります。

クリーニング ツールをフォルダー全体に適用するには、-subF を使用します。削除しようとしているユーザー リストがそのフォルダー内のすべての共有ファイルで共通のものであることを必ず考慮に入れてください。

クリーンアップ ツール使用する前に、共有ファイルをバックアップします。

1. QVS 実行可能ファイルのコピーを作成します。デフォルトでは、QVS.exe は *C:\Program Files\QlikView\Server* にインストールされています。
2. QVS.exe のコピーが格納されているフォルダーに移動し、クリーンアップ ツールを検証モードで実行します。例:
   "C:\<Temporary_path>\QVS.exe -x
   “C:\ProgramData\QlikTech\Documents\FinanceAnalysis.qvw.Shared” -v
3. *CleaningTool_MACHINENAME.log* 確認ファイル ログを見つけます。コマンドでログを指定しなかった場合は、デフォルトで *C:\ProgramData\QlikTech\QlikViewServer* に保存されます。
   共有ファイル オブジェクトが破損している場合、そのオブジェクトのそれぞれの種類がログに示されます。破損したエントリを特定できた場合は、オブジェクト ID が示されます。
4. 破損したエントリがある場合、再度クリーンアップ ツールを削除モードで実行します。
   削除プロセスで破損したオブジェクトが削除または修正されて、新しい共有ファイルが作成されます。サフィックス *_clean* で識別できる新しいファイル (例:*MYFILENAME.QVW.TShared_clean*) は、ソース共有ファイルと同じフォルダ内に配置されます。

> *新しいファイルは、ソース ファイルよりも大きい場合があります。*

5. 古い破損した共有 ファイルを新しいファイルと置き換えます。この操作はどの QlikView Server サービスも稼働していないときに行う必要があります。

例

Example 1: 共有 ファイルの分析

Windows コマンドプロンプトで次のコマンドを実行して共有 ファイルを分析し、*C:\logs* フォルダー内にログ ファイルを作成します。

```
QVS.exe -x "C:\ProgramData\QlikTech\Documents\TESTFILE.QVW.TShared" -v -l "C:\logs"
```

Example 2: ファイル所有者の設定

Windows コマンドプロンプトで次のコマンドを実行して、共有 ファイル内のサーバー オブジェクトの所有者をユーザー UserX に設定します。

```
QVS.exe -x "C:\ProgramData\QlikTech\Documents\TESTFILE.QVW.TShared" -p -so UserX
```

Example 3: ファイル所有者の置き換え

Windows コマンドプロンプトで次のコマンドを実行して、共有 ファイル内のサーバー オブジェクトの所有者を UserX から UserY に置き換えます。

```
QVS.exe -x "C:\ProgramData\QlikTech\Documents\TESTFILE.QVW.Shared" -p -ro UserX UserY
```

Example 4: 出力形式の変更

Windows コマンドプロンプトで次のコマンドを実行すると、オリジナルの共有 ファイルの形式を新しい形式に変換できます。

```
QVS.exe -x "C:\Temp\1.QVW.Shared" -p -f tx
```

Example 5: 特定のユーザーからの非共有 エントリの削除

Windows のコマンドプロンプトで次のコマンドを実行すると、指定したユーザー UserX に関連付けられている非共有 エントリがすべて削除されます。

```
QVS.exe -x "C:\ProgramData\QlikTech\Documents\TESTFILE.QVW.TShared" -p -du0 UserX
```

Example 6: テキスト ファイルで指定されているユーザー セットからのすべてのエントリの削除

Windows のコマンドプロンプトで次のコマンドを実行すると、Users.txt 列テキスト ファイルで指定されているユーザーのリストに関連付けられているすべてのエントリ(共有 エントリを含む) が削除されます。

```
QVS.exe -x "C:\ProgramData\QlikTech\Documents\TESTFILE.QVW.Shared" -p -df1 "C:\temp\Users.txt"
```

Users.txt ファイルの例:

```
DOMAIN\User1
```

DOMAIN\User2

DOMAIN\User3

...

DOMAIN\UserX

Example 7: テキスト ファイルで指定されているユーザー セットからのすべてのエントリの削除 (フォルダー全体から)

フォルダー内の共有ファイルのセット全体を、削除対象のユーザーの共通リストで処理するオプションもあります。

Windows のコマンドプロンプトで次のコマンドを実行すると、Users.txt 列テキスト ファイルで指定されているユーザーのリストに関連付けられているすべてのエントリ(共有エントリを含む) が削除されます。'Documents' フォルダー内のすべての共有ファイルの場合:

```
QVS.exe -x "C:\ProgramData\QlikTech\Documents" -p -subF -df1 "C:\temp\Users.txt"
```

Users.txt ファイルの例:

DOMAIN\User1

DOMAIN\User2

DOMAIN\User3

...

DOMAIN\UserX

IPv6 構成

QlikView は、インターネット プロトコル IPv6 およびデュアル スタック IPv6-IPv4 構成に対応しています。

QlikView Server サービス (QVS) 用の IPv6 構成

QlikView Server 展開をさまざまなネットワーク構成に適応させるように、IPv6 設定をカスタマイズすることができます。IPv6 構成を QlikView Server サービス (QVS) 用にカスタマイズするには、*Settings.ini* ファイルを開いて以下のパラメータに追加します。

IPv6 構成および既定値の説明

[Name] (名前)	**説明**	**既定値**
ClusterMulticastIpV6Addr	リンクローカル スコープ IPv6 マルチキャスト アドレス。既定値: すべてのノードのアドレス	`FF02::1`
ClusterMulticastIpV6Loop	発信マルチキャスト データグラムのループバックを有効化または無効化します。	`true`
ClusterMulticastIpV6Hops	パケットの使用年限を制限します。1 に設定した場合、マルチキャストはローカル サブネットにのみ使用できます。	`1`

QVS *Settings.ini* ファイルの既定の場所は *%ProgramData%\QlikTech\QlikViewServer* です。

QVS を実行しているすべてのマシンは、同じ IPv6 設定を装備している必要があります。

IPv6 フォーマットを使用する QlikView サービスのクラスタリング

QlikView 管理コンソール (QMC) でサービスをクラスタリングする場合、マシン名またはその IPv6 アドレスのいずれかを使用できます。マシンの IPv6 アドレスを使用することにした場合は、このアドレスを角括弧で囲む必要があります。例: `[fe80::dd3d:36bb:e284:af99]`

証明書を使用する場合の IPv6 構成

QlikView Server 展開で認証に証明書を使用している場合、およびお使いの展開で IPv6 プロトコルのみを使用するように構成した場合は、QlikView Management Service (QMS) および QlikView Server サービスで `UseCertificatesIpvSix` 設定を有効化する必要があります。

QMS の場合は、QMS *exe.config* ファイルを開きます。既定では *%Program Files%\QlikView\Management Service* にあります。次の設定を追加します。

```
<add key=" UseCertificatesIpvSix " value="true"/>
```

QVS の場合は、*Settings.ini* ファイルを開きます。既定では *%ProgramData%\QlikTech\QlikViewServer* にあります。次の設定を追加します。

```
UseCertificatesIpvSix=1
```

QVS を実行しているすべてのマシンは、同じ `UseCertificatesIpvSix` 設定を装備している必要があります。

2.3 ログとエラー コード

QlikView Server からのすべてのアラートは、Windows のイベント ログに表示されます。

QlikView Server からのログ

詳細なセッション ログはログ ディレクトリにあり、これは QlikView Management Console (QMC) で [**システム (System)**] > [**設定 (Setup)**] の順でクリックし、[**ログ (Logging)**] タブで指定します。既定の場所は *%ProgramData%\QlikTech\QlikViewServer* です。

ログ ファイルの分割 (新規作成) を、毎日、毎週、毎月、毎年、なしに設定できます。パフォーマンス ログの間隔を 1 分もしくはそれ以上に設定できます。

ログ間隔を 1 分ごとのように小さい値で設定すると、パフォーマンスにマイナスの影響を与える場合があります。

セッションのログ

1 セッションの定義は、1 つのドキュメントに 1 人のユーザーが接続することです。

セッション ログは、セッションが終わる度に更新されます。これは、セッション開始時には、ログ エントリは作成されないことを意味します。

セッション ログのファイル名は、*Sessions*.log* で、* はサーバー名と分割する間隔を示します。セッション ログの各エントリには、次の項目が含まれます。

セッション ログのエントリのリスト

エントリ	説明
Exe Type	QVS ビルドの種類。 例 : "RLS64" = 64 ビット リリース ビルド
Exe Version	QVS のフル バージョン番号。 例: "11.00.11076.0409.10"
Server started	QVS が開始された日付および時刻。
タイムスタンプ	ログ エントリが作成された日付および時刻。
ドキュメント	アクセスした QlikView ドキュメント。
Document Timestamp	アクセスしたドキュメント ファイルのタイムスタンプ。
QlikView User	QlikView セクション アクセス ユーザー ID (使用されている場合)
Exit Reason	セッションの終了理由。 • 「Socket closed」 = クライアントによる終了 • 「LRU」= 新規ユーザー優先で最も長い間使用されていないとして終了 • 「Shutdown」= その他の理由からサーバーが終了 *これは完全なリストではありません。オペレーション システムから返される終了値もあります。*
セッション ID	セッションの ID。
Session Start	セッションが開始された時間。
Session Duration	セッションの長さ (時間: 分: 秒)
CPU Spent (s)	セッションが使用した CPU 秒。
Bytes Received	セッション中にサーバーが受信したバイト数。
Bytes Sent	セッション中にサーバーが送信したバイト数。
Calls	セッション中の QlikView コール数 (双方向)。

エントリ	説明
選択	セッション中に行われた QlikView の選択数。
Authenticated User	認証済み Windows NT® ユーザー ID (あれば)。
Identifying User	クライアント ユーザー識別。
Client Machine Identification	クライアント マシン識別。 デフォルトでは、Windows Management Instrumentation (WMI) に対する呼び出しの、universally unique identifier (UUID) 受信者です。 UUID が使用できない場合は、代わりに次の ID のいずれかが表示されます。 • コンピュータの MAC address • コンピュータ名 • ユニークなマシン ID (セッションで使用されたブラウザがプライベート モードであった場合)
(Serial Number)	QlikView クライアントのシリアル番号 (QlikView Desktop および QlikView プラグインがインストールされているクライアントのみ)。
Client Type	クライアントの種類: • 「Windows Exe」= QlikView Desktop および QlikView プラグイン • 「Ajax」= QVPX プロトコルを使用しているすべてのクライアント • 「Unknown」
Client Build Version	QlikView クライアントのビルド バージョン。
Secure Protocol	セキュア プロトコル: • 「On」は暗号化通信が使用された場合 (通常 Windows クライアント)。 • 「Off」は暗号化通信が使用されなかった場合。
Tunnel Protocol	「Tunnel」は QVS トンネル通信が使用された場合。
Server Port	サーバーに使用されたポート。
Client Address	サーバーに接続 (上記「Server Port」項目で指定されたポートを使用) しているクライアントのクライアント IP 番号。
Client Port	クライアント ポート。
Cal の種類	Client Access License (CAL) の種類: • 「User」= Named User CAL • 「Session」= Session CAL • 「Usage」= Usage CAL • 「Document」= Document CAL

エントリ	説明
Cal Usage Count	Usage CAL の数。

パフォーマンスのログ

パフォーマンス ログは、QMC で [**システム (System)**] > [**設定 (Setup)**] の順でクリックし、[**ログ (Logging)**] タブで指定した間隔で更新されます。デフォルトの間隔は 5 分です。サーバーが開始あるいは停止した際には、追加のエントリが入力されます。ログのファイル名は、*Performance*.log* で、* はサーバー名と分割する間隔を示します。

ログの各エントリには、次の項目が含まれます。

パフォーマンス ログのエントリのリスト

エントリ	説明
Exe Type	QVS ビルドの種類。 例 : “RLS64” = 64 ビット リリース ビルド
Exe Version	QVS のフル バージョン番号。 例: “11.00.11076.0409.10”
Server started	QVS が開始された日付および時刻。
タイムスタンプ	ログ エントリが作成された日付および時刻。
EntryType	エントリの種類: • 「Server starting」= スタートアップ • 「Normal」= 通常のインターバルのログ エントリ • 「Server shutting down」= シャットダウン
ActiveDocSessions	インターバルの間、そしてインターバルの終わりにまだ存在する活動を示すドキュメントのセッション* 数
DocSessions	インターバルの終わりに存在するドキュメントのセッション* 合計数
ActiveAnonymousDocSessions	インターバルの間、そしてインターバルの終わりにまだ存在する活動を示す匿名ユーザーのドキュメントのセッション* 数
AnonymousDocSessions	インターバルの終わりに存在する匿名ユーザーのドキュメントのセッション* 合計数
ActiveTunneledDocSessions	インターバルの間、そしてインターバルの終わりにまだ存在する活動を示すトンネル接続のドキュメントのセッション* 数
TunneledDocSessions	インターバルの終わりに存在するトンネル接続のドキュメントのセッション* 合計数
DocSessionStarts	インターバルの間に開始されたドキュメントのセッション* 数

エントリ	説明
ActiveDocs	ユーザー アクティビティが存在していたインターバルの、終了時にロードされていたドキュメントの数。
RefDocs	終了時にセッションが存在しているインターバルの、終了時にロードされていたドキュメントの数。
LoadedDocs	インターバルの終了時にロードされていた、ドキュメントの総数。
DocLoads	インターバル中にロードされた、新規ドキュメントの数。
DocLoadFails	インターバル中にロードに失敗した、ドキュメントの数。
Calls	インターバル中に実行された、QVS に対するコールの総数。
選択	インターバル中に実行された、選択コールの数。
ActiveIpAddrs	インターバル中にアクティブになったことがあり、インターバルの終了時にもまだ存在していた、異なる IP アドレスの数。 *同一 IP アドレスに由来するトンネル セッションと複数のユーザーは、区別できないので注意が必要です。*
IpAddrs	インターバルの終了時に接続されていた、異なる IP アドレスの総数。 *同一 IP アドレスに由来するトンネル セッションと複数のユーザーは、区別できないので注意が必要です。*
ActiveUsers	インターバル中にアクティブになったことがあり、インターバルの終了時にもまだ存在していた、異なる NT ユーザーの数。 *匿名ユーザーは識別できないので注意が必要です。*
Users	インターバルの終了時に接続されていた、異なる NT ユーザーの総数。 *匿名ユーザーは識別できないので注意が必要です。*
CPULoad	インターバル中の、QVS からの平均 CPU ロード。
VMAllocated(MB)	インターバル** の終了時点における、QVS に割り当てられた仮想メモリのサイズ (MB)

エントリ	説明
VMCommitted(MB)	インターバル** の終了時点における、QVS が実際に使用した仮想メモリのサイズ (MB) この数値は、VMAllocated(MB) の一部です。許容外の応答時間を回避するため、物理メモリのサイズを超過しないようにします。
VMFree(MB)	QVS** で使用可能な割り当てられていない仮想メモリのサイズ (MB)
VMLargestFreeBlock(MB)	QVS で使用可能な、割り当てられていない仮想メモリの最大連続ブロックのサイズ (MB)。この数値は VMFree(MB) の一部です。
UsageCalBalance	「-1.00」= Usage CAL はありません。
CacheHits	一般キャッシュヒット数
CacheLookups	一般キャッシュルックアップ数
CacheObjectAdded	一般キャッシュに追加されたオブジェクト数
CacheBytesAdded	一般キャッシュに追加されたバイト数
CacheTimeAdded	一般キャッシュへの新規オブジェクト追加での所要時間
CacheReplaced	一般キャッシュ内で置き換えられたオブジェクト数

* 1 ユーザー + 1 ドキュメント = 1 ドキュメント セッション

**VMAllocated(MB) + VMFree(MB) = QVS プロセスに使用可能な合計最大仮想メモリ量。

サーバー サイド拡張 ログ

サーバーサイド拡張 (SSE) ログのファイル名は、*SSE*.log* で、* はサーバー名と分割する間隔を示します。SSE ログの各エントリには、次の項目が含まれます。

サーバーサイド拡張 ログのエントリのリスト

エントリ	説明
Severity	• Debug (デバッグ): 開発者がデバッグを行う場合に有用な情報です。このレベルでは大量のログ情報が生成されるので、通常の操作では役に立ちません。 • 情報: レポート、測定のスループットなどに関して収集される通常の操作メッセージ。何も対処する必要はありません。 • Warn (警告): エラー メッセージではなく、何もを措置を講じないとエラーが発生する場合があることを示します (例えば、ファイル システムが 85% 使用されているなど)。一定の時間内に各アイテムを解決する必要があります。 • エラー: 開発者または管理者に通知される緊急性のない障害。一定の時間内に各アイテムを解決する必要があります。 • Fatal (致命的): プライマリシステム内の障害を示します。直ちに修正する必要があります。 • Off (オフ): ライセンス ログ以外に、ログが生成されていません。
日付と時刻	ログ エントリが作成された日付および時刻。
ProcessId	ログ メッセージの発信元のプロセスの ID。
ThreadId	ログ メッセージがファイルに書き込まれたときに使用されたスレッドの ID。
UserId	ユーザーの ID。
QixRequestId	要求の発信側によって確立された ID。このメンバーが存在しない場合、RPC 呼び出しが通知であると見なされます。
AppId	分析接続を介したサーバーサイド拡張 (SSE) プラグインに対する呼び出しを含むアプリの ID。
App Title	分析接続を介した SSE プラグインに対する呼び出しを含むアプリのタイトル。
SSEPlugin	SSE プラグインに対する呼び出し時にログ メッセージが作成された場合の、そのプラグインのマッピング/エイリアス、例えば Python プラグインの SSEPython。SSE プラグインに対する呼び出しがなくログ メッセージが作成された場合、例えば SSE の初期化中は、この値はダッシュ (-) です。
SSEPluginAddress	SSE プラグインへの分析接続を定義する、コロンで区切られた 2 つの要素。 • <Host>: プラグインの DNS 名 (または IP アドレス)。 • <Port>: プラグインの待ち受けポート。通常は 50051 です。 例えば、localhost:50051。
メッセージ	ログ メッセージ。

イベントのログ

イベント ログは、QVS から Windows のイベント ログにログが書き込まれる度に更新されます。保存される情報は、Windows イベント ログに書き込まれた情報のコピーです。イベント ログのファイル名は *Events*.log* で、* はサーバー名と分割する間隔を示します。

QMC の [**システム (System)**] > [**設定 (Setup)**] > [**QlikView Server**] > [**ログ (Logging)**] タブにある [**イベント ログ レベル (Event Log Verbosity)**] ラジオ ボタンを使用して、レベルを設定します。選択されたレベルによって、イベント ログに以下の入力が書き込まれます。

- **Low** (低): エラー メッセージ
- **Medium** (中): エラーおよび警告 メッセージ
- **High** (高): エラー、警告、および情報 メッセージ

ログの各エントリには、次の項目が含まれます。

イベント ログのエントリのリスト

エントリ	説明
Server started	QVS が開始された日付および時刻。
[日付と時刻]	ログ エントリが作成された日付および時刻。
SeverityID	重要度レベルごとの ID: • 1 = エラー (Error) • 2 = 警告 (Warning) • 4 = 情報 (Information)
EventID	イベントの種類ごとの一意の ID。
Severity	イベントの重要度レベル: • エラー • 情報 (Information) • 警告 (Warning)
メッセージ	イベントの説明。

エンドユーザーの監査ログ

エンドユーザーの監査ログには、選択のクリアやアクティブ化されたシート、ブックマークの適用、アクセスのあったレポート、最大化されたオブジェクトなどに関するユーザー選択情報が含まれます。

AUDIT_<machinename> という名前のログ ファイルは、*%ProgramData%\QlikTech\QlikViewServer* に保存されます。

*QMC の [**システム (System)**] > [**設定 (Setup)**] > [**QlikView Servers**] > [**ログ (Logging)**] タブで [**監査詳細ログを有効化 (Enable Extensive Audit Logging)**] チェック ボックスを選択して詳細な監査ログを有効にします (ブックマークの付いているすべての選択をログするなど)。ただし、QVS におけるユーザー選択のログは、選択表示ボックス オブジェクトの動作を基に登録されます。そのため、選択数が多い場合その詳細はログに残らない可能性があります。*

エンドユーザーの監査ログのエントリのリスト

エントリ	説明
Session ID	セッション ID
Server started	QVS が開始された日付および時刻。
Timestamp	ログ エントリが作成された日付および時刻。
Document	アクセスしたドキュメントへのパスとその名前。
Type	選択やブックマークなど、行われた選択の種類。 使用できるタイプの概要については、下記の表をご覧ください。
User	ユーザー名。
Message	選択の種類やドキュメントで作成されたアプリケーション ブックマークに関する情報 (たとえば、「Apply Server\Bookmark15」)。 このフィールドに表示される可能性のあるメッセージの概要については、下記のテーブルを参照してください。
Id	操作に接続されているオブジェクトの ID (例えば、"Document\SH03")。操作に接続されたオブジェクトが存在しない場合は、この項目は空になります。
Session	セッション番号

エンドユーザーの監査ログでの種類とメッセージ

エンドユーザーの監査ログのタイプとメッセージ項目に投稿されるタイプとメッセージは、下記に掲載されています。

エンドユーザーの監査ログでは、"XXX" と "YYY" は、QlikView ドキュメントの値で、置換されます。

エンドユーザーの監査ログで見つかった種類とメッセージ

[Type] (種類)	メッセージ	説明
Action	action (#) [XXX]	アクション # は XXX で実行されました。数値は次のアクションのうちの 1 つに対応します。 • Info = 0 • すべてをロック = 2 • すべてをアンロック = 3 • すべての選択をクリア = 4 • ロック済みを含めすべての選択をクリア = 5 • 元に戻す = 6 • やり直し = 7 • ファイルを閉じる = 8 • 次のタブへ = 9 • 前のタブへ = 10 • エクスポート = 11 • 起動 = 12 • マクロ = 13 • ブックマークの呼び出し = 14 • ブックマークの上書き = 15 • ブックマークの作成 = 16 • レポートの印刷 = 17 • シートの選択 = 18 • シートの印刷 = 19 • オブジェクトの印刷 = 20 • オブジェクトを元のサイズに戻す = 21 • オブジェクトを最小化する = 22 • オブジェクトを最大化する = 23 • オブジェクトを選択する = 24 • 除外値の選択 = 25 • 他項目の選択のクリア = 26 • 絞込値の選択 = 27 • ロック = 28 • アンロック = 29 • パレートの選択 = 30

[Type] (種類)	メッセージ	説明
Action	action (#) [XXX]	• 変数の設定 = 31 • 項目の選択 = 32 • 項目の切り替え選択 = 33 • URL を開く= 34 • ドキュメントチェーン = 35 • 項目の選択をクリア = 36 • リロード = 37 • ステート名の設定 = 38 • ステートの転送 = 39 • ステート内容の切り替え = 40 • ダイナミック更新 = 41
Bookmark	Apply XXX	ブックマークXXX は、適用されました。
Bookmark Selection	XXX	ブックマークが選択されたので、選択 XXX が行われました。このタイプの入力は、詳細な監査ログが選択された場合にのみ、記録されます。
Document	Document XXX	ドキュメントXXX は展開または閉じられました。
Export	Sheet Object XXX	シートオブジェクトXXX はエクスポートされました。
Maximize	Sheet Object XXX	シートオブジェクトXXX は最大化されました。
Minimize	Sheet Object XXX	シートオブジェクトXXX は最小化されました。
Print	Sheet Object XXX	シートオブジェクトXXX は印刷されました。
Report	Accessed report XXX	レポートXXX へのアクセスがありました。
Restore	Sheet Object XXX	シートオブジェクトXXX は復元されました。
Selection	Clear All	全選択がクリアされました。
Selection	XXX	選択 XXX が行われました。
SendToExcel	Sheet Object XXX	シートオブジェクトXXX が Microsoft Excel に送られました。
Sheet Object	Sheet Object XXX	シートオブジェクトXXX に適用できるさまざまなアクティビティ。
Session Collaboration	Session Collaboration Initiated, ID:XXX	ID XXX のセッションのコラボレーションが開始しました。
Session Collaboration	Session Collaboration user XXX joined session, ID:YYY	ユーザーXXX が、ID YYY のセッションのコラボレーションに参加しました。
Session Collaboration	Session Collaboration user XXX left session, ID:YYY	ユーザーXXX が、ID YYY のセッションのコラボレーションから脱退しました。

次のサンプルは、ブックマーク(“Bookmark01”) が選択された場合のログ エントリを示しています。ログは、全体を把握しやすくするためにテーブル形式で表示しています。

(“Bookmark01”) が選択されている場合の、エンドユーザーの監査ログの例

エントリ	値
Session ID	b5134c4f-7f3d-4107-a37b-d842e9452d93
Server started	20130506T101733.000+0900
Timestamp	20130506T102328.000+0900
Document	C:\ProgramData\QlikTech\Documents\Test.qvw
Type	ブックマーク
User	QlikTech\jsmith
Message	Apply Server\Bookmark01
Id	Document\SH03
Session	3667

詳細な監査ログが選択されている場合、ブックマークが選択されたために行われた選択の詳細を記すログ エントリ(複数可) が、上記のログ エントリの後に続く場合があります。これらログ エントリでは、「ブックマーク選択」にタイプ項目が設定されます。

マネージャの監査ログ

監査ログを使うと、システムのタスクや設定で行われた変更をトラッキングして、誰がいつその変更を行ったかを確認できます。

監査ログは *%ProgramData%\QlikTech\ManagementService\AuditLog* に保存されます。テーブルごとにフォルダが作成されます。作成されるフォルダの数は、お使いのインストールの設定に応じて異なります。各フォルダには、タスクへ行われた変更が記載された日付ごとのファイルが含まれます。ログは、タブ区切りファイルです。

下記のタブには、すべての監査ログ ファイルに共通のエントリが表示されています。各監査ログ ファイルには、各種類のログ ファイル専用のエントリがさらに含まれています。

すべての監査ログ ファイルに共通のエントリのリスト

エントリ	説明
TransactionID	トランザクション ID は、同時に行われた変更をトラッキングするのに便利です。
ChangeType	操作の種類: Update (新規や変更されたエントリ) もしくは Delete (削除済みエントリ)。
ModifiedTime	変更が行われた日付と時刻 (UTC)
ModifiedByUser	ユーザー インターフェースで変更を行ったユーザー。System は、ユーザーではなくシステムが変更を行ったことを意味します。
[ID]	変更された (更新あるいは削除された) ID 行。

以下は、AlertEmail テーブルの例です。ログは、全体を把握しやすくするためにテーブル形式で表示しています。この例には、すべてのエントリが示されているわけではありません。

AlertEmail のマネージャの監査ログの例

エントリ	値
TransactionID	455a241d-8428-4dc7-ba67-4ae7cb21cf3d
ChangeType	Update
ModifiedTime	20100202T151254.000+0900
ModifiedByUser	MyDomain\mjn
[ID]	b3745325-cee7-4fe7-b681-9c9efe22fc5c
DistributionServiceID	8846d7dd-bb3f-4289-9c9b-b0ca71b7c3b2
EmailAddress	mjn

以下は QDSCluster テーブルの例です。2 つの例における TransactionID は同じです。これは、変更が同時に行われたことを意味します。この例には、すべてのエントリが示されているわけではありません。

QDSCluster のマネージャの監査ログの例

エントリ	値
TransactionID	455a241d-8428-4dc7-ba67-4ae7cb21cf3d
ChangeType	Update
ModifiedTime	20100202T151254.000+0900
ModifiedByUser	MyDomain\mjn
[ID]	a37f242c-6d80-42da-a10c-1742d2ec927f
DistributionServiceID	8846d7dd-bb3f-4289-9c9b-b0ca71b7c3b2
QDSWebAdress	http://computer-mjn:4720/qtxs.asmx
CurrentWorkorderID	96bff2dc-f1ea-84d2-b6c4-ea58bf5c98e5

タスク パフォーマンス サマリー

タスク パフォーマンス サマリーは、タスクのパフォーマンス情報の記録に使用します。

タスク パフォーマンス サマリーをアクティブにするには、次の手順を実行してください。

1. テキスト エディタで *Settings.ini* ファイルを開きます。デフォルトでは、このファイルは次の場所に保存されています。
   C:\Windows\system32\config\systemprofile\AppData\Roaming\QlikTech\QlikViewBatch
2. *Settings.ini* ファイル内にある次のセクションを見つけます。

```
[Settings 7]

InterfaceLanguage=English
```

```
InstalledLIBID110={4D121C39-415E-11D1-934D-0040333C91CC}
```

3. [Add] (追加) `EnableQVBProcessSummary=1` を追加し、タスク パフォーマンス サマリーをアクティブにします。

   > *Settings.ini ファイルの最終行は空白にする必要があります。*

4. *Settings.ini* ファイルを保存します。
5. QlikView Distribution Service (QDS) を再起動します。
   QDS の再起動が完了すると、タスク ログが更新されます。

タスク パフォーマンス サマリーの出力例

エントリ	値
`[Name]` (名前)	qvb.exe
`PID`	1360
`Peak CPU` (ピーク時の CPU)	50,0%
`Peak Physical RAM` (ピーク時の物理 RAM)	26.00 Mb
`Peak Virtual RAM` (ピーク時の仮想 RAM)	21.69 Mb
`Average CPU` (平均 CPU)	CPU: 1,0%
`Average Physical RAM` (平均物理 RAM)	24.47 Mb
`Average Virtual RAM` (平均仮想 RAM)	20.37 Mb
`Peak Total CPU` (ピーク時の合計 CPU)	58,3%
`Peak Total Physical RAM` (ピーク時の合計物理 RAM)	6143.49 Mb
`Peak Total Virtual RAM` (ピーク時の合計仮想 RAM)	12285.17 Mb
`Elapsed Time` (経過時間)	00:00:36.4692722

Reload performance log

各タスクに専用の Reload performance log *.xml* ファイルを作成できるようにします。このログ ファイルには、タスクのリロード パフォーマンスのメタデータとプロセスのサマリーが収集されます。

次の手順を実行します。

1. 既定で *%System32%\config\systemprofile\AppData\Roaming\QlikTech\QlikViewBatch* に格納されている QVB *Settings.ini* ファイルを開きます。
2. `[Settings 7]` の下に次の行を追加します。

   ```
   EnableQVBReloadMetadata=1
   ```

3. *Settings.ini* ファイルを保存します。

リロードが実行されるたびに、タスクのリロード パフォーマンス ログの *.xml* ファイルが作成され、既定では *%ProgramData%\QlikTech\DistributionService\TaskResults* に保存されます。*.xml* ファイルの名前の形式は、次のとおりです。

ReloadMetaData_machine-name_20180904T104446_Document-name.xml

ここで、

- <machine-name> は実行したマシンの名前です
- <20180904T104446> は実行した日付と時刻です
- <Document-name> はリロードされたドキュメントの名前です

タスクのリロード パフォーマンス ログ ファイルには、次の `reload_meta` パフォーマンス項目があります。

リロード パフォーマンス ログの `reload_meta` および `static_byte_size` のエントリのリスト

エントリ	説明
`cpu_time_spent_in_ms`	CPU によるリロードの実行にかかった時間 (ミリ秒単位)。
`logical_cores`	CPU のコアの数。
`total_memory`	マシン上で使用可能な物理 RAM の合計。
`static_byte_size`	ドキュメントの静的メモリ使用量。

タスクのリロード パフォーマンス ログ ファイルには、次の `ProcessSummary` パフォーマンス項目があります。これらのエントリは、タスク パフォーマンス サマリー ログ ファイルに示されているエントリと同じです。参照 : タスク パフォーマンス サマリー

リロード パフォーマンス ログの `ProcessSummary` エントリのリスト

エントリ	説明
`App`	リロードされたドキュメントの名前。
[日付]	20180904T104446 の形式で示される日付。
`CurrentProcessCpu`	現在の CPU 使用率 (パーセント単位)。例: 99.991681。
`PeakPhysMemUsedByProc`	プロセッサが使用する物理 RAM の最大量 (バイト単位)。
`PeakVirtualMemUsedByProc`	プロセッサが使用する仮想 RAM の最大量 (バイト単位)。
`AvgCurrentProcessCpu`	CPU の平均使用率 (パーセント単位)。例: 80.81025。
`AvgPhysMemUsedByProc`	プロセッサが使用する平均物理 RAM (バイト単位)。
`AvgVirtualMemUsedByProc`	プロセッサが使用する平均仮想 RAM (バイト単位)。
`TotalCpu`	マシン上で使用可能な CPU の合計。
`TotalPhysMem`	マシン上で使用可能な物理 RAM の合計。
`TotalVirtualMem`	マシン上で使用可能な仮想 RAM の合計。

リロード パフォーマンス ログには、`FieldMetadata` および `TableMetadata` のエントリを示すこともでき、これを使用して QlikView でテーブル ビューアーに表示できる項目とテーブルについて説明します。

QIX performance log

QIX performance log には、QIX Engineのパフォーマンスに関する詳細情報が含まれています。既定では、QIX Performance log ファイルは無効になっています。

QIX performance log の有効化

QIX performance log を有効にするには、`QixPerformanceLogVerbosity` 行を QlikView Server Service (QVS) *Settings.ini* ファイルに追加し、その後に適切なレベルを続けます。例:

```
QixPerformanceLogVerbosity=3
```

QIX performance log のレベルは次のとおりです。

- 0 = Off (オフ)
- 1 = Fatal (致命的)
- 2 = Error (エラー)
- 3 = Warning (警告)
- 4 = Info (情報)
- 5 = Debug (デバッグ)

QIX performance log を有効にして、`QixPerformanceLogVerbosity` をレベル 3 または 2 に設定した場合、次の 4 つのレベルも *Settings.ini* ファイルに追加されます。

```
WarningProcessTimeMs
ErrorProcessTimeMs
WarningPeakMemory
ErrorPeakMemory
```

警告またはエラー イベントをいつトリガーするかを判断するために、これらの 4 つのレベルが必要です。

次の手順を実行します。

1. QlikView Server Service (QVS) *Settings.ini* ファイルを開きます。既定では、*%ProgramData%\QlikTech\QlikViewServer* にあります。
2. 以下の行を追加します。
   ```
   QixPerformanceLogVerbosity=3
   ```
3. *Settings.ini* ファイルを保存します。
4. QlikView Server サービス (QVS) を再始動します。

> *QIX performance log ファイルが有効になると、かなり大量のデータが生成されます。したがって、限られた期間にのみこのログ ファイルを有効にすることを推奨します。*

次の表には、QIX performance log に含まれているエントリが示されています。

QIX performance log のエントリのリスト

エントリ	説明
[日付と時刻]	エンジンがログ メッセージをファイルに書き込んだ時刻。

エントリ	説明
ProcessId	ログ メッセージの発信元のエンジン プロセスの ID。
ThreadId	エンジンがログ メッセージをファイルに書き込んだときに使用されたスレッドの ID。
SessionId	QIX メソッド呼び出しが行われたエンジン セッションの ID。
CServerId	要求を処理したサーバー インスタンスの ID。
Server started	エンジンが開始された時間。
メソッド	呼び出された QIX メソッドの名前。
RequestId	QIX メソッド呼び出しが処理された要求の ID。
Target	QIX メソッド呼び出しのターゲットのメモリアドレス。
RequestException	QIX メソッド呼び出しの結果として発生した例外 (存在する場合) の ID。
AnyException	返されたエラー コード
ProcessTime	要求の処理に必要であった時間の合計。
WorkTime	要求によって実際に作業が行われた時間の合計。
LockTime	要求が内部ロックを待機しなければならなかった時間の合計。
ValidateTime	要求によって検証に使用された時間の合計。
TraverseTime	ハイパーキューブ内での走査のために、スレッドまたはファイバーによって費やされた時間 (ミリ秒単位)。
Handle	要求を処理したインターフェースの ID。このインターフェースは、グローバル、特定のシート、特定のオブジェクトなどが可能です。
DocId	QlikView ドキュメントのパスとその名前。
ObjectId	QlikView ドキュメントに含まれているオブジェクトの ID。
NetRAM	現在の RAM の割り当て数 (バイト単位)。
PeakRAM	ピーク時の RAM の割り当て数 (バイト単位)。
ObjectType	QlikView ドキュメントに含まれているオブジェクトの種類。

3 QlikView インストール

このセクションでは QlikView のインストールの方法について説明します。また、インストールの更新、修復、変更など、各種メンテナンス タスクについても説明します。

3.1 QlikView Server をインストールする

本書では、QlikView Server のインストールとライセンスの付与に必要な手順の概要を説明します。QlikView Desktop のインストール方法については、「QlikView Desktop のインストール」を参照してください。

QlikView サーバーをインストールする前に

QlikView サーバーをインストールする前に、以下の点を考慮する必要があります。

- Microsoft IIS をウェブ サーバーとして使用する場合は、QlikView Server より前にインストールしてください。
- QlikView Server はドメイン コントローラーとして機能するサーバーにはインストールできません。
- QlikView Server をインストールするには、インターネット プロトコル IPv4 または IPv6 が必要です。
- QlikView Server/Publisher をインストールすると、いくつかのセキュリティ グループが作成されます。インストールに従って、その他のセキュリティ グループをいくつか作成する必要があります。これらを正しく設定して、確実で適切なサービスの実行と、適切な機能へのアクセスができるようにする必要があります。インストールを開始する前に、**「セキュリティ グループ」** (*QlikView Publisher のリポジトリ (page 29)* 内) の記載を確認してください。
- 設定の大半が初期のファイルの場所に依存するため、QlikView Server インストール完了後のフォルダ移動は推奨されません。インストール後に QlikView Server を移動する必要がある場合は、QlikView サーバーを一度アンインストールしてからもう一度インストールし直してください。
- QlikView Publisher ライセンスをアクティブにすると、以前に定義したタスクはすべて削除されます。

セットアップの手順

1. 製品のダウンロード から、QlikView Server インストールの実行可能ファイルをダウンロードします。
   - Microsoft Windows x64 バージョン: *QlikViewServer_x64Setup.exe*

   詳細については、「*インストール ファイルのダウンロード (page 111)*」を参照してください。
2. 実行可能な QlikView Server インストールを実行します。
3. [ユーザー アカウント コントロール (User Account Control)] ダイアログが表示されたら、**[はい (Yes)]** をクリックして、プログラムがこのコンピュータ上で変更を行えるようにします。
4. [ようこそ (Welcome)] ダイアログで **[次へ (Next)]** をクリックします。
5. サーバー ロケーションの地域を選択します。**次へ** ボタンをクリックして進みます。
6. ライセンス使用許諾書を読み、**[同意する (I accept the terms in the license agreement)]** を選択し、**[次へ (Next)]** ボタンをクリックします。
7. QlikView Server の顧客情報を入力します。**次へ** ボタンをクリックして進みます。
8. 指定したフォルダにすべてのファイルがインストールされます。インストールされたファイルのルート フォルダを変更する場合は、**[変更 (Change)]** をクリックして場所を指定します。**[次へ (Next)]** ボタンをクリックして、続行します。

9. 実行したいインストールのタイプを選択します。
    - **1 台のコンピューターに QlikView Webserver をフル インストール (Full installation, Single machine with QlikView Web Server):** QlikView Web Server をウェブ サーバーとして 1 台のコンピュータにインストールし、すべてのコンポーネントを起動します。
    - **1 台のコンピューターに Microsoft IIS をフル インストール (Full installation, Single machine with Microsoft IIS):** Microsoft IIS をウェブ サーバーとして 1 台のコンピューターにインストールし、すべてのコンポーネントを起動します。このオプションは、ターゲット コンピューターに IIS がインストールされている場合にのみ利用できます。
    - **カスタム インストール、プロファイルの選択 (Custom installation, select profiles):** このオプションが選択されている場合は、インストールに含めたいプロファイルをダイアログの [プロファイル (Profiles)] セクションから選択します。
        - **QlikView Server:** QlikView Server、Directory Service Connector、QlikView Server のサンプル ファイルがインストールされます。
        - **エンジンのリロード/配布 (Reload/ Distribute Engine):** Reload Engine および QlikView Distribution Service がインストールされます。
        - **Management Console:** QlikView Management Service および QlikView 管理コンソール (QMC) がインストールされます。
        - **Webserver:** QlikView Web Server がインストールされます。

    インストールする機能をさらに設定するには、[**設定 (Config**)] をクリックします。終わったら [**次へ (Next)**] をクリックします。

    事前定義された機能の構成を使用するには、[**次へ (Next)**] をクリックします。

10. QlikView Server のアカウントを設定し、実行する Publisher サービスを選択します。**次へ** ボタンをクリックして進みます。

    > *QlikView サービスの実行に使用するアカウントには、ローカル管理者権限が必要です。*

    また、[サービスで後ほど使用するアカウントを指定したい (**I want to specify the account to be used for the services later**)] を選択することもできます。
11. ドロップダウン リストから IIS Website を選択して、[**次へ (Next)**] をクリックします。

    > *このステップは、**ステップ 8** で [**Full installation, Single machine with Microsoft IIS**] が選択されている場合にのみ適用されます。それ以外の場合は次のステップに直接進みます。*

12. サービス認証方法を選択します。
    - **デジタル証明書の使用 (Use digital certificates):** デジタル証明書と SSL/TLS を使用して QlikView Server 間の通信を認証します。この方法は、すべてのサーバーが共通 Windows Active Directory にアクセスできない環境や、証明書の認証によって提供されるセキュリティが必要な場合に推奨されます。デジタル証明書は、Windows Server 2008 R2 以降で**のみ**サポートされている点に留意してください。
    - **QlikView Administrators Group の使用 (Use QlikView Administrators Group):** ローカル Windows グループ QlikViewAdministrator でのメンバーシップに基づき、QlikView サービス

間の通信を認証します。この方法は、QlikView インストールの一部であるすべてのサーバーが共通の Windows Active Directory を使用して認証できる環境で使用することができます。

次へ ボタンをクリックして進みます。

13. **[インストール (Install)]** ボタンをクリックし、インストールを開始します。

この操作を完了するには、数分かかることがあります。

14. インストールが完了したら [**完了 (Finish)**] をクリックします。
15. Windows® からいったんログオフして再度ログオンすると、インストール中に追加されたグループ メンバーが更新されます。

Windows® からいったんログオフして再度ログオンするだけで十分ですが、QlikView Server の機能を有効にするには、コンピュータを再起動することをお薦めします。

インストールのログ

QlikView Server インストールを実行している間、セットアップの手順を記録します。ログ ファイルは次の通りです。

- Microsoft Windows x64 バージョン:*QlikViewServerx64.wil*

ログ ファイルは、ユーザーの *Temp* フォルダに保存されています (*%UserProfile%\AppData\Local\Temp* など)。インストールをする度に、新しいファイルが生成され、古いログ ファイルは上書きされます。

MSI パッケージを取得する

インストールに MSI パッケージが必要な場合は、以下の手順を実行し *.exe* ファイルから抽出します。

1. *.exe* ファイルを実行してインストールを開始し、最初のダイアログが開くまで待ちます。
2. パス *%UserProfile%\AppData\Local* の *Temp* フォルダにある MSI ファイル (通常 *ed34g.msi* のような名前で保存) を検索します。
3. 別の場所に *.msi* ファイルをコピーします。
4. *.exe* ファイルを使ったインストールを終了します。
5. *.msi* ファイルを使って QlikView Server をインストールします。

インストールを完了する

QlikView Server のインストールが正常に終了したら、QlikView Management Console (QMC) を登録して、ソフトウェアを有効化する必要があります。

QMC を起動する際にアクセスが拒否されたら、Windows からいったんログオフして再度ログオンすると、インストール中に追加されたグループ メンバーが更新されます。

サーバーでリアルタイムのウイルス対策を実行することは、QlikView Server のパフォーマンスに影響します。ユーザー ドキュメントやソース ドキュメント、ログ ディレクトリ、.pgo ファイルは、ウィルス対策スキャンから除外することを推奨します。

Microsoft IIS を実行する

タイムアウトを処理する

この処理は、タイムアウトを返す非常に大きな QlikView ドキュメントを使用する場合のみ必要です。

タイムアウトの処理は以下の手順に従ってください。

1. テキスト エディタ (Notepad など) で *%ProgramFiles%\QlikView\Server\QlikViewClients\QlikViewAjax\web.config* ファイルを開きます。
2. 次のテキストを検索します。
   ```
   <httpRuntime requestValidationMode="2.0" />
   ```
3. テキストを次のように編集します。
   ```
   <httpRuntime requestValidationMode="2.0" executionTimeout="900"/>
   ```
4. ファイルを保存します。

ASP.NET を有効にする

Microsoft IIS を Web サーバーとして使用している場合、QlikView Server のサンプル ページおよび拡張機能 (QlikView Server トンネルなど) が適切に動作するようASP.NET を有効にしてください。

パフォーマンスを最適化する

Microsoft IIS および AJAX 起動中にパフォーマンスを最適化するには、ウェブ サーバーで圧縮を行います。

IIS http 圧縮の設定方法について詳しくは、下記をご覧ください。
HTTP 圧縮

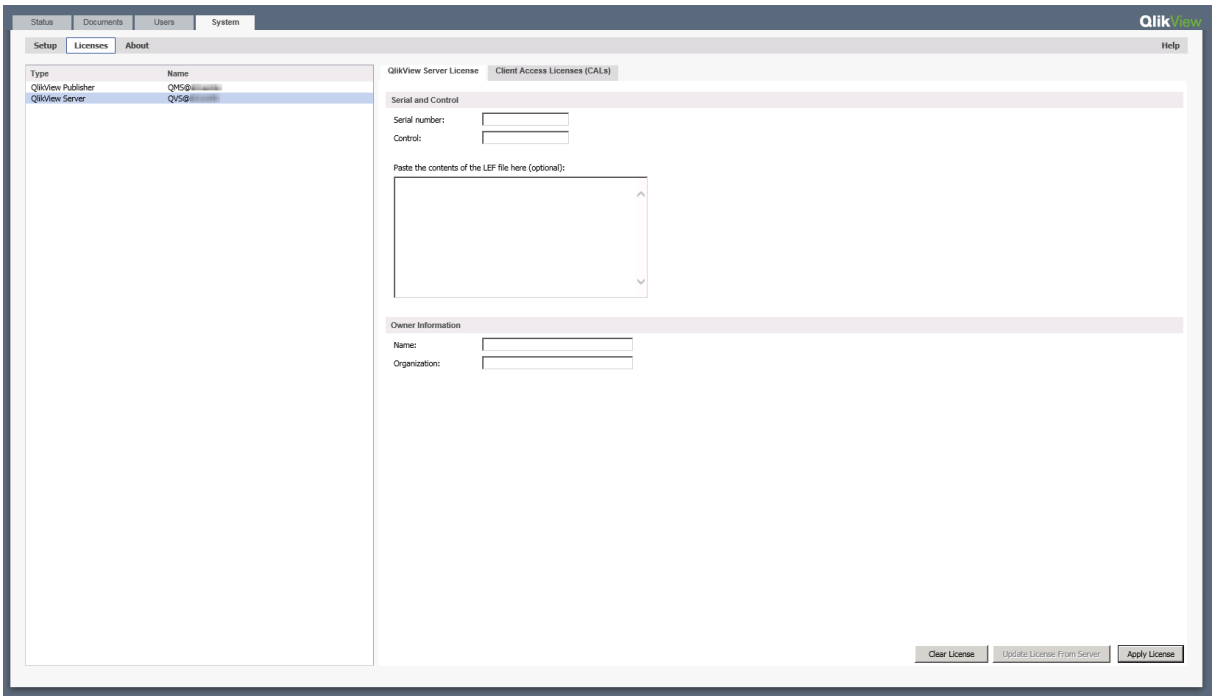
ライセンス

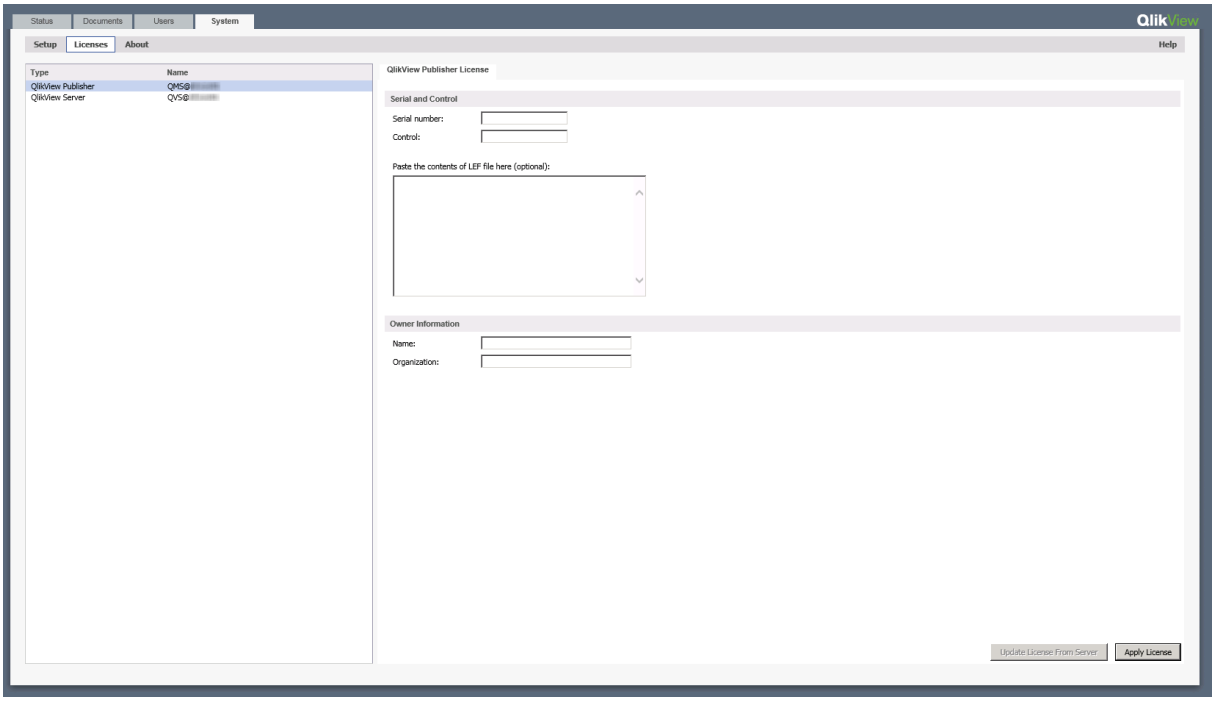
ライセンスは QlikView Server を認証し、特定のコンピュータ上で起動させるために使用します。

QlikView Server のライセンスを入力するには次の手順に従います。

1. QMC で [**システム (System)**] > [**ライセンス (Licenses)**] に移動します。
2. QlikView Server または Publisher を選択します。
3. [**QlikView Server ライセンス (QlikView Server License)**] または [**QlikView Publisher ライセンス (QlikView Publisher License)**] タブ (QlikView Server と Publisher のいずれかを選択したかによって異なります) の [**シリアル番号 (Serial number)**] と [**コントロール (Control)**] フィールドを入力します。

QlikView Publisher ライセンスをアクティブにすると、以前に定義したタスクはすべて削除されます。





QMC の QlikView Server/Publisher License タブ

ライセンスは、ドキュメントを開くたびにチェックされます。ライセンス認証ファイル (LEF) で指定された時間制限に達すると、QVS は自動的にオフライン モードに入ります。つまり、QMC からはアクセスできますが操作不能です。

QlikView Server 用のライセンス認証ファイル (LEF) である *lef.txt* は、*%ProgramData%\QlikTech* に自動的に保存されます。

QlikView Publisher 用の *PubLef.txt* ファイルは、*%ProgramData%\QlikTech\ManagementService\Publisher LEF* に保存されます。

QlikView LEF サーバーから新規の *lef.txt* ファイルをダウンロードするには [**サーバーからライセンスを更新 (Update License from Server)**] をクリックします。これは主に、Client Access License (CAL) の数を更新する際に使用します。

インターネットから LEF 情報にアクセスできない場合は、最寄の販売代理店から取得できます。その場合、*lef.txt* を上記のロケーションにコピーするか、QMC の QlikView Server/Publisher License タブのそれぞれの対応する項目に LEF データを貼り付けます。詳細な指示に関しては、販売代理店にお問い合わせください。

3.2 インストール ファイルのダウンロード

Qlik ダウンロード サイトには、Qlik 製品のインストールとアップグレードに必要なファイルが用意されています。Qlik コミュニティ内の「サポート」>「製品ニュース」>「製品のダウンロード」のサイトから確認できます。

次の手順を実行します。

1. 製品のダウンロード に移動します。
2. **Qlik データ分析** または **Qlik データ統合** を選択し、製品を選択します。
3. フィルターを使用して、可能なダウンロードのリストを絞り込みます。
4. **アセットのダウンロード** テーブルの **ダウンロードリンク** 列にあるリンクをクリックして、ダウンロードを開始します。

3.3 デジタル証明書によるサーバーの構成

サービス認証方法としてデジタル証明書を選択した場合、その証明書によって QlikView サーバー マシン上で実行されているサービス間に信頼性が創出されます。QlikView の新しいインスタンスを作成するときに、証明書がインストールされます。

スタンドアロン展開では、すべてのサービスが同じマシン上で実行されます。マルチサーバー環境に QlikView ノードをインストールする場合は、各サーバー上で有効化するサービスのみをインストールする必要があります。ノードをインストールするたびに完全インストールを実行した場合は、QlikView Management Service (QMS) の複数のインスタンスが作成されます。複数の QMS サービスを実行している場合、QMS は展開内のその他のノードに証明書を配布する役割があるので、証明書に不一致が生じます。インストーラを実行するときには、必ずカスタム インストールを選択して、有効化する必要のあるサービスのみをインストールします。

QlikView 構成のすべてのサーバーで同じ Windows Administrator を使用するようお勧めします。

セキュリティの構成

QlikView 展開をできるだけ安全にするには、すべての QlikView サーバーでセキュア ソケット レイヤー (SSL) セキュリティを構成します。

QlikView サーバーでの SSL の有効化

Directory Service Connector (DSC)、QlikView Web Server (QVWS)、QlikView Management Service (QMS)、QlikView Distribution Service (QDS)、および QlikView Server (QVS) で SSL を使用するサーバー間で、証明書サービス認証を有効化するには、以下を実行します。

1. QlikView 管理コンソールを実行している QlikView Management Service を停止します。
2. メモ帳を管理者として実行します。
3. QMS 構成ファイルをメモ帳で開きます。
4. キーの `UseWinAuthentication` の値を `true` から `false` に変更します。
5. 変更内容を保存します。
6. QMS サービスを開始します。

QMS サービスを実行するサーバー上に証明書が正しく設定されていることを確認するには、[スタート] メニューから Microsoft Management Console (MMC) を実行します。

次に、システムの DSC、QDS、QVWS、IIS サービスで上の手順を繰り返します。

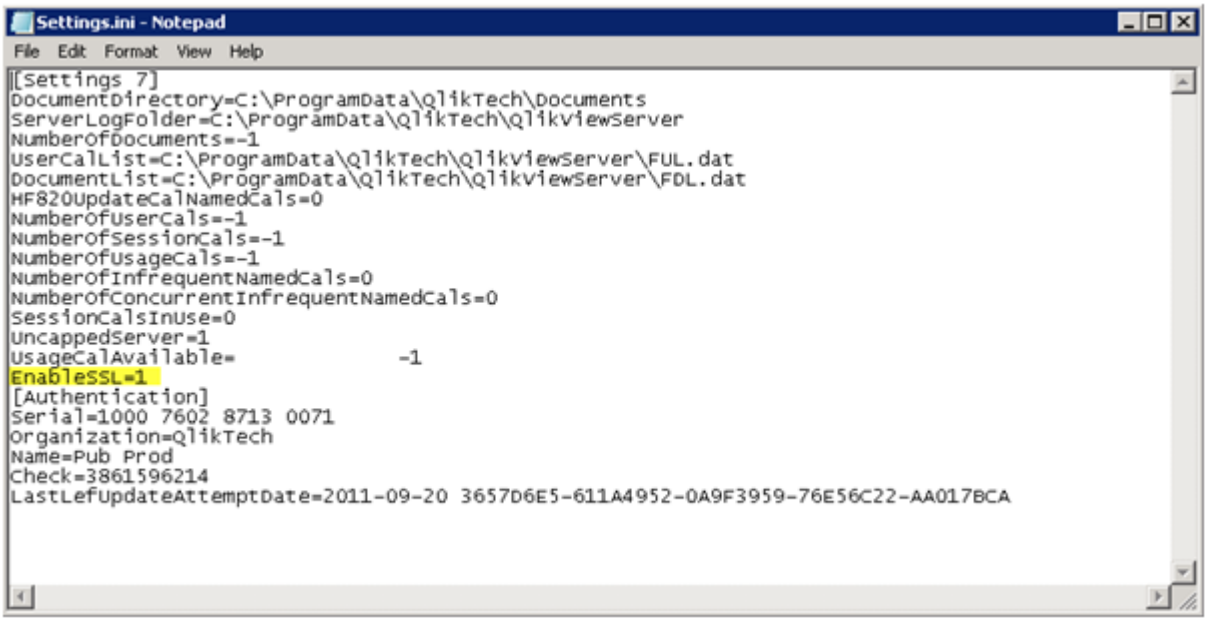
IIS および QlikView Server で証明書の信頼性を構成するには、ポート 4750 (QVWS が使用するものと同じポート) を使用します。ウェブ サーバーのユーザーによる HTTPS アクセスの有効化に使用される証明書は変更されません。

QlikView Server (QVS) 用 SSL の有効化

QlikView サーバー サービス (QVS) に SSL を構成するには、さらに以下の手順を実行します。

QVS サービスの *Settings.ini* ファイルを編集するには、以下の手順を実行します。

1. QVS サービスを停止します。
2. メモ帳を管理者として実行します。
3. メモ帳で *Settings.ini* ファイルを開きます。
4. `[Settings 7]` セクションに `EnableSSL=1` を追加します。



5. 変更内容を保存します。
6. QVS サービスを開始します。

QlikView Service Dispatcher (ライセンスサービス) の SSL の有効化

ライセンスサービスの Secure Socket Layer (SSL) セキュリティを有効にする必要があります。ライセンスサービスは、Service Dispatcher を介して管理されます。

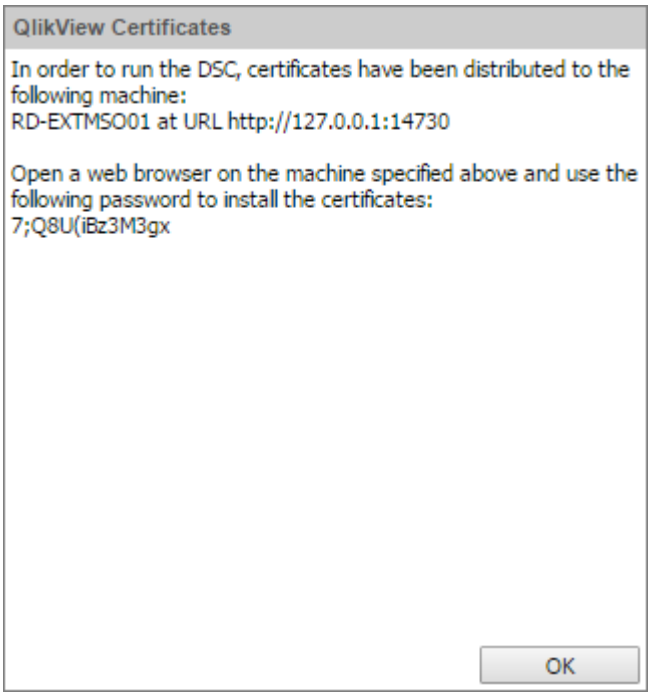
1. Service Dispatcher を停止します。
2. メモ帳を管理者として実行します。
3. メモ帳で、*Services.conf* ファイル (*C:\Program Files\QlikView\ServiceDispatcher\services.conf*) を開きます。
4. *[licenses.parameters]* セクションで、変更
   `-qv-auth-mode=ntlm`
   に変更します
   `-qv-auth-mode=cert`
5. 変更内容を保存します。
6. Service Dispatcher を起動します。

QlikView サービスの追加

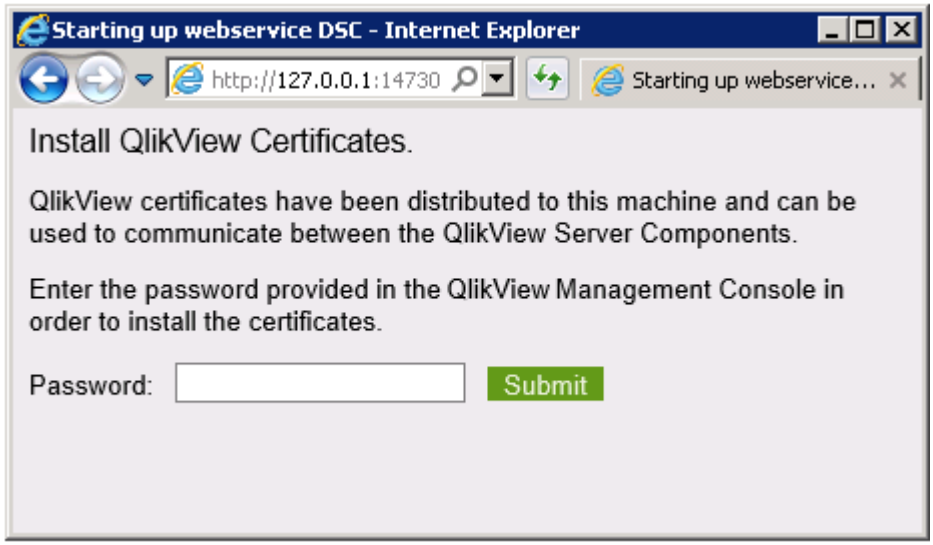
QlikView サービスを追加するには、以下の手順を実行します。

1. QlikView 管理コンソールを開きます。
2. [**System**] (システム) タブをクリックし、[**Setup**] (設定) をクリックして、すべての QlikView サービスを表示します。
3. 新しいサービスを追加するには、QlikView Servers パネル内右側にある [**Add**] (追加) アイコンをクリックします。

4. テキスト ボックスに **サービスの URL** を入力して、[**Apply**] (適用) をクリックします。新しいエントリが、左側パネルのツリー表示で利用可能になります。各サービスを新しいサービスとして追加し、既存のサービスを削除します。
5. サービスを追加すると、[**QlikViewCertificates**] (証明書) ウィンドウが表示されます。



6. 新しいサービスを追加しているサーバー上で Web ブラウザを開き、URL と、QlikView 管理コンソールの [**QlikView Certificates**] (証明書) ウィンドウに表示されているポート (14720、14730、または 14750) を入力します。
7. [QlikView 管理コンソール **QlikView Certificates**] (証明書) ウィンドウに表示されているパスワードを入力します。



8. 成功するとメッセージが表示され、パスワードが正しく、QlikView サービスがそのポートを経由してアクセスできることが確認されます。

この時点で、[スタート] メニューからMMC を実行し、追加の QlikView サービスを実行するサーバー上で証明書が適切にインストールされているか確認できます。

証明書の更新

証明書が失効した、または間もなく失効する場合、あるいは、機密性の高いデータに新しい暗号化鍵を生成する場合、新しい証明書を生成します。忘れずに古い証明書のコピーを作成してください。

証明書が失効するのは 10 年後ですが、いつでも更新できます。証明書の有効期限は QMC に表示されています。有効期限まで残り30 日以下になると、QlikView 管理コンソール に警告が表示されます。

> *証明書は置き換えるべきではありませんが、更新は可能です。既存の証明書を削除すると、結果的にデータを復号化できなくなる可能性があります。*

証明書の失効以外にも、証明書のひとつがコンピュータ名とリンクされることから、たとえば、コンピュータの交換やコンピュータ名の変更などの理由で、更新が必要になることが考えられます。

証明書を更新するには、クラスター内の各マシンで以下の手順を実行します。

1. すべての QlikView サービスをシャットダウンします (順序は関係ありません)。
2. 現在使用中のマシンに、交換の必要がある有効な証明書がある場合は、構成フラグ **InstallingNewCertificatesAndCryptoKey** Qlik License Service を除くすべての QlikView サービス。
3. すべての QlikView サービスを開始します (順序は関係ありません)。
4. [**System**] (システム) タブをクリックし、[**Setup**] (設定) をクリックします。
5. サービスを選択し、そのサービスの [**General**] (基本設定) タブをクリックします。
6. ウィンドウ右下にある [**Apply**] (適用) ボタンをクリックし、指示に従って証明書をインストールします。
7. 更新された証明書を必要とする各サービスに、上記の手順を繰り返し実行します (順序は関係ありません)。certificates.
8. すべての QlikView サービスをシャットダウンします (順序は関係ありません)。
9. 構成フラグ **InstallingNewCertificatesAndCryptoKey** を前の手順で有効化した場合は、すべてのサービスでフラグを無効化します。
10. すべてのサービスを開始します。最初に QlikView Management Service (QMS) を開始します。

開始時に新しい証明書が見つかると(新しい暗号化鍵を含む)、サービスはすべての機密性の高いデータを新しい暗号化鍵で再暗号化します。

> *古い証明書は (現在、実質上廃止されてはいるものの)、削除しないように強くお勧めします。データの古いバックアップを復元する必要が生じた場合、データの復号化には、古い証明書 (と対応した暗号化キー) が必要になります。*

インストールされている製品の証明書を更新する場合は、Qlik License Service より前に QlikView Management Service (QMS) を再起動する必要があります。この順序でサービスを開始することにより、正しい証明書セットがエクスポートされ、Qlik License Service で使用できるようにします。Qlik License Service のステータスは、Qlik Service Dispatcher を起動して停止することによって管理できます。

構成 **InstallingNewCertificatesAndCryptoKey** フラグ

このフラグを true に設定して有効化した場合、サーバー マシンにインストールされている既存の証明書は無視されます (CryptoAlgorithm を抽出する場合を除く)。このフラグは DSC、QDS、QVWS で使用されますが、QMS では用いられず、既定では無効化 (false に設定) されています。

証明書を更新するときは、新しい証明書の取得を可能にするためにこのフラグを有効化します。証明書の更新が済んだら、すべてのサービスでフラグを false に設定します。

フラグを有効化するには、

`InstallingNewCertificatesAndCryptoKey=True`
を次の構成ファイルに追加します。

- *C:\Program Files\QlikView\Distribution Service\QVDistributionService.exe.config*
- *C:\Program Files\QlikView\Directory Service Connector\QVDirectoryServiceConnector.exe.config*
- *C:\Program Files\QlikView\Server\Web Server\QVWebServer.exe.config*

復号化できないデータによる サービスの不具合

サービスの起動時、各サービスがすべての暗号化データ エントリにアクセスできるか検証されます。サービスで復号化できないデータが検出されると、エラーを報告し、サービスの実行が停止されます。

サービスでデータを復号化できない理由は 2 つあります。

1. 証明書が見つからない - 必要な暗号化キーを含む証明書がない。この問題を解決するには、証明書をバックアップから再インストールして、サービスを再起動します。
2. 暗号化されたデータを復号化できない - この問題を解決するには、復号化できないデータを消去します。

破損したデータの消去方法

復号化できないデータを消去するため、非表示になっている構成 `EraseUndecryptableData` フラグを一時的に有効化するには、以下の手順を実行します。

1. サービスを停止します。
2. メモ帳を管理者として実行します。
3. 構成ファイルをメモ帳で開きます。
4. `EraseUndecryptableData` のエントリを追加して `true` に設定します。
5. ファイルを保存します。
6. サービスを再始動します。

サービスが起動すると、データの復号化できない部分のみが消去されています。

7. サービスを停止し、構成ファイルを開いて `EraseUndecryptableData` のエントリを削除します。
8. ファイルを保存し、サービスを再始動します。
   サービスは通常どおりに開始します。

QMC で、消去したデータを再入力します。復号化できないデータエントリのすべてがすでにサービスのログ ファイルに出力されており、QMC に再入力する必要があるデータを示します。

3.4 サイレントインストール

サイレントインストールを起動すると、限定したダイアログ数で、もしくはダイアログなしで QlikView がインストールされます。つまり、サイレントインストール パッケージを作成する場合は、すべての機能やプロパティ、ユーザー選択を把握しておく必要があります。また、Windows Installer Service の標準プロパティが必要な場合もあります。

サイレントインストールを準備するには、QlikView *Setup.exe* ファイルから MSI ファイルを抽出する必要があります。

サイレントインストールは異なるインターフェース レベルで実行可能です。

インターフェース レベル

コマンド	**[Type] (種類)**
/qn	完全なサイレントインストール。
/qb	基本的なユーザー インターフェース。

+ サインをインターフェース レベルのコマンドの最後に追加すると、インストールの最後にモーダル ダイアログが開き、インストールが正常に終了したかどうかが表示されます。

QlikView で推奨されるサイレントインストールのコマンドラインは次の通りです。

msiexec /i QlikViewServerx64.msi Addlocal="all" IS_NET_API_LOGON_ USERNAME="Domain\username" IS_NET_API_LOGON_PASSWORD="password /qn+

または、

QlikViewServer_x64Setup.exe /s /v"/qn+ Addlocal="all" IS_NET_API_LOGON_ USERNAME="Domain\username" IS_NET_API_LOGON_PASSWORD="password"

上記コマンドが、インストールの最後に表示されるモーダル ダイアログとともにすべての機能をインストールします。

インストールする機能を限定する場合は、*all* の部分を機能名に変更します。複数の機能にインストールを限定する場合は、各機能名をコンマで区切ります。

インストール可能な機能は次の通りです。

- DirectoryServiceConnector
- ManagementService
- QVS

- QvsDocs
- Webserver
- DistributionService
- SupportTools
- QvsClient (サブ機能プラグインとAjaxZfc 付き)
- MsIIS (サブ機能 QvTunnel とQlikView Settings Service 付き)

> *インストールにサブ機能を含む場合は、インストールする機能一覧を含む必要があります。*

msiexec /i QlikViewServerx64.msi ADDLOCAL="all" DEFAULTWEBSITE="2" /qn+

このコマンドラインがすべての機能をインストールします。これには仮想ディレクトリからデフォルト以外の別のウェブサイトが含まれます。これには、Microsoft Internet Information Services (IIS) がインストールされているマシンと複数のウェブサイトが必要です。また、サイトの番号も必要です。仮想ディレクトリがインストールされているサイトの番号に *DEFAULTWEBSITE* を設定します。ウェブサイト数を調べるには、IIS を確認します。

インストール手順のログを記録するには、次のコマンドを使用します。

*msiexec /i QlikViewServerx64.msi ADDLOCAL="all" DEFAULTWEBSITE="2"/L*v log.txt /qn+*

設定

サイレントインストール パッケージを設計する場合に、知っておくと便利な設定は次の通りです。

サイレントインストール設定

構成	説明
前提条件	.NET Framework 4.8 以上 *.NET Framework 4.8 を動作させるには、Windows 10 を Anniversary update ビルド 1607 以降にアップデートする必要があります。*
デフォルトのインストール先フォルダ (INSTALLDIR)	ProgramFilesFolder\QlikView
Windows Installer のバージョン	3.1 スキーマ 301
デフォルトの言語	英語 (米国) 1033
管理者権限の必要性	はい
INSTALLEVEL	100。デフォルトではすべての機能を 101 に設定
機能	「インストール (Install)」と呼ばれる隠し機能があります。これを削除することはできません。
IIS	4 つの仮想ディレクトリとアプリケーション プールがインストールされています。
サービス	5 つのサービスがインストールされています。

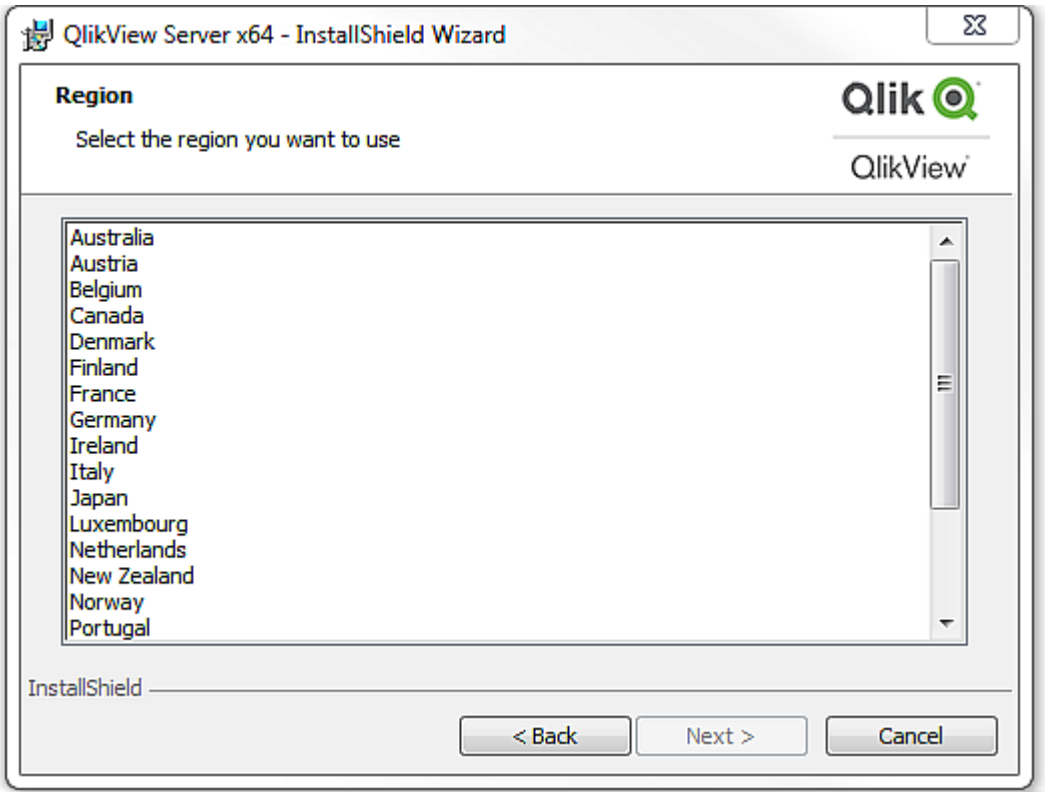
ダイアログ

QlikView のインストールは多数のダイアログで構成されており、これらには [カスタム設定 (Custom Setup)] や [ウェブサイト (Website)] ダイアログが含まれます。すべてのダイアログには重要なプロパティが設定されています。プロパティ値を検索するには、詳細ログが作成されるテストインストールを行います。プロパティ値は使用する言語やオペレーション システムによって異なる場合があります。

地域 (Region)

このダイアログは、地域を指定するために使用します。

プロパティ:*REGION_LIST*

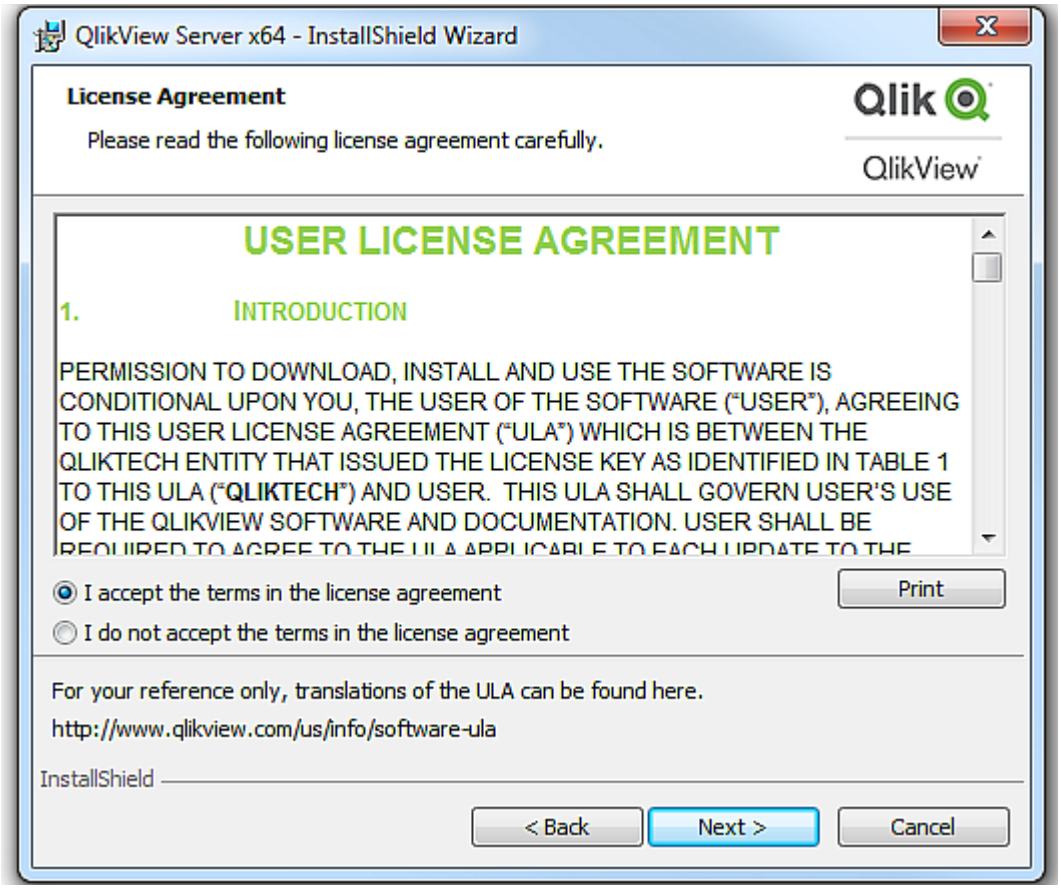


[地域 (Region)] ダイアログ

ライセンス使用許諾 (License Agreement)

このダイアログには選択した地域用のライセンス使用許諾が表示されます。

ラジオ ボタン:*AgreeToLicense = "Yes"*



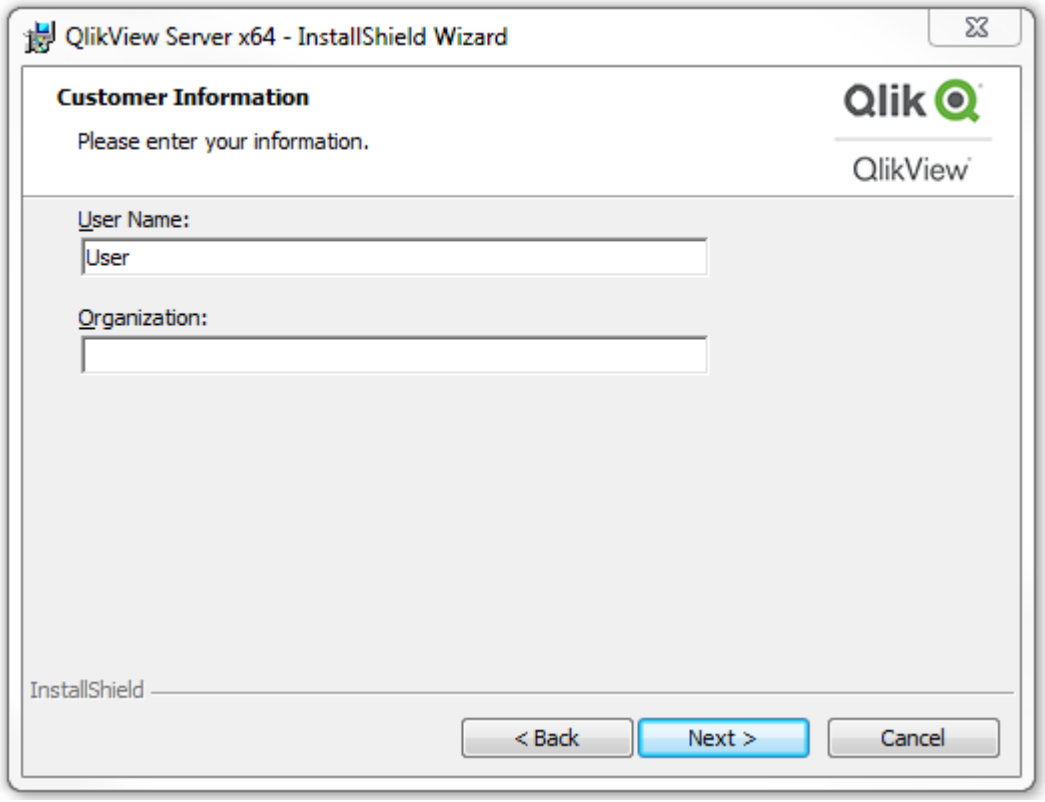
[ライセンス (License)] ダイアログ

顧客情報 (Customer Information)

このダイアログは、顧客情報を入力するために使用します。

プロパティ:

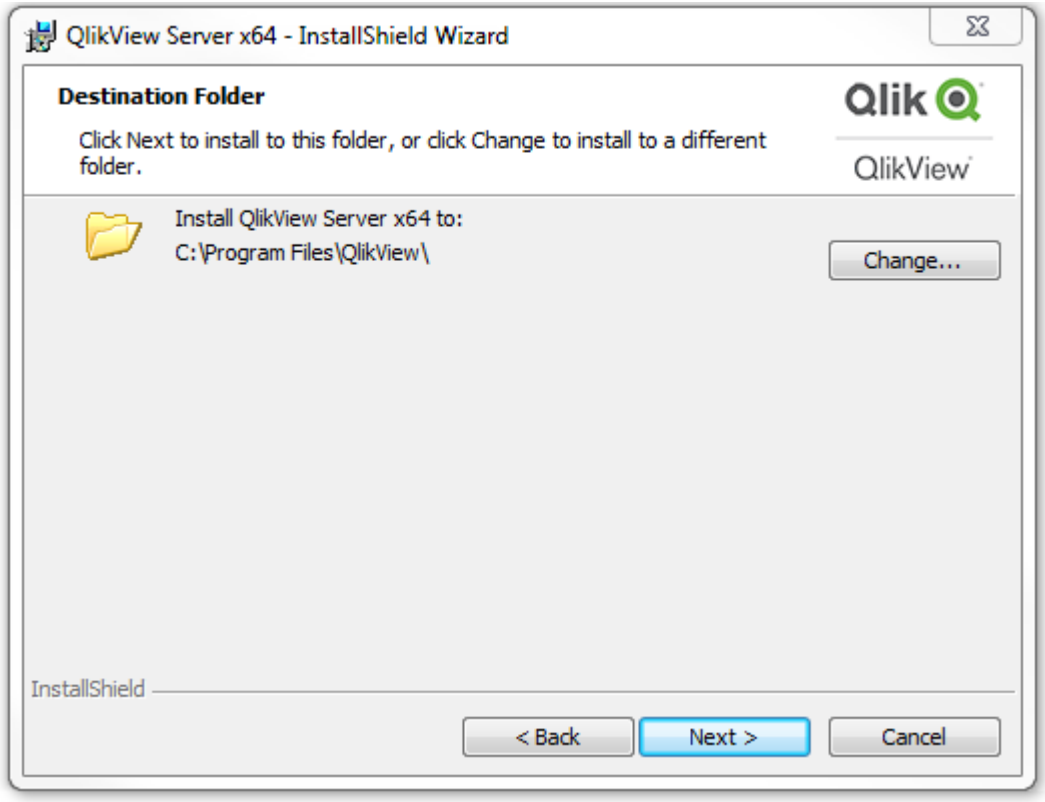
- *USERNAME*
- *COMPANYNAME*



[顧客情報 (Customer Information)] ダイアログ

インストール先 フォルダ (Destination Folder)

このダイアログは、デフォルトのインストール先 フォルダを設定するために使用します。



[インストール先 フォルダ (Destination Folder)] ダイアログ

プロファイル (Profiles)

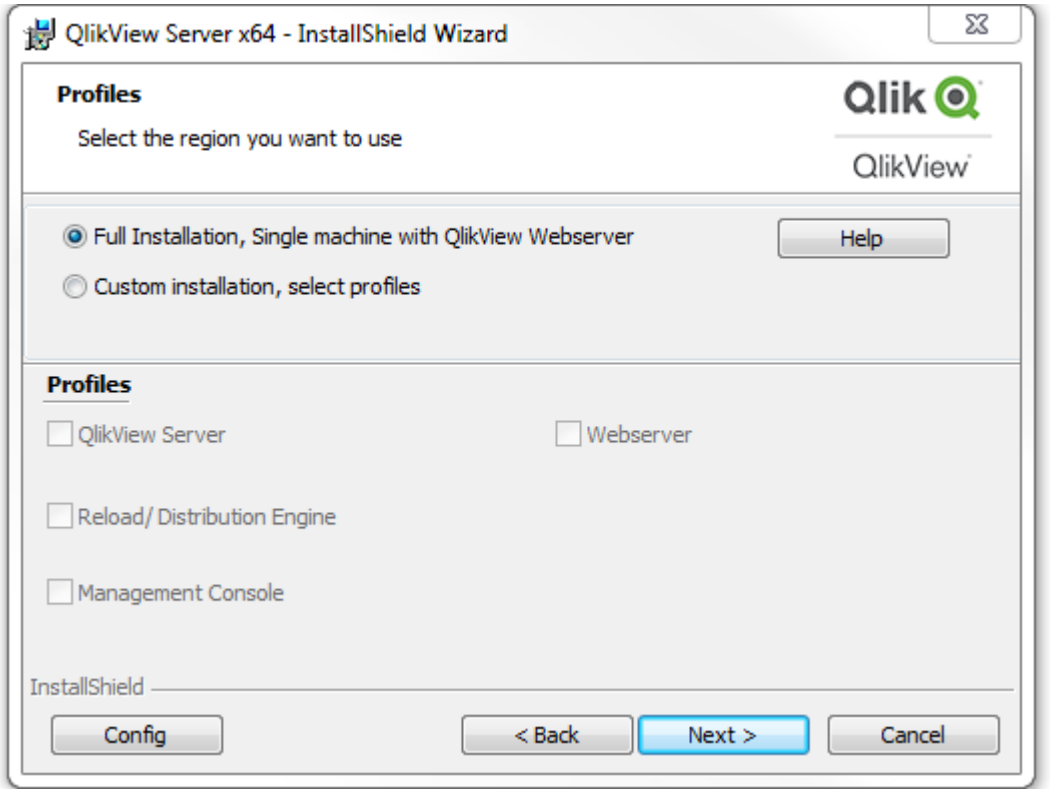
このダイアログには、選択可能な複数のプロファイルとともにそれに関連したいくつかのプロパティがあります。

[1 台のコンピュータに QlikView Web Server をフル インストール (**Full Installation, Single machine with QlikView Webserver**)] を選択すると、1 台のマシンに、QlikView の起動に必要な QlikView Web Server を含むすべてのコンポーネントがインストールされます。IIS を使用したい場合は、[**1 台のコンピュータに Microsoft IIS をフル インストール (Full installation, single machine with Microsoft IIS)**] を選択します (このオプションは、マシンに Microsoft IIS がインストールされている場合にのみ利用できます)。

カスタム インストールを実行する場合は、[カスタム インストール、プロファイルの選択 (**Custom installation, select profiles**)] を選択して、インストールするプロファイルを選択します。**Webserver** プロファイルを選択すると、ユーザーは QlikView Web Server と IIS のいずれかを選択できます (IIS がマシンにインストールされている場合のみ)。

プロパティ:

- *PROPQVS*: QlikView Server
- *PROPDS*: Publisher
- *PROPQMC*: Management Console
- *PROPWEB*、*PROPIIS* = 1 か 2: Webserver Webserver
- *PROPIIS* (IIS がインストール済みの場合) または *PROPSTATE*: 単一マシンにインストール



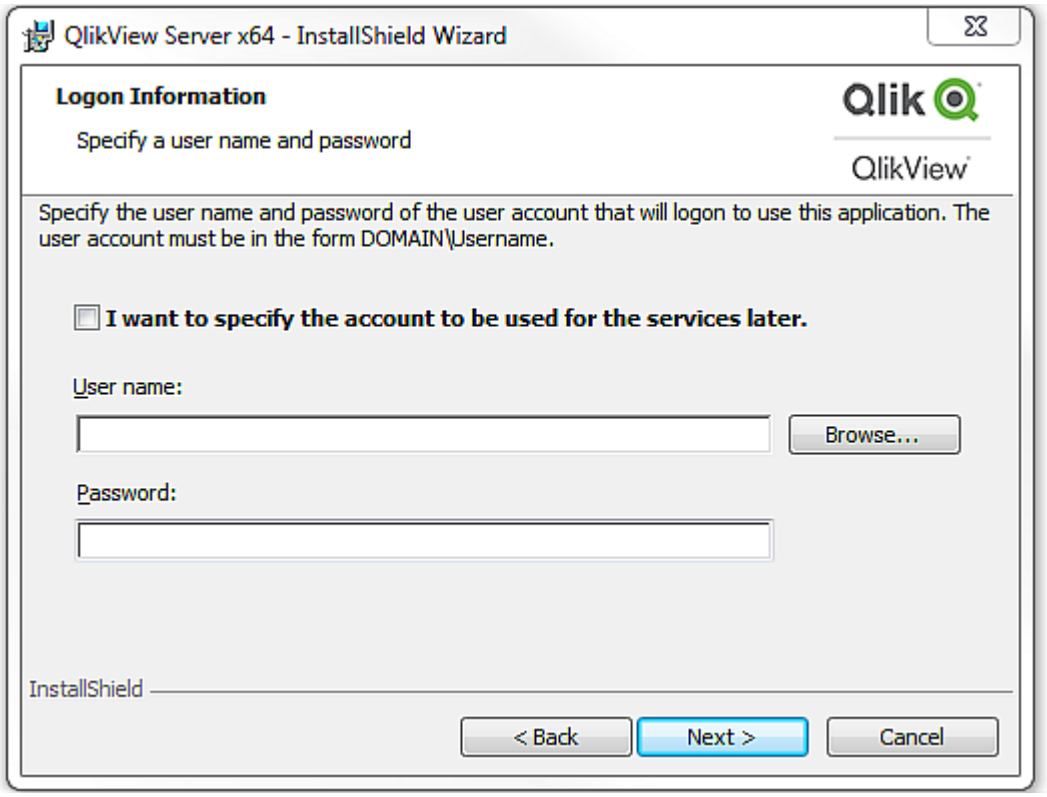
[プロファイル (Profiles)] ダイアログ

ログイン情報 (Logon Information)

このダイアログは、インストールしたサービスを起動させるユーザーを指定するために使用します (オプション)。入力して **[次へ (Next)]** をクリックすると、カスタム アクション (Custom Action) が入力したユーザーが有効であることを確認します。カスタム アクションは InstallShield が実行しますが、これが正常に機能するには、マシンがドメインベースのサーバーに接続している必要があります。

プロパティ:

- *LOCALSERVICE*
- *IS_NET_API_LOGON_USERNAME*
- *IS_NET_API_LOGON_PASSWORD*

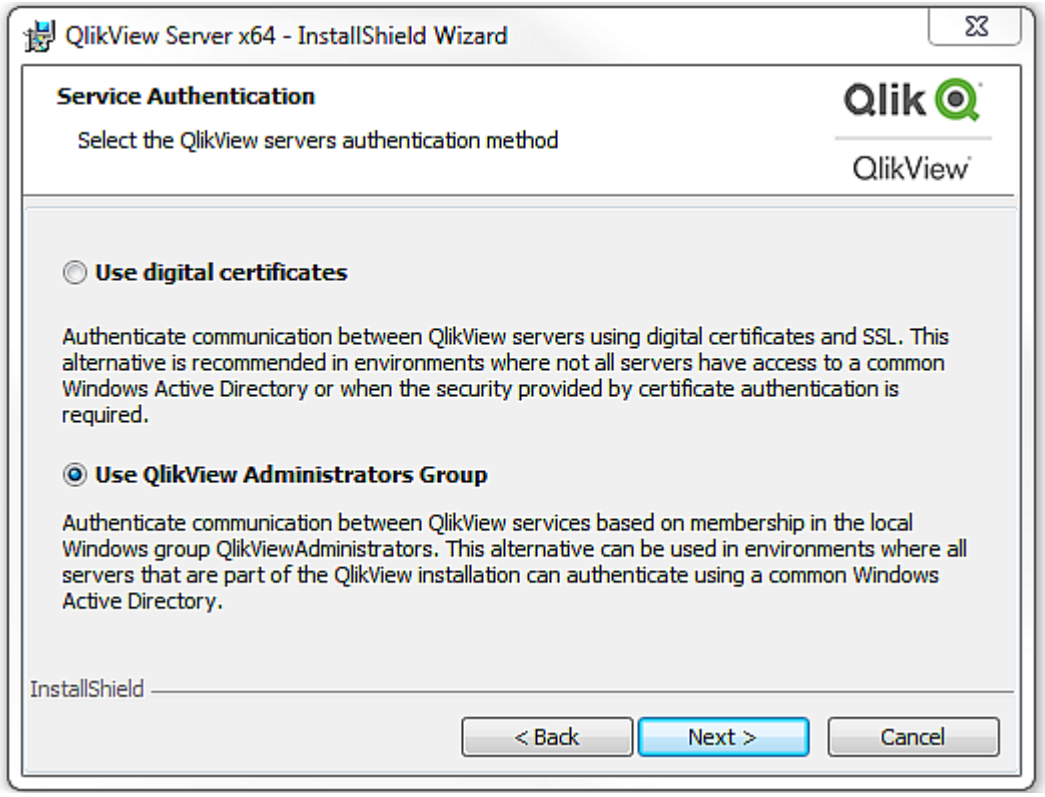


[ログイン情報 (Logon Information)] ダイアログ

サービス認証 (Service Authentication)

このダイアログは、サービス認証タイプを選択する際に使われます。デフォルトで QlikView Administrators Group が選択されています。

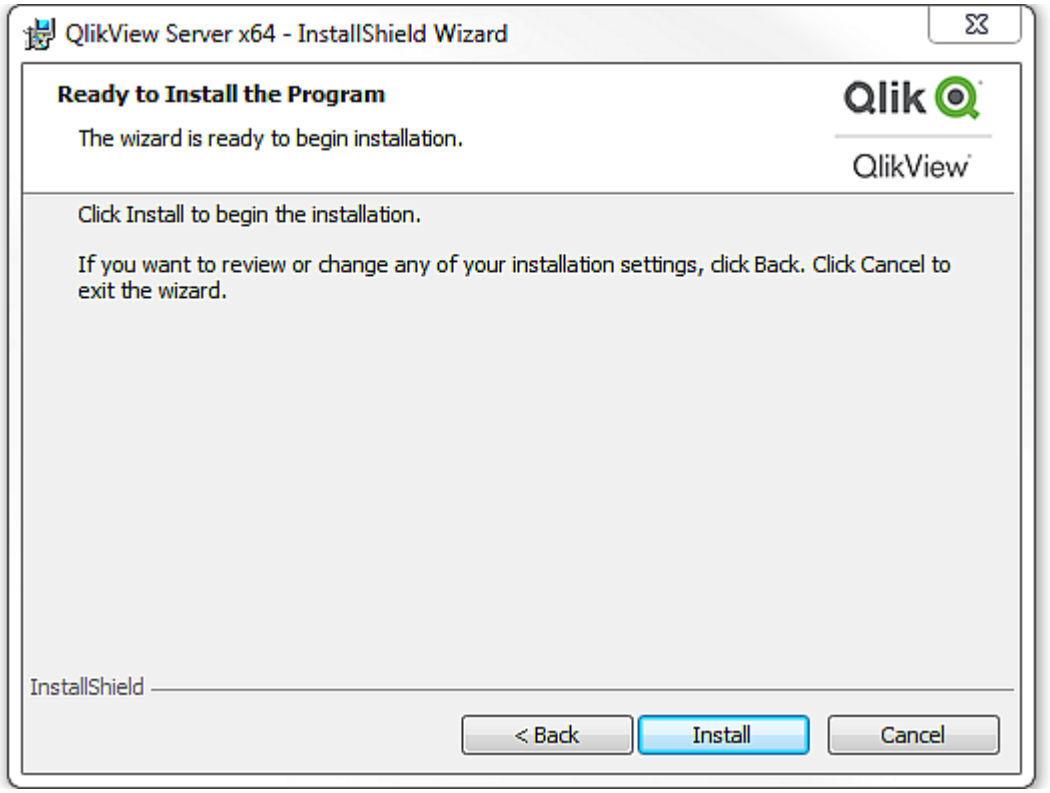
プロパティ:*PROPCERT* (1 = デジタル証明書、2 = QlikView Administrators Group)



[サービス認証 (Service authentication)] ダイアログ

インストールの準備完了 (Ready to Install)

これは最後に表示されるダイアログです。**[インストール (Install)]** ボタンをクリックし、インストールを開始します。



[インストールの準備完了 (Ready to Install)] ダイアログ

その他のダイアログ

カスタム設定 (Custom Setup)

このダイアログは [プロファイル (Profiles)] ダイアログで **[設定 (Config)]** をクリックすると表示されます。

[カスタム設定 (Custom Setup)] ダイアログ

ウェブサイト (Website)

このダイアログは [プロファイル (Profiles)] ダイアログで、ウェブ サーバーとして IIS を選択すると表示されます。

プロパティ:*DEFAULTWEBSITE*

[ウェブサイト(Website)] ダイアログ

MST

MST ファイルは、ソースである MSI ファイルを直接変更することなく、MSI が実行するインストール動作を変更することができます。MST ファイルは MSI とコンピュータ間でフィルタのような働きをし、インストール手順をカスタマイズします。たとえば、QlikView Server のデフォルトのインストール先フォルダ *%ProgramFiles%\QlikView* を MST ファイルで *C:\QlikView* に変えると、デフォルトのフォルダが変更されます。プロパティは事前に設定可能なため、ダイアログを使っても同じ操作が可能です。つまり、ダイアログの設定を限定的にしてインストールを行えます。

MST ファイルを作成するには、MSI をリパッケージングする InstallShield AdminStudio などが必要です。

> *Qlik が MST ファイルを提供することはありません。また、顧客もしくはパートナーが作成した MST ファイルについていかなる責任も負いません。*

サイレント アンインストール

QlikView で推奨されるサイレント アンインストールのコマンド ラインは次の通りです。

QlikViewServer_x64Setup.exe /x /s /v"/qn"

上記のコマンド ラインは、すべての機能を完全にサイレントに削除します。

+ サインをインターフェース レベルのコマンドの最後に追加すると、インストールの最後にモーダル ダイアログが開き、インストールが正常に終了したかどうかが表示されます。

3.5 QlikView Server で Qlik ライセンス サービス通信のプロキシを構成する

プロキシで Qlik ライセンス サービスとライセンス バックエンド間の通信を処理できます。

Qlik License Service は QlikView April 2019 以降のリリースに組み込まれており、QlikView Server が署名付きキー ライセンスを使用して有効化されている場合に使用されます。Qlik License Service にはライセンスに関する情報が保管され、製品の有効化と権利の管理の際に Qlik によってホストされている License Back-end Service と通信します。License Back-end Service へのアクセスとライセンス情報の取得にはポート 443 が使用されます。

マルチノード展開の場合は、Qlik License Service は QlikView Management Service (QMS) が実行されているマシンにインストールされます。Qlik License Service のステータスは、Windows マシンで実行中のサービスのリストにある Qlik Service Dispatcher を起動して停止することによって管理できます。

Qlik ライセンス サービスと Qlik ライセンス バックエンド間の通信をプロキシで処理するように構成できます。

QlikView Server で、Qlik ライセンス サービスのプロキシの構成は、コマンド行パラメータを使って実行されます。HTTP と HTTPS スキームは両方ともサポートされています。

HTTP トンネル経由で通信する際、QlikView Server June 2020 以降の NTLM およびライセンス サービスに対する基本認証機能を使用できます。これにより、トンネル プロキシ上の認証が可能となり、より安全な環境を構成できます。

次の手順を実行します。

1. Qlik Service Dispatcher を停止します。これは、Qlik ライセンス サービスの実行を処理します。
2. *service.conf* ファイルに移動します。これは、デフォルトで次の場所にあります: *%Program Files%\QlikView\ServiceDispatcher\service.conf*
3. セクション `[licenses.parameters]` の位置を確認します。これは、デフォルトで次の行を含みます:
   ```
   [licenses.parameters]
    -qv-mode=true
    -app-settings="..\Licenses\appsettings.json"
   ```
4. 下記のように行 `-proxy-uri=http://myproxy.example.com:8888` を追加します:
   ```
   [licenses.parameters]
    -qv-mode=true
    -proxy-uri=http://myproxy.example.com:8888
    -app-settings="..\Licenses\appsettings.json"
   ```
   「http://myproxy.example.com」は貴社のプロキシのアドレスであり、「8888」はプロキシで使用されるポートです。

   > *プロキシ URI には、ドメイン名でなく IP アドレスを指定できます (例: `-proxy-uri=http://10.76.124.124:1337`)。*

5. *%ProgramFiles%\QlikView\Licenses* に進み、`Encrypt-Password.ps1 [password for proxy access]` を実行します。

```
Encrypt-Password.ps1 123456
```
生成された暗号化パスワードをコピーして、次のステップで使用します。

6. トンネリングプロキシで認証を必須とするには、*services.conf* ファイルに次の行を追加します:
```
-proxy-uri=[the uri of the proxy]
-proxy-auth-mode=ntlm|basic|(leave empty for no authentication)
-proxy-user=[username without domain]
-proxy-encrypted-password=[password]
-proxy-domain=[the domain] (only for NTLM)
```
7. *services.conf* ファイルを保存して閉じます。
8. Qlik Sense Service Dispatcher を再起動します。
9. マルチノードインストールがある場合、インストールですべてのノードにこれらのステップを繰り返してください。

3.6 QlikView Server の優先暗号スイートの構成

Qlik License Service が署名付きキーライセンスの暗号化と復号化に使用する優先暗号スイートをランク付けできます。

Qlik License Service は QlikView Server April 2019 以降のリリースに含まれています。

> *認証プロトコルとして mTLS または NTLM を使用するように QlikView Server を構成できます。ただし、NTLM サービスを使用する場合は、優先暗号スイートを構成できません。*

Qlik License Service が証明書サービス認証を使用するように設定されている場合は、相互 TLS 認証 (Mutual TLS Authentication (mTLS)) を使用します。このプロトコルにより、サーバーとクライアントの両方からの要求が確実に信頼されます。Qlik License Service はポート 9200 でリッスンします。

> *TLS 1.2 は、QlikView 12.0 以降でサポートされています。*

次のリストは、サポートされている暗号スイートを示しています。

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA25
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Qlik License Service の優先暗号スイートを構成するには、次の手順を実行します。

1. *service.conf* ファイルを開きます。
   デフォルトのパスは *%Program Files%\QlikView\ServiceDispatcher\service.conf* です。
2. 次のセクションに移動します。
   ```
   [license.parameters]
   -qv-mode=true
   -qv-auth-mode=cert
   ```
3. 次のように、暗号のコンマ区切りリストをセクションに追加します。
   ```
   [license.parameters]
   -qv-mode=true
   -cipher-suites=TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_
   SHA
   -qv-auth-mode=cert
   ```
4. ファイルを保存して閉じます。
5. Qlik License Service の実行を処理する QlikView Server Service Dispatcher を再起動します。
6. マルチノード環境を使用している場合は、ノードごとに上記の手順を繰り返します。

3.7 グループ ポリシーを使用した MSI パッケージの導入

この章では、主に QlikView プライグインを想定しています。

(基本設定)

今日、共通した課題となるのは、ユーザーの権限が制限されているネットワーク環境や特定のユーザー グループに、どのような方法でアプリケーションを導入するかということです。このセクションでは、アクティブ ディレクトリ環境においてグループ ポリシーを使用した Microsoft Windows Installer (*.msi*) パッケージの導入方法について簡単に説明します。

QlikView の *.msi* パッケージには、インストール先のワークステーションに Windows Installer サービスのバージョン 2.0 以降がインストールされている必要があります。

MSI パッケージを導入する

.msi ファイルを取得したら、ネットワーク上の共有フォルダに保存してください。アプリケーションをインストールするユーザーやコンピュータが、そのフォルダの読み取りアクセス権を持っていることを確認します。ユーザーやコンピュータでパッケージが使用可能になったら、グループ ポリシー オブジェクトによりインストール パッケージが作成されたことが通知されます。

パッケージは各ユーザー、もしくはコンピュータごとに通知できます。ユーザーごとにパッケージの通知を行うには、**[ユーザー設定 (User Configuration)] > [ソフトウェア設定 (Software Settings)]** を使用し、コンピュータごとに通知を行うには **[コンピュータ設定 (Computer Configuration)] > [ソフトウェア設定 (Software Settings)]** を使用します。どちらも、グループポリシー オブジェクトの編集画面にあります。

ユーザーごとにパッケージの通知を行う方法には、割り当てと公開の 2 通りがあります。コンピュータごとにパッケージの通知を行う場合は、公開のみが利用できます。

ユーザーごとにパッケージを公開すると、[プログラムの追加と削除] ダイアログの [ネットワークからプログラムを追加] にリスト表示 (通知) されます。

[プログラムの追加と削除] ダイアログ

各ユーザーがインストールを完了するには **[追加]** ボタンをクリックする必要があります。

コンピュータごとにパッケージを公開するには、パッケージをインストール後にコンピュータを再起動します。すると、すべてのユーザーがアクセス可能になります。

割り当てる方法で通知されたパッケージは、**[ネットワークからプログラムを追加]** にもリストされるので、そこから追加を実行できます。このオプションは、さらにインストール パッケージを起動するいくつかの方法を提供します。

- (インストール パッケージを追加する) デスクトップやスタート メニューのショートカット: ショートカットを追加して、それをクリックすることにより、インストール パッケージを実行できます。
- ファイルの関連付け: ユーザーが通知されたアプリケーションに関連付けられたファイルを開こうとすると、インストール プログラムが起動します。

割り当てを通知された場合にインストールを実行する方法はまだいくつかありますが、QlikView のインストールには適用できないため、このドキュメントの範囲外とします。

QlikView プラグイン インストール パッケージは、ショートカットやファイルの関連付けを追加しません。よって、割り当てオプションを使用した QlikView インストール パッケージの通知は推奨されません。

通知

通知するということは、管理者がロックダウンされたアカウントでインストール パッケージを実行する許可をユーザーに与えることを意味します。

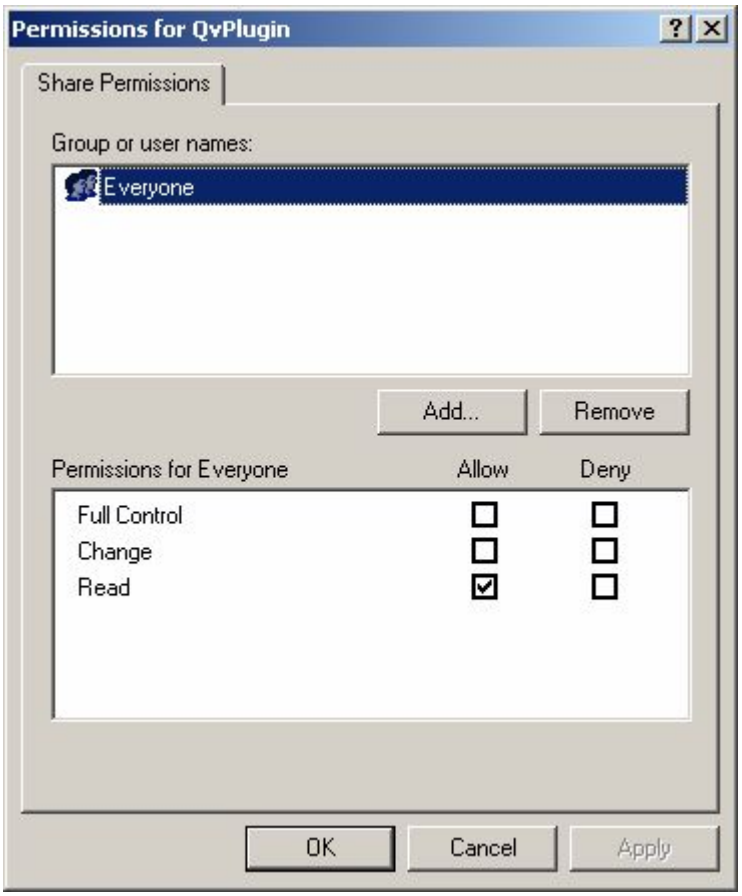
パッケージが通知されると、いわゆる「エントリポイント」がインストール先のシステムにロードされます。エントリポイントは一般的に、[プログラムの追加と削除] ダイアログにリスト表示される、ショートカットやファイルの関連付けです。

ステップ バイ ステップ ガイド

このセクションでは、アクティブ ディレクトリ上の複数のマシンに QlikView プラグイン用の *.msi* パッケージを通知するグループ ポリシーの段階的な手順を提供します。

グループ ポリシーを生成するには次の手順を実行します。

1. *.msi* パッケージを含むフォルダを参照します。パッケージをインストールするために、許可されたネットワークユーザーに対してフォルダを共有します。

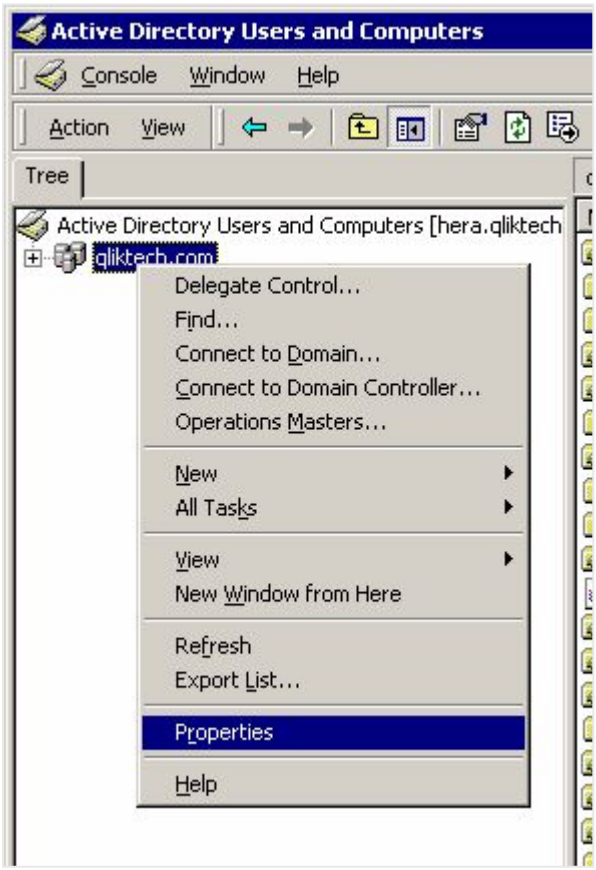


フォルダを共有する

2. 管理ツールから**[アクティブ ディレクトリ ユーザーとコンピュータ (Active Directory Users and Computers)]** を開き、パッケージを展開したい **[組織単位 (OU) (Organizational Unit (OU))]** をハイライトします。

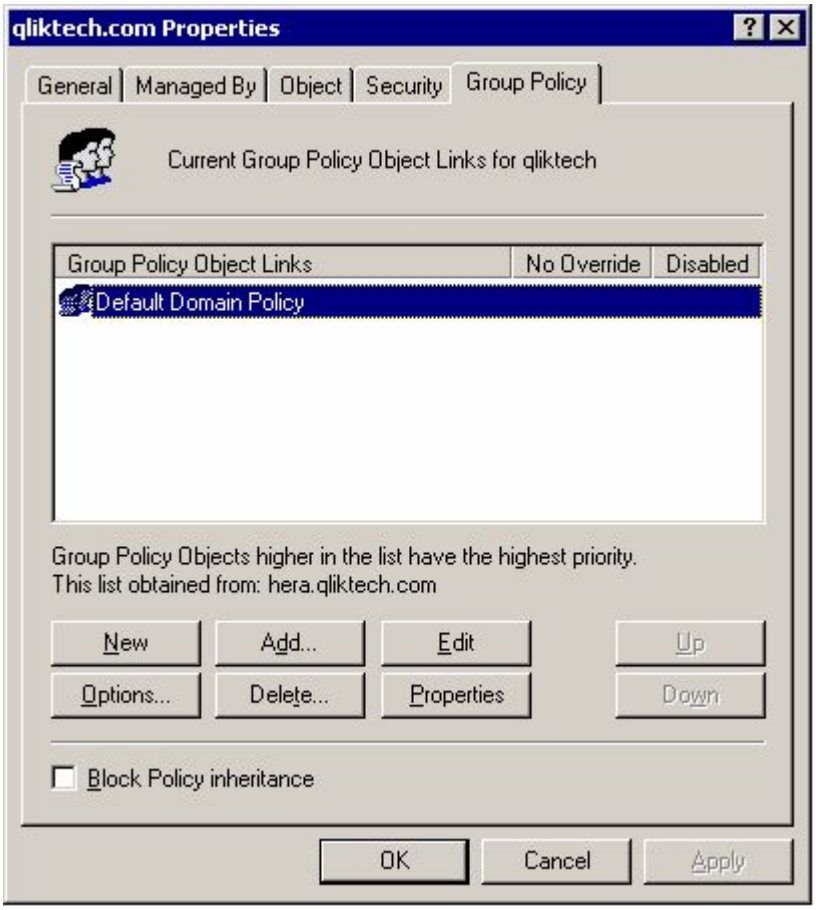
パッケージを展開したい組織単位 (Organizational Unit) をハイライトする

3. 右クリックして、**[プロパティ (Properties)]** を選択します。



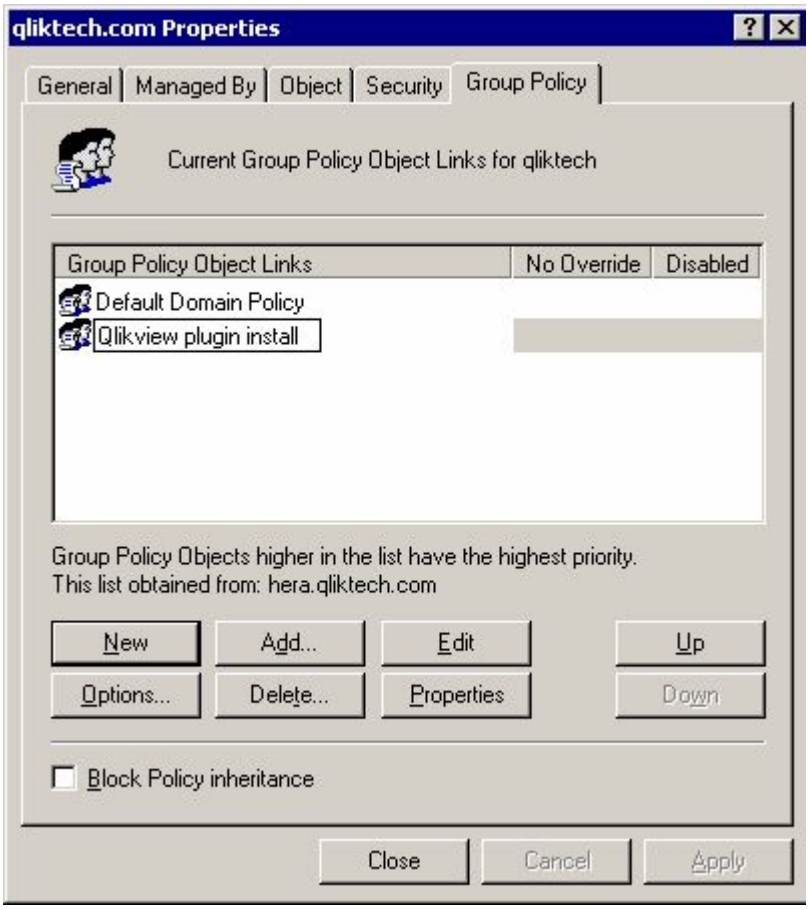
プロパティを選択する

4. **[グループ ポリシー (Group Policy)]** タブを選択し、**[新規 (New)]** をクリックして、適切な名前を入力します。



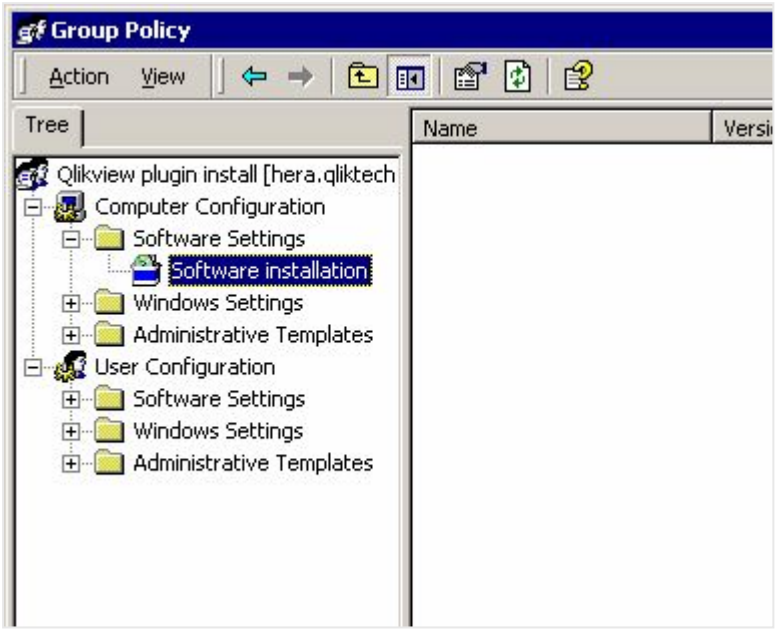
名前を付ける

5. 新規に作成したグループ ポリシー オブジェクトをハイライトし、**[編集 (Edit)]** をクリックします。



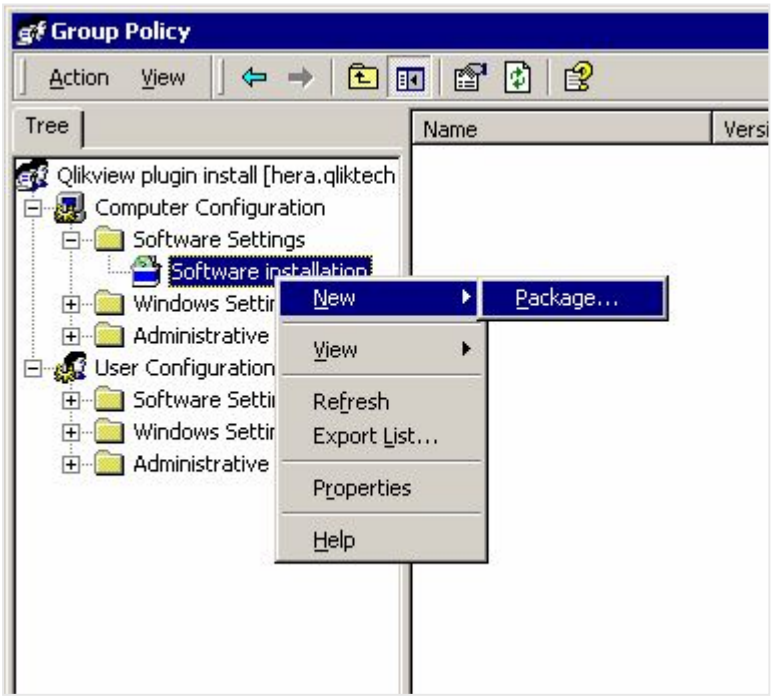
新規グループ ポリシー オブジェクトをハイライトする

6. パッケージの設定方法によって、**[コンピュータの構成 (Computer Configuration)]** > **[ソフトウェアの設定 (Software Settings)]** または **[ユーザーの構成 (User Configuration)]** > **[ソフトウェアの設定 (Software Settings)]** の順で選択します。今回のケースでは **[コンピュータの構成 (Computer Configuration)]** > **[ソフトウェアの設定 (Software Settings)]** を選択します。



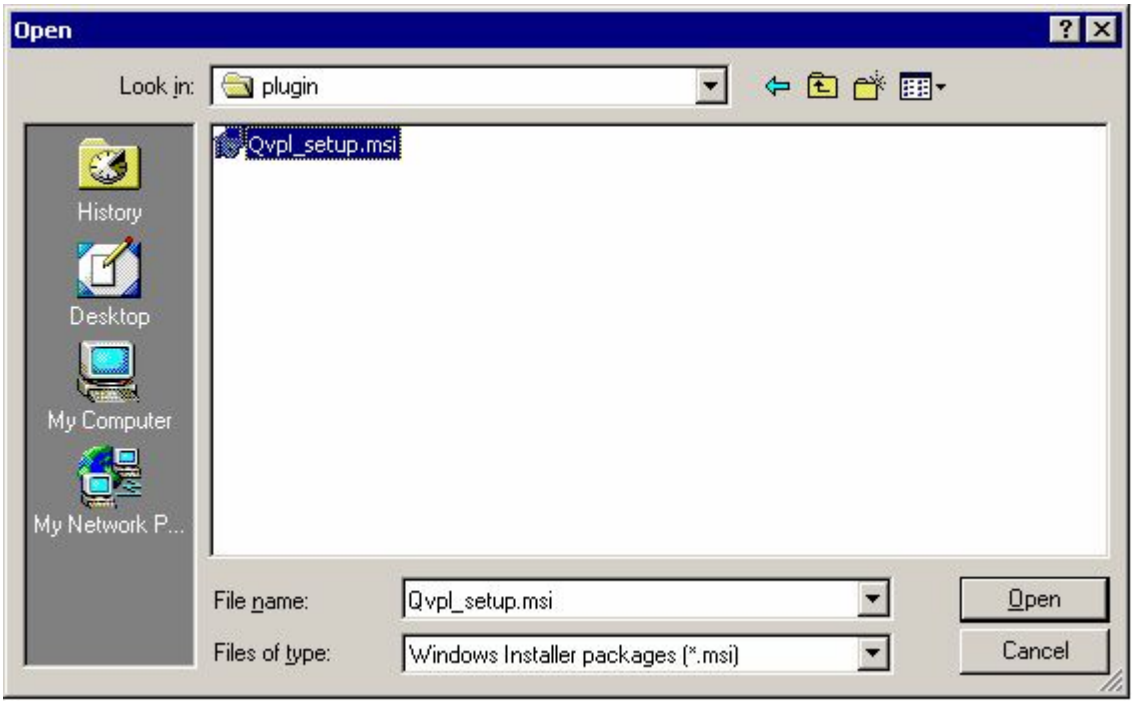
ソフトウェアの設定 (Software Settings) を選択する

7. **[ソフトウェア インストール (Software installation)]** を右 クリックし、**[新規作成 (New)]** > **[パッケージ (Package...)]** を選択します。インストール パッケージの格納場所を指定する、ポップアップ ウィンドウが開きます。



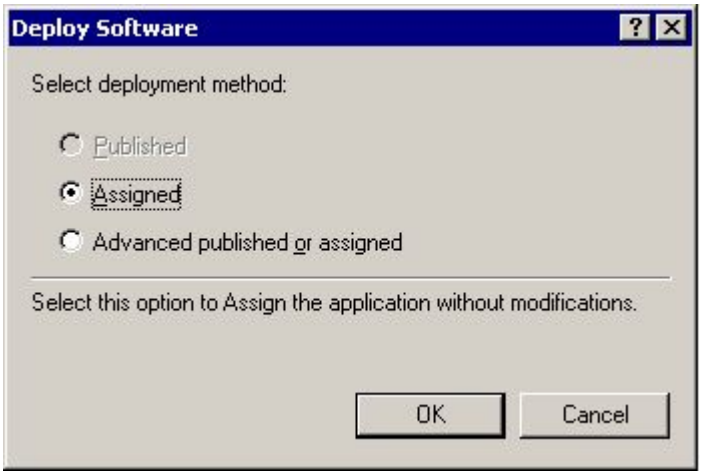
新規パッケージを作成する

8. インストール パッケージ (今回のケースでは *QvPluginSetup.msi*) を検索して選択し、**[開く(Open)]** をクリックします。



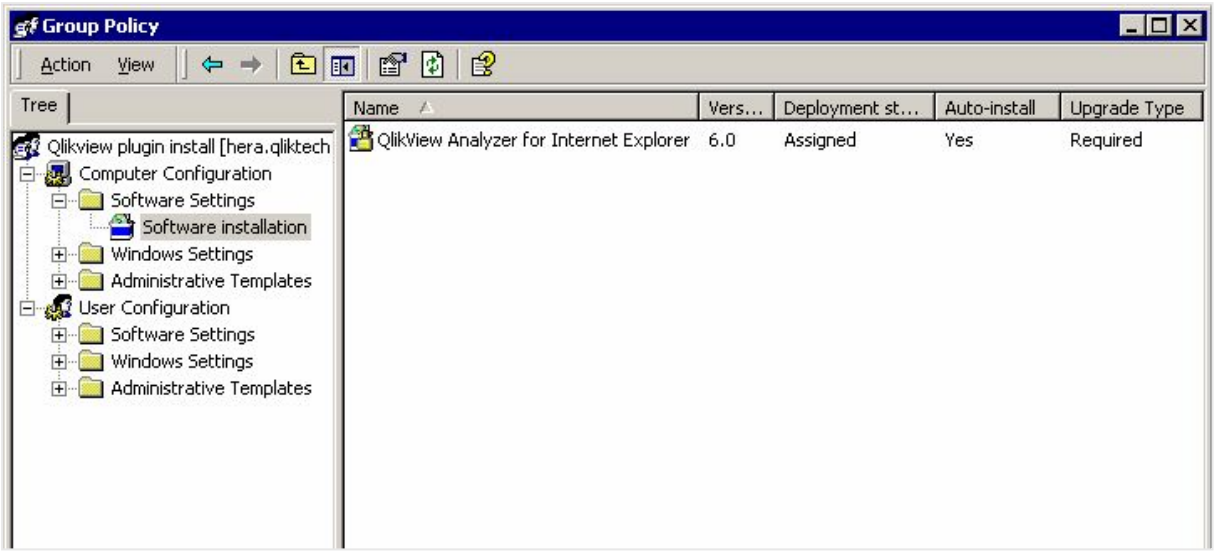
インストール パッケージを開く

9. 展開方法として **[割り当て (Assigned)]** を選択し、**[OK]** ボタンをクリックします。インストールは **[コンピュータの構成 (Computer Configuration)]** に適用されるため、**[割り当て (Assigned)]** 展開方法のみが使用可能です。



展開方法を選択する

10. これで展開ルールの準備が整いました。組織単位 (OU) 上のすべてのマシンで、自動的に展開したプログラムを取得できます。実際には、コンピュータの再起動時にインストール プログラムが実行され、その OU 上のコンピュータにログインしているすべてのユーザーが、インストールされたプログラムを起動できます。このルールは、多くの異なる OU に適用できます。



展開ルールの準備を整える

4 QlikView のアップグレードとアップデート

このセクションでは、QlikView Server を最新リリースにアップグレードする方法についての情報を確認できます。ここでは、有効な *アップグレードでのメンテナンス契約 (page 140)* など、アップグレードを成功させるのに必要な要件についても確認できます。*QlikView Server のアップグレードと更新 (page 141)* ページでは、QlikView Server 展開を異なるコンピュータまたはコンピュータのクラスターに移行する方法についての情報を確認できます。

4.1 アップグレードでのメンテナンス契約

QlikView Server および QlikView Desktop をアップグレードする場合は、有効なメンテナンス契約が存在することが重要です。有効なメンテナンス契約がないままアップグレードを試みると、QlikView は **Unlicensed モード (ライセンスのないモード)** となり、機能が制限されます。

メンテナンス契約には有効期間があり、それぞれに特定の契約終了日が設けられています。これは、メンテナンス契約終了日として指定された日付より後にリリースされたバージョンの QlikView に対しては、そのメンテナンス契約が有効性を持たないことを意味します。ただし、契約終了日以前にリリースされた QlikView バージョン (Desktop または Server、お使いのインストールに応じて) なら、いずれのバージョンであってもそのメンテナンス契約は有効です。

メンテナンス契約についての情報 (有効期間と契約終了日を含めて) は、ライセンス認証ファイル (LEF) に保存されています。メンテナンス契約の有効期間は LEF ファイルに指定されている契約終了日をチェックすることで確認できます。QlikView Server の場合は、QMC にある LEF ファイルをチェックしてください。QlikView Desktop の場合、LEF ファイルはローカル ドライブにあります。通常、LEF はインストール時にコンピューターに自動的に転送されて保存されます。ただし時折、この手順でエラーが発生して LEF ファイルが正常に転送されない場合があります。このようなケースに関する情報は、「ライセンス認証 ファイル エディター」ページに記載されています。

メンテナンス契約の有効性はアップグレード中に自動的にチェックされます。アップグレードしたい QlikView バージョンに対してメンテナンス契約が有効かどうかがわからない場合には、アップグレードをお控えください。有効なメンテナンス契約がないままアップグレードを試みると、QlikView (Desktop または Server) は **Unlicensed モード (ライセンスのないモード)** となり、機能が制限されます。QlikView Desktop の場合、Unlicensed モードは Personal Edition と呼ばれています。

> *該当の QlikView バージョンに対してメンテナンス契約が有効でない状態でアップグレードを開始すると、警告メッセージが表示されます。この警告メッセージが **表示されるのは、** リクエストした QlikView バージョンに対してメンテナンス契約が有効性を持たない場合のみです。*

QlikView Desktop または Server がライセンスのないモードに制限されてしまった場合でも、以前のバージョンに戻すことが可能です。ダウングレードは以下の手順で行います。

古い QlikView Desktop バージョンの復元

QlikView Desktop を以前のインストールの状態に戻すには、現在インストールされているバージョンをアンインストールし、その後、有効なメンテナンス契約のある古いバージョンをインストールします。

古い QlikView Server バージョンの復元

より新しいバージョンの QlikView Server にアップグレードする前に、「*バックアップとアップグレードの準備 (page 150)*」に記載されている順を十分に確認してください。ここではお客様の QlikView Server インストール バージョンのバックアップ (QlikView Publisher Repository (QVPR) データベースも含めて) 手順が説明されています。アップグレードの前にこのバックアップを作成しておくことで、将来新しいインストールが Unlicensed モードに制限された場合でも、旧バージョンの QlikView Server に戻すことが可能になります。

QlikView Server は以下の手順で以前のバージョンに戻します。

- 有効なライセンスのない QlikView Server をアンインストールします。
- 有効なメンテナンス契約のある、古いバージョンの QlikView Server をインストールします。
- QVPR およびデータディレクトリのバックアップを復元します。

4.2 QlikView Server のアップグレードと更新

QlikView Server をアップグレードする際、同じサーバーでアップグレードすることも、アップグレードして異なるサーバーに移行することもできます。このトピックでは、QlikView Server の新しいバージョンにアップグレードするために実行すべきステップについて概説し、証明書など、インストールを異なるマシン名で別のサーバーに移行するためのステップが含まれます。

このドキュメントでは、QlikView Server 12.00 以降を実行しているインストールをアップグレードおよび移行する方法について説明します。インストールで QlikView Server 11.20 以前のバージョンを実行している場合は、次を参照してください: *QlikView Server の 11.20 から November 2017 以降へのアップグレードと移行 (page 146)*でのみ有効です。QlikView Desktop をアップグレードする方法については、「QlikView Desktop のアップグレードと更新」を参照してください。

アップグレード時には、*.Shared* ファイル名拡張子を持つ共有ファイルは、自動的に *.Tshared* ファイルに変換されません。ファイルの詳しい変換方法については、「*共有ファイルのクリーンアップと変換 (page 83)*」を参照してください。共有ファイル内のすべてのブックマークとユーザー オブジェクトは、アップグレード中に保存されます。

要件

Qlik NPrinting を使用する場合、Qlik NPrinting バージョンは QlikView バージョン以上である必要があります。QlikView May 2023 IR にアップグレードする場合、Qlik NPrinting May 2023 IR 以上に平行してアップグレードする必要があります。詳細については、「Qlik NPrinting のアップグレード」を参照してください。

ベストプラクティス

QlikView をアップグレードする場合、以下の基本原則を考慮する必要があります。

- QlikView Server インストールの適切なバックアップが作成されたことを確認してください。バックアップするファイルとフォルダーの詳しいリストについては、「*バックアップとアップグレードの準備 (page 150)*」を参照してください。
- 予定された停止期間中にアップグレードを実行します。アップグレードを成功させるには、すべての QlikView を停止する必要があります。

- デフォルトでは、QlikView Server を削除するとライセンス情報と設定内容が保存されるよう設定されています。この情報は、後にそのシステムにインストールされる QlikView Server に適用されます。
- QlikView Server インストールをアップグレードする前に、有効なメンテナンス契約が結ばれていることをお確かめください。有効なメンテナンス契約がないままアップグレードを試みると、QlikView Server の機能が制限される結果となります。「*アップグレードでのメンテナンス契約 (page 140)*」を参照してください。
- QlikView の通信にデジタル証明書による認証を使用している場合、QlikView Management Service (QMS) を実行しているマシン以外のすべてのマシンに、アップグレード時に作成される新しい証明書をインストールする必要があります。参照:*証明書の更新 (page 115)* 。

同じマシン上でのアップグレード

同じマシンで QlikView 展開をアップグレードする場合は、各サーバーを個別にアップグレードします。複数のサーバーがある場合は、サーバーごとにこれらの手順を繰り返します。開始する前に、展開の稼働時間を最大化するようにアップグレードを計画してください。

アップタイムの最大化

エンドユーザーのシステム アップタイムを最大化するには、次の手順に従います。

開始する前に、QlikView 展開をバックアップしてください。

バックアップとアップグレードの準備 (page 150)

1. QlikView Management Service (QMS) を停止します。これを行うと、QlikView 管理コンソールは使用できなくなります。
2. 次の順序で QlikView サービスをアップグレードします (インストーラーにサービスの再始動を依頼)。
    a. QlikView Web Server (QVWS)
    b. Directory Service Connector (DSC)
    c. QlikView Server (QVS)
    d. QlikView Distribution Service (QDS)
    e. QlikView Management Service (QMS)
3. QMS を起動して、QlikView 管理コンソールを再度使用可能にします。

単一ノードの実装のアップグレード

単一サーバー サイトで QlikView Server をアップグレードするには:

開始する前に、QlikView サイトをバックアップしてください。

バックアップとアップグレードの準備 (page 150)

1. インストールで認証にデジタル証明書を使用している場合は、その証明書のバックアップを作成します。同じマシン上で QlikView Server インストールをアップグレードする場合は、証明書は自動的に更新されます。ただし、いずれの場合も証明書のバックアップを作成することを推奨します。参照:*証明書のバックアップと復元 (page 155)*。

2. 最新バージョンの QlikView Server を 製品のダウンロード からダウンロードします。
詳細については、「*インストール ファイルのダウンロード (page 111)*」を参照してください。
3. QlikView サービスを停止します。アップグレードプロセス中はすべてのサービスが停止され、自動的に再起動されますが、それでもアップグレードの前にすべてのサービスを停止することを推奨します。実行タスクが中断されることがないように、アップグレード手順の直前にグレースフル シャットダウンを実行して、QlikView Distribution Service (QDS) のみをシャットダウンします。グレースフル シャットダウンの詳細については、「QlikView Distribution Service を停止させる」を参照してください。
4. インストール プログラムを管理者として実行し、画面上の指示に従います。インストールの段階的な手順については、次を参照してください: *QlikView Server をインストールする (page 106)*。
5. インストール時に、サービス認証方法を選択します。**[Use digital certificates]** (デジタル証明書の使用) または **[Use QlikView Administrators Group]** (QlikView Administrators Group の使用) のいずれかを選択します。これまでデジタル証明書を使用していた場合は、アップグレードの際にもこのオプションを選択する必要があります。
6. インストール プロセスが終了したら、マシンを再起動して、すべてのサービスが適切に始動することを確認します。
7. QlikView 管理コンソール を開き、QlikView Server および QlikView Publisher のライセンス情報を適用します。
8. サーバーを再起動して、ライセンス情報を適用します。

マルチサーバー展開のアップグレード

マルチサーバー サイトをアップグレードするには:

1. アップグレードを実行する前に、各マシンですべてのサービスを停止します。
2. インストールで認証にデジタル証明書を使用している場合は、QlikView Management Service を実行しているマシンに保存されている証明書のバックアップを作成します。同じマシン上で QlikView Server をアップグレードする場合は、証明書は自動的に更新されます。ただし、いずれの場合も証明書のバックアップを作成することを推奨します。参照: *証明書のバックアップと復元 (page 155)*。
3. マルチサーバー設定の各マシンでアップグレード手順を実行します。
4. デジタル証明書を使用する場合は、QlikView Management Service (QMS) を実行しているマシンを除き、QlikView サービスを実行しているすべてのマシンに新しい証明書をインストールします。この手順の詳細については、次を参照してください:*証明書の更新 (page 115)* 。

別のマシンでのアップグレード

別のマシンにアップグレードする最も簡単な方法は、最初に現在のマシンでアップグレードしてから、新しいターゲットマシンに移行することです。マルチサーバー サイトを新しいマシンにアップグレードする場合は、サーバーごとにこれらの手順を繰り返します。

ターゲット マシンへの QlikView Server のインストール

1. 最新バージョンの QlikView Server を 製品のダウンロード からダウンロードします。
詳細については、「*インストール ファイルのダウンロード (page 111)*」を参照してください。
2. QlikView Server のインストール ウィザードを起動し、画面上の指示に従います。インストールの段階的な手順については、次を参照してください: *QlikView Server をインストールする (page 106)*。

3. インストール時に、サービス認証方法を選択します。[**Use digital certificates**] (デジタル証明書の使用) または [**Use QlikView Administrators Group**] (QlikView Administrators Group の使用) のいずれかを選択します。現在のマシン上のインストールで認証方法として証明書を使用している場合は、必ず [**Use digital certificates**] (デジタル証明書の使用) を選択します。
4. インストール プロセスが終了したら、マシンを再起動して、すべてのサービスが適切に始動することを確認します。
5. QlikView 管理コンソール を開き、QlikView Server および QlikView Publisher のライセンス情報を適用します。

> *QlikView Server ライセンスは一度に 1 つのインストールにのみ適用可能であるため、現在のマシンでインストールをシャットダウンした後、ターゲット マシン上の新しいインストールにライセンス情報を適用します。*

QlikView Server バックアップの移行と復元

最新バージョンの QlikView Server を現在のマシンとターゲット マシンの両方にインストールしたら、次に現在のマシンからインストールの内容を移行して、ターゲット マシン上で復元することができます。お使いのインストールで、認証方法として QlikView Administrators Group またはデジタル証明書のいずれを使用しているかによって、手順が異なります。

移行手順を開始する前に、必ず元のマシンの QlikView Server のバックアップを作成します。適切なバックアップがないと、QlikView Server インストールをターゲット マシン上で復元することができません。「*バックアップとアップグレードの準備 (page 150)*」を参照してください。

> *インストールで認証にデジタル証明書を使用している場合は、現在のマシン上で証明書のバックアップを作成することは極めて重要です。参照:証明書のバックアップと復元 (page 155)*。

QlikView Administrators Group を使用するインストールの移行

1. 最新バージョンの QlikView Server を現在のマシンとターゲット マシンの両方にインストールしたら、現在のマシンのバックアップを適切に作成します。「*バックアップとアップグレードの準備 (page 150)*」を参照してください。
2. 現在のマシンとターゲット マシンの両方ですべての QlikView サービスを停止します。
3. ターゲット マシンで、*%ProgramData%\QlikTech\ManagementService\QVPR* フォルダを削除するか、または名前を変更します。これがバックアップ元のバージョンと置き換えられます。
4. QVPR フォルダを現在のマシンからターゲット マシンにコピーします (フォルダ名をメモしておきます)。
5. 次のフォルダにあるすべての *.xml* ファイルを編集して、現在のマシン名への参照すべてを、ターゲット マシン名に置き換えます。
    - *%ProgramData%\QlikTech\ManagementService*
    - *%ProgramData%\QlikTech\ManagementService\QVPR*
6. QlikView サービスを再始動します。最初に QlikView Management Service を始動し、1 分待ってから、その他のサービスを任意の順で始動します。
7. SourceDocuments フォルダとマウントされたフォルダを復元します。

- ソース ドキュメントを既定の *%ProgramData%\QlikTech\SourceDocuments* フォルダに保存している場合は、すべてのソース ドキュメントをターゲット マシン上の同じ場所に移動します。
- ソース ドキュメントを別のフォルダの場所に保存している場合は、ソース ドキュメントフォルダのパスを QlikView 管理コンソール に追加します。これを行うには、[Source Folders] (ソース フォルダ) の [*追加*] セクションを確認します。
- マウントされたフォルダにタスクを配布している場合は、マウントされたフォルダへのパスを再挿入します。これを行うには、[フォルダ] の [*Mounter Folders*] (マウントされたフォルダ) セクションを確認してください。

8. 元のサーバー マシンをシャットダウンします。

デジタル証明書を使用するインストールの移行

証明書を使用する QlikView Server インストールを移行する際、一部の設定が暗号化されます。QlikView が、暗号化にもともと使われた証明書にアクセスできない場合、これらの設定は復号化できません。移行のために現在のコンピュータからターゲット コンピュータに証明書を復元すると、移行した設定を復号化できます。復号化されると、これらの設定は、ターゲット マシンの証明書に格納されている暗号化キーを使用して再び暗号化されます。

1. 最新バージョンの QlikView Server を現在のマシンとターゲット マシンの両方にインストールしたら、現在のマシンのバックアップを、証明書も含めて適切に作成します。「*バックアップとアップグレードの準備 (page 150)*」を参照してください。
2. 現在のマシンとターゲット マシンの両方ですべての QlikView サービスを停止します。
3. 現在のマシンから証明書のバックアップをターゲット マシンにコピーして、適切な場所に保存します。
4. MMC (Microsoft Management Console) を使用して、証明書を現在のマシンからターゲットマシンに復元します。この段階的な手順については、次を参照してください:*証明書の復元 (page 157)*。元の証明書を保存すると、MMC で 2 セットの証明書を確認できるはずで、それらには 2 つの異なる有効期限があります。
5. ターゲット マシンで、*%ProgramData%\QlikTech\ManagementService\QVPR* フォルダを削除するか、または名前を変更します。これがバックアップ元のバージョンと置き換えられます。
6. QVPR フォルダを現在のマシンからターゲット マシンにコピーします (フォルダ名をメモしておきます)。
7. 次のフォルダにあるすべての *.xml* ファイルを編集して、現在のマシン名への参照すべてを、ターゲット マシン名に置き換えます。
   - *%ProgramData%\QlikTech\ManagementService*
   - *%ProgramData%\QlikTech\ManagementService\QVPR*
8. QlikView サービスを再始動します。最初に QlikView Management Service を始動し、1 分待ってから、その他のサービスを任意の順で始動します。
9. SourceDocuments フォルダとマウントされたフォルダを復元します。
   - ソース ドキュメントを既定の *%ProgramData%\QlikTech\SourceDocuments* フォルダに保存している場合は、すべてのソース ドキュメントをターゲット マシン上の同じ場所に移動します。
   - ソース ドキュメントを別のフォルダの場所に保存している場合は、ソース ドキュメントフォルダのパスを QlikView 管理コンソール に追加します。これを行うには、[Source Folders] (ソース フォルダ) の [*追加*] セクションを確認します。

- マウントされたフォルダにタスクを配布している場合は、マウントされたフォルダへのパスを再挿入します。これを行うには、[フォルダ] の [*Mounter Folders*] (マウントされたフォルダ) セクションを確認します。

移行されたファイルが適切に暗号化されている場合は、タスク、ブックマーク、およびその他すべてのカスタム設定が QlikView 管理コンソールに配置され、表示されるはずです。

10. 元のサーバー マシンをシャットダウンします。

マルチサーバー展開のアップグレードと移行

マルチサーバー インストールのアップグレードと移行を行うときには、マルチサーバー展開内のマルチサーバー マシンそれぞれで前述の手順を実行します。

必要な手順の概要は以下のとおりです。

1. マルチサーバー設定の各マシンでアップグレード手順を実行します。
2. マルチサーバー インストール内の現在のマシンそれぞれのバックアップを作成します。
3. インストールで認証にデジタル証明書を使用している場合は、QlikView Management Service を実行しているマシン上で証明書のバックアップを作成します。
4. ターゲット マシンそれぞれに、実行中のライセンス バージョンの QlikView Server をインストールします。
5. インストールで認証にデジタル証明書を使用している場合は、QMS がインストールされているターゲット マシンで証明書を復元します。
6. インストールの各マシン専用のバックアップを移行して復元します。例えば、QVPR フォルダは、QlikView Management Service を実行するターゲット マシンにのみ移行する (そしてマシン名を変更する) 必要があります。
7. SourceDocuments フォルダを復元します。
8. 元のサーバー マシンをシャットダウンします。
9. デジタル証明書を使用する場合は、QlikView Management Service (QMS) を実行しているマシンを除き、QlikView サービスを実行しているすべてのマシンに新しい証明書をインストールします。この手順の詳細については、次を参照してください: *証明書の更新 (page 115)*

QlikView Server の 11.20 から November 2017 以降へのアップグレードと移行

QlikView Server をアップグレードする場合、同じサーバー上でアップグレードすることも、アップグレードして別のサーバーに移行することもできます。このトピックでは、QlikView Server 11.20 から新バージョンにアップグレードする場合に実行する必要のある手順の概要を説明します。これには、異なるマシン名を持つ別のサーバーに移行する手順も含まれています。

アップグレードと移行を行う前に、必ず QlikView Server 展開のバックアップを適切に作成してください。バックアップするファイルとフォルダーの詳細なリストについては、「*バックアップとアップグレードの準備 (page 150)*」を参照してください。

QlikView Server 11.20 からのアップグレードの際の変更と問題の詳細なリストは、次の Qlik サポートの記事を参照してください。「QlikView 11.20 無期限アップグレードの終了: 既知の問題と製品の動作の変更。

QlikView Server 11.20 から QlikView Server 12.10 以降にアップグレードするときに、バックエンド ファイル システムが原因でインストールに各種の問題が発生する場合があります。QlikView Server 12.10 以降のバージョンではディスクをより集中的に使用するので、QlikView 11.20 より大規模なファイル サーバーを必要とします。QlikView 展開を計画する場合には、ストレージの種類およびリソース容量に留意することが重要です。詳細については、次の Qlik サポートの記事を参照してください。「QlikView and its backend File Share System」(QlikView とそのバックエンド ファイル共有システム)

同じマシン上でのアップグレード

同じマシン上で QlikView Server をアップグレードするには、以下を実行します。

1. お使いの QlikView Server 11.20 インストールのバックアップを作成します。インストールのバックアップを作成することは常に重要ですが、同じマシン上でアップグレードする場合は、このステップは絶対必要というわけではありません。「*バックアップとアップグレードの準備 (page 150)*」を参照してください。
2. 最新バージョンの QlikView Server を 製品のダウンロード からダウンロードします。
詳細については、「*インストール ファイルのダウンロード (page 111)*」を参照してください。
3. QlikView サービスを停止します。アップグレードプロセス中はすべてのサービスがインストーラーによって停止され、自動的に再起動されますが、それでもアップグレードを進める前にすべてのサービスを停止することを推奨します。
4. インストール プログラムを管理者として実行し、画面上の指示に従います。インストールの段階的な手順については、次を参照してください: *QlikView Server をインストールする (page 106)*。

   証明書を使って、QlikView Server 11.20 インストールを QlikView Server November 2017 以降にアップグレードする際、アップグレードを開始する前に証明書を削除します。インストール プログラムを起動すると、証明書が検出された場合に警告ウィンドウが表示されます。証明書は、Microsoft Management Console (MMC) を使用して削除します。詳細については下記を参照してください。証明書の削除 (page 158)

5. インストール時に、サービス認証方法を選択します。[**Use digital certificates**] (デジタル証明書の使用) または [**Use QlikView Administrators Group**] (QlikView Administrators Group の使用) のいずれかを選択します。これまでデジタル証明書を使用していた場合は、アップグレードの際にもこのオプションを選択する必要があります。

   QlikView 11.20 から November 2017 以降にアップグレードする場合は、デジタル証明書を選択します。その場合は古い証明書をバックアップして復元する必要はありません。初めて QlikView Management Service を起動するときには、自動的に新しい証明書が作成されてインストールされます。

6. インストール プロセスが終了したら、マシンを再起動して、すべてのサービスが適切に始動することを確認します。
7. QlikView 管理コンソールを開き、QlikView Server および QlikView Publisher のライセンス情報を適用します。
8. サーバーを再起動して、ライセンス情報を適用します。

マルチサーバー展開でのアップグレード

マルチサーバー インストールをアップグレードするには、以下の手順を実行します。

- アップグレードを実行する前に、各マシンですべてのサービスを停止します。
- マルチサーバー設定の各マシンでアップグレード手順を実行します。

別のマシンでのアップグレードと移行

QlikView Server のアップグレードと移行を別のマシンで実行する場合は、このセクションにある手順に従います。

QlikView Server を別のマシンでアップグレードするには、以下の手順を実行します。

1. 現在のマシンで、QlikView Serverの 11.20 インストールのバックアップを作成します。「*バックアップとアップグレードの準備 (page 150)*」を参照してください。
2. QlikView Server の最新バージョンを 製品のダウンロード からダウンロードします。
3. QlikView Server のアップグレード ウィザードを起動し、画面上の指示に従います。インストールの段階的な手順については、次を参照してください: *QlikView Server をインストールする (page 106)*。
4. インストール時に、サービス認証方法を選択します。[**Use digital certificates**] (デジタル証明書の使用) または [**Use QlikView Administrators Group**] (QlikView Administrators Group の使用) のいずれかを選択します。これまでデジタル証明書を使用していた場合は、アップグレードの際にもこのオプションを選択する必要があります。

   > *QlikView 11.20 から November 2017 以降にアップグレードする場合は、デジタル証明書を選択します。その場合は古い証明書をバックアップして復元する必要はありません。初めて QlikView Management Service を起動するときには、自動的に新しい証明書が作成されてインストールされます。*

5. インストール プロセスが終了したら、マシンを再起動して、すべてのサービスが適切に始動することを確認します。
6. QlikView 管理コンソール を開き、QlikView Server および QlikView Publisher のライセンス情報を適用します。
7. ライセンス情報の適用後に、サーバーを再起動するよう要求されます。

バックアップの移行と復元:

1. 現在のマシンとターゲット マシンの両方ですべての QlikView サービスを停止します。
2. ターゲット マシンで、*ProgramData|QlikTech|ManagementService|QVPR* フォルダーを削除するか、または名前を変更します。これがバックアップバージョンと置き換えられます。
3. ターゲット マシンで、*ProgramData|QlikTech|ManagementService* にある `qvpr_<TargetMachineName>.ini` ファイルを削除あるいは名前を変更します。
4. QVPR フォルダーと`qvpr_<CurrentMachineName>.ini` ファイルを現在のマシンからターゲット マシンにコピーします (フォルダ名をメモしておきます)。
5. `.ini` のファイル名を `qvpr_<CurrentMachineName>.ini` から`qvpr_<TargetMachineName>.ini` に変更します。

6. *ProgramData\QlikTech\ManagementService* フォルダにある .xml ファイルおよび `Config.xml` ファイルで、現在のマシン名へのすべての参照が、ターゲット マシン名をポイントするように変更します。
7. QlikView サービスを再始動します。最初に QlikView Management Service を始動し、1 分待ってから、その他のサービスを任意の順で始動します。
8. **SourceDocuments** フォルダーを復元します。
   SourceDocuments フォルダーを復元するときに、次の 2 つのオプションがあります。
   - ソース ドキュメントを既定の *ProgramData\QlikTech\SourceDocuments* フォルダに保存している場合は、すべてのソース ドキュメントをターゲット マシン上の同じ場所に移動します。
   - ソース ドキュメントを別のフォルダの場所に保存している場合は、SourceDocuments フォルダーのパスを QlikView 管理コンソールに追加します。これを行うには、[Source Folders] (ソース フォルダー) の [*追加*] セクションを確認します。
9. 元のサーバー マシンをシャットダウンします。

マルチサーバー展開のアップグレードと移行

マルチサーバー インストールを QlikView Server 11.20 から QlikView Server November 2017 以降にアップグレードし、移行する場合は、マルチサーバー展開内の各マシンで前述の手順を実行します。

手順の概要:

1. マルチサーバー インストール内の各マシンのバックアップを実行します。
2. ターゲット マシンそれぞれに、実行中のライセンス バージョンの QlikView Server をインストールします。
3. インストールの各マシン専用のバックアップを移行して復元します。例えば、QVPR フォルダは、QlikView Management Service を実行するターゲット マシンにのみ移行する (そしてマシン名を変更する) 必要があります。
4. SourceDocuments フォルダーを復元します。
5. 元のサーバー マシンをシャットダウンします。

5 QlikView のバックアップと復元

このセクションには、QlikView Server インストールの完全なバックアップを作成する方法に関する情報が記載されています。QlikView Server インストールで認証にデジタル証明書を使用している場合は、証明書のバックアップを作成し、安全な場所に保管することは極めて重要です。ここには、証明書のバックアップと復元に関する専用のドキュメントがあります。

5.1 バックアップとアップグレードの準備

旧バージョンの QlikView から最新バージョンにアップグレードする場合に、必ず適切なバックアップを実行して、環境を正しく準備しておきます。アップグレードの前に、すべての重要なファイル (オリジナルの QlikView 展開以降に作成したカスタマイズを含む) を安全な場所にバックアップする必要があります。このトピックは、バックアップする必要のあるファイルの基本的なチェックリスト、および重要な考慮事項を提供することを目指しています。このトピックのガイドラインは、スタンドアロン展開または QlikView Web サーバーを使用するマルチサーバー展開に適用されます。

ファイルのバックアップ

手動でファイルをバックアップすることも、独自のバックアップ スクリプトを作成して、ファイルが選択した場所に自動的にバックアップされるようにすることもできます。QlikView 展開では、バックアップすべき最も重要なファイルは、*ProgramData* の [QlikTech] フォルダ、および *Program Files* の [QlikView] フォルダに含まれています。これら両方のディレクトリのコピーを作成して、バックアップが適切に行えるようにします。

QlikView Server データディレクトリ

単一ノードの QlikView Server 展開では、バックアップすべき最も重要なファイルは、*C:\ProgramData\QlikTech* にある [QlikTech] フォルダです。このディレクトリには、QlikView サービスそれぞれのサブフォルダが含まれています。各サブフォルダには、展開をカスタマイズしたときに編集した可能性のある構成ファイルと設定ファイルが含まれています。QlikView サーバーをアップグレードするときに、オリジナルの構成を復元する必要がある場合、ファイルをバックアップすることは重要です。

QlikView 管理コンソールを使用して、アプリケーション データ フォルダに含まれているすべての構成ファイルの概要を取得します。QMC では、構成ファイル、ファイル パス、変更したその他のカスタム設定の場所を確認することができます。

QlikView Server 展開をバックアップするときには、通常は以下をバックアップします。

- QVPR データベース (.zip ファイルにバックアップ)
- 構成ファイル (.config ファイル)
- 設定ファイル (.ini ファイル)
- ログ ファイル
- ドキュメント
- ブックマーク (*.Shared* ファイルまたは *.TShared* ファイルに保存)
- ユーザー オブジェクト (*.Shared* ファイルまたは *.TShared* ファイルに保存)
- タスク (QVPR データベースに保存)

証明書を使って、QlikView Server 11.20 インストールを QlikView Server November 2017 以降にアップグレードする際、アップグレードを開始する前に証明書を削除します。インストール プログラムを起動すると、証明書が検出された場合に警告ウィンドウが表示されます。証明書は、Microsoft Management Console (MMC) を使用して削除します。詳細については下記を参照してください。証明書の削除 (page 158)

以下の表は、以上のアイテムに関する情報を提供します。ここでお使いの展開に保存します。

ProgramData

ProgramData フォルダ

フォルダ名	内容の説明
DirectoryServiceConnector	構成ファイルと設定ファイル ログ ファイル リソース フォルダとサービス キー
DistributionService	構成ファイルと設定ファイル ログ ファイル タスクのバージョンは、QVPR データベースから QlikView Distribution Service に送信されるので、Distribution Service フォルダが見つからない場合でも、引き続き QVPR データベースのバックアップからこのタスクを復元することができます。
ドキュメント	ドキュメントに関連する *.qvf* または *.qvw* ファイルとその他のファイル ブックマークおよびユーザー オブジェクトは *.Shared* ファイルに保存されます
ManagementService	このフォルダは、QVPR データベースと *Backup* フォルダを含むようにアップアップするために非常に重要です。QVPR データベースは、ここで *.zip* ファイルとして毎日自動的にバックアップされます。これは、破損のリスクを軽減するために自動的にバックアップされる唯一のデータディレクトリです。 構成ファイルと設定ファイル ログ ファイル タスク - このフォルダをバックアップして、すべてのタスクを保存します。
QlikView ドキュメント	PDF ヘルプ ドキュメント
QlikViewBatch	このフォルダには QVB ログ ファイルが含まれており、バックアップする必要があるのは、ログを有効にした場合だけです。 QlikView November 2017 以降では、このフォルダに QVS に関連するログ ファイルも含まれています。

QlikViewServer	このフォルダは、バックアップを行うために非常に重要です。これには *Settings.ini* が含まれており、その他のサービスの Program Files にある *.exe.config* ファイルと同じです。
SourceDocuments	このフォルダには ソース ドキュメントが含まれており、QlikView Publisher でユーザー ドキュメントの作成に使用されます。
Webserver	ログ ファイル 構成 ファイル service_key

Program Files フォルダには QMC からアクセスできない構成 ファイルが含まれているので、これらのファイルは手動でのみ編集できます。ここでバックアップのために最も重要なファイルは QlikView サービスの config ファイルであり、重要な構成と設定 ファイルが含まれています。

Program Files

Program Files フォルダ

フォルダ名	内容の説明
DirectoryServiceConnector	QVDirectoryServiceConnector 構成 ファイルが含まれています。手動で変更を行った場合に、バックアップすることが重要です。
DistributionService	QVDistributionService 構成 ファイルが含まれています。手動で変更を行った場合に、バックアップすることが重要です。
例	サブ フォルダが含まれており、QlikView ドキュメントおよびその他すべての関連データなどがあります。
ManagementService	QVManagementService 構成 ファイルが含まれています。手動で変更を行った場合に、バックアップすることが重要です。
QvPlugin	ローカライズされたヘルプ コンテンツに対応するための言語です。
QvProtocol	*qvp.dll* が含まれています
サーバー	QVWebServer 構成 ファイルを含んでいる Web Server サブ フォルダです。 手動で変更を行った場合に、バックアップすることが重要です。
テーマ	カスタム テーマを作成した場合に、このフォルダをバックアップに含めることが重要です。
Web	*Web.config* 構成 ファイルが含まれています。 手動で変更を行った場合に、バックアップすることが重要です。

QVPR データベース ファイル

QVPR データベースは、.zip ファイルとして次の場所にバックアップされます。
C:\ProgramData\QlikTech\ManagementService\QVPR\Backups このバックアップ ファイルには、新しい QlikView 環境に移行する必要がある .xml ファイルと .bak ファイルが含まれています。

これはデータディレクトリのバックアップの一部ですが、QlikView Publishing Repository の構成ファイルと設定が含まれているので、最も重要なコンポーネントです。既定では、QVPR は毎日 zip ファイルとして *C:\ProgramData\QlikTech\ManagementService\QVPR\Backups* にバックアップされます。バックアップの頻度、および QMC でバックアップ ファイルを保存する場所は、変更することができます。

QlikView Web Server もしくは Microsoft IIS

QlikView のメジャー バージョン間でアップグレードすると、Microsoft IIS 設定は自動的にデフォルトに戻ります。インストールで Microsoft IIS Web Server を使用している場合は、アップグレードを実行する前に Microsoft IIS 設定をバックアップすることが重要です。

このトピックは、QlikView Web Server を使用するときにバックアップを作成する方法に重点を置いています。Microsoft IIS ウェブ サーバーを使用する場合は、IIS ウェブサイト、証明書、および構成ファイルをバックアップする方法について、Microsoft ドキュメントを参照してください。バックアップの原理は、両方の種類のウェブ サーバーで似ています。ただし、IIS で実行するカスタム認証ソリューションなどを作成している場合は、バックアップの場所や変更に関する専用のドキュメントを参照するか、元々カスタマイズを作成したコンサルタントにお問い合わせください。

ログ ファイル

ログ ファイルには、展開での問題に対するトラブルシューティングに役立つ重要な情報が含まれています。このログ ファイルには多数のエントリが含まれている可能性があるので、ストレージが問題である場合は、維持したいファイルのみを選択します。ただし、すべてのログ ファイルをバックアップすることをお勧めします。

ライセンス

既定では、QlikView Server を削除するとライセンス情報と設定内容が保存されるよう設定されています。この情報は、QlikView Server の後継のインストールに再度適用されます。QlikView では 2 つのライセンスを使用しており、アップグレード時に次の場所に追加されます。

- QlikView Server ライセンス - このライセンス ファイル (LEF) は *C:\ProgramData\QlikTech* に保存されます。
- QlikView Publisher ライセンス - このライセンス ファイル (LEF) は *C:\ProgramData\QlikTech\ManagementService\Publisher LEF* に保存されます。

証明書

QlikView をインストールするときに、デジタル認証に QlikView Administrators Group を使用するか、またはデジタル証明書をインストールすることを選択できます。デジタル証明書を選択し、QlikView 12.00 以降を実行している場合は、この証明書をバックアップすることが重要です。

QlikView での証明書の機能については、次を参照してください。*証明書の信頼性 (page 162)*。

単一のスタンドアロン QlikView サーバーは、常に次の 3 つの証明書を使用しています。

証明書

場所	発行先	発行元	説明
ローカル コンピュータ/個人	*<マシン名>*	QlikViewCA	サーバー
ローカル コンピュータ/個人	QVProxy	QlikViewCA	Client
ローカル コンピュータ/信頼されたルート証明機関	QlikViewCA	QlikViewCA	Root

証明書を使用して QlikView インストールのさまざまなサービスを認証し、機密情報を安全に保管します。アップグレードして復元するときには、QlikView サービスを適切に起動して実行できるように、認証には証明書が必要です。

QlikView 12.00 以降では、証明書は絶対に削除せず、常に安全な場所にバックアップしておくことが重要です。

QlikView 11.20 以前を実行している場合は、暗号化に別の方法が使用されています。つまり、元の証明書を新しいインストールに復元することはできないので、新しい証明書を作成する必要があります。

証明書を使って、QlikView Server 11.20 インストールを QlikView Server November 2017 以降にアップグレードする際、アップグレードを開始する前に証明書を削除します。インストール プログラムを起動すると、証明書が検出された場合に警告 ウィンドウが表示されます。証明書は、Microsoft Management Console (MMC) を使用して削除します。詳細については下記を参照してください。証明書の削除 (page 158)

証明書の更新

マルチサーバー QlikView 環境では QlikView Management Service (QMS) が認証機関であり、証明書の処理と配布に関して中央ノードのような役割を果たします。証明書を作成してより多くのマシンに追加するには、QMS にルート サービスとクライアント証明書をインストールする必要があります。

新しいマシンをアップグレードするか、QlikView 展開で復元するときには、QlikView 管理コンソール を使用して証明書を配布する必要があります。QMS と追加するマシンとの間で、証明書を交換する必要があります。このためには、QMC で追加するマシンへの URL を入力します。[**適用**] をクリックするとポップアップ ウィンドウが開き、リモート サーバー マシンに入力する必要のあるパスワードが表示されます。パスワードが許可されたら、リモート サーバー マシン上でサービスを再起動します。サービスを再起動すると、証明書の作成および別のマシンへの配布のプロセスが完了します。

詳細については下記を参照してください。*証明書の更新 (page 115)*。

証明書のバックアップ

MMC (Microsoft Management Console) を使用して、選択した場所にすべてのデジタル証明書をバックアップします。この段階的な手順については、次を参照してください:*証明書のバックアップと復元 (page 155)*。

カスタム コンテンツのバックアップ

カスタム認証やカスタム セキュリティ ソリューションなどのカスタム コンテンツを、展開に追加している場合があります。このカスタマイズは、自身の組織または外部のコンサルティング会社によって作成されていますが、作成元がどこであっても、自身のカスタマイズを文書化してバックアップする責任があります。カスタマイズのバックアップまたは移行の方法が不確かな場合は、元々のカスタマイズを作成したコンサルタントに問い合わせることをお勧めします。

既定のファイルの場所の変更

QlikView 展開の一部として、既定のファイルの場所を変更する必要がある場合があります。アップグレードを実行すると、オリジナルのフォルダの場所が復元され、カスタムのファイルの場所が失われます。バックアップの前に QMC を使用して、既定で *ProgramData* の QlikTech アプリケーション データに保存されている、構成ファイル

と設定ファイルへのすべてのパスの概要を取得することができます。アップグレード後に自身の選択した場所にフォルダを保持するには、作成したカスタム ファイル パスのバックアップを作成する必要があります。関連する構成ファイルを開き、追加したカスタムの場所を確認します。

構成ファイル

QlikView サービスすべてに構成ファイルがあり、展開の要件に適合するように編集することができます。各 QlikView サービスに構成ファイルと設定ファイルがあり、QlikView データディレクトリのサブ フォルダに保存されています。詳細については、次の表を参照してください。*QlikView Server データディレクトリ (page 150)*。自身のカスタマイズを作成している場合は、関連する QlikView サービス用に構成ファイルを編集します。

QlikView November 2018 から、展開 (QlikView Server Service、QVS を除く) 内のサービスに対して、QlikView 管理コンソール (QMC) から直接適用された既定値以外の値をすべて監視できます。QMC で [**ステータス**] > [**サービス**] に移動し、QlikView Server 展開のサービスの 1 つを選択します。1 つ以上のカスタム config 値が所定の場所にある場合、画面右側の情報タブにリストされます。このリストには、どの config 設定がどのマシン上で変更され、既定値と比較された既存の値は何であるかが示されます。同じサービスを実行しているマシン間の不一致もリストされています。詳細については下記を参照してください。サービス。

変更された構成ファイルと設定ファイルを、アップグレードされた展開に復元すると、Qlik で後続のリリースおよびアップデートに追加されている重要な変更が上書きされる場合があります。したがって、紛失を避けるため、構成ファイルと設定ファイルに行ったすべての変更またはカスタマイズをメモしておくことが重要です。アップグレードプロセスが完了したら、これらの変更を新しい config ファイルに付加する必要があります。このアプローチに従った場合は、すべての最新の config ファイルおよび以前の展開でのすべてのカスタマイズが、確実にお使いの展開に含められます。

例えば、QlikView Distribution Service で独自のカスタマイズを作成した場合、*QVDistributionService.exe.config* ファイルに変更を行います。これをバックアップするには、*C:\Program Files\QlikView\Distribution Service* フォルダに移動し、*QVDistributionService.exe.config* ファイルのコピーを作成します。アップグレード後に、カスタマイズをこのファイルに付加します。

マルチサーバー展開

QlikView を別のマシン、クラスター、その他の場所からバックアップする場合は、アップグレードする各マシンのバックアップを作成します。単一サーバー インストールの場合と同じ手順に従います。共有アプリケーション データ フォルダ (ファイル共有) を異なる場所で使用するマルチサーバー展開の場合、確実にこのフォルダもバックアップに含めます。

5.2 証明書のバックアップと復元

証明書のバックアップ

証明書のバックアップをとり、安全な場所に保存することは極めて重要です。証明書が損失すると、機密情報も失われます。

復号化できないデータによるサービスの不具合 (page 116)。

QlikView Management Service (QMS) を実行しているサーバー上で、バックアップを作成する必要のある 3 つの QlikView 証明書のリストをここに示します。

証明書

場所	発行先	発行元	説明
ローカル コンピュータ/個人	<マシン名>	QlikViewCA	サーバー
ローカル コンピュータ/個人	QVProxy	QlikViewCA	Client
ローカル コンピュータ/信頼されたルート証明機関	QlikViewCA	QlikViewCA	Root

QlikView Management Service (QMS) では、証明書を作成し、QlikView インストール内のすべてのサービスに配布するので、その他のサービスを実行しているサーバー上での証明書のバックアップ作成は任意です。これらのサービスのいずれかで証明書が見つからない場合、QMS では展開の一部となっているマシンに新しい証明書を配布します。

MMC (Microsoft Management Console) を使用して、選択した場所に証明書のバックアップを保存します。MMC の詳細については、下記を参照してください。*Microsoft Management Console の使用 (page 159)*。

証明書のバックアップを行うには、以下の手順を実行します。

1. MMC を開きます。
2. [**File**] (ファイル) をクリックし、[**Add/Remove Snap in**] (スナップの追加/削除) をクリックします。
3. [**Certificates**] (証明書) を選択して [**Add**] (追加) をクリックします。
4. [**Computer account**] (コンピュータ アカウント) を選択して [**次へ**] をクリックします。
5. [**Local computer**] (ローカル コンピュータ) を選択します。[**Finish**] (完了) をクリックし、メイン ウィンドウで [**OK**] をクリックします。
6. [**Certificates**] (証明書) ノードを展開し、次の証明書フォルダを選択します。
   - **Personal** (パーソナル)
   - **Trusted Root certificate Authorities** (信頼できるルート証明書権限)
7. バックアップを作成する証明書を右クリックし、[**All Tasks**] (すべてのタスク) をクリックして [**Export**] (エクスポート) をクリックします。
8. [**Certificate Export Wizard**] (証明書のエクスポート ウィザード) で、[**Yes, export private key**] (はい、秘密キーをエクスポートします) をクリックして [**次へ**] をクリックします。
9. [**Export all extended properties**] (すべての拡張プロパティをエクスポートする) と [**Include all certificates in the certification path if possible**] (可能であればすべての証明書を証明書パスに含める) を選択します。[**次へ**] をクリックします。

   秘密キーをエクスポートし、すべての拡張プロパティをエクスポートします。
10. パスワードを入力して確認します。**[次へ]** をクリックします。
11. ファイル名を入力し、バックアップの場所を選択して、[**次へ**] をクリックします。
12. [**Finish**] (完了) をクリックしてバックアップを作成します。

証明書の検索およびそのバックアップの方法については、「*証明書の信頼性 (page 162)*」を参照してください。

証明書の復元

証明書が万一紛失した場合は、サービスが停止します。情報はログ ファイル上で確認できます。以前に証明書のバックアップを行っている場合は、QlikView Management Service を実行しているマシンで MMC (Microsoft Management Console) を使用して、証明書を復元することができます。復元用に使用できるバックアップがないときは、アクセスできないデータ (保護された秘密情報) を消去し、あとで再入力する必要があります。

次のタブに、復元する必要のある 3 つの証明書が示されます。

証明書

場所	発行先	発行元	説明
ローカル コンピュータ/個人	<マシン名>	QlikViewCA	サーバー
ローカル コンピュータ/個人	QVProxy	QlikViewCA	Client
ローカル コンピュータ/信頼されたルート証明機関	QlikViewCA	QlikViewCA	Root

証明書を復元するには、以下の手順を実行します。

1. MMC を開きます。
2. [**File**] (ファイル) をクリックし、[**Add/Remove Snap in**] (スナップの追加/削除) をクリックします。
3. [**Certificates**] (証明書) を選択して [**Add**] (追加) をクリックします。
4. [**Computer account**] (コンピュータ アカウント) を選択して [**次へ**] をクリックします。
5. [**Local computer**] (ローカル コンピュータ) を選択します。[**Finish**] (完了) をクリックし、メイン ウィンドウで [**OK**] をクリックします。
6. [**Certificates**] (証明書) ノードを展開し、次の証明書フォルダを選択します。
   - **Personal** (パーソナル)
   - **Trusted Root certificate Authorities** (信頼できるルート証明書権限)
7. [**Certificates**] (証明書) フォルダを右クリックし、[**Trusted Root Certification Authorities**] (信頼できるルート証明書権限) で [**All Tasks**] (すべてのタスク) をクリックして、[**Import**] (インポート) をクリックします。
8. [**Certificate Import Wizard**] (証明書のインポート ウィザード) で、証明書のバックアップを保存する場所を探します。証明書ファイルを視覚化するには、[**File name**] (ファイル名) の横にあるドロップダウン メニューから [**Personal Information Exchange (*.pfx;*.p12)**] 書式を選択します。
9. ルート証明書を選択して [**Open**] (開く) をクリックします。[**次へ**] をクリックします。
10. 証明書がエクスポートされたときに作成されたパスワードを入力します。[**Mark this key as exportable**] (このキーをエクスポート可能にする) と [**Include all extended properties**] (すべての拡張プロパティを含める) を選択します。[**次へ**] をクリックします。
11. 次のウィンドウで、[**次へ**]、[**Finish**] (完了) をクリックします。
12. インポートが成功した場合は、MMC に証明書が表示されています。
13. ステップ 7 から 12 を繰り返し実行して、[**Personal**] (パーソナル) で [**Certificates**] (証明書) フォルダにサーバー証明書とクライアント証明書をインポートします。

証明書がないことに起因するサービスの不具合

QMS サービスが停止した場合は、新しいランダム SecretsKey を開始時に作成した証明書の新しいセットが必要になります。ここで QMS は他のサービスから証明書をたずねられる可能性があります。

他のサービスが停止した場合は、サービスは特殊モードで開始し、このサービスは QMS の証明書を取り扱うことができます。ローカルのコンピュータ上で特定のポートを参照し、QlikView 管理コンソール で指定されたパスワードを入力する必要があります。このあと、サービスは再始動し、通常モードで稼働します。このとき、新しく受け取った証明書と鍵が使用されます。

復号化できないデータによるサービスの不具合 (page 116)

QlikView Server インストール移行時の証明書の復元

証明書を使用する QlikView Server インストールを移行する際、一部の設定が暗号化されます。QlikView が、暗号化にもともと使われた証明書にアクセスできない場合、これらの設定は復号化できません。移行のために現在のコンピュータからターゲット コンピュータに証明書を復元すると、移行した設定を復号化できます。復号化されると、これらの設定は、ターゲット マシンの証明書に格納されている暗号化キーを使用して再び暗号化されます。

QlikView Server インストールの移行については、下記を参照してください。*QlikView Server のアップグレードと更新 (page 141)*。

証明書の削除

証明書は絶対に削除しないようお勧めします。証明書が損失すると、機密情報も失われます。ただし、QlikView Server を 11.20 から November 2017 以降にアップグレードする場合のように、特定の状況では証明書を削除する必要があります。

Microsoft Management Console (MMC) を使用して証明書を削除します。参照 : Microsoft Management Console の使用

1. MMC を開きます。
2. [**File**] (ファイル) をクリックし、[**Add/Remove Snap in**] (スナップの追加/削除) をクリックします。
3. [**Certificates**] (証明書) を選択して [**Add**] (追加) をクリックします。
4. [**Computer account**] (コンピュータ アカウント) を選択して [**次へ**] をクリックします。
5. [**Local computer**] (ローカル コンピュータ) を選択します。[**Finish**] (完了) をクリックし、メイン ウィンドウで [**OK**] をクリックします。
6. [**Certificates**] (証明書) ノードを展開し、次の証明書フォルダを選択します。
   - **Personal** (パーソナル)
   - **Trusted Root certificate Authorities** (信頼できるルート証明書権限)
7. 以下の証明書のみを削除します。

証明書

場所	発行先	発行元	説明
ローカル コンピュータ/個人	<マシン名>	QlikViewCA	サーバー

場所	発行先	発行元	説明
ローカル コンピュータ/個人	QVProxy	QlikViewCA	Client
ローカル コンピュータ/信頼されたルート証明機関	QlikViewCA	QlikViewCA	Root

必ず上記に示されている証明書のみを削除してください。

構成ファイル

次のテーブルには編集が必要になる可能性のある各構成ファイルの場所が示されています。

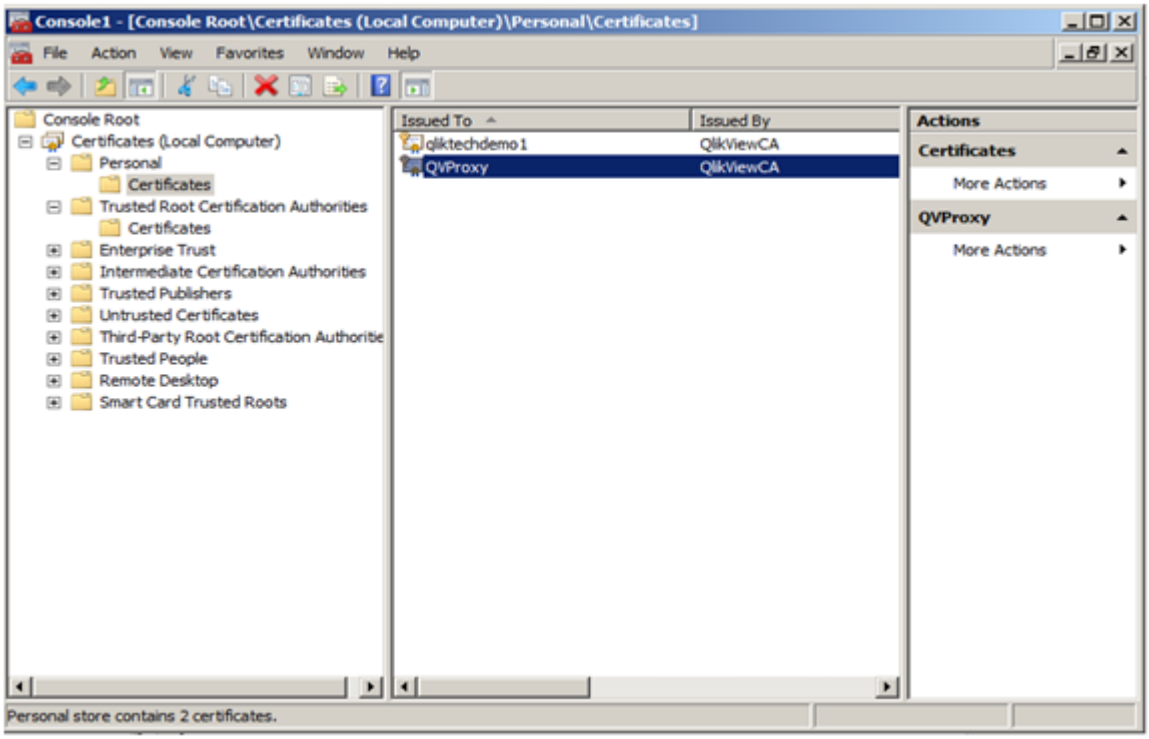
構成ファイル

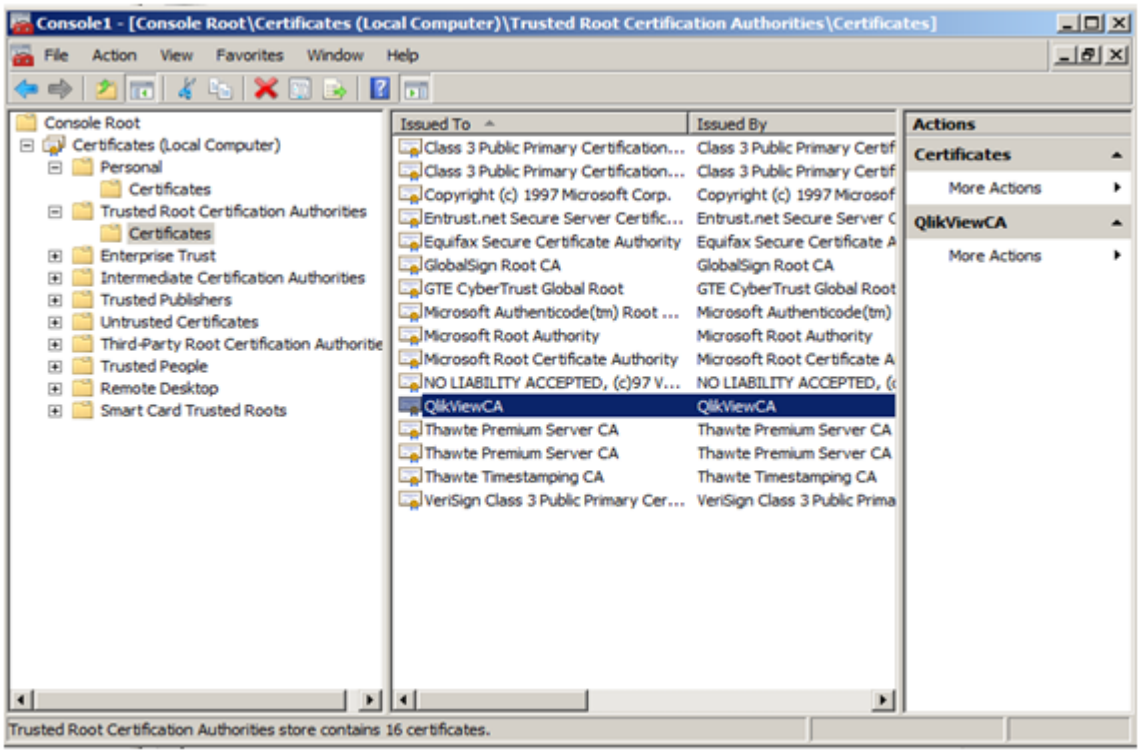
Service	デフォルトのパス
QMS	*C:\Program Files\QlikView\Management Service\QVManagementService.exe.config*
DSC	*C:\Program Files\QlikView\Directory ServiceConnector\QVDirectoryServiceConnector.exe.config*
QDS	*C:\Program Files\QlikView\Distribution Service\QVDistributionService.exe.config*
QVWS	*C:\Program Files\QlikView\Server\Web Server\QVWebServer.exe.config*
IIS	*C:\Program Files\QlikView\Server\Web Server Settings\QVWebServerSettingsService.exe.config* *C:\Program Files\QlikView\Server\QlikViewClients\QlikViewAjax\web.config*
QVS	*C:\ProgramData\QlikTech\QlikViewServer\Settings.ini*

Microsoft Management Console の使用

証明書は追加された証明書スナップインを使って、QlikView 管理コンソールで視覚的に確認することができます。QlikView 証明書は、[**Personal**] (パーソナル) > [**Certificates** and **Trusted Root Certification Authorities**] (証明書と信頼できるルート証明書権限) > [**Certificates**] (証明書) フォルダにあります。

上の図は、QlikView Server 設定で適切にインストールされた証明書を示しています。QlikView 管理コンソール内のサーバー上の QlikView サービスすべてで、図に示されている証明書が構成されています。


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorite
Trusted People
Remote Desktop
Smart Card Trusted Roots
Issued To
Issued By
qliktechdemo1
QlikViewCA
QVProxy
QlikViewCA
Actions
Certificates
More Actions
QVProxy
More Actions
Personal store contains 2 certificates.


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorite
Trusted People
Remote Desktop
Smart Card Trusted Roots
Issued To
Issued By
Class 3 Public Primary Certification...
Class 3 Public Primary Certif
Copyright (c) 1997 Microsoft Corp.
Copyright (c) 1997 Microsof
Entrust.net Secure Server Certific...
Entrust.net Secure Server C
Equifax Secure Certificate Authority
Equifax Secure Certificate A
GlobalSign Root CA
GTE CyberTrust Global Root
Microsoft Authenticode(tm) Root ...
Microsoft Authenticode(tm)
Microsoft Root Authority
Microsoft Root Certificate Authority
Microsoft Root Certificate A
NO LIABILITY ACCEPTED, (c)97 V...
QlikViewCA
Thawte Premium Server CA
Thawte Timestamping CA
VeriSign Class 3 Public Primary Cer...
VeriSign Class 3 Public Prima
Actions
Certificates
More Actions
QlikViewCA
More Actions
Trusted Root Certification Authorities store contains 16 certificates.

6 セキュリティ

QlikView Server/Publisher のセキュリティは、以下のパートで構成されます。

- 証明書: QlikView Server では、デジタル認証を選択した場合、認証と承認に証明書を使用します。証明書はサーバー間の信頼性を提供します。さらに、機密性の高いデータに対しては、動的暗号化鍵が使用されます。
- プラットフォームの保護: プラットフォーム自体はどのように保護され、また通信および操作はどのように行われるべきか。
- 認証: ユーザーは誰か、またその身元をどうやって認証するか。QlikView は、統合 Windows 認証 (IWA) や HTTP ヘッダー、チケッティングといった標準認証プロトコルを用いて、データへのアクセスを要求するすべてのユーザーに対し認証を行います。
- ドキュメントレベルでの許可: ユーザーはドキュメントへのアクセスを許可されているか。QlikView は、Document Metadata Service (DMS) または Windows NTFS といったサーバー側の機能を用いて、ファイル レベルでのアクセス権を判断します。
- データレベルでの許可: ユーザーはデータの全部または一部の閲覧を許可されているか。QlikView は、ドキュメントレベルでの機能 (Section Access) とサーバー側での削除機能 (QlikView Publisher) の組み合わせを用いて行および項目レベルでのデータセキュリティを実装します。

6.1 証明書

証明書とは、ドメインのクライアントとサーバー間の通信を暗号化するのに使用されるキーを含むデータファイルです。証明書はまた、ドメインがその証明書を発行した組織にとって既知であることも確認します。証明書には、キーについての情報、所有者のアイデンティティに関する情報、および証明書の内容が正しいことを検証した組織のデジタル署名が記載されています。通信の暗号化には、一対のキー (パブリックおよびプライベートキー) が使用されます。

Qlik 製品は、相互通信時に証明書を使用します。また、異なるコンピュータにインストールされたコンポーネント間の通信のために、製品内でも証明書を使用します。これらは、標準の TLS 証明書です。

証明書を発行する組織である認証局は、証明書に「署名」します。貴社のドメインが既知のものであることを示すため、認証局から証明書を取得するよう手配できます。また、独自の証明書を発行して署名することもできます (「自己署名証明書」)。

一般的なエラー

サイトが既知のものかどうかを把握することは一般的にセキュリティ上重要であるため、ブラウザで証明書に関連するエラー メッセージが表示され、通信をブロックする可能性があります。

一般的なエラーは、認証局に関連するものです。たとえば、認証局が存在しない、あるいは証明書が失効している場合、大部分のブラウザのデフォルトセキュリティレベルでは、「証明書に署名がありません」、「証明書が期限切れです」などのメッセージが表示され、通信が停止されます。セキュリティ管理者がその証明書が有効であることを把握している場合、エラーがその証明書について無視されるよう例外を作成できます。

その他の一般的なエラーは、ドメインの命名方法に関連したものです。例えば、companyname.com は www.companyname.com とは違っており、localhost はサーバー名と異なるドメインです。完全修飾ドメイン名とは、ドメインのあいまいでない名前のことです。例えば、companyname.com のサーバーの名前は mktg-SGK で、そう参照できますが、完全修飾ドメイン名は mktg-SGK.companyname.com となります。(これはホワイトリストと呼ばれます。)

暗号化とキー

Qlik 製品の証明書で使用される種類の暗号化では、一対のキーが必要です (非対称暗号)。そのうちの 1 つ、パブリックキーは共有されます。もう1 つのキーであるプライベートキーは、所有者のみが使用します。

PEM は、パブリック証明書の ASCII テキストフォーマットです。プラットフォーム間を超えて使用できます。

証明書とキーペアは認証局から取得するか、あるいは生成することができます。証明書に署名してもらうには、署名リクエストも生成する必要があります。

証明書の信頼性

QlikView Server では、デジタル認証を選択した場合、認証と承認に証明書を使用します。証明書はサーバーマシン間の信頼性を提供します。さらに、機密性の高いデータに対しては、動的暗号化鍵が使用されます。QlikView の既定の構成では、Windows の信頼関係に依存します (ハードコードされた暗号化鍵)。

証明書には暗号化鍵が含まれているので、証明書のバックアップを安全な場所に保管しておくことが重要です。参照: 証明書のバックアップと復元 (page 155)

QlikView Server は、マシン名で (IP アドレスや完全修飾ドメイン名でなく) 参照する必要があります。

アーキテクチャ

QlikView サーバーインストールでは、証明書は、複数のサーバー上にあるサービス間の通信を認証および許可します。証明書にはパスワードや接続文字列など、データの暗号化と復号化を処理する SecretsKey が含まれます。

QlikView 内の複数のサーバー展開で証明書を構成すると、信頼性を確立するために、QlikView Administration Group における依存関係は削除されます。また、証明書を使用すると、Active Directory (AD) やその他のユーザーディレクトリを共有しなくても、異なるドメインにある QlikView サービス間で信頼できるドメインを構築できます。

ここで説明している構成の手順は、QlikView サービス間の信頼できるドメインにのみ当てはまります。エンドユーザーの通信の安全を確保するために SSL/TLS や証明書を使用する場合は、個別に設定する必要があります。

QlikView Server では、認証と承認に以下のデジタル証明書を使用します。

証明書

場所	発行先	発行元	説明
ローカル コンピュータ/個人	<マシン名>	QlikViewCA	サーバー
ローカル コンピュータ/個人	QVProxy	QlikViewCA	Client
ローカル コンピュータ/信頼されたルート証明機関	QlikViewCA	QlikViewCA	Root

証明書は Microsoft Management Console (MMC) から管理されます。

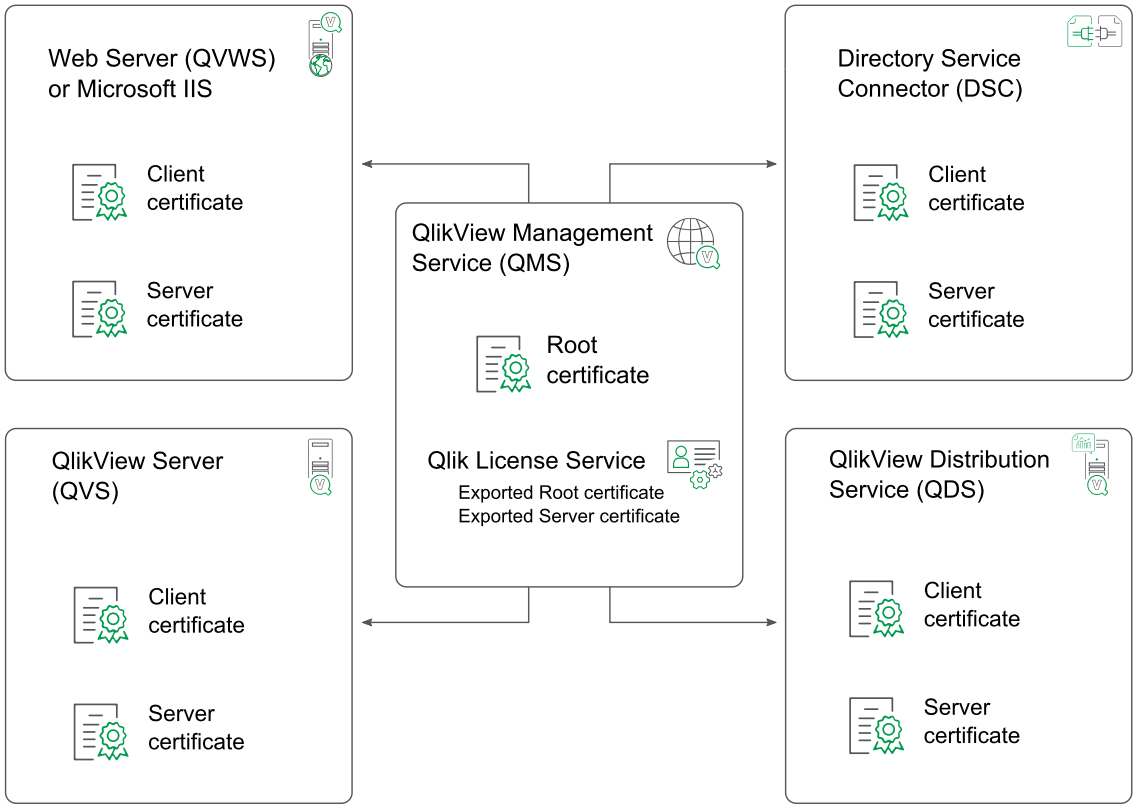
アーキテクチャは、証明書マネージャまたは Certificate Authority (CA) として機能する QlikView Management Service (QMS) に基づいています。QMS は証明書を作成して、QlikView インストールのあらゆるサービスに配布することができます。

QMS はセキュリティソリューションの重要な部分であり、安全な場所から管理して証明書ソリューションを安全に維持する必要があります。

インストールのルート証明書は QMS サーバーに保存されています。インストールに加わる予定の QlikView サービスを伴うサービスはすべて、QMS に追加された際にルート証明書を使用して署名された証明書を受け取ります。QMS (CA) は、キーと所有者の ID が含まれているデジタル証明書を発行します。プライベート キーは公に利用することはできず、QlikView サービスによって秘匿されます。証明書を使うと、QMS はサービスの信頼性を確認できます。つまり、QMS は「このサーバー上で構成されているサービスはマイ インストールのサービスである」と保証する責任を負っているのです。

サーバーが証明書を受け取った後、QlikView サービス間の通信は HTTPS (SSL/TLS 暗号化) を使用して暗号化されます。この証明書は、サーバー上のサービス間の通信のみを保護します。エンド ユーザーとの通信は保護しません (つまり、証明書は QlikView Plug-In、クライアント、または QVS とのウェブ サーバー通信では使用されません)。

次の図はマルチノード QlikView Server 展開を示しており、ここで QMS (Certificate Authority) はその他のサービスがインストールされているコンピュータに証明書を配布します。



Qlik License Service

QlikView April 2019 以降では、Qlik License Service が必ずインストールされ、署名付きキーを使用して QlikView Server にライセンスが付与されている場合にのみ有効化して使用されます。Qlik License Service は、QlikView Management Service (QMS) が実行されているマシンにインストールされ、他のサービスとは異なる方法で証明書を処理します。

QlikView Management Service (QMS) を初めて起動する場合には、ルート証明書とサーバー証明書が自動的にエクスポートされ、Qlik License Service で使用可能になります。これらの証明書は、次のファイルにエクスポートされます。

- root.pem
- server.pem
- server_key.pem
  このファイルにはサーバーの証明書キーが書き込まれています。

既定では、これらのファイルは次の場所に保管されます:
%ProgramData%\QlikTech\LicenseService\Exported Certificates。

インストールされている製品の証明書を更新する場合は、Qlik License Service より前に QlikView Management Service (QMS) を再起動する必要があります。この順序でサービスを開始することにより、正しい証明書セットがエクスポートされ、Qlik License Service で使用できるようにします。Qlik License Service のステータスは、Qlik Service Dispatcher を起動して停止することによって管理できます。

要件

証明書の信頼性が適切に機能するには、以下の要件を満たす必要があります。

- 証明書の信頼性は部分的に実装できません。QlikView インストールですべてのサービスによって使用されるか、まったく使用されません。
- 証明書の信頼性は、Windows Server 2008 以降によってのみサポートされています。
- すべてのコンピュータで QlikView Server 12.00 以降を使用していることを確認します。QlikView Server 11.20 以前では、暗号化に別の方法が使用されています。古い証明書は、QlikView 12.00 以降を実行しているインストールと互換性がないので、新しい証明書を作成する必要があります。
- QlikView Server を最初にインストールする場合は、何も変更せずに QlikView サービスをインストールして設定します。証明書の使用を設定する前に、QlikView サービスが展開されているサーバー (コンピュータ) 上でサービスを開始して停止します。
- セクション アクセス管理は、証明書の信頼性が設定されている環境では設定できません。
- QlikView Management Service (QMS) を実行しているコンピュータ上では、アップデートを行うたびに、必ず次の 3 つの証明書のバックアップを作成します。

証明書

場所	発行先	発行元	説明
ローカル コンピュータ/個人	*<マシン名>*	QlikViewCA	サーバー
ローカル コンピュータ/個人	QVProxy	QlikViewCA	Client
ローカル コンピュータ/信頼されたルート証明機関	QlikViewCA	QlikViewCA	Root

証明書のバックアップ方法については、次を参照してください:*証明書のバックアップと復元 (page 155)*。

さらに、以下のセクションで説明されている技術要件も満たさなくてはなりません。

証明書のポート

このセクションでは、証明書の信頼性を構成するときに、オープンにする必要があるポートについて説明します。

次のテーブルに記載されたポートは、サービス間の通信で必要になり、「オープン」として構成する必要があります。

QlikView のポートの詳細については、下記を参照してください。*ポート (page 19)*。

結果として生じたネットワーク内での QlikView サーバーの場所と QVS 通信のルーティングに応じて、ファイアウォールの設定を変更する必要があるかもしれません。

サービス間の通信用ポート

Service	ポート	SSL/TSL -対応ポート
QlikView Server	4747, 4749	4749
QlikView Distribution Service	4720	4720
QlikView Web Server	4750, 80, 443	4750, 443
QlikView Management Service	4780, 4799	4780, 4799
Directory Service Connector	4730	4730

次のテーブルに記載されたポートは、ローカル サーバー上での証明書のインストール手順で必要になります。

これらのポートはサービス間の通信では使用されません。

証明書インストール用ポート

Service	ポート
QlikView Distribution Service	14720
Directory Service Connector	14730
QlikView Web Server	14750

次のテーブルに記載されたプロトコルは、このセクションで説明したポートでの通信に使用されます。

ポート通信用プロトコル

Service	ポート
QlikView Server	SSL/TSL を介した QVPX
その他のすべてのサービス	SSL/TSL を介した SOAP

各サービスの配布済み証明書をインストールするには、コンソールへの物理的なアクセスまたはコンソールへのリモート アクセス (リモート デスクトップ機能の使用など) が必要です。

6.2 プラットフォームの保護

機能

ドキュメントのダウンロードおよび/または印刷、Microsoft Excel へのエクスポート機能は、サーバーにおいてそれぞれのドキュメントに対しユーザー レベルで規制を適用できます。

特別なアカウント

管理者アカウント

管理者アカウントには、QlikView Publisherのタスクで作成される全ドキュメントへのアクセス権が付与されます。管理者アカウントの特性は次の通りです。

- QVS 上のファイルすべてにアクセス権を付与
- QlikView マネージメントコンソール (QMC) へのアクセス権は付与しない
- 各ドキュメントに許可されているクライアントのタイプを尊重する (例 : タスクを作成したユーザーによって、AJAX クライアントがブロックされている場合、管理者アカウントは、AJAX クライアントを使用して、QlikView ドキュメントを開くことはできません)

匿名ユーザー アカウント

QVS がマシン上で初めて起動するとき、匿名ユーザー用に Windowsアカウントが作成されます。アカウントは、ローカル ネットワークのマシン名 (name) を使用して IQVS_name と名付けられます。

対象のマシンがドメイン サーバーである場合、ドメイン アカウントとして匿名アカウントが作成されるか、あるいはローカル マシン アカウントとして作成されます。

フォルダやファイルを匿名のクライアントからアクセス可能にするには、それぞれのフォルダやファイルに匿名のアカウントへの読み取り権限を与える必要があります。

> *QVS を起動し、権限の付与を行う前に匿名アカウントを作成します。匿名のアカウントを手動で作成しないでください。*

QlikView Administrators

QlikView Administrators グループは、QlikView マネージメントコンソール (QMC) へのアクセス権限の付与、また Windows Authentication を使用している場合は各サービス間の許可に用いられます。

通信

AJAX クライアントの保護

AJAX クライアントは、クライアントのブラウザと QlikView Web Server (QVWS) または Microsoft IIS の間での通信用プロトコルとして HTTP または HTTPS を使用します。HTTP プロトコル (HTTPS) 上で SSL/TSL 暗号化を使用してブラウザと Web サーバー間の通信を保護するよう強くお勧めします。通信は暗号化されなければ、明確なテキストとして送信されます。

ウェブ サーバーと QVS 間の通信では、下記に示すように QVP が用いられます。

プラグインの保護

QlikView プラグインと QVS の通信には 2 つの方法があります。

- プラグインと QVS が QVP (ポート 4747) を用いて通信可能であれば、次で説明したセキュリティが適用されます。

サーバー通信 (page 168)

- 通信に QVP を使用できない、あるいはクライアントがプラグイン内で選択した場合は、HTTP を用いてウェブ サーバーにトネリングされます。

ウェブ サーバーで HTTPS が有効化されている場合は、トンネルは SSL/TLS を用いて暗号化されます。

サーバー通信

QVS 通信には、デフォルトで暗号化された QVP プロトコルが用いられます。Microsoft Enhanced Cryptographic Provider がインストールされている場合、QVP プロトコルは、キーの変更に 1024 ビット RSA、データ暗号化に 256 ビット AES GCM を用いることで保護できます。Microsoft Base Cryptographic Provider を使用している場合は、キーの変更に 512 ビット RSA、データ暗号化に 128 ビット AES CBC を用いることで通信を保護できます。

サービス通信

QlikView プラットフォーム (QVS、DSC、QMC、QDS、QVWS) に属する各種サービスは、すべてウェブ サービスを用いて通信します。ウェブ サービスの認証には、Integrated Windows Authentication (IWA) が用いられます。

SSL とTLS のサポート

QlikView での SSL とTLS のサポートは次の表のとおりです。

SSL とTLS のサポート

-	SSL v3.0	TLS v1.3	TLS v1.2	TLS v1.1	TLS v1.0
QlikView May 2023	√	√	√	-	-
QlikView May 2022	√	-	√	√	√

6.3 認証

QlikView では、(ブラウザを使用するか、または QlikView Desktop クライアントを介してドキュメントをダウンロードして開くかのどちらかで) QlikView Server によりセッションを確立する場合に、ユーザーが認証される必要があります。実装環境の大半でユーザー認証が必要とされますが、QlikView は匿名でのアクセスを許可するように設定することも可能です。

QlikView のコンテキストでは、ほとんどの場合にユーザー認証が外部のエンティティに対して実行され、外部で認証されたユーザー ID を QlikView Server に渡すために使用されます。そのようなシナリオの場合、QlikView では QlikView へのアクセス前に実行される認証により、ユーザー ID の一部のトークンが QlikView に送信され、信用されるようにします。

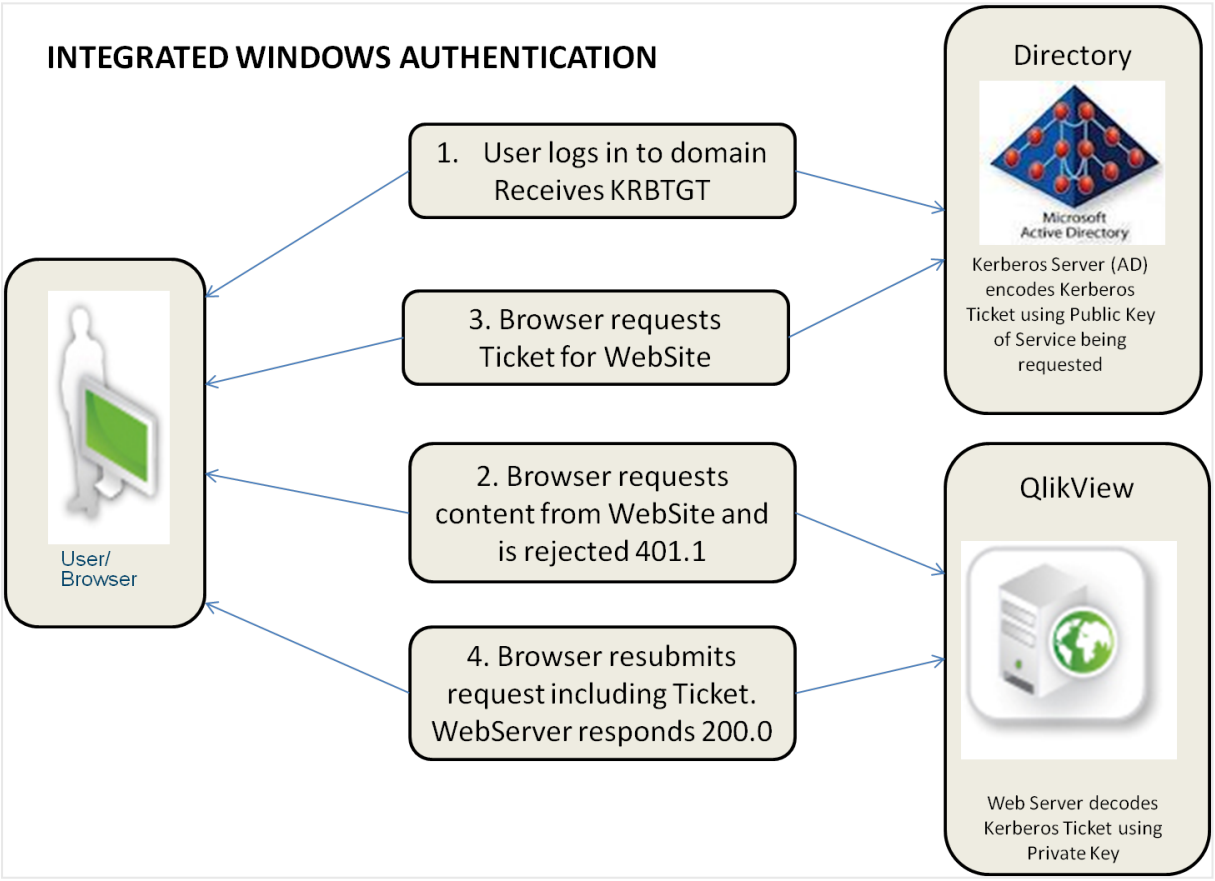
Windows ユーザー環境で QlikView Server を使用する場合の認証

Windows ユーザーに基づく環境での QlikView Server に対する認証処理 (Active Directory の組み込みなど) はシンプルです。手順は以下の通りです。

1. ユーザーがクライアント マシンの Windows オペレーティング システムにログインする際、ユーザーの認証情報の検証が行われます。
2. その後ユーザーがデスクトップのブラウザを使用するなどの方法で QlikView Server (QVS) とのセッションを確立しようとする場合、QVS では組み込みの Integrated Windows Authentication (IWA) を使用できます。
3. ログインしたユーザーの ID は、Kerberos または NTLM のどちらかのセキュリティ ソリューションを使用して QlikView Server に送信されます。このソリューションは煩わしい設定なしでシングル サインオン機能を提供します。許可交換がユーザーの特定に失敗した場合は、ブラウザに Windows ユーザーのアカウント名とパスワードを求めるメッセージが表示されます。

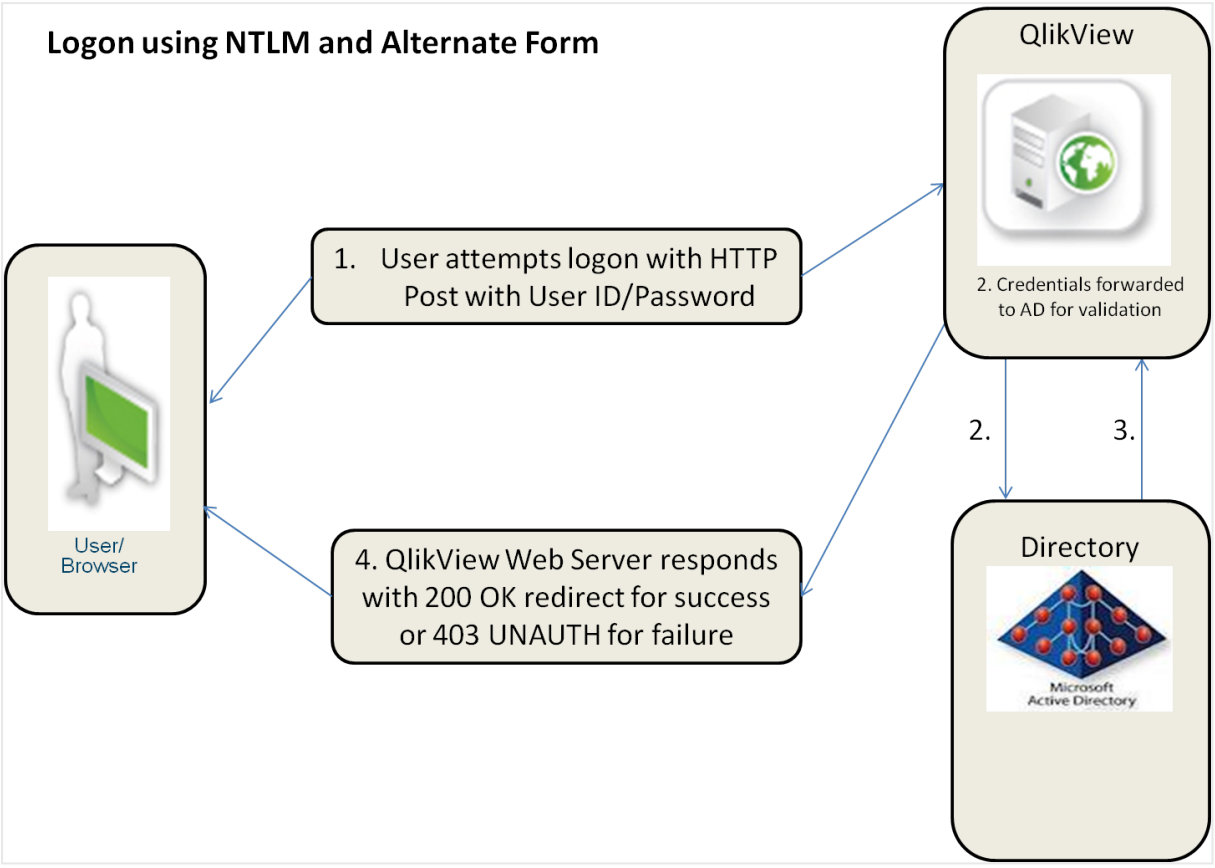
ユーザー グループを QlikView システムに転送することはできません。これは Directory Service Connector (DSC) によって解決する必要があります。そうでなければ何も行いません。

下の図は IWA の標準的な許可フローを示したものです。



Windows ユーザー環境で QlikView Server を使用する場合の認証

下の図は、NTLM と代替ログインの組み合わせの許可フローを示しています。これは、IWA の標準的なフローとは異なります。



NTLM と代替フォームを使用した許可

許可プロセスは環境に応じて異なります。

- ローカル エリア ネットワーク (LAN): LAN 環境の Windows ユーザーの認識において最も一般的かつ適しているのは IWA です。認証処理はワークステーションへのログイン時に実行され、QlikView はこの ID を利用します。
- マルチドメイン環境: ワークショップのドメインとサーバーのドメイン間の信頼性が確立されていないマルチドメイン環境が存在する構造において、あるいはリバースプロキシ上で使用する場合は、社内ネットワーク IWA は回避すべきです。このような環境では、認証された ID を既存の外部 SSO サービスと QlikView カスタム チケット交換のいずれかを使用して QlikView に公開するように QlikView 展開を構成します。

既存のシングル サインオン (SSO) ソフトウェア パッケージを使用した QlikView Server での認証

SSO の基本構造がすでに存在する環境 (例: CA SiteMinder®、IBM® WebSeal、Oracle® Oblix など) の場合、QlikView では、SSO 基本構造によって提供されるシングル サインオンの HTTP ヘッダー挿入方法を利用できます。これは、煩わしい設定なしでシングル サインオンが提供されることを意味します。SSO 基本構造ソフトウェア パッケージは、以下のように設定できます。

- リピート ユーザーのアクセスの取得: リソースを保護するようソフトウェア パッケージを設定できます。ユーザーが QlikView へのアクセス権を要求すると、そのユーザーが過去に SSO 認証ページにサインインしたことがある場合には、SSO パッケージによってアクセス権が付与されます。

- 新規ユーザーのログイン: SSO パッケージの既存のセッションがない場合、ユーザーは SSO パッケージのログイン ページにリダイレクトされます。ログイン後、最初に要求した URL にリダイレクトされます。

どちらの場合も、ユーザーが SSO ソフトウェアに対し正しく認証されていればユーザー名が HTTP ヘッダーに挿入され、そのヘッダー内の値は、QlikView サーバーが認証済みのユーザー ID として受け取る値となります。

SSO ソフトウェアが機能していない限り、HTTP ヘッダー方法による QlikView Server に対する認証を使用することはできません。HTTP ヘッダーは容易にスプーフィングされてしまいます。ユーザーにとってソフトウェア パッケージがコンテンツにアクセスする唯一のパスである場合、上記で述べたすべての SSO ソフトウェア パッケージは、この種類のスプーフィング攻撃に対する保護を提供します。

QlikView が HTTP ヘッダーに ID を挿入するための特定のツールや製品を推奨または支持することはありません。このアプローチはユーザーが内部アクティブ ディレクトリに存在しないエクストラネットの実装に非常に適しています。認証処理は、リバース プロキシまたはエンド ユーザーの QlikView コンテンツの使用を妨害する ISAPI フィルターにより実行されます。

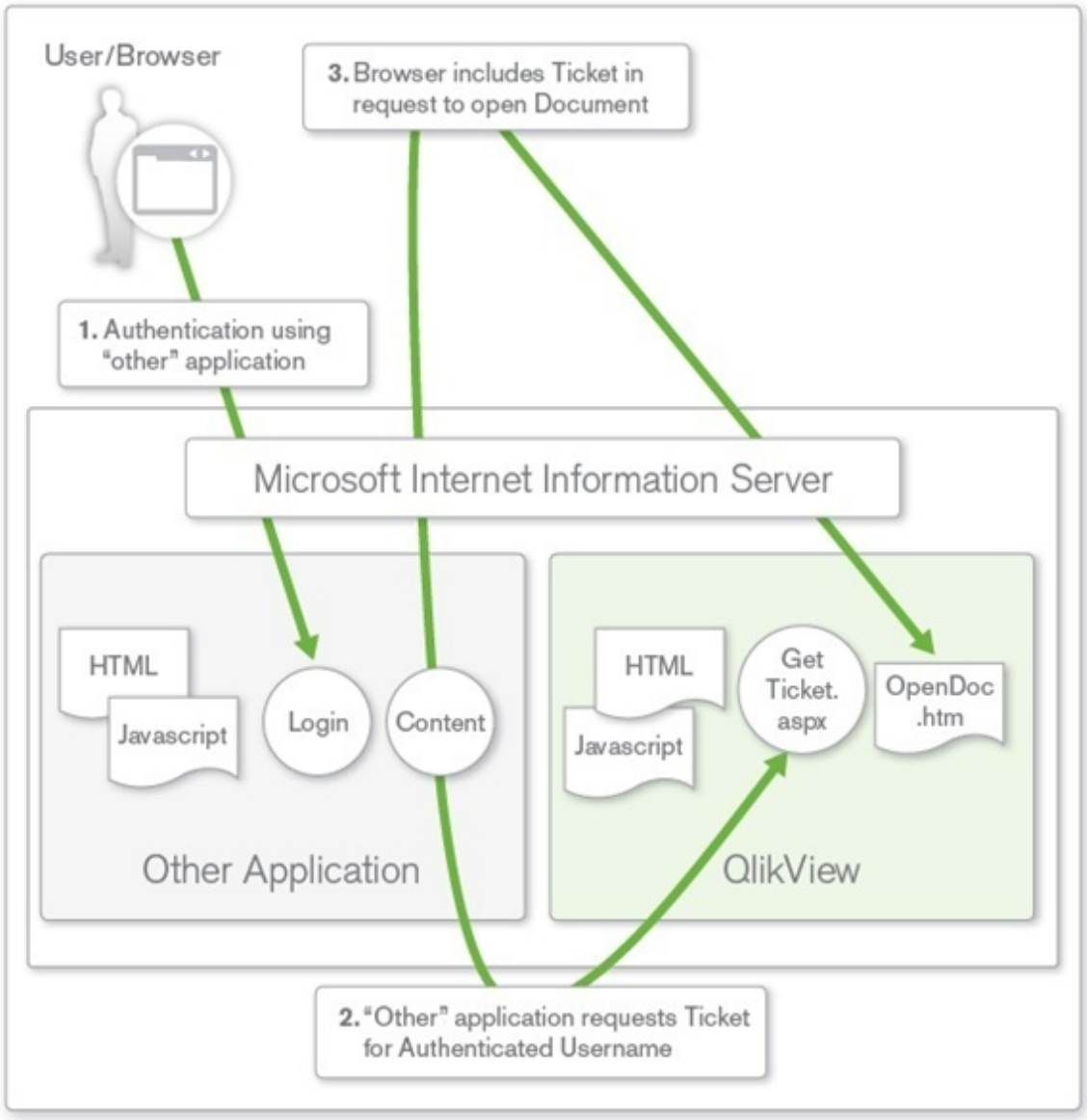
IWA またはシングル サインオン ソフトウェアを用いない認証

上記の方法がどちらも適切ではない場合、QlikView では、第 3 のシングル サインオン方法として Custom Ticket Exchange (CTE) を使用できます。

CTE では、ユーザーはその他のシステムに先立ち許可を受けている必要があります。

1. サードパーティ システムには、サード パーティ システムの認証ユーザーのために、QVS から (QlikView では「チケット」と呼ばれる) 認証トークンを要求する権利と責任が付与されています。正しい許可を受けたユーザーのみに対しチケットを要求する作業は、サード パーティ システムの責任のもとで行う必要があります (たとえば、QVS はユーザーの許可ステータスに関する知識を備えていません)。
2. その後システムが許可トークンをユーザーに渡し、ユーザーはこれを用いて QVS とのセッションを開くよう要求します。
3. QVS はチケットが有効かどうか確認し、許可ユーザーにセッションを公開します。

チケッティング認証は、主に QlikView コンテンツをサードパーティのアプリケーションやポータルに埋め込む場合に適用することができ、QlikView への一般的なアクセスを提供するために使用されることは滅多にありません。CTE を実行するためにチケットを要求してこれを渡すには、通常多少のカスタム開発が必要になります。



IWA またはシングル サインオン ソフトウェアを用いない認証

カスタム ユーザーを使用した QlikView Server 認証

上記の 3 つすべての方法ではシングル サインオンの原理を使用しており、ユーザー ID とパスワードは QlikView Server の外部で保管され、外部エンティティが認証を担当します。QlikView Publisher のカスタム ユーザー機能を使用してユーザーの資格情報を QlikView Server 環境に保管することも可能ですが、あまり一般的ではありません。この場合は、ユーザーとパスワードが QlikView 環境内で定義および保管され、QlikView 展開の Web 層でフォーム認証が実行されます。このソリューションは、小規模なスタンドアロンの QlikView Server 展開に適しており、ユーザー定義を複数のシステムで使用可能な環境で使用することはできません。このような環境では、上記で述べたシングル サインオン ソリューションのいずれかを使用することが推奨されます。

フォームが異なる許可には、それぞれ異なるウェブ サーバー インスタンスが必要です。その後それぞれのウェブ サーバーが、ユーザーの要求を同一の QVS インスタンスに転送します。

カスタム ユーザーを使用した QlikView Server 認証

6.4 許可 (Authorization)

ユーザーが認証されると(システムがユーザーの身元を確認すると)、セキュリティ権限割り当ての最初の手順が完了したことになります。次の手順は、ユーザーがアプリケーションやデータに対し保有している権限やアクセス権を理解することです。この手順は許可と呼ばれます。基礎レベルでは、管理者はユーザーおよび/またはグループのリスト、ならびにアクセスの対象範囲と共に Access Control List (ACL) を生成します。ユーザーがアクセスを要求すると、システムは ACL でユーザーの認証 ID を検索し、ユーザーがそのアクセスを実行するのに適した権限を管理者から付与されているかどうか検証します。

QlikView Desktop を用いた QlikView ドキュメントへの直接的なアクセスは、常に Windows NTFS ファイル セキュリティにより管理されます。ウェブベースの QlikView Management Console (QMC) へのアクセスは、特定のローカル Windows グループに属する Windows ユーザーに限定されています。

ドキュメントレベルでの許可

ユーザーが認証されると、通常は QlikView Server が独自に許可を処理します。QlikView Server では、Windows NTFS 権限として ACL 情報を保存する (ユーザーが Windows ユーザーID を用いて認証された場合にのみ適用)、あるいは QlikView 内の内部レポジトリ(Document Metadata Service/DMS) に ACL 情報を保存する方法のいずれかを選択できます。NTFS とDMS のどちらを選択するかで、QlikView Server 内の全ドキュメントへのアクセスが決定します。

NTFS とDMS

QlikView Server は、Windows ファイル システムの NTFS 権限を使って許可情報を保存します。NTFS 許可モードでは、QlikView Server が、認証済みユーザーが基本的な QlikView ドキュメント ファイル (*.qvw* または *.qvf*) に対する NTFS 権限を所有しているかどうかを検証し、指定した QlikView ドキュメントへのアクセスを管理します。これはオペレーティング システム権限とACL に用いられる Windows NTFS に基づき行われます。認証済みユーザーの権限は、サーバー管理者がディレクトリプロパティオプションを通じ、標準的な Windows Explorer 機能を用いて設定します。

Windows NTFS の代替として、QlikView は独自の ACL、DMS を利用できます。この場合、NTFS とは異なり、非 Windows ユーザーおよびグループに対しアプリケーションやデータへのアクセスが認可されます。DMS は、グループのメンバーが記録された既存の Directory Service Provider (アクティブ ディレクトリやその他の LDAP など) と完全に統合します。このメカニズムにより、QlikView Server は既存の企業アカウントおよびグループ構造を再利用できます。許可されたユーザーまたはグループは QlikView ドキュメントの隣にあるメタファイルに記録され、QMC を使って管理されます。

NTFS はデフォルトのドキュメント許可モデルで、すべてのユーザーとグループがアクティブ ディレクトリまたは QlikView Server ホストにローカルで識別された場合に適しています。NTFS の許可は、QlikView ドキュメントが格納されているディレクトリから継承されるか、あるいは QlikView Publisher 配信タスクを用いて割り当てられます。

認証ユーザーID が Windows ユーザー アカウントではない場合は DMS が必要です。DMS の許可は、QMC を用いて明示的に割り当てられるか、QlikView Publisher 配信タスクを用いて割り当てられます。

> *web チケットを使用してユーザーを認証すると、たとえアクティブ ディレクトリの形式でユーザー名を送信しても、そのユーザーは Windows の正規ユーザーにはなりません。つまり、web チケットを使う場合は、DMS 認証を使用する必要があります。*

データレベルでの許可

データレベルでの許可では、ドキュメント レベルまたはドキュメント内の特定のデータに対するアクセスの許可または拒否を設定できます。

データレベルでの許可には 2 つの種類があります。

- 動的データ削減: ユーザーがデータにアクセスを試みた際、ユーザーがそのデータの閲覧を許可されているかどうか判断します。
- 静的データ削減: QlikView Publisher によって行われ、ユーザーに対しデータが利用可能になった場合、ユーザーがそのデータの閲覧を許可されているかどうか判断します。

データの静的/動的分割はそれぞれ単独で使用できますが、データレベルでの許可と組み合わせることも可能です。

動的データ削除

動的データ分割は、QlikView ドキュメントの一部である Section Access のコンセプトを用いて QlikView 内で行われます。

セクション アクセス管理は、QlikView Management Console (QMC) で設定されています。詳細については、QMC のヘルプを参照してください。

静的データ削除

大規模な実装および/または許可機能の一元管理を行う場合は、QlikView Server/Publisher が用いられます。部門や機能には、通常すべての関連データを含むあらゆる分析ニーズを網羅した「マスター」アプリケーションがあり、このマスター ドキュメントは目的の対象者のニーズおよびアクセス権限に応じて分別 (「分割」) される必要があります。QlikView Publisher は QlikView ドキュメントに利用可能なデータをリロードし、Section Access テーブルを更新して、サイズの大きな QlikView ドキュメントを特定のフィールド内の値に基づき小さなサイズに分割します。

この「分割と配信」により、多数のデータフィールドを含むファイルをフィールドのコンテンツごとに細分化し、権限のあるユーザーやグループに対しそのアクセス権限に応じて配信を実行できます。

ソース ファイルをこの方法で分割・配信するメリットとして、このプロセスで作成されるドキュメントは、そのスクリプト環境にソース データへの明示的な参照が含まれない点が挙げられます。このため、ユーザーが QlikView Desktop を介してドキュメントを利用する際、ソース データの格納場所を閲覧することはできません。ユーザーのニーズに関連するすべてのデータは、ドキュメントに含まれます。

管理者は、QMC を使用してソース *.qvw*、*.qvf* または *.qvd* ファイルにタスクを作成することでこの作業を実行できます。基本的なレベルでの手順は以下の通りです。

管理者は、QMC を使用してソース *.qvw*、*.qvf* または *.qvd* ファイルにタスクを作成することでこの作業を実行できます。基本的なレベルでの手順は以下の通りです。

1. ソース ドキュメント (*.qvw*、*.qvf*、または *.qvd* のいずれか) でデータ分割基準を適用します (データを分割するフィールド名を選択するなど)。
2. 新しく作成された (分割された) ファイルに配賦条件を適用します。
    a. いずれかの DMS または NTFS を使用して認証特権を適用します。
    b. 配信の種類 (たとえば、*.qvw* または *.qvf* ファイルまたは *.pdf* レポート)。
    c. 新しく作成されたファイルの場所を選択します。
3. タスク完了時の通知基準 (メール通知など) を適用します。

新たに作成したファイルには、ユーザーまたはグループが閲覧を認可されたデータのみが含まれます。これは、データが分割基準に応じてマスター ドキュメントから「分割」されたためです。このプロセスが「静的データ分割」と呼ばれるのはこのためです。各ファイルには認可されたデータしか存在しないため、認可されていない人物がデータを閲覧するリスクを回避できます。

6.5 QVD 暗号化

QVD ファイル内の機密情報を顧客提供のキーペアで暗号化して、データへのアクセスを制御することができます。暗号化キーは証明書によって管理されます。証明書は QlikView Distribution Service (QDS) を実行するユーザーの証明書ストアに格納する必要があります。

暗号化は、暗号化が有効になっていて証明書の拇印が追加されている *settings.ini* ファイルで構成されます。QVD 暗号化はデフォルトでは有効になっていません。

エンジンは拇印を読み取ってから、Windows CNG キー ストアからキーを取得します。次に、エンジンはデータの暗号化に使用される新しいデータ暗号化キー (DEK) を生成します。

> *DEK は再利用されないため、1 つのファイルが侵害された場合でも、他のすべてのファイルに対して暗号化が引き続き有効です。*

以下は暗号化されています:

- データ (テーブルと項目)

QVD ヘッダーは暗号化されません。暗号化パラメーターは、追加のメタデータとして QVD ヘッダーに格納されます。

> *既存の QVD を再ロードして、settings.ini ファイルで QVD 暗号化を有効にした後で暗号化する必要があります。*

Qlik Sense および QlikView の古いバージョンは、暗号化された QVD ファイルを読み取るときにエラーを返します。

暗号化証明書の概要

暗号化キーは、証明書を使用して管理するのが最適です。証明書は QlikView Distribution Service (QDS) を実行するユーザーの証明書ストアに格納する必要があります。

暗号化証明書は、暗号化キーの周りのシェルとして機能します。証明書の有効期限が切れている場合で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は、2 種類のキーを使用します。

- データ暗号化キー
- キー暗号化キー

データ暗号化キー

データ暗号化キー (DEK) は、データの AES-256 暗号化用に自動生成されたキーです。暗号化されたオブジェクトごとに新しいキーが生成されます。

キー暗号化キー

キー暗号化キー (KEK) は、データ暗号化キーの安全な非対称暗号化のための秘密キーと公開キーのペアです。公開キーはデータの暗号化に使用され、秘密キーは公開キーで暗号化されたデータの復号化に使用されます。

RSA アルゴリズムを使用するキーのみがサポートされています。

キーの暗号化に使用されるキーは、*settings.ini* ファイルで指定されます。Microsoft Cryptography Next Generation(CNG) Key Storage Provider に格納されています。これは、Windows 証明書ストアに格納されている証明書に含まれています。

QVD 暗号化の使用

これは、QlikView で QVD 暗号化機能を使用するための一般的なワークフローです。

1. 暗号化証明書を作成: *Windows PowerShell を使用して暗号化証明書を作成 (page 179)*
2. QVD 暗号化を有効にし、キーを指定: *QVD 暗号化の有効化 (page 177)*
3. マルチノード展開の場合、暗号化証明書をエクスポート: *Windows PowerShell を使用して暗号化証明書をエクスポート (page 181)*
4. マルチノード展開の場合、すべてのノードで暗号化証明書をインポート: *Windows PowerShell を使用して暗号化証明書をインポート (page 183)*

必ず証明書をバックアップしてください。証明書が失われると、暗号化された QVD を開くことができない場合があります。必要な限り、証明書のバックアップを安全に保管するのはユーザーの責任です。

Qlik Sense 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。

QVD 暗号化の有効化

Qlik Associative Engine は、*settings.ini* ファイルで暗号化キーの拇印を定義することによって構成されます。`enableEncryptQvd=1` を定義して QVD 暗号化を有効にします。次に、証明書から *拇印* 項目の値をコピーし、*settings.ini* の `encryptionKeyThumbprint` 項目に貼り付けます。

証明書は QlikView Distribution Service (QDS) を実行するユーザーの証明書ストアに格納する必要があります。

次の手順を実行します。

1. 証明書マネージャツール (certmgr.msc) を開きます。
2. 証明書を見つけます。

3. 証明書を右クリックして **[Open]** (開く) を選択します。
4. **[詳細]** タブで、**[拇印]** 項目を選択し、値をコピーします。
5. 適切な *settings.ini* ファイルを見つけます。
   QlikView Desktop の場合、*settings.ini* ファイルは *C:\Users\<user>\AppData\Roaming\QlikTech\QlikView* にあります。
   QlikView Server の場合、*settings.ini* ファイルは *C:\Windows\System32\config\systemprofile\AppData\Roaming\QlikTech\QlikViewBatch* にあります。
6. *settings.ini* ファイルで、QVD 暗号化を有効にします: `enableEncryptQvd=1`。次に、拇印値を `encryptionKeyThumbprint` 項目に貼り付けます。

   ```
   enableEncryptQvd=1 encryptionKeyThumbprint=563888bb6aea55eb0d33d9d8b909e0d2ef26ffbd
   ```
7. *Settings.ini* ファイルを保存します。

QlikView 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) 拇印を受け入れます。

証明書の拇印に、**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、次のように `encryptionKeyThumbprint` 項目に入力します。

```
encryptionKeyThumbprint=563888bb6aea55eb0d33d9d8b909e0d2ef26ffbd
```

組織にキー ローテーション ポリシーがある場合、キーが変更されたときに拇印定義を更新する必要がある場合があります。
QVD が新しいキーで保存されるまで、古いキーを含む証明書をサーバーに保存してください。

暗号化証明書の管理

証明書の管理に使用できるツールは多数ありますが、このドキュメントでは、Windows PowerShell と Microsoft Management Console を使用した証明書の作成と配布に焦点を当てています。

他のツールを使用する場合、要件は次のとおりです。

- RSAキーが使用される
- キーは CNG KeyStorageProvider に格納される
- 証明書は、エンジンを実行しているユーザーの証明書ストアに格納される

必ず証明書をバックアップしてください。証明書が失われると、暗号化された QVD を開くことができない場合があります。必要な限り、証明書のバックアップを安全に保管するのはユーザーの責任です。

暗号化証明書は、展開内のすべてのノードにエクスポートする必要があります。

Windows PowerShell を使用して暗号化証明書を作成

証明機関 (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、QlikView Distribution Service (QDS) を実行するユーザーの証明書ストアに格納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

Windows Server 2016 以降の PowerShell を使用して証明書を作成する場合、少なくとも次のパラメーターを定義する必要があります。

> *包括的なドキュメントについては、「Microsoft New-SelfSignedCertificate ドキュメント」を参照してください。*

-Subject

新しい証明書の件名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の相対識別名 (RDN とも呼ばれる) の場合、各件名の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ている場合は、各件名相対識別名をセミコロン (;) で区切ります。

```
-Subject <Certifcate name>
```

-KeyAlgorithm

新しい証明書に関連付けられる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** である必要があります。

```
-KeyAlgorithm RSA
```

-KeyLength

新しい証明書に関連付けられているキーの長さをビット単位で指定します。

```
-KeyLength <Key length, e.g.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。このパラメーターの許容値は次のとおりです。

- Exportable
- ExportableEncrypted (既定値)
- 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、デフォルトのストアは **Cert:\CurrentUser\My** です。それ以外の場合は、このパラメーターに **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

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

> *包括的なドキュメントについては、「Microsoft New-SelfSignedCertificate ドキュメント」を参照してください。*

-DnsName

証明書の件名の別名拡張に含める1つ以上の文字列を指定します。最初の DNS 名は、件名と発行者名としても保存されます。

```
-DnsName <Certifcate name>
```

-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、デフォルトのストアは **Cert:\CurrentUser\My** です。それ以外の場合は、このパラメーターに **Cert:\CurrentUser\My** を指定する必要があります。

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

New-SelfSignedCertificate 既定値 Windows Server 2012 R2

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

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

例: PowerShell for Windows Server 2016 以降を使用してデータ暗号化証明書を作成する

この例では、test というユーザーが、件名が MyTestCert で、キーの長さが 4096 ビットの自己署名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 に格納されます。

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"
```

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 を使用して暗号化証明書をエクスポート

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 cmdlet parameters

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

> *包括的なドキュメントについては、「Microsoft New-SelfSignedCertificate 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\<certificate thumbprint>
```

-FilePath

エクスポートする PFX ファイルのパスを指定します。

```
-FilePath <FileName>.pfx
```

-Password

エクスポートされたPFX ファイルを保護するために使用され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。このパラメーターを指定しないと、エラーが表示されます。

```
-Password <Password or variable>
```

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、プレーン テキストのパスワード文字列の安全な文字列を作成し、$mypwd 変数に格納します。彼は **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\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、拇印 563888bb6aea55eb0d33d9d8b909e0d2ef26ffbd で暗号化証明書を実際にエクスポートします。前のステップ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 Management Console を使用した暗号化証明書のバックアップ

常に証明書のバックアップが必要です。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、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。必要な限り、証明書のバックアップを安全に保管するのはユーザーの責任です。

証明書をバックアップするときのエクスポートと同じ手順を使用できます。*Windows PowerShell を使用して暗号化証明書をエクスポート (page 181)* を参照してください。

暗号化証明書をバックアップするもう1 つの方法は、Microsoft Management Console でそれを行うことです。以下の例は、Microsoft Management Console 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 Management Console を開きます。Windows の検索 メニューで mmc と入力して開きます。
2. Console ウィンドウで、**[ファイル] > [スナップインの追加/削除]** をクリックします。

3. [スナップインの追加または削除] 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. Console ウィンドウの左側の [Console Root] 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. 中央のペインで、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]** を選択して、**[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、**[Personal Information Exchange – 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。

    > *[正常にエクスポートされた場合、秘密キーを削除]* 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]** ボックスをオンにし、パスワードを作成して確認します。

    > *このパスワードは、秘密キーを使用して証明書を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たことを示すメッセージが表示され、秘密キー付きの SSL 証明書が選択した場所に保存されます。

Windows PowerShell を使用して暗号化証明書をインポート

他のマシン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、QlikView Distribution Service (QDS) を実行するユーザーの証明書ストアに格納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 cmdlet parameters

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

包括的なドキュメントについては、「Microsoft Import-PfxCertificate ドキュメント」を参照してください。

-CertStoreLocation

証明書がインポートされるストアのパスを指定します。このパラメーターが指定されていない場合、現在のパスが宛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 <FileName>.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。このパラメーターが指定されていない場合、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 というユーザーが、以前に PFX ファイルにエクスポートされた拇印 `563888BB6AEA55EB0D33D9D8B909E0D2EF26FFBD` の暗号化証明書をインポートします。

1. まず、プレーンテキストのパスワード文字列の安全な文字列を作成し、`$mypwd` 変数に格納します。彼は **`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を続行します。前のステップ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 Management Console を使用した暗号化証明書の復元

証明書を復元するときのインポートと同じ手順を使用できます。*Windows PowerShell を使用して暗号化証明書をインポート (page 183)* を参照してください。

Microsoft Management Console を使用した暗号化証明書のバックアップ (page 182) で説明されているように、Microsoft Management Console を使用して証明書をバックアップした場合は、以下の例に従って SSL 証明書を復元します。

> *復元する暗号化証明書は、QlikView Distribution Service (QDS) を実行するユーザーの証明書ストアに格納する必要があります。*

次の手順を実行します。

1. SSL 証明書をインストールする Windows サーバーで、Microsoft Management Console を開きます。Windows の検索 メニューで `mmc` と入力して開きます。
2. Console ウィンドウで、**[ファイル] > [スナップインの追加/削除]** をクリックします。
3. [スナップインの追加または削除] 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. Console ウィンドウの左側の [Console Root] ペインで、[証明書 (現在のユーザー)] を展開し、[個人] フォルダを右クリックして、**[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 ウィザードへようこそ] 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。

   > *デフォルトでは、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 証明書がエクスポートまたはバックアップされたときに作成され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。つまり、必要に応じて SSL 証明書をバックアップまたはエクスポートできます。

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]** を選択して **[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. インポートが成功したことを示すメッセージが表示され、秘密キー付きの SSL 証明書が個人ストア (フォルダ) に保存されます。

7 ライセンス QlikView

ライセンスにより、組織内での QlikView ソフトウェアの使用状況を管理できます。

7.1 概要

QlikView Server 展開には、シリアル番号とコントロール ナンバーまたは署名付きキーによってライセンスが付与されます。QlikView Server ライセンスは、アクセス権のタイプとCAL (クライアント アクセス ライセンス) のいずれかに基づいています。インストールされている QlikView Server には QlikView Publisher ライセンスを組み込むこともできます。

QlikView の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、製品使用条件、および次のライセンス付与サービスのリファレンス ガイドをお読みください:

- Qlik 法的規約
- Qlik 製品使用条件
- Qlik ライセンス付与サービス リファレンス ガイド

7.2 統一ライセンス

QlikView、Qlik Sense、QlikView の April 2019 リリース以降、お客様は複数の展開で統一ライセンスを使用できます。統一ライセンスでは、次の展開の組み合わせにおいて同じ署名付きキーを共有します。

- 展開数でQlik Sense Enterprise
- 複数の QlikView Server 展開
- QlikView Server 展開とQlik Sense Enterprise 展開

同じ署名付きキーを複数の展開に適用することにより、同じタイプのユーザーとアクセス権を共有することができます。ユーザーは、Professional または Analyzer のアクセス権割り当てを使用して接続されているすべての展開にアクセスできます。

署名付きキーを QlikView Server 展開に適用し、Professional および Analyzer アクセスを構成する方法の詳細な手順については、以下を参照してください。 *で Professional アクセス権とAnalyzer アクセス権を構成するQlikView Server (page 190)* 。

7.3 QlikView Server ライセンス

QlikView Server ライセンスの期限とアクセス権の割り当ては、ライセンス認証方法に応じて、ライセンス認証ファイル (LEF) または [License Definition] (ライセンス定義) によって定義されます。QlikView Server ライセンスは、アクセス権のタイプとCAL (クライアント アクセス ライセンス) のいずれかに基づいています。

ユーザーベースとキャパシティベースのライセンス

ユーザーベース ライセンスでは、事前定義された数のアクセス権割り当てが付与され、一意の特定されたユーザーに割り当てることが可能です。QlikView Server でのユーザーベース ライセンスは、Professional および Analyzer ユーザー ライセンスとクライアント アクセス ライセンス (CAL) のいずれかです。

キャパシティベース ライセンスでは、QlikView にアクセスするための事前定義された数のアクセス権割り当てが付与され、特定または匿名のユーザーが使用可能です。QlikView Server でのキャパシティベース ライセンスは、Analyzer Capacity アクセス権とCAL のいずれかに基づいています。

アクセス権のタイプ

Professional および Analyzer ユーザー ライセンス (ユーザーベース) とAnalyzer Capacity ライセンス (キャパシティベース) は組み合わせることができます。これらのライセンスは、サブスクリプション ベースで、署名付きキーを使用して有効化されます。[License Definition] (ライセンス定義) でのライセンスの詳細は、QlikView 管理コンソール で確認できます。参照 : QlikView Server ライセンス。

- Professional アクセス権とAnalyzer アクセス権 (ユーザーベース) は、Qlik Sense の場合のようにしてユーザーに割り当てられます。[License Definition] (ライセンス定義) により2 つのタイプのアクセス権の配布が決まります。
- Analyzer Capacity(キャパシティベース) は、使用可能な機能に関してAnalyzer アクセス権に似ています。Analyzer Capacity は、特定または匿名のユーザーに割り当てることができます。ユーザーは、6 分単位で消費される毎月の Analyzer 時間割り当てを共有します。

CAL

User および Document CAL (ユーザーベース) とSession および Usage CAL (キャパシティベース) は組み合わせることができます。CAL は、サブスクリプション ベースか永続的です。シリアル番号とコントロール ナンバーで構成されるライセンス キーを使用して有効化されます。

- User および Document CAL (ユーザーベース): QlikView ドキュメントへのアクセスのために一意で特定されたユーザーに割り当てられます。LEF ファイルにより、インストール環境で使用可能な CAL のタイプと数が決まります。
- Session および Usage CAL (キャパシティベース): すべての (特定または匿名) ユーザー QlikView ドキュメントにアクセスし、消費できます。LEF ファイルにより、インストール環境で使用可能な CAL のタイプと数が決まります。

制限事項

アクセス権のタイプ (Professional、Analyzer、Analyzer Capacity) とCAL (User、Document、Session、Usage) を組み合わせることはできません。QlikView Server ライセンスは、ユーザーベース アクセス権とキャパシティベース アクセス権 クオータの両方で構成されています。例:

- アクセス権のタイプに基づいてライセンスを購入する場合、ユーザーのライセンスには、Professional アクセス権、Analyzer アクセス権、Analyzer Capacity アクセス権で構成されるさまざまなクオータを含めることができます。
- CAL に基づいてライセンスを購入する場合、ユーザーのライセンスには、User、Document、Session、または Usage CAL によるさまざまなクオータを含めることができます。

Professional アクセス権とAnalyzer アクセス権の動的割り当て

QlikView Server は、Professional および Analyzer タイプのアクセス権の動的割り当てに対応しています。Professional アクセス権とAnalyzer アクセス権の動的割り当ては QlikView 管理コンソール で有効にすることができます。「Professional アクセス権とAnalyzer アクセス権」を参照してください。

動的割り当ての仕組み:

- Professional および Analyzer の両タイプのアクセス権について動的割り当てが有効になっている場合は、ログインするユーザーに Professional アクセス権が自動的に割り当てられます (選択可能な場合)。選択できない場合は、ユーザーにAnalyzer アクセス権が割り当てられます。Analyzer アクセス権を選択できない場合は、ユーザーに Analyzer Capacity アクセス権が割り当てられます。Analyzer Capacity を選択できない場合、ユーザーは QlikView にアクセスできません。
- Professional タイプのアクセス権についてのみ動的割り当てが有効になっている場合は、ログインするユーザーに Professional アクセス権が自動的に割り当てられます (選択可能な場合)。選択できない場合は、ユーザーに Analyzer Capacity アクセス権が割り当てられます。Analyzer Capacity を選択できない場合、ユーザーは QlikView にアクセスできません。
- Analyzer タイプのアクセス権についてのみ動的割り当てが有効になっている場合は、ログインするユーザーに Analyzer アクセス権が自動的に割り当てられます (選択可能な場合)。選択できない場合は、ユーザーに Analyzer Capacity アクセス権が割り当てられます。Analyzer Capacity を選択できない場合、ユーザーは QlikView にアクセスできません。

動的割り当てを有効にすると、ユーザーに二重に割り当てられる可能性があります。これは、インストール環境で使用可能なライセンスの数に影響することがあります。

QlikView Server 署名付きキー

署名付きキーで QlikView にライセンスを付与すると、ライセンス定義やアクセス権の割り当てなどのライセンス情報は QlikView 展開の外部にあるライセンス バックエンドに保管されます。接続されている展開では同じ License Back-end を使用します。接続されている展開のリストにあるユーザーは、アクセス権割り当てと一緒に、インストールされている QlikView との間で共有されます。これは、インストールされている QlikView で使用可能な Professional および Analyzer のアクセス権割り当ての数に影響します。

QlikView Server ライセンス キー

ライセンス キーは、シリアル番号とコントロール ナンバーで構成されています。このキーは、CAL に基づいて QlikView Server ライセンスを有効化する場合に使用されます。CAL は、ライセンス付与のためだけに使用され、データ アクセス目的のユーザー認証では使用されません。

QlikView Server のライセンス キーは、付与されたライセンス数のノードが任意の時点で稼働していれば、必要な数のサーバーにインストールすることができます。

コールド スタンドバイ環境をインストールし、稼働可能な状態にしておくことができますが、稼働環境がシャットダウンされるより前に稼働状態 (Windows サービスを開始することはできません) や使用中にすることはできません。

インストールされている QlikView Server に接続するため、各クライアントには クライアント アクセス ライセンス (CAL) が必要です。CAL は QlikView Server と共に購入し、サーバーのシリアル番号と関連付けられます。CAL は、QlikView クライアント プログラムに転送したり、異なる QlikView Server クラスター間で転送したりすることはできません。クラスターごとに別個の CAL が必要です。

7.4 QlikView Publisher ライセンス

QlikView Publisher ライセンスにより、インストールされている QlikView Server に先進のロード機能や配布モデルなどの機能が追加されます。専用の LEF ファイルにより、QlikView Publisher ライセンスの機能が決まります。
このライセンスは永続的で、シリアル番号とコントロール ナンバーで構成されるライセンス キーを使用して有効化されます。

7.5 QlikView Desktop

QlikView Desktop は次のライセンス オプションに対応しています。

- ローカル クライアント ライセンス: 完全でライセンス付与されたバージョンの QlikView Desktop。ローカル クライアント ライセンスは、ライセンス認証ファイル (LEF) によって定義され、ライセンス キーを使用して有効化されます。
- Personal Edition。個人、学生、または小規模なスタートアップ向けのライセンスなしバージョンの QlikView Desktop。QlikViewPersonal Edition の詳細については、次を参照してください:QlikView Personal Edition

QlikView Desktop は、Professional アクセス権と Analyzer アクセス権、または CAL アクセス権を使用して、インストールされている QlikView Server に接続できます。

7.6 で Professional アクセス権と Analyzer アクセス権を構成する QlikView Server

QlikView April 2019 以降は、Professional および Analyzer ユーザー ライセンスを適用できます。Professional および Analyzer ユーザー ライセンスは署名付きキーを使用して有効化されます。CAL ライセンスから Professional および Analyzer ユーザー ライセンスに移行する場合は、新しいタイプのアクセス権をユーザーに割り当てる必要があります。統一ライセンスを使用する場合は、ユーザーおよびユーザーの Professional アクセス権と Analyzer アクセス権を接続されている QlikView および Qlik Sense の展開と共有できます。

QlikView へのライセンス付与の詳細については、次を参照してください: *ライセンス QlikView (page 187)*

CAL ライセンスから Professional および Analyzer ユーザー ライセンスに切り換えるには、次の操作を行う必要があります。

- 署名付きキーを QlikView Server Service (QVS) に適用することにより、Professional および Analyzer ユーザー ライセンスを有効化する。
- Professional アクセス権と Analyzer アクセス権をユーザーに割り当てる。

制限事項

Professional および Analyzer ユーザー ライセンスで QlikView にライセンスを付与する場合は、すべての QlikView Server Service (QVS) インスタンスで同じライセンスと署名付きキーを共有する必要があります。異なる署名付きキーを同じインストール内の別の QVS インスタンスに適用すると、最後に適用された署名付きキーが他の QVS インスタンスに伝搬し、前の署名付きキーが上書きされます。

Professional および Analyzer ユーザー ライセンスを使用してインストールされている QlikView にライセンスを付与する場合、QVS インスタンスの数は最大許容数に制限されます。ライセンスの詳細は、QlikView 管理コンソールの [**License Definition**] (ライセンス定義) ボックスで確認できます。

Professional および Analyzer ユーザー ライセンスの有効化

次の手順を実行します。

1. QlikView 管理コンソールで、[**システム**] に移動し、[**ライセンス**] タブを開きます。
2. **QlikView Server** を選択して QlikView Server ライセンス メニューを開きます。
3. [**QlikView Server ライセンス**] タブで、[**Use Signed Key License**] (署名付きキー ライセンスを使用する) チェック ボックスをオンにします。
   メニューが切り替わり、署名付きキーを使用する QlikView Server を有効化するための項目が表示されます。
4. 専用項目に署名付きキーを入力し、[**Apply License**] (ライセンスを適用) を選択します。
5. ポップアップ ウィンドウに、QlikView Server (QVS) を再起動する必要があることを示すメッセージが表示されます。[**OK**] を選択して再起動し、新しいライセンスを適用します。
6. QlikView Server (QVS) が再起動すると、新しいライセンスが適用されます。[**QlikView Server ライセンス**] タブの [**License Definition**] (ライセンス定義) ボックスに、ライセンスの詳細が表示されます。このテキストは編集できません。
7. インストールされている QlikView の QlikView Server クラスターごとにこのプロセスを繰り返します。

Professional アクセス権と Analyzer アクセス権の割り当て

インストールされている QlikView Server に Professional および Analyzer のユーザー ライセンスを適用したら、Professional アクセス権と Analyzer アクセス権をユーザーに割り当てる必要があります。CAL ライセンスから切り替える場合は、新しい種類のアクセス権の 1 つをユーザーに手動で付与することが必要です。詳細については下記を参照してください。*これまで CAL アクセス権が割り当てられていたユーザー (page 193)*

Professional アクセス権と Analyzer アクセス権は、インストールされている QlikView のディレクトリ サービス プロバイダのいずれかのリストにあるユーザーにのみ付与できます。

Professional アクセス権の割り当て

次の手順を実行します。

1. QlikView 管理コンソールで、[**システム**] に移動し、[**ライセンス**] タブを開きます。
2. **QlikView Server** を選択し、[**Professional and Analyzer access**] (Professional および Analyzer アクセス権) タブを開きます。

3. [**Professional Access**] (Professional アクセス権) を選択します。
4. [**Assigned Users**] (割り当てられているユーザー) の、  検索フィールドで、アイコンをクリックします。アクセス権の割り当てウィンドウが開きます。
5. 専用検索フィールドでユーザーを検索します。セミコロン区切りのリストを入力することにより、複数のユーザーを同時に検索できます。検索条件に適合するユーザーは [**検索結果**] のリストに表示されます。
6. プロフェッショナル アクセス権を付与するユーザーを選択し、[**追加**] をクリックします。
7. [**OK**] を選択してアクセス権の割り当てを確認します。アクセス権の割り当てウィンドウが閉じます。
8. [**適用**] を選択してアクセス権の割り当てを確認します。
9. Professional アクセス権を付与されたユーザーのリストが [**Assigned Users**] (割り当てられているユーザー) に表示されます。

アクセス権の割り当ての削除

ユーザーから Professional アクセス権を削除するには、  削除アイコンをクリックします。[**適用**] を選択して確認します。

アクセスの削除が適用される前にキャンセルする場合は、ユーザー行の  元に戻すアイコンをクリックします。このオプションは、[**適用**] を選択する前にのみ選択できます。

Analyzer アクセス権の割り当て

次の手順を実行します。

1. QlikView 管理コンソールで、[**システム**] に移動し、[**ライセンス**] タブを開きます。
2. **QlikView Server** を選択し、[**Professional and Analyzer access**] (Professional および Analyzer アクセス権) タブを開きます。
3. [**Analyzer Access**] (Analyzer アクセス権) を選択します。
4. [**Assigned Users**] (割り当てられているユーザー) で、  検索フィールドで、アイコンをクリックします。アクセス権の割り当てウィンドウが開きます。
5. 専用検索フィールドでユーザーを検索します。セミコロン区切りのリストを入力することにより、複数のユーザーを同時に検索できます。検索条件に適合するユーザーは [**検索結果**] のリストに表示されます。
6. Analyzer アクセス権を付与するユーザーを選択し、[**追加**] をクリックします。
7. [**OK**] を選択してアクセス権の割り当てを確認します。アクセス権の割り当てウィンドウが閉じます。
8. [**適用**] を選択してアクセス権の割り当てを確認します。
9. Analyzer アクセス権を付与されたユーザーのリストが [**Assigned Users**] (割り当てられているユーザー) に表示されます。

アクセス権の割り当ての削除

ユーザーから Analyzer アクセス権を削除するには、  削除アイコンをクリックします。[**適用**] を選択して確認します。

アクセスの削除が適用される前にキャンセルする場合は、ユーザー行の  元に戻すアイコンをクリックします。このオプションは、[**適用**] を選択する前にのみ選択できます。

Professional アクセス権とAnalyzer アクセス権の動的割り当て

QlikView Server は、Professional および Analyzer タイプのアクセス権の動的割り当てに対応しています。Professional アクセス権とAnalyzer アクセス権の動的割り当ては QlikView 管理コンソールで有効にすることができます。「Professional アクセス権とAnalyzer アクセス権」を参照してください。

動的割り当ての仕組み:

- Professional および Analyzer の両タイプのアクセス権について動的割り当てが有効になっている場合は、ログインするユーザーに Professional アクセス権が自動的に割り当てられます (選択可能な場合)。選択できない場合は、ユーザーにAnalyzer アクセス権が割り当てられます。Analyzer アクセス権を選択できない場合は、ユーザーに Analyzer Capacity アクセス権が割り当てられます。Analyzer Capacity を選択できない場合、ユーザーは QlikView にアクセスできません。
- Professional タイプのアクセス権についてのみ動的割り当てが有効になっている場合は、ログインするユーザーに Professional アクセス権が自動的に割り当てられます (選択可能な場合)。選択できない場合は、ユーザーに Analyzer Capacity アクセス権が割り当てられます。Analyzer Capacity を選択できない場合、ユーザーは QlikView にアクセスできません。
- Analyzer タイプのアクセス権についてのみ動的割り当てが有効になっている場合は、ログインするユーザーに Analyzer アクセス権が自動的に割り当てられます (選択可能な場合)。選択できない場合は、ユーザーに Analyzer Capacity アクセス権が割り当てられます。Analyzer Capacity を選択できない場合、ユーザーは QlikView にアクセスできません。

> *動的割り当てを有効にすると、Professional アクセス権または Analyzer アクセス権が手動で割り当てられているユーザーには二重に割り当てられることになります。これは、インストール環境で使用可能なライセンスの数に影響することがあります。手動の割り当てを削除し、全面的に動的割り当てを使用することにより、アクセス権の二重割り当てを防止できます。参照:*Professional アクセス権とAnalyzer アクセス権。

これまで CAL アクセス権が割り当てられていたユーザー

CAL ライセンスからProfessional および Analyzer ユーザー ライセンスに切り換えると、ユーザーに割り当てられていた CAL は無効になります。Professional アクセス権とAnalyzer アクセス権を手動で割り当てる必要があります。CAL からProfessional および Analyzer ユーザー ライセンスに切り換えると、*AllocatedCALinfo.txt* が自動的に生成されて *%ProgramData%\QlikTech\QlikViewServer* に保存されます。このテキスト ファイルには、Professional および Analyzer ユーザー ライセンスに切り換える前に Named User CAL とDocument CAL が割り当てられていたユーザーのセミコロン区切りリストが書き込まれています。

AllocatedCALinfo.txt ファイルを使用して正しいタイプのアクセス権を QlikView ユーザーに割り当てることができます。セミコロン区切りリストを QlikView 管理コンソールの Professional アクセス権または Analyzer アクセス権の割り当てウィンドウ内にコピーしてリストに含まれるユーザーを取り込み、新しいタイプのアクセス権を付与します。アクセス権割り当ての段階的な手順については、次を参照してください:*Professional アクセス権の割り当て (page 191)*、*Analyzer アクセス権の割り当て (page 192)*。

複数の展開でのユーザーの共有

QlikView、Qlik Sense、QlikView の April 2019 リリース以降、お客様は複数の展開で統一ライセンスを使用できます。統一ライセンスでは、次の展開の組み合わせにおいて同じ署名付きキーを共有します。

- 複数の Qlik Sense Enterprise 展開
- 複数の QlikView Server 展開
- QlikView Server 展開と Qlik Sense Enterprise 展開

同じ署名付きキーを複数の展開に適用することにより、同じタイプのユーザーとアクセス権を共有することができます。ユーザーは、Professional または Analyzer のアクセス権割り当てを使用して接続されているすべての展開にアクセスできます。

署名付きキーで QlikView にライセンスを付与すると、ライセンス定義やアクセス権の割り当てなどのライセンス情報は QlikView 展開の外部にあるライセンス バックエンドに保管されます。QlikView Server 展開の Qlik License Service 部分によって問い合わせられるライセンス バックエンド。ポート 443 を開いて License Back-end と通信できるようにしておく必要があります。参照： *アーキテクチャ (page 10)*、*ポート (page 19)*。

統一ライセンスを使用する場合、接続されている展開では同じ License Back-end を使用します。接続されている展開のリストにあるユーザーは、アクセス権割り当てと一緒に、インストールされている QlikView との間で共有されます。これは、インストールされている QlikView で使用可能な Professional および Analyzer のアクセス権割り当ての数に影響します。

統一ライセンスを使用して QlikView にライセンスを付与すると、接続されている展開間で共有されるユーザーはフルネームではなくユーザー名で表示されることがあります。この状況は、ユーザーが接続されている展開で登録されていても、QlikView Server では登録されていない場合に発生します。共有ユーザーの情報が正しく表示されるようにするには、それらのユーザーを QlikView Server 展開で登録する必要があります。共有ユーザーを登録するには、接続されている展開に問い合わせる新しいディレクトリサービス プロバイダを設定し、ユーザーの情報を取得します。

7.7 OEM

基本設定

OEM 機能は、Original Equipment Manufacturer (OEM) ライセンスで販売された QlikView Server の乱用を防止するとともに、OEM 製品および QlikView 製品全般からの収益を保護します。また、この機能によって QlikView OEM パートナー、QlikView 再販パートナー、QlikView 直属のアカウント マネージャー間の販売経路の対立を防止できます。

OEM 機能には、次のような制約があります。

- OEM パートナーが販売する QlikView Server では、同 OEM パートナーが提供する QlikView アプリケーション以外は起動できません。
- OEM パートナーが販売する QlikView アプリケーションは、同 OEM パートナーが提供する QlikView Server 以外では起動できません。

機能の詳細

OEM 機能の詳細は次の通りです。

キーの付いたタグは、QlikView Server のライセンス認証ファイル (LEF) で OEM_PRODUCT_ID. この LEF タグはそれぞれの OEM パートナーが QlikView Desktop とともに発行し、QlikView Server を実装する際に必要に応じて QlikView Server ライセンスからタグへのリンクが生成されます。

QlikView Desktop の [ユーザー プリファレンス (User Preferences)] ダイアログを使って、OEM 開発者は QlikView ドキュメント ファイルにハッシュ キーを埋め込むことができます。ハッシュキーは OEM パートナーの QlikView デスクトップライセンスに存在するキー OEM_PRODUCT_ID に基づいており、40 文字の 16 進文字列 (大文字) で、ドキュメントプロパティとドキュメント メタデータに格納されます。ダイアログでは、QlikView ドキュメント ファイルを作成するすべてのキーにラベルを付けることができます。また同じキーを、同一の顧客用の複数のドキュメントに使用することも可能です。

LEF にタグを持つ QlikView Server のみが、OEM_PRODUCT_ID その QlikView Server と一致するキーを持つ QlikView ドキュメント ファイルをパブリッシュする権利を有します。デフォルトでは、標準的な OEM ではない QlikView Server では、すべての QlikView ドキュメント ファイルを開くことができますが、一致しない QlikView Server でファイルが無断で開かれないように設定された、OEM パートナー専用のキーを含んだドキュメント ファイルは開けません OEM_PRODUCT_ID.

以下のテーブルは OEM 機能の例の一部です。

QEM 機能の例

-	***Normal.qvw***	***OEM 1.qvw***	***OEM 2.qvw***
通常の QlikView Server	ファイルは開く	ファイルは開かない	ファイルは開かない
OEM 1 (ライセンス リースなし)	ファイルは開かない	ファイルは開く	ファイルは開かない
OEM 2 (ライセンス リースなし)	ファイルは開かない	ファイルは開かない	ファイルは開く

QlikView Desktop では、PRODUCT_ID を含むドキュメント ファイルはユーザー モードで開きます。