App Bridge Monitor
Agent 監視サービス
Windows Agent 設定ガイド

Ver.1.19.5

目次

１．本書の役割

本書は、App Bridge Monitor Windows Agent の監視設定について説明するものです。

２．Windows Agent のインストール

App Bridge Monitor Windows Agent のインストール方法は、以下のガイドを参照して下さい。

対象環境	参照ガイド
一般 Windows 環境 （Azure Cloud Services 以外）	App Bridge Monitor Agent 監視サービス Windows Agent インストールガイド
Azure Cloud Services	App Bridge Monitor Agent 監視サービス Windows Agent インストールガイド Azure Cloud Services 編

３．Windows Agent と監視設定

App Bridge Monitor Windows Agent の監視設定は、Windows Agent による対象設定と Web サイトによるエラー判定条件設定で実施します。

監視項目	Windows Agent（監視対象設定）	Web サイト（エラー判定条件）
イベントログ監視	監視対象とするイベントログを指定する。デフォルトでシステム、アプリケーションが対象となる	エラーとするソース、メッセージ ID などを指定する
テキストログ監視	監視対象とするフォルダパス、ファイルマスクなどを指定する	エラーとする文字列などを指定する
Windows サービス監視	監視対象とする Windows サービスを指定する	ー
プロセス監視	監視対象とするプロセスを指定する	エラーとするプロセス数などを指定する
CPU ビジー監視	監視する CPU を指定する。デフォルトで全ての CPU が対象となる	エラーとするビジー率などを指定する
ディスクビジー監視	監視するディスク装置を指定する。デフォルトで全ディスク装置が対象となる	エラーとするビジー率などを指定する
ディスク容量監視	監視するドライブを指定する。デフォルトで全ハードディスクが対象となる	エラーとする空き容量などを指定する
物理メモリ監視	デフォルトで監視対象となる	エラーとする空き容量などを指定する。デフォルトではエラー対象とならず、統計情報のみ取得される
仮想メモリ監視	デフォルトで監視対象となる	エラーとする空き容量などを指定する
SQL Databases 監視 Azure SQL Databases 監視	監視するデータベースを指定する	エラーとするデータベース空き容量などを指定する
ネットワークビジー監視	デフォルトで全 NIC が対象となる	ー（統計情報のみでエラー通知は実施されません）

Web サイトでのエラー判定条件設定の詳細は、「App Bridge Monitor Agent 監視サービス エラー判定条件ガイド」を参照願います。

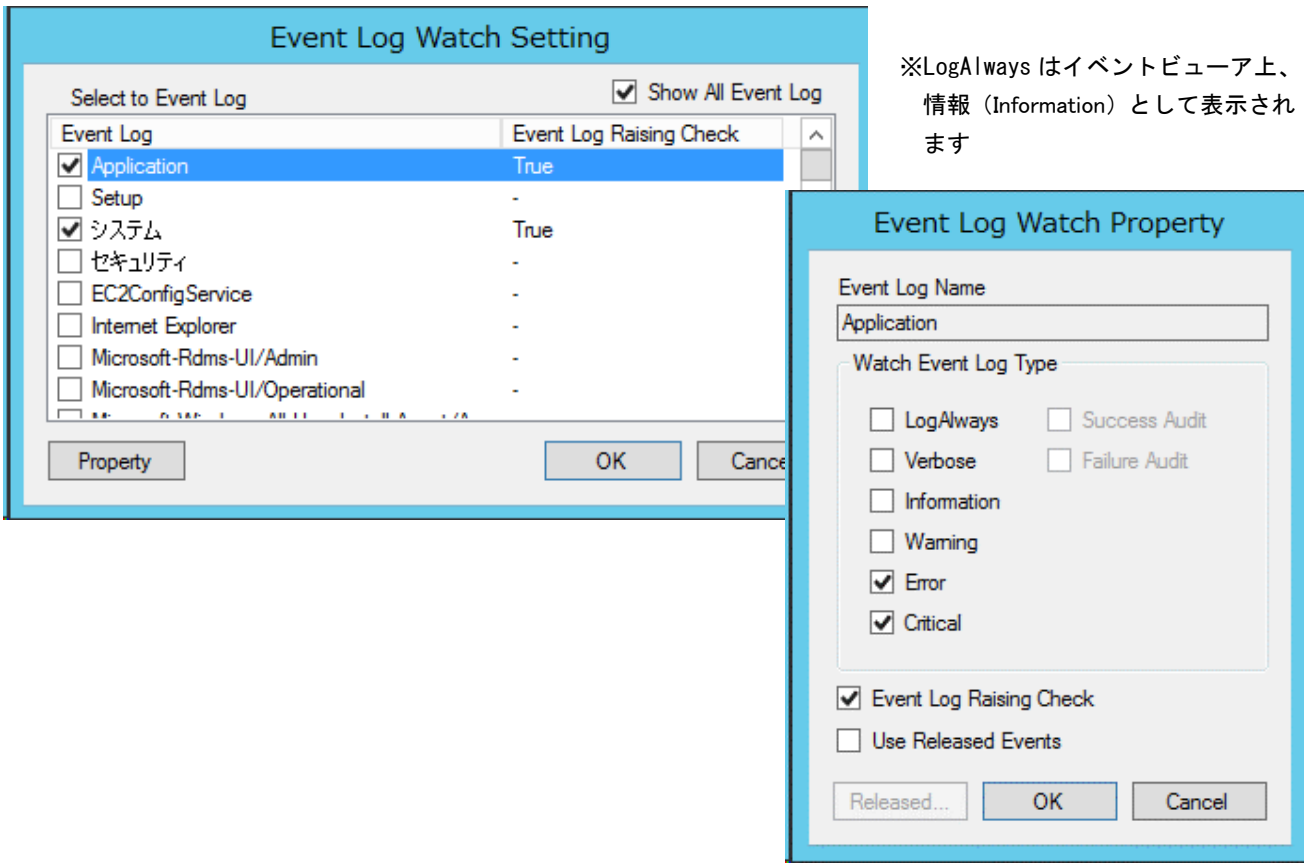
４．監視設定

Agent では、監視対象を設定します。監視条件の設定は、「App Bridge Monitor Agent 監視サービスエラー判定条件ガイド」を参照して下さい。

4.1 イベントログ監視の設定

4.1.1 監視対象のイベントログ設定

監視対象のイベントログを設定します。
Service Control のメニューから「Setting」－「Watch Service」－「Event Log」を選択し、監視対象のイベントログをチェックします。[Property]ボタンをクリックすると監視対象とするイベントの種類（レベル）を設定できます。設定した内容は App Bridge Monitor サービスが再起動されるまで反映されません。



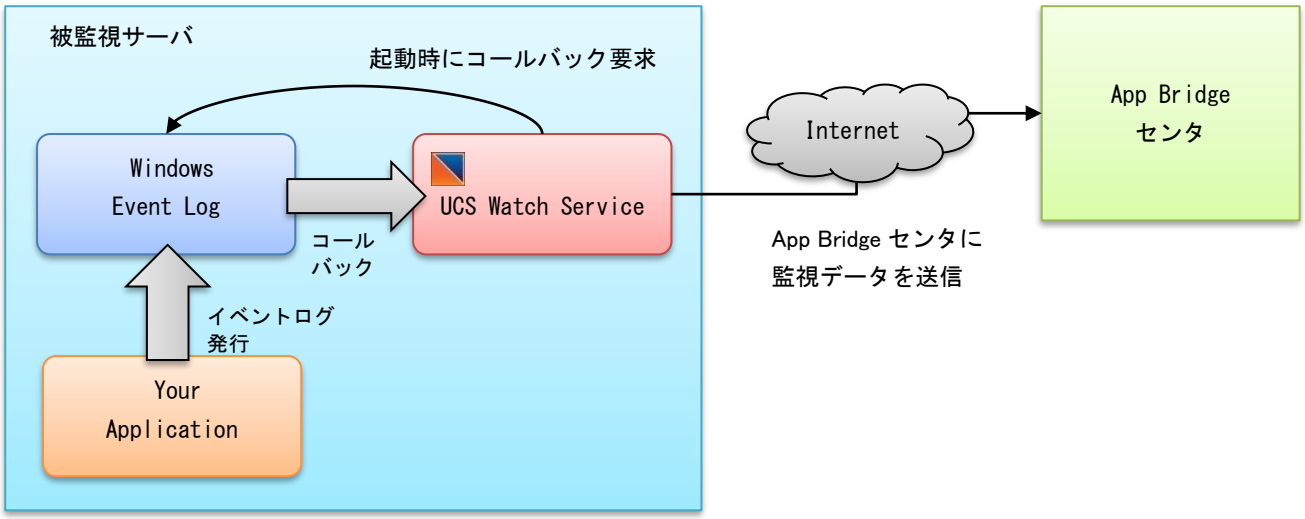
※LogAlways はイベントビューア上、情報（Information）として表示されます

発生したイベントログは即時処理され、監視設定で設定したエラー判定条件（※1）に従って処理されます。初期状態では種類が Error、Critical のメッセージをエラーとしています。Event Log Watch Property で表示される Event Log Name が監視設定の各種条件に設定するログ名となります。

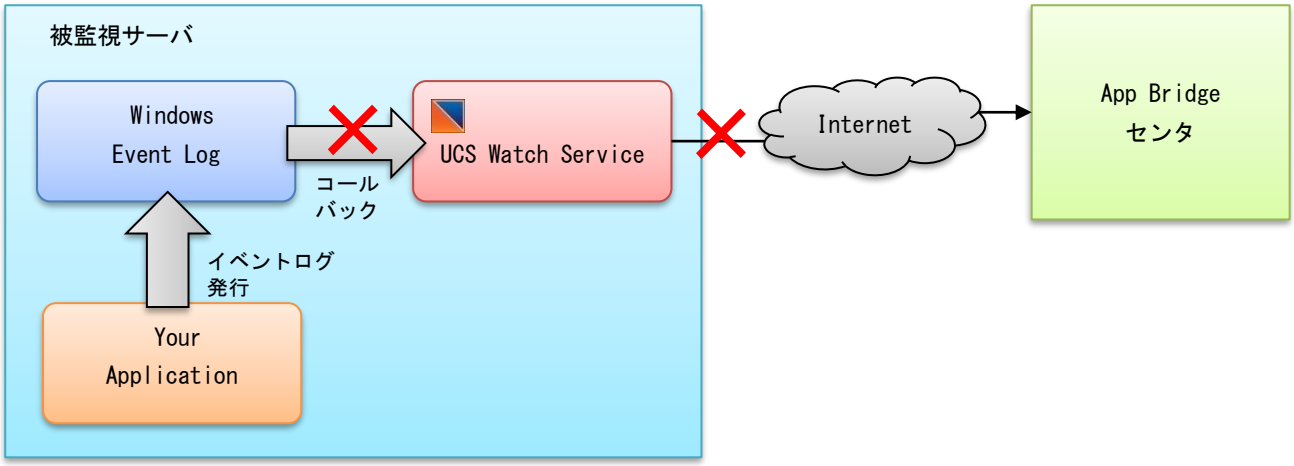
※1：エラー判定条件、除外判定条件の設定については、「App Bridge Monitor Agent 監視サービスエラー判定条件ガイド」を参照して下さい。

4.1.2 Event Log Raising Check

イベントログ監視を実施するため、UCS Watch Service（※1）は、サービス起動時に Windows Event Log（Windows 標準サービス）に対してコールバックを要求します。Windows Event Log はイベントログが発生すると要求に従って UCS Watch Service に発生したイベントログをコールバックし、コールバックを受け取った UCS Watch Service は、App Bridge センタにその内容を送信します。



しかし、何らかの問題が発生し、Windows Event Log がサービス再起動した場合など、コールバックが中断される事象を確認しています。この状況では、UCS Watch Service は、Windows Event Log のコールバックを待ち続けるため、結果としてイベントログの発生を検知できなくなります。

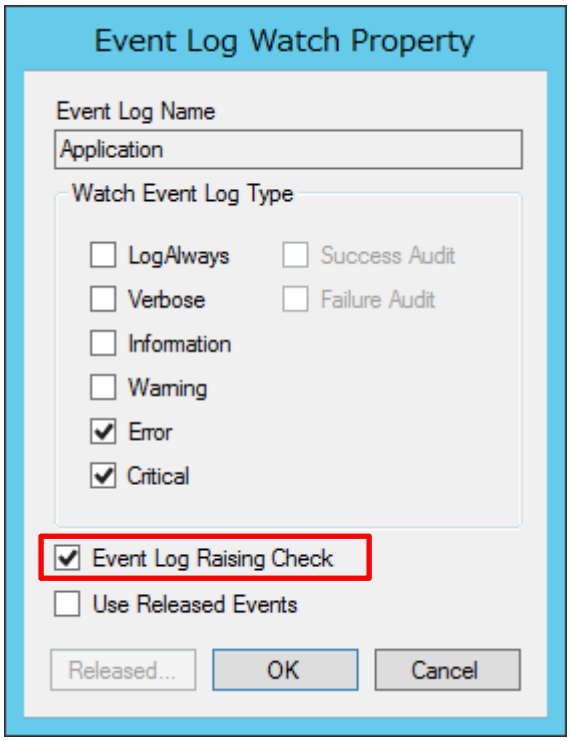


Event Log Raising Check は、この問題の影響を最小化することを目的にしています。

Event Log Raising Check が設定されると、UCS Watch Service は、5 分間隔でイベントログを発行します。発行したイベントログのコールバックが 2 分間以内に確認できない場合、UCS Watch Service は、利用者に通報したのち、異常終了します。その後、UCS Leading Service（※1）が UCS Watch Service を自動的に再起動するため、UCS Watch Service による Windows Event Log 監視が再開されます。イベントログ監視が再開できない場合、同様の動作が繰り返されます。UCS Leading Service による UCS Watch Service の再起動が既定回数（通常 3 回）を超えた場合、UCS Leading Service は、UCS Watch Service を再起動せず、UCS Watch Service の停止を利用者に通報します。

※1：App Bridge Monitor Windows Agent を構成する Windows サービスの 1 つです。詳細は、App Bridge Monitor Agent 監視サービス Windows Agent インストールガイドの「7. Windows Agent のサービス制御 / 7.1 Windows サービス構成」を参照して下さい。

Event Log Raising Check は、システムイベントログ監視、アプリケーションイベントログ監視の何れか、または両方で設定することができます。



Event Log Raising Check によって発行されるイベントログは、以下のとおりです。

4.1.3 同一イベントの送信抑止

同一イベントの連続発生による監視データ大量送信を防ぐため対応するため、同一イベントのデータ送信を抑止します。

（１）抑止条件

5 秒以内に同じイベントログ、同じソース、同じイベント ID のイベントが複数件発生した場合、2 件目以降のイベントを送信抑止します。

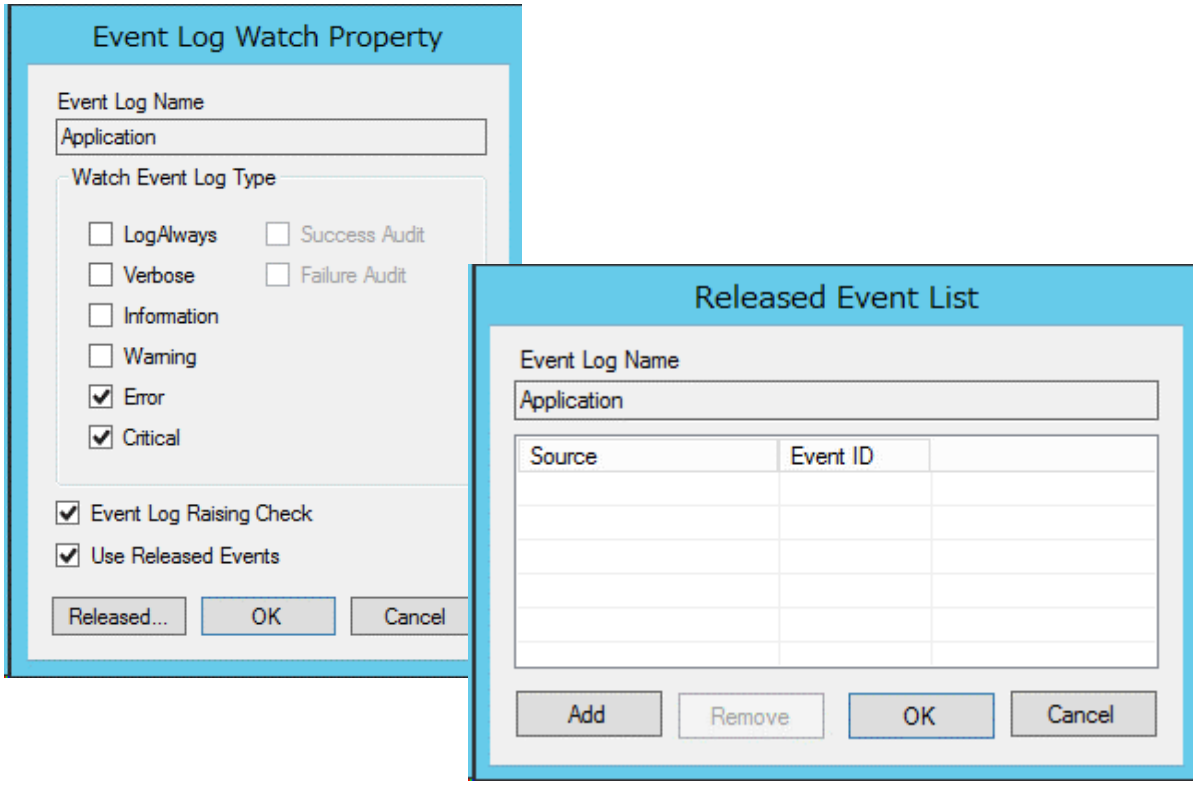
（２）抑止発生通知

通知メッセージの書き込み抑止が発生した場合、抑止発生の通知メッセージを発生させます。当該通知メッセージは、他の通知メッセージと同様に処理され、通知されます。
生成される通知メッセージの詳細は、マニュアル「App Bridge 通知メッセージガイド/イベントログ監視/0020-020-A」を参照下さい。

（３）抑止の除外

抑止対象外のイベントを登録することで、同一イベントの送信抑止を解除することができます。解除登録されたイベントは、発生した全件がセンタに送信されるため、大量に発生時にした場合、ネットワーク帯域の消費、監視処理遅延を招く可能性があります。これらを考慮し、設定して下さい。

抑止対象外のイベントを登録するには、Event Log Watch Property の画面で「Use Released Events」をチェックし、「Released」ボタンを押下後、表示される画面で除外対象のソース、イベント ID を登録して下さい。



4.1.4 通知メッセージの書き込み抑止

センタの負荷を軽減し、電子メールの大量送信を回避するため、以下の条件で通知メッセージの書き込みを抑止します。書き込み抑止された通知メッセージは、センタに記録されず、通知されません。

（１）書き込み抑止条件

同一サーバインスタンスの同一イベント（※1）をから生成された通知メッセージの書き込み件数を発生日時（分）内 10 メッセージに抑止します

※1：同じイベントログ（システム、アプリケーションなど）の同一ソース、同一イベント ID を同一イベントとします

（２）抑止発生通知

通知メッセージの書き込み抑止が発生した場合、抑止発生の通知メッセージを発生させます。当該通知メッセージは、他の通知メッセージと同様に処理され、通知されます。

生成される通知メッセージの詳細は、マニュアル「App Bridge 通知メッセージガイド/センタ発信の通知メッセージ」を参照下さい。

4.1.5 イベントログ監視中の例外対応

イベントログを出力しているアプリケーションのインストール/アンインストールや設定変更によって、イベントログ監視で例外が発生するケースが確認されています。例外発生時でもイベントログ監視を適切に継続するため、App Bridge Monitor Agent では以下の対応を実施します。

（１）監視対象除外と通知

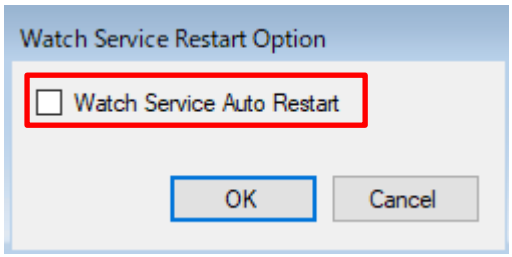
イベントログ監視で例外を検知した場合、当該イベントログを監視対象外とし、例外発生した旨を通知します。例外が発生していないイベントログの監視は継続されます。

（２）サービス再起動による回復

本事象発生時、App Bridge Monitor Agent/UCS Watch Service を再起動することで、対象外となったイベントログ監視が回復する場合があります。例外発生が通知された場合は、App Bridge Monitor Agent/UCS Watch Service の再起動をご検討下さい。サービス再起動は、Service Control のメニューから「Services」－「Watch Service」－「Stop/Start」で実施頂けます。

（３）再起動オプション

App Bridge Monitor Agent では、イベントログ監視例外発生時にサービス再起動を自動化するオプションを用意しています。当該オプションを利用するためには、Service Control のメニューから「Setting」－「Watch Service」－「Restart Option」を選択し、「Watch Service Auto Restart」にチェックします。設定した内容は App Bridge Monitor サービスが再起動されるまで反映されません。



なお、再起動オプションを設定する場合、以下の点に留意下さい。

- App Bridge Monitor Agent/UCS Watch Service が停止している間、監視がすべて停止します。
- 再起動後もイベントログ監視の例外が発生した場合、App Bridge Monitor Agent/UCS Watch Service の再起動が繰り返されます。再起動が既定回数（通常 3 回）を超えた場合、UCS Watch Service は再起動せず、UCS Watch Service の停止を利用者に通報します。

4.2 テキストログ監視の設定

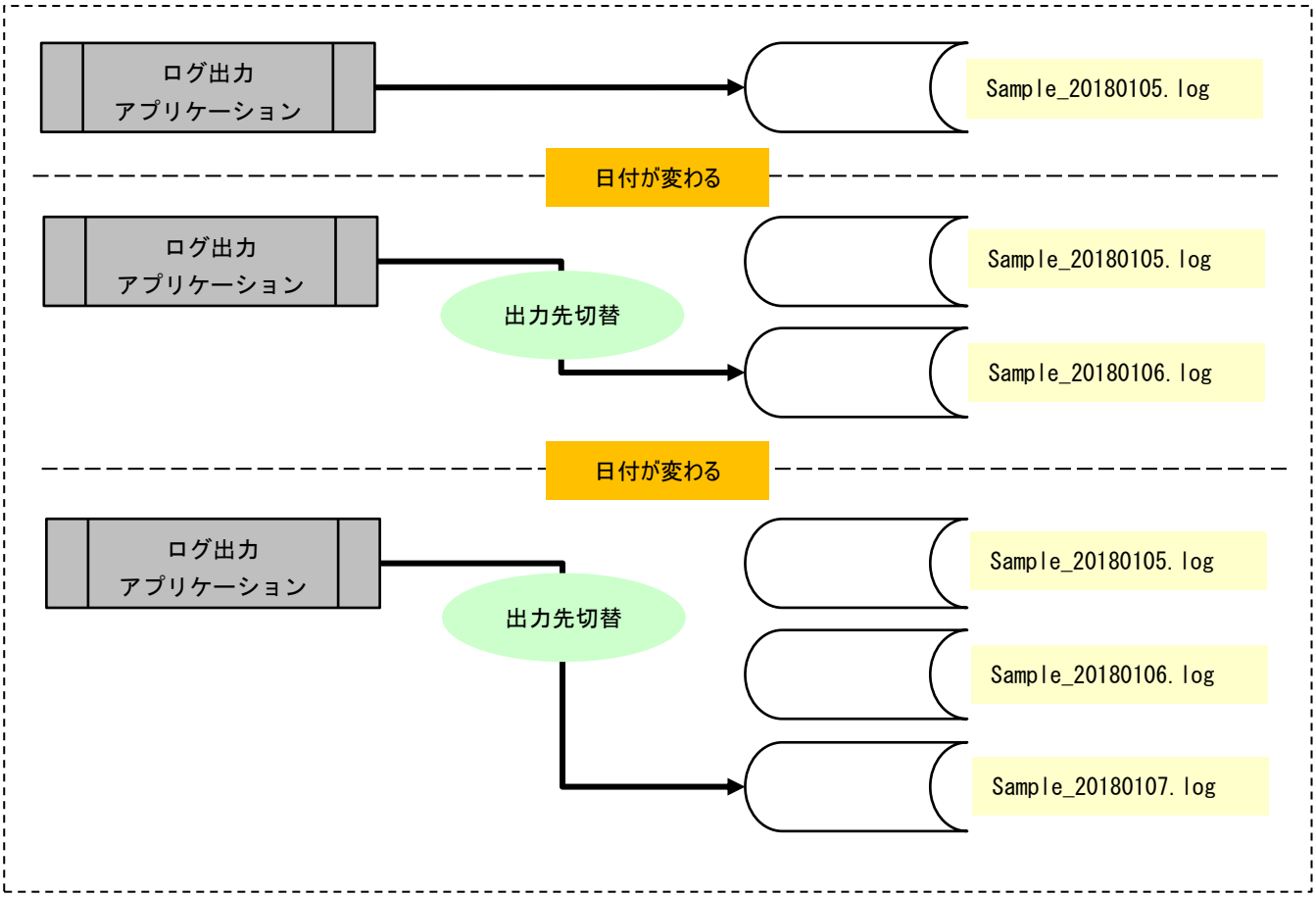
4.2.1 ログローテーション

テキストログ監視では、以下のログローテーションを行うテキストログファイルの監視が可能です。

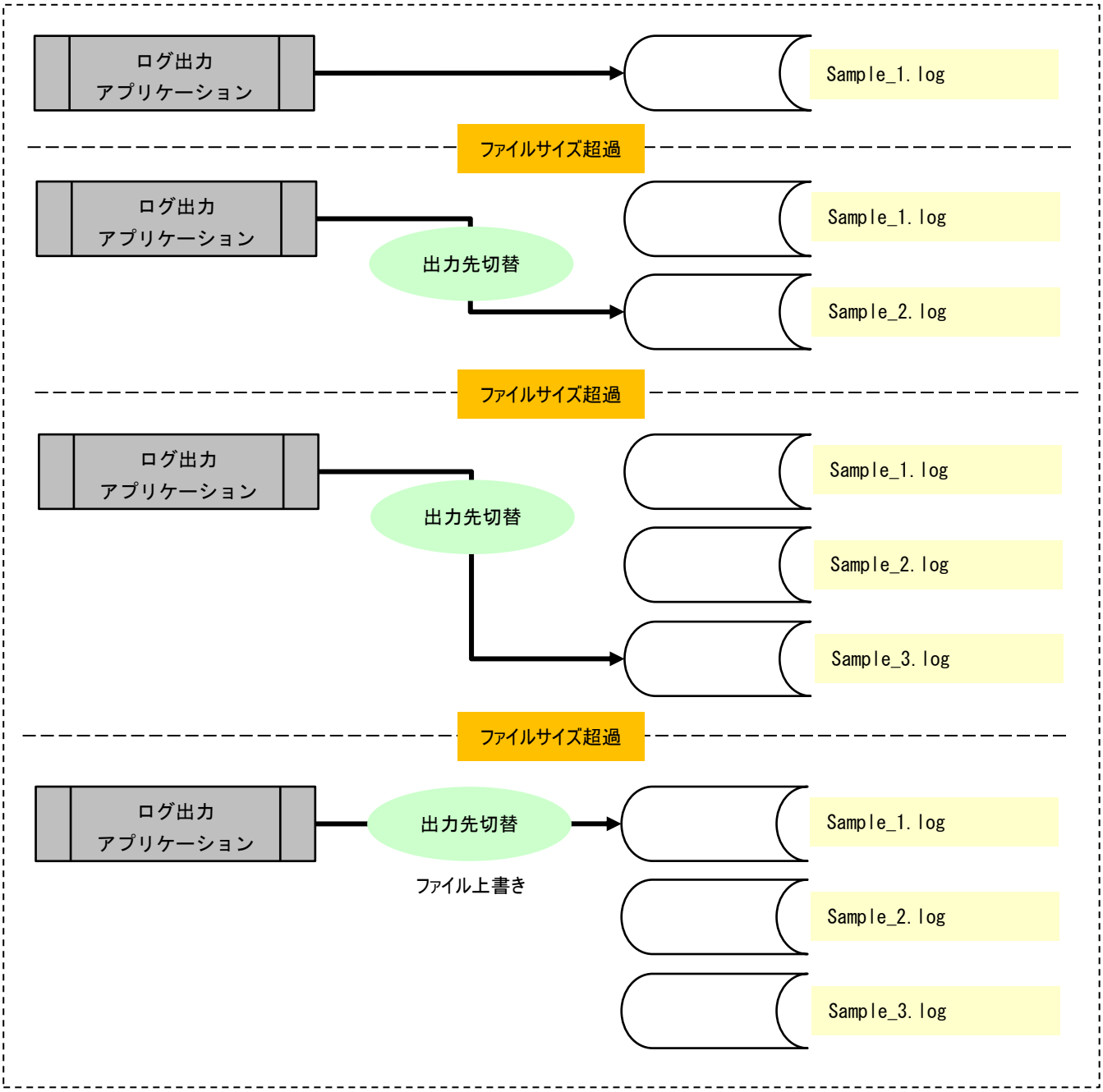
（１）LogRotation1

固定された複数のログファイル名でローテーションするパターンです。ログ出力アプリケーションは、日付が変わった、ログファイルのサイズが閾値を超えた、などを契機として、ログファイルの出力先を切り替えます。切り替えられた出力先にログファイルが既に存在している場合、既存のファイルは削除され、ログファイルが新たに作成されます。このパターンでは、多くの場合、ログファイル名に日付、世代番号などが付与されます。

（例１：日付でローテーションされる場合）



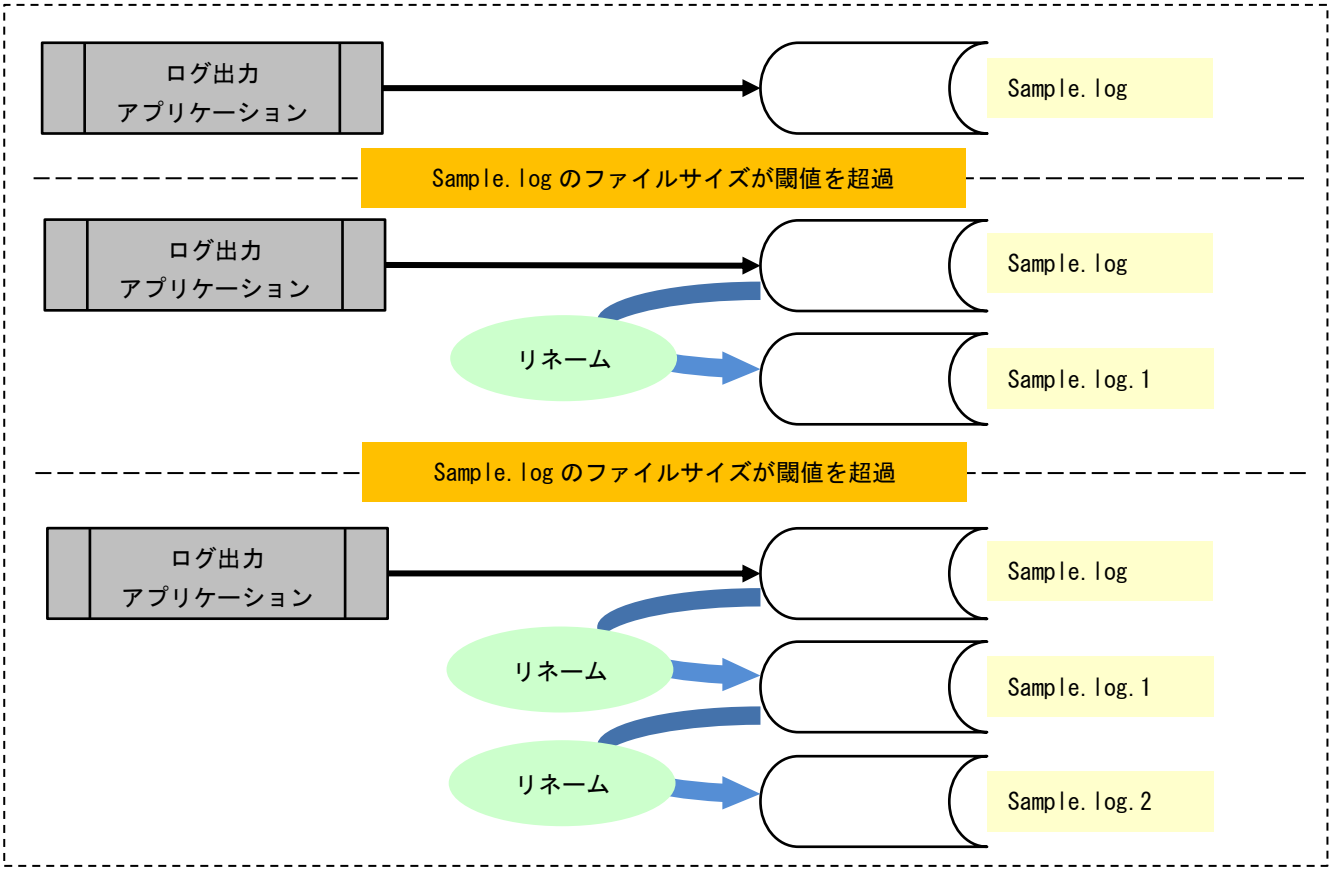
（例２：ファイルサイズ超過でローテーションされる場合）



（２）LogRotation3

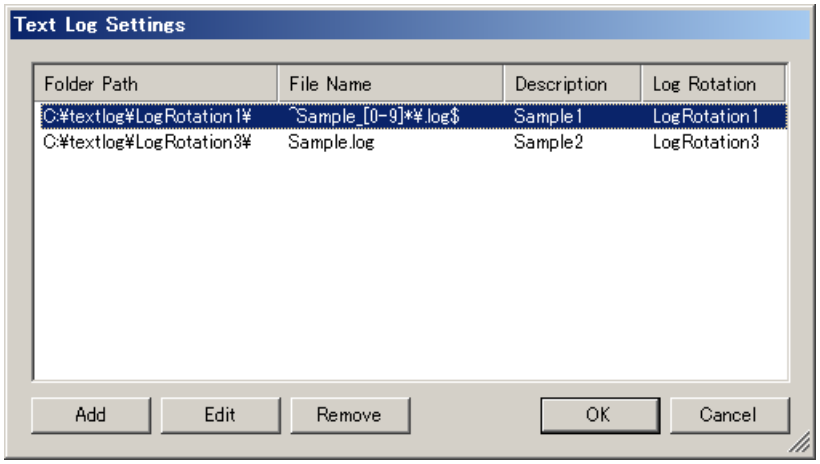
固定された単一のログファイル名を持ち、ローテーションによって当該ファイルを同一フォルダ内でリネームするパターンです。ログ出力アプリケーションは、常に同じ出力先にログを出力しますが、日付が変わった、ログファイルのサイズが閾値を超えた、などを契機として、ログファイルがリネームされます。このパターンでは、多くの場合、リネーム後のファイル名に日付、世代番号などが付与されます。

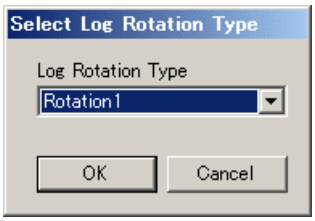
（例：ファイルサイズでローテーションされる場合）



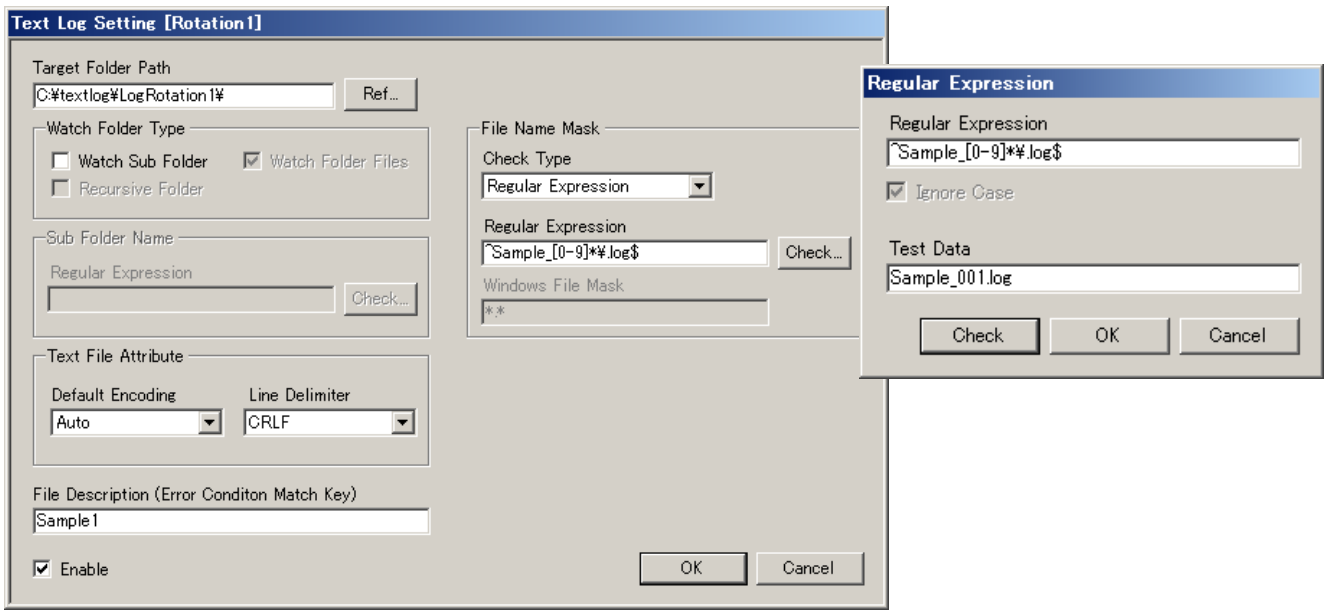
4.2.2 テキストログ監視の設定

監視対象のテキストログを設定します。
Service Control のメニューから「Setting」-「Watch Service」-「TextLog」を選択し、[Add]をクリックし、対象のローテーションタイプを選択した後、監視対象のテキストログを登録して下さい。



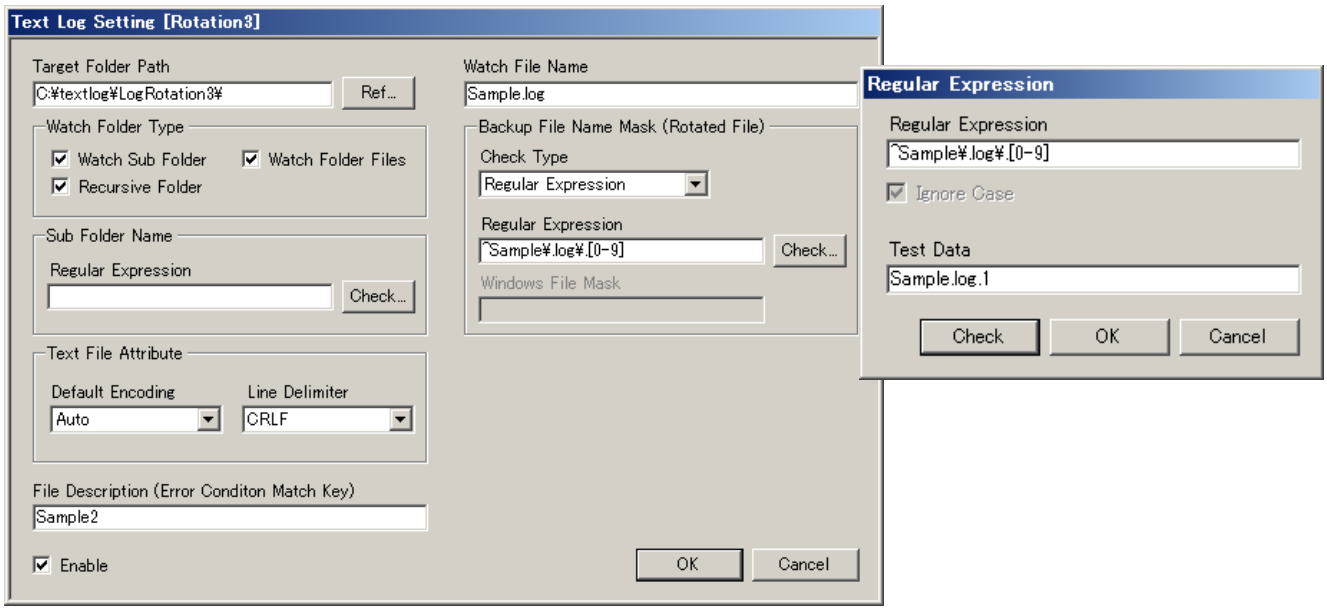


（１）テキストログ監視の設定（LogRotaion1）



設定項目	項目の説明	設定内容
Target Folder Path	監視対象となるフォルダのパス	監視対象フォルダのフルパス
Watch Folder Type/ Watch Sub Folder	監視対象フォルダのサブフォルダのファイルを監視対象とする	
Watch Folder Type/ Watch Folder Files	監視対象フォルダ直下のファイルを監視対象とする	
Watch Folder Type/ Recursive Folder	監視対象サブフォルダを再帰的に処理する	Watch Folder Type/Watch Sub Folder をチェックした場合に有効
Sub Folder Name/ Regular Expression	処理対象のサブフォルダ名を示す正規表現	Watch Folder Type/Watch Sub Folder をチェックした場合に有効
File Name Mask/ Check Type	監視対象ファイル名のマスク種類	以下から選択します ・Regular Expression（正規表現） ・Windows File Mask
File Name Mask/ Regular Expression	監視対象となるファイル名を示す正規表現	Check Type：Regular Expression を選択した場合に有効
File Name Mask/ Windows File Mask	監視対象ファイル名を示す Windows ファイルマスク	Check Type：Windows File Mask を選択した場合に有効
Text File Attribute/ Default Encoding	監視対象ファイルの文字コード テキストファイルに BOM（Byte Order Mark）が存在する場合 BOM に従った文字コードが使用される。テキストファイルに BOM が存在しない場合本設定内容が使用される	以下から選択します ・Auto（OS の標準文字コード） ・UTF8 ・Unicode_BE ・Unicode_LE ・ASCII ・Shift-JIS
Text File Attribute/ Line Delimiter	監視対象ファイルの改行コード	以下から選択します ・CRLF ・CR ・LF
File Description	監視対象ファイルの説明	任意の値を設定する。適用するエラー判定条件を判定する際に使用されます
Enable	テキストログ監視を有効とする場合チェックする	

（２）テキストログ監視の設定（LogRotaion3）



設定項目	項目の説明	設定内容
Target Folder Path	監視対象となるフォルダのパス	監視対象フォルダのフルパス
Watch Folder Type/ Watch Sub Folder	監視対象フォルダのサブフォルダのファイルを監視対象とする	
Watch Folder Type/ Watch Folder Files	監視対象フォルダ直下のファイルを監視対象とする	
Watch Folder Type/ Recursive Folder	監視対象サブフォルダを再帰的に処理する	Watch Folder Type/Watch Sub Folder をチェックした場合に有効
Sub Folder Name/ Regular Expression	処理対象のサブフォルダ名を示す正規表現	Watch Folder Type/Watch Sub Folder をチェックした場合に有効
Watch File Name	監視対象となるファイル名	
Backup File Name Mask (Rotated File)/ Check Type	バックアップファイル（※1）名のマスク種類	以下から選択します ・Regular Expression（正規表現） ・Windows File Mask
Backup File Name Mask (Rotated File)/ Regular Expression	バックアップファイル（※1）名を示す正規表現	Check Type：Regular Expression を選択した場合に有効
Backup File Name Mask (Rotated File)/ Windows File Mask	バックアップファイル（※1）名を示す Windows ファイルマスク	Check Type：Windows File Mask を選択した場合に有効
Text File Attribute/ Default Encoding	監視対象ファイルの文字コード テキストファイルに BOM（Byte Order Mark）が存在する場合 BOM に従った文字コードが使用される	以下から選択します ・Auto（OS の標準文字コード） ・UTF8 ・Unicode_BE ・Unicode_LE ・ASCII ・Shift-JIS
Text File Attribute/ Line Delimiter	監視対象ファイルの改行コード	以下から選択します ・CRLF ・CR ・LF
File Description	監視対象ファイルの説明	任意の値を設定する。適用するエラー判定条件を判定する際に使用されます
Enable	テキストログ監視を有効とする場合チェックする	

※1：ローテーションによりリネームされた監視対象ファイルを指します

（３）補足説明

テキストログ監視では、監視対象フォルダ（Target Folder Path）及びそのサブフォルダに存在し、監視対象ファイル名のマスク（File Name で指定された Windows マスク、または正規表現（※1））に該当するテキストファイルを監視対象とします。

テキストログ監視は 1 分ごとに実施され、処理対象となったテキストログファイルの前回差分レコードを、監視設定で設定したエラー判定条件（※2）に従ってチェックします。エラー判定条件に該当し、除外判定条件に該当しないとき、エラーと判断されます。初期状態のエラー判定条件ではテキストログに“ERROR”の文言（大文字、小文字は無視）が含まれる場合、エラーとしています。

エラー判定条件、除外判定条件は、2 分ごとに更新が確認されます。監視設定で設定した内容を即時反映したい場合、App Bridge Monitor サービスの再起動が必要です。

大量のテキストファイルが監視対象となった場合、多くの CPU、メモリを消費する場合があります。全体の監視対象ファイル数を 500 ファイル未満に抑えることを推奨します。

※1：正規表現については、「App Bridge 正規表現ガイド」を参照して下さい
※2：エラー判定条件、除外判定条件の設定については、「App Bridge Monitor Agent 監視サービスエラー判定条件ガイド」を参照して下さい

4.2.3 通知メッセージの書き込み抑止

センタの負荷を軽減し、電子メールの大量送信を回避するため、以下の条件で通知メッセージの書き込みを抑止します。書き込み抑止された通知メッセージは、センタに記録されず、通知されません。

（１）書き込み抑止条件

同一サーバインスタンスの同一テキストファイルをから生成された通知メッセージの書き込み件数を発生日時（分）内 10 メッセージに抑止します

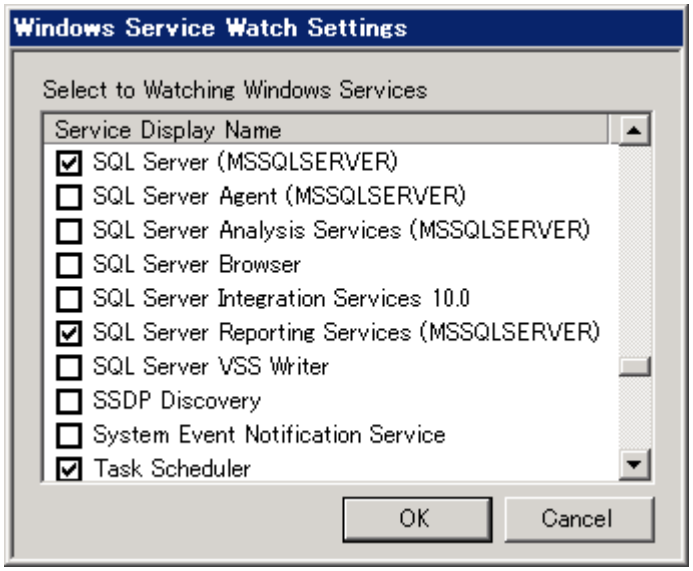
（２）抑止発生通知

通知メッセージの書き込み抑止が発生した場合、抑止発生の通知メッセージを発生させます。当該通知メッセージは、他の通知メッセージと同様に処理され、通知されます。

生成される通知メッセージの詳細は、マニュアル「App Bridge 通知メッセージガイド/センタ発信の通知メッセージ」を参照下さい。

4.3 Windows サービス監視の設定

監視対象の Windows サービスを設定します。
Service Control のメニューから「Setting」－「Watch Service」－「Service」を選択し、表示された画面で監視対象のサービスをチェックします。設定した内容はすぐに適用されます。

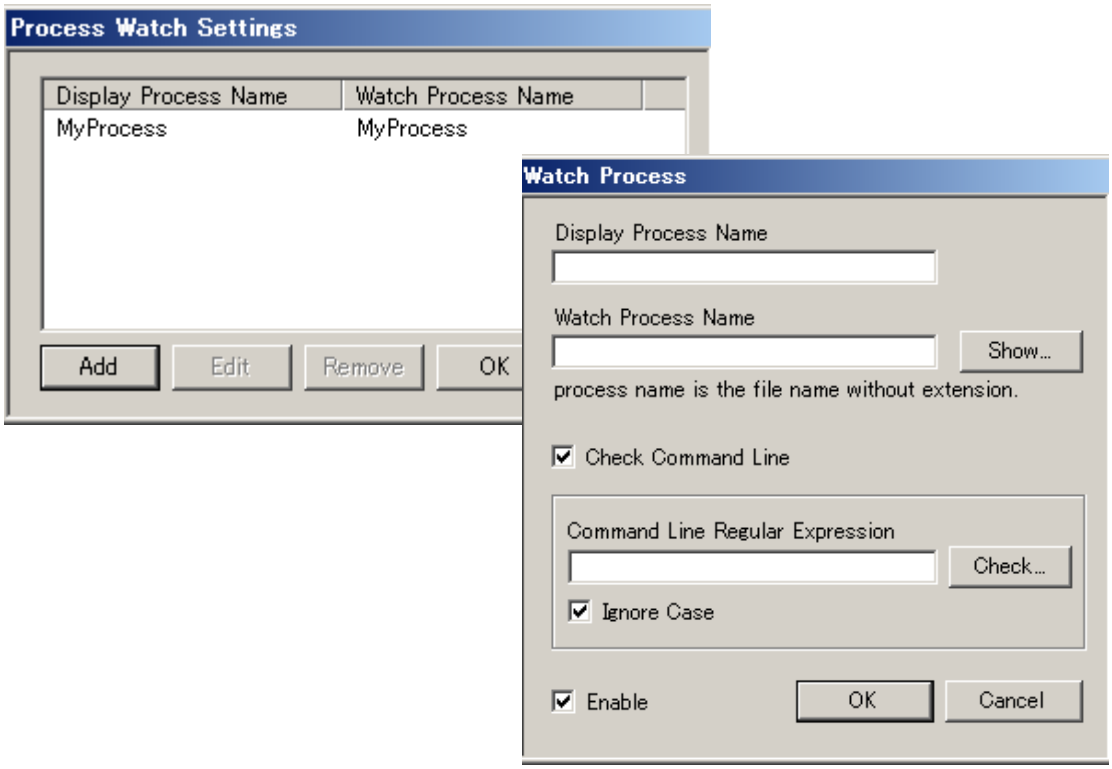


サービスの状態は 1 分間隔で確認され、以下のとおり判定されます。

判定結果	サービスの状態
Good	Running
Warning	StartPending
Warning	ContinuePending
Error	上記以外

4.4 プロセス監視の設定

監視対象のプロセスを設定します。
Service Control のメニューから「Setting」－「Watch Service」－「Process」を選択し、表示された画面に監視対象のプロセス名を登録します。設定した内容はすぐに適用されます。



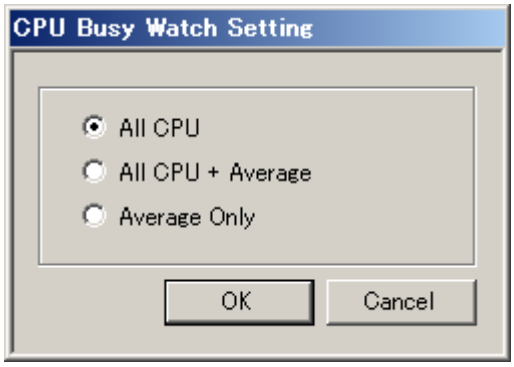
項目	内容	備考
Display Process Name	プロセスエラー判定条件と比較する表示名	サロゲートペア文字、制御文字以外の 1～50 文字
Watch Process Name	監視対象のプロセス名。拡張子部分は省かれる	サロゲートペア文字、制御文字以外の 1 から 256 文字で system は入力不可
Command Line Regular Expression	コマンドラインを比較する正規表現。比較元の様式は、ファイルパス 引数	引数の評価が可能となる
Ignore Case	正規表現で英字大文字と小文字を区別しない場合チェック	
Enable	有効とする場合チェック	

プロセスの状態は 1 分間隔で確認されます。監視設定で設定したエラー判定条件（※1）に従って処理されます。初期状態のエラー判定条件はプロセス数がゼロのものをエラーとしています。

※1：エラー判定条件、除外判定条件の設定については、「App Bridge Monitor Agent 監視サービスエラー判定条件ガイド」を参照して下さい

4.5 CPU ビジー監視の設定

CPU ビジー監視を設定します。
Service Control のメニューから「Setting」-「Watch Service」-「CPU Busy」を選択し、表示された画面で監視対象を設定します。設定内容はすぐに適用されます。



設定項目	内容	備考
All CPU	監視対象ノードの各プロセッサについて、CPU ビジーの状態を表示させます	
All CPU + Average	各プロセッサ及び CPU ビジーの Average の値を表示させます	
Average Only	CPU ビジーの Average の値のみを表示させます	

CPU ビジー監視は、監視設定で設定したエラー判定条件（※1）に従って処理されます。初期状態のエラー判定条件は、ビジー率 90%以上の状態が 15 分間以上、継続したものをエラーとしています。

※1：エラー判定条件、除外判定条件の設定については、「App Bridge Monitor Agent 監視サービスエラー判定条件ガイド」を参照して下さい

4.6 ディスクビジー監視の設定

ディスクビジー監視を設定します。
Service Control のメニューから「Setting」-「Watch Service」-「Disk Busy」を選択し、表示された画面で監視対象を設定します。設定内容はすぐに適用されます。

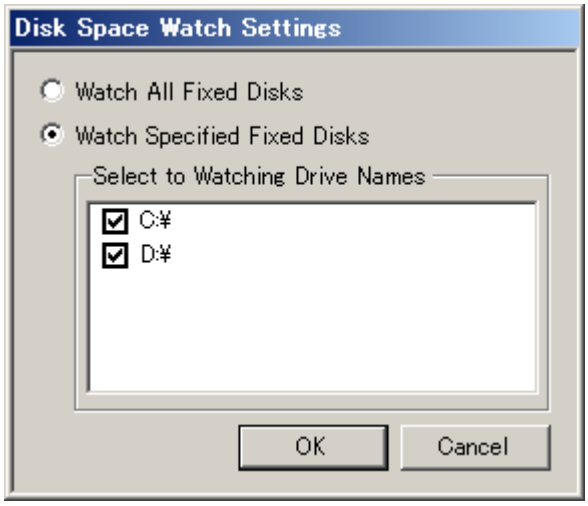
設定項目	項目の説明	備考
Watch All Physical Disks	全ての物理ドライブをディスクビジー監視対象とする	
Watch Specified Physical Disks	Select to Watching Physical Disk Names で指定された物理ディスクをディスクビジー監視対象とする	

ディスクビジー監視は、監視設定で設定したエラー判定条件（※1）に従って処理されます。初期状態のエラー判定条件は、ビジー率 90%以上の状態が 15 分間以上、継続したものをエラーとしています。

※1：エラー判定条件、除外判定条件の設定については、「App Bridge Monitor Agent 監視サービスエラー判定条件ガイド」を参照して下さい

4.7 ディスク容量監視の設定

ディスク容量の監視を設定します。
Service Control のメニューから「Setting」-「Watch Service」-「Disk Space」を選択し、表示された画面で監視対象を設定します。設定内容はすぐに適用されます。



設定項目	項目の説明	備考
Watch All Fixed Disks	全ての固定ディスクをディスク容量監視対象とする	
Watch Specified Fixed Disks	Select to Watching Drive Names で指定されたディスクをディスク容量監視対象とする	

ディスク容量監視は、監視設定で設定したエラー判定条件（※1）に従って処理されます。初期状態のエラー判定条件は、空き容量が 10%以下の状態のものをエラーとしています。

※1：エラー判定条件、除外判定条件の設定については、「App Bridge Monitor Agent 監視サービスエラー判定条件ガイド」を参照して下さい

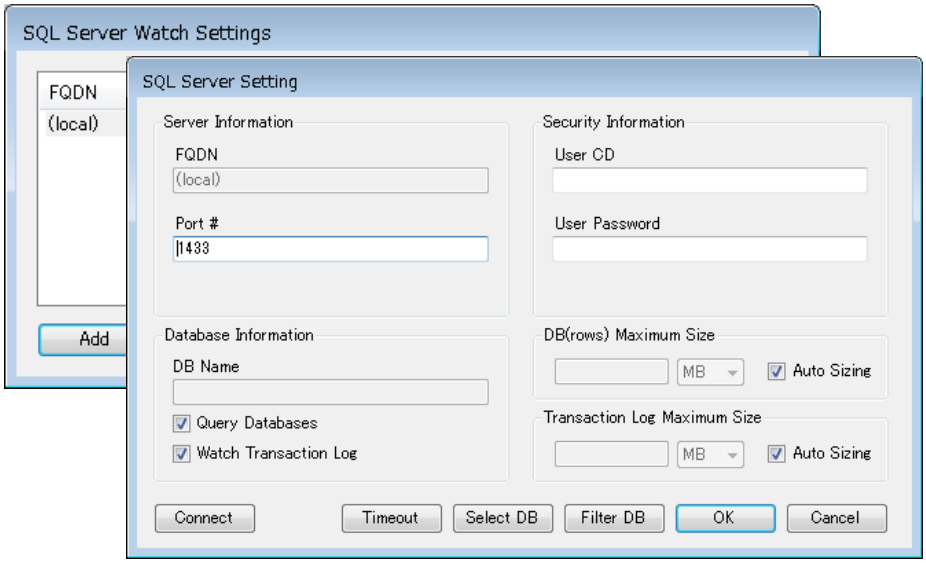
4.8 SQL Server 監視/Local Databases の設定

4.8.1 対象 SQL Server とデータベース

対象とする SQL Server は、SQL Server 2008 以降であり、監視するデータベースは、Agent がインストールされたサーバの SQL Server が管理するユーザデータベースに限られます。

4.8.2 データベース容量監視の設定

データベース容量監視対象のデータベースを設定します。
Service Control のメニューから「Setting」-「Watch Service」-「SQL Server」-「Local Databases」を選択し、監視対象のデータベースを登録して下さい。

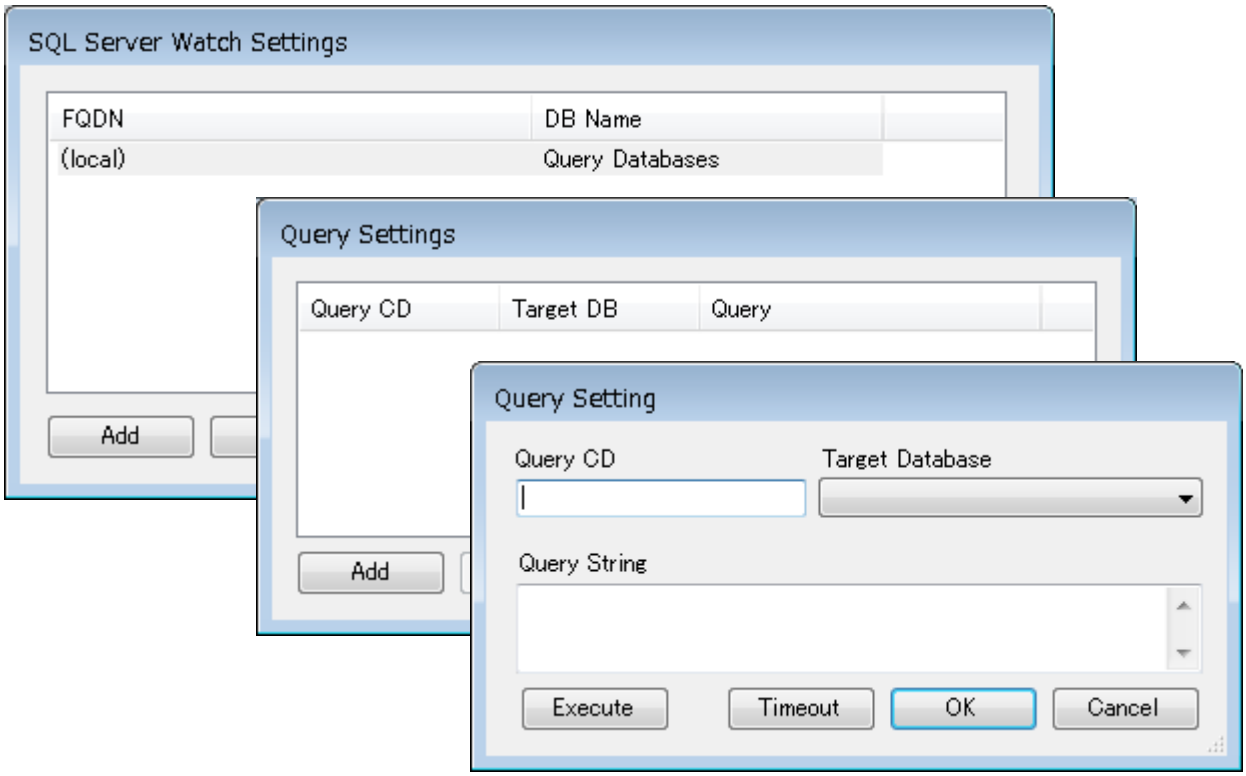


設定項目	項目の説明	設定内容
Server Information/ Port #	アクセスポート番号	SQL Server にアクセスする際のポート番号(通常 1433) を指定します
Database Information/ DB Name	監視対象のデータベース名	Database Information/Query Databases をチェックしている場合、入力できません
Database Information/ Query Databases	複数データベースの監視	SQL Server のユーザデータベースを検索して監視対象を決定する場合にチェックします。[Select DB]ボタンで対象データベースの抽出、[Filter DB]ボタンで対象データベースの除外を指定できます
Database Information/ Watch Transaction Log	トランザクションログの監視	トランザクションログの容量監視を実施する場合チェックします
Security Information/ User CD	アクセスユーザ CD	データベースにアクセスするための SQL ユーザを指定します
Security Information/ User Password	アクセスユーザパスワード	データベースにアクセスするためのパスワードを指定します
DB(rows) Maximum Size	データベース最大サイズ	空き容量を算出する場合に使用する最大容量を指定します。Auto Sizing がチェックされている場合、現在の容量を最大サイズとします
Transaction Log Maximum Size	トランザクションログ最大サイズ	空き容量を算出する場合に使用する最大容量を指定します。Auto Sizing がチェックされている場合、現在の容量を最大サイズとします

4.8.3 データベース応答監視の設定

データベース容量監視を設定したデータベースに任意のクエリーを発行し、応答時間を監視します。

Service Control のメニューから「Setting」-「Watch Service」-「SQL Server」-「Local Databases」を選択します。対象のデータベースを選択して[Query]ボタンをクリックし、クエリーを登録して下さい。



設定項目	項目の説明	設定内容
Query CD	Query を識別するコード	任意の名称を指定します
Target Database	Query を実行するデータベース	データベース容量設定で「Database Information/Query Databases」にチェックを付けた場合、表示されます。クエリーを実行するデータベースを選択して下さい
Query String	応答時間を監視する Query	Select などの SQL を入力します。複数の SQL を実行する場合;(セミコロン)で区切ります。複数の SQL が指定された場合、個々の SQL を実行した合計時間を応答時間として取り扱います

登録された Query は 5 分ごとに実行され、応答時間を記録します。応答時間は監視照会で確認できます。但し、データベース容量監視で通信エラーが発生した場合、データベース応答監視は実行されません。

4.8.4 アクセスユーザの必要権限

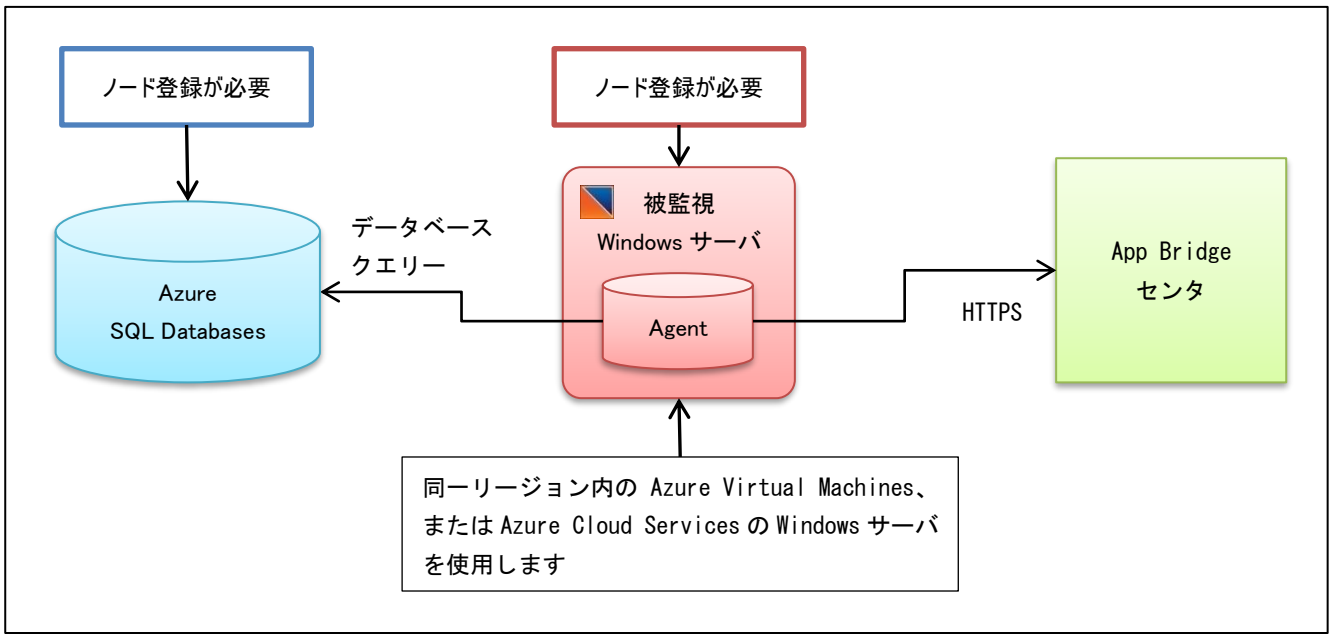
アクセスユーザとして設定するSQLユーザには、masterデータベースに関する参照権限（ロールに制約はありません）と監視対象のユーザデータベースに対するdb_owner権限、および、サーバロールとしてVIEW SERVER STATE権限が必要です。

masterデータベースに対する参照権限は、ユーザデータベースの取得及び存在確認に使用するために必要となります。また、ユーザデータベースに対するdb_owner権限はデータベースの使用量を算出するために必要となります。データベース容量監視はsys.dm_db_partition_statsより使用ページ数からデータベース使用量を算出するため、sys.dm_db_partition_statsを参照するためのdb_owner権限が必要となります。VIEW_SERVER_STATE権限はサーバのパフォーマンスやリソースの使用状況などの情報を参照するために必要となります。

4.9 SQL Server 監視/Azure Databases の設定

4.9.1 Databases Host ノードの登録

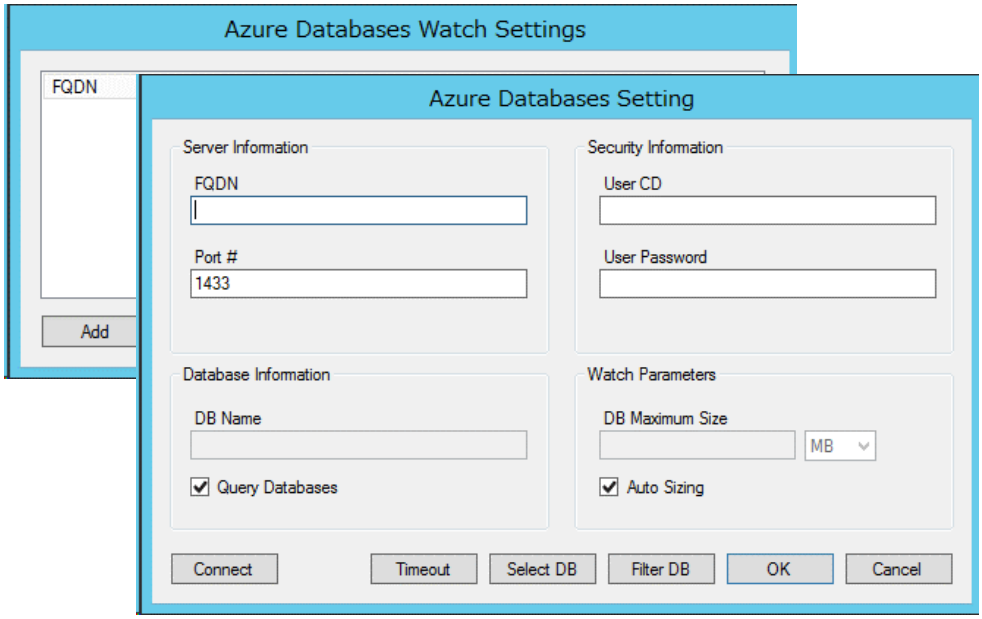
SQL Server 監視/Azure Databases 監視を実施するためには、クエリーを発行するためのノード（Windows サーバ）に加え、Databases Host として登録したノードが必要です。



次項以降の設定は、Windows Agent をインストールした被監視サーバ上で実施します。

4.9.2 データベース容量監視の設定

データベース容量監視対象のデータベースを設定します。
Service Control のメニューから「Setting」-「Watch Service」-「Azure SQL Databases」を選択し、監視対象のデータベースを登録して下さい。
データベースを登録する際、Smart Download の画面が表示されます。ガイダンスに従って内容を入力して下さい。Smart Download では Databases Host として登録したノード CD を設定します。



設定項目	項目の説明	設定内容
Server Information/ FQDN	監視対象 DB の FQDN	監視対象 FQDN を指定します
Server Information/ Port #	監視対象 DB のポート番号	監視対象のポート番号（通常 1433）を指定します
Database Information/ DB Name	監視対象 DB のデータベース名	Database Information/Query Databases をチェックしている場合、入力できません
Database Information/ Query Databases	複数データベースの監視	SQL Server のユーザデータベースを検索して監視対象を決定する場合にチェックします。[Select DB]ボタンで対象データベースの抽出、[Filter DB]ボタンで対象データベースの除外を指定できます
Security Information/ User CD	アクセスユーザ CD	データベースにアクセスするための SQL ユーザを指定します
Security Information/ User Password	アクセスユーザパスワード	データベースにアクセスするためのパスワードを指定します
Watch Parameters/ DB Maximum Size	監視対象 DB の容量監視で使用する最大容量	Watch Parameters/Auto Sizing をチェックしている場合、入力できません
Watch Parameters/ Auto Sizing	最大容量の自動取得	最大容量を契約容量とする場合チェックします。監視中に契約容量が変更されると最大容量も自動変更されます

SQL Server 監視/Azure Databases 容量監視では、現在使用量と最大容量（「Watch Parameters/DB Maximum Size」で指定した値、または、「Watch Parameters/Auto Sizing」によって取得した値）より使用率を算出し、エラー判定を行います。

Attention! ご注意ください！

Azure ポータルのデータベース使用量と App Bridge Monitor のデータベース使用量は異なります

Azure ポータルで表示されるデータベース使用量と App Bridge Monitor で表示されるデータベース使用量は、以下のとおり異なります。ご注意下さい。

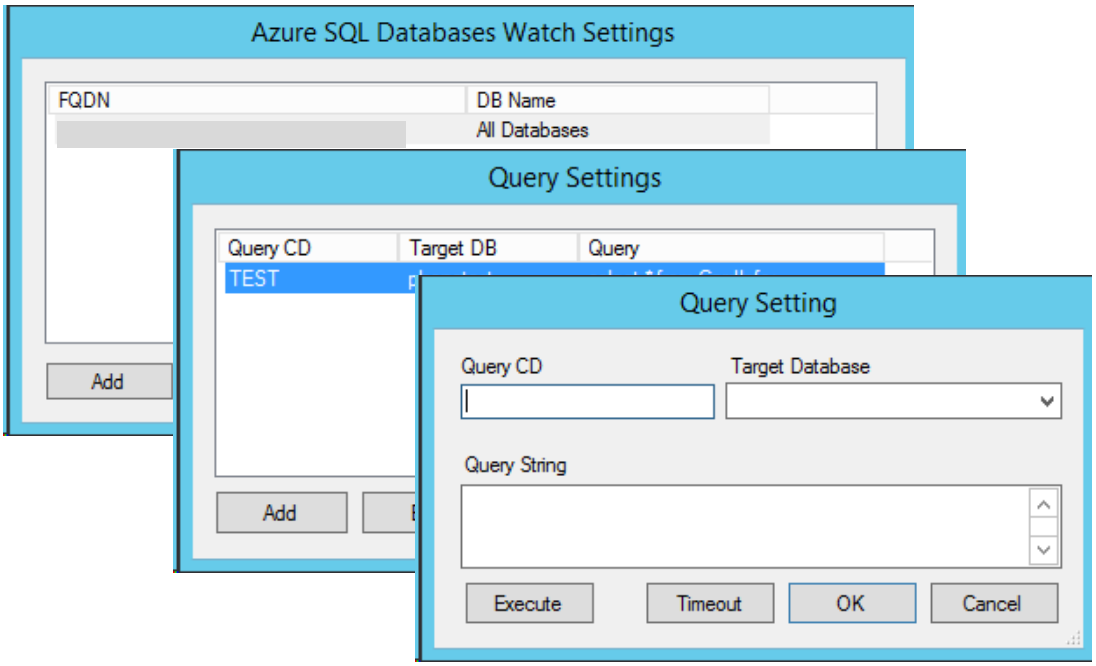
項目	Azure ポータル	App Bridge Monitor
表示内容	SQL Server によって確保されている容量	SQL Server によって確保されている容量の内、実際にデータが保存されている容量
算出式	sys.dm_db_partition_stats の reserved_page_count カラム合計値×8×1024	sys.dm_db_partition_stats の used_page_count カラム合計値×8×1024

※ sys.dm_db_partition_stats の詳細は以下の URL をご参照下さい。
<<https://msdn.microsoft.com/ja-jp/library/ms187737(v=sql.120).aspx>>

4.9.3 データベース応答監視の設定

データベース容量監視を設定したデータベースに任意のクエリーを発行し、応答時間を監視します。

Service Control のメニューから「Setting」-「Watch Service」-「SQL Azure SQL Databases」を選択します。対象のデータベースを選択して[Query]ボタンをクリックし、クエリーを登録して下さい。

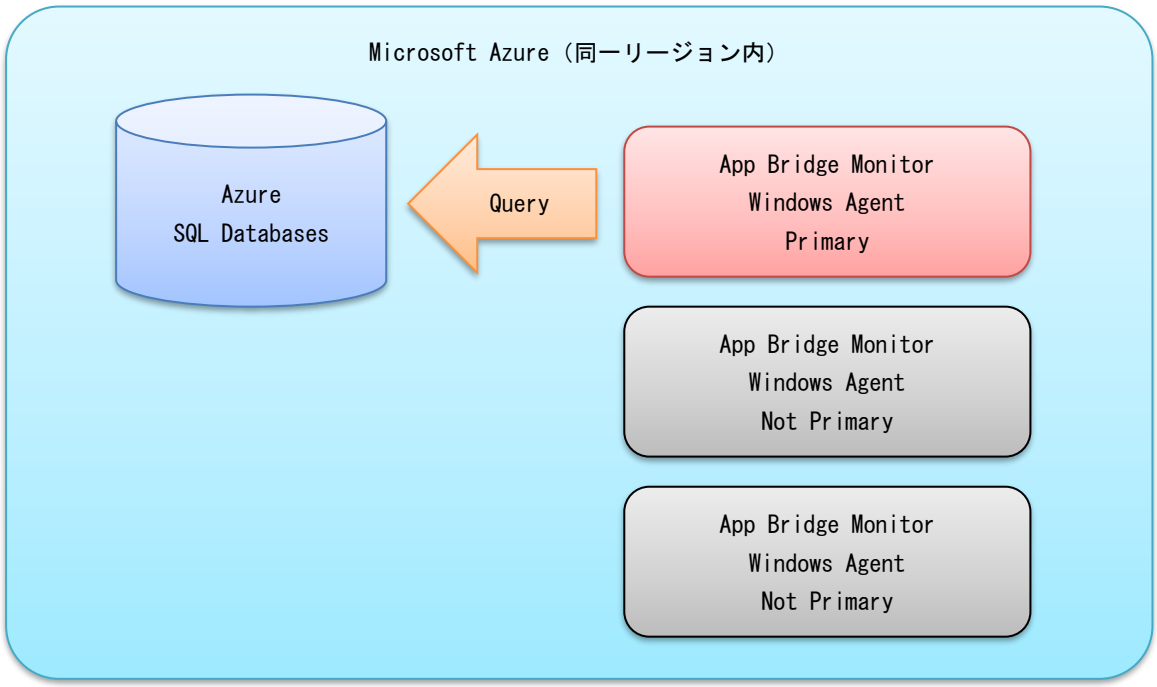


設定項目	項目の説明	設定内容
Query CD	Query を識別するコード	任意の名称を指定します
Target Database	Query を実行するデータベース	データベース監視容量設定で「Database Information/Query Databases」にチェックを付けた場合、表示されます。クエリーを実行するデータベースを選択して下さい
Query String	応答時間を監視する Query	Select などの SQL を入力します。複数の SQL を実行する場合；(セミコロン) で区切ります。複数の SQL が指定された場合、個々の SQL を実行した合計時間を応答時間として取り扱います

登録された Query は 5 分ごとに実行され、応答時間を記録します。応答時間は監視照会で確認できます。但し、データベース容量監視で通信エラーが発生した場合、データベース応答監視は実行されません。

4.9.4 スケーリング制御している Agent からの監視

スケーリング制御している Agent から Azure Databases を監視する場合、Windows Agent は、同一ノード内でプライマリとなるサーバインスタンスを決定し、当該プライマリインスタンスがデータベースを監視します。



4.9.5 アクセスユーザの必要権限

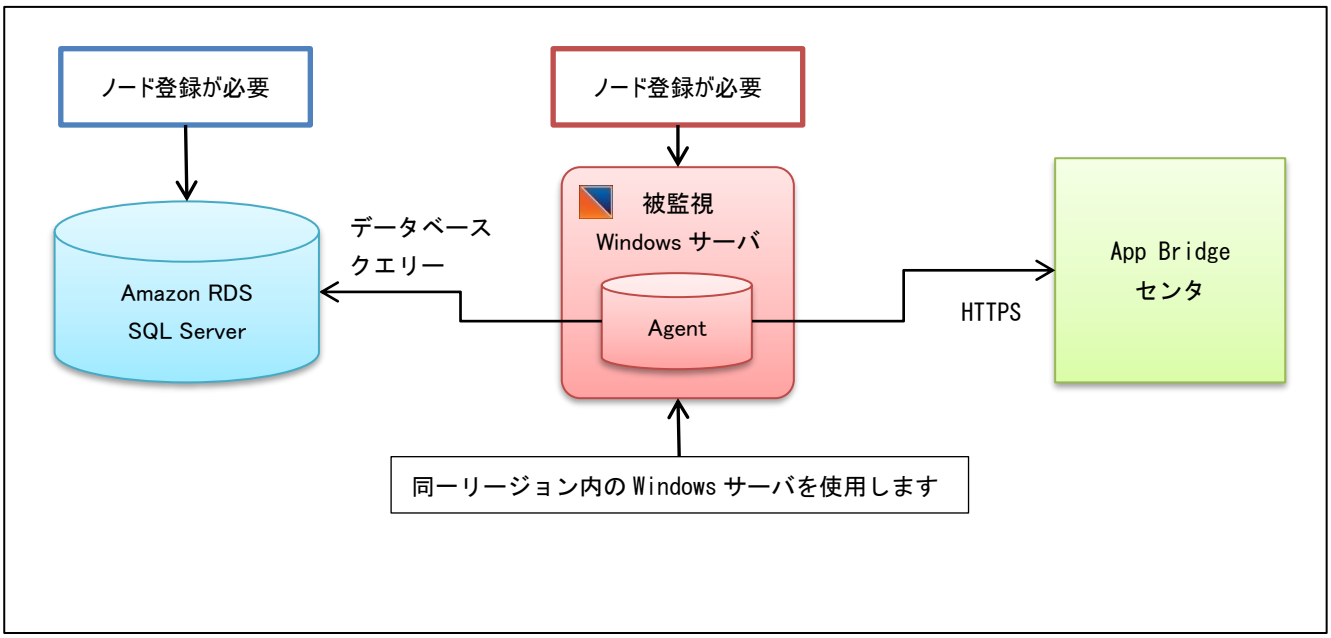
アクセスユーザとして設定する SQL ユーザには、master データベースに関する参照権限（ロールに制約はありません）と監視対象のユーザデータベースに対する db_owner 権限、および、サーバロールとして VIEW SERVER STATE 権限が必要です。

master データベースに対する参照権限は、ユーザデータベースの取得及び存在確認に使用するために必要となります。また、ユーザデータベースに対する db_owner 権限はデータベースの使用量を算出するために必要となります。データベース容量監視は sys.dm_db_partition_stats より使用ページ数からデータベース使用量を算出するため、sys.dm_db_partition_stats を参照するための db_owner 権限が必要となります。VIEW_SERVER_STATE 権限はサーバのパフォーマンスやリソースの使用状況などの情報を参照するために必要となります。

4.10 SQL Server 監視/Amazon RDS Databases の設定

4.10.1 Databases Host ノードの登録

SQL Server 監視/Amazon RDS Databases 監視を実施するためには、クエリーを発行するためのノード（Windows サーバ）に加え、Databases Host として登録したノードが必要です。



次項以降の設定は、Windows Agent をインストールした被監視サーバ上で実施します。

4.10.2 データベース容量監視の設定

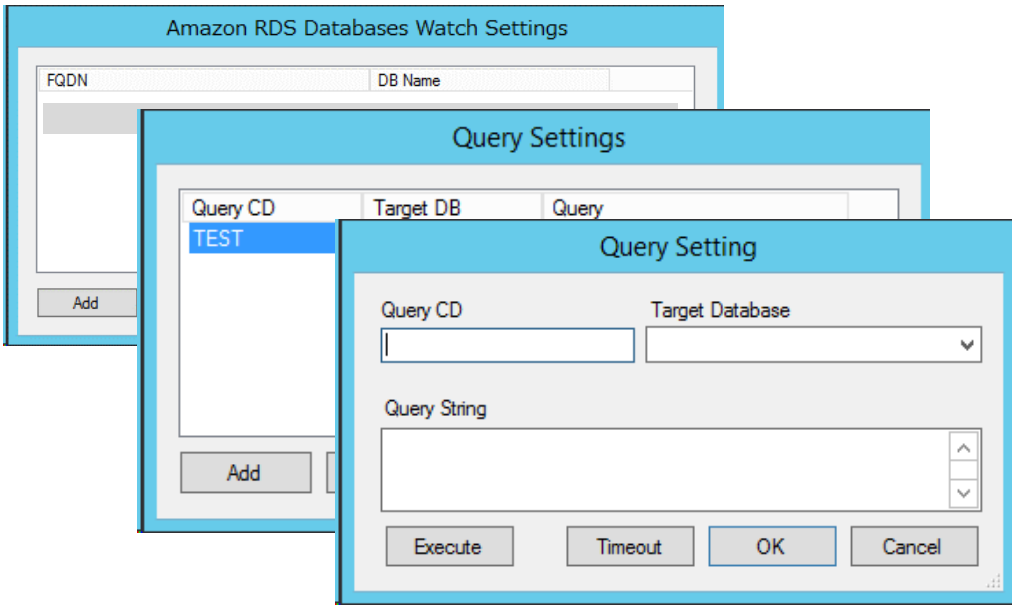
データベース容量監視対象のデータベースを設定します。
Service Control のメニューから「Setting」-「Watch Service」-「SQL Server」-「Amazon RDS Databases」を選択し、監視対象のデータベースを登録して下さい。
データベースを登録する際、Smart Download の画面が表示されます。ガイダンスに従って内容を入力して下さい。Smart Download では Databases Host として登録したノード CD を設定します。

設定項目	項目の説明	設定内容
Server Information/ FQDN	監視対象 DB の FQDN	監視対象 SQL Databases サーバの FQDN を指定します
Server Information/ Port #	監視対象 DB のポート番号	監視対象 SQL Databases サーバのポート番号（通常 1433）を指定します
Database Information/ DB Name	監視対象 DB のデータベース名	Database Information/Query Databases をチェックしている場合、入力できません
Database Information/ Query Databases	複数データベースの監視	SQL Databases サーバのユーザデータベースを検索して監視対象を決定する場合にチェックします。[Select DB]ボタンで対象データベースの抽出、[Filter DB]ボタンで対象データベースの除外を指定できます
Security Information/ User CD	アクセスユーザ CD	データベースにアクセスするための SQL ユーザを指定します
Security Information/ User Password	アクセスユーザパスワード	データベースにアクセスするためのパスワードを指定します
Watch Parameters/ DB Maximum Size	監視対象 DB の容量監視で使用する最大容量	Watch Parameters/Auto Sizing をチェックしている場合、入力できません
Watch Parameters/ Auto Sizing	最大容量の自動取得	Auto Sizing がチェックされている場合、現在の容量を最大サイズとします

4.10.3 データベース応答監視の設定

データベース容量監視を設定したデータベースに任意のクエリーを発行し、応答時間を監視します。

Service Control のメニューから「Setting」-「Watch Service」-「SQL Server」-「Amazon RDS Databases」を選択します。対象のデータベースを選択して[Query]ボタンをクリックし、クエリーを登録して下さい。



設定項目	項目の説明	設定内容
Query CD	Query を識別するコード	任意の名称を指定します
Target Database	Query を実行するデータベース	データベース容量監視容量設定で「Database Information/Query Databases」にチェックを付けた場合、表示されます。クエリーを実行するデータベースを選択して下さい
Query String	応答時間を監視する Query	Select などの SQL を入力します。複数の SQL を実行する場合；（セミコロン）で区切ります。複数の SQL が指定された場合、個々の SQL を実行した合計時間を応答時間として取り扱います

登録された Query は 5 分ごとに実行され、応答時間を記録します。応答時間は監視照会で確認できます。但し、データベース容量監視で通信エラーが発生した場合、データベース応答監視は実行されません。

4.10.4 アクセスユーザの必要権限

アクセスユーザとして設定するSQLユーザには、masterデータベースに関する参照権限（ロールに制約はありません）と監視対象のユーザデータベースに対するdb_owner権限、および、サーバロールとしてVIEW SERVER STATE権限が必要です。

masterデータベースに対する参照権限は、ユーザデータベースの取得及び存在確認に使用するために必要となります。また、ユーザデータベースに対するdb_owner権限はデータベースの使用量を算出するために必要となります。データベース容量監視はsys.dm_db_partition_statsより使用ページ数からデータベース使用量を算出するため、sys.dm_db_partition_statsを参照するためのdb_owner権限が必要となります。VIEW_SERVER_STATE権限はサーバのパフォーマンスやリソースの使用状況などの情報を参照するために必要となります。

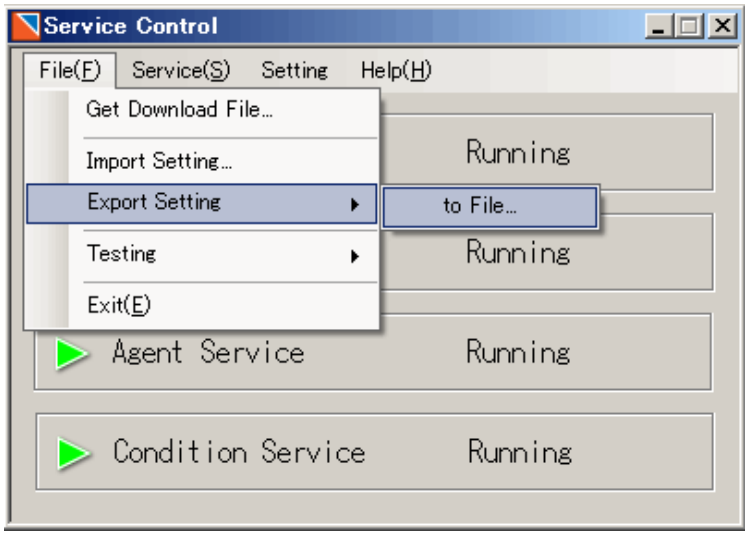
５．Agent 監視設定引継ぎ

5.1 ファイルによる Agent 監視設定引継ぎ

Agent の設定内容を別のノードに引き継ぎたい場合、ファイルによる引継が利用できます。監視設定を別ノードへ引き継ぐためには、以下のステップを実施して下さい。

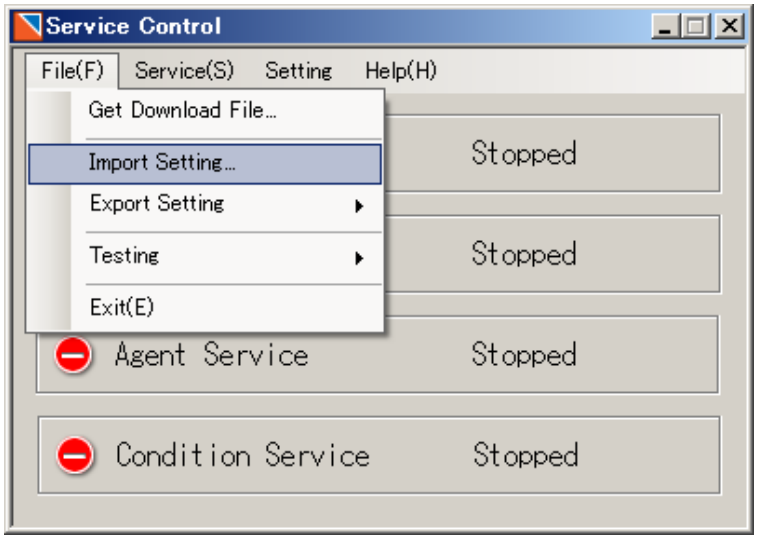
（１）監視設定ファイルのエクスポート

引き継ぎ元のサーバで監視設定ファイルをエクスポートします。監視設定ファイルのエクスポートは、Service Control のメニューから「File」－「Export Setting」－「to File」を選択します。エクスポートするファイルのファイル名は、「UCSExportFile.ini」として下さい。



（２）監視設定ファイルのインポート

エクスポートした監視設定ファイルを引き継ぎ先のサーバにコピーし、インポートします。監視設定ファイルのインポートは、Service Control の「All Service」-「Stop」で App Bridge の全サービスを停止して、Service Control のメニューから「File」－「Import Setting」を選択します。



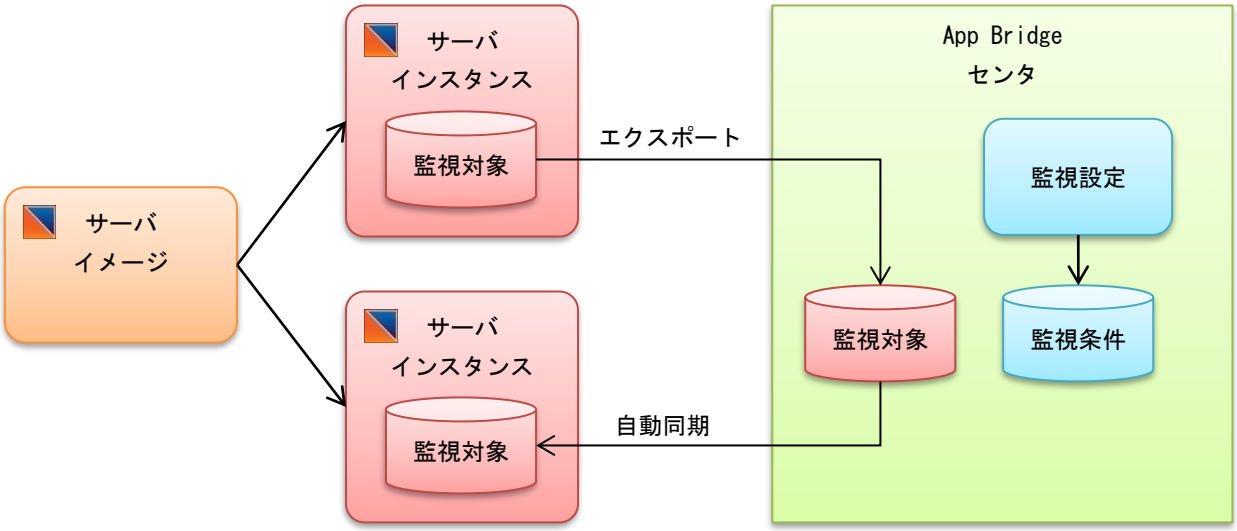
インポート後、Service Control は再起動されます。Service Control の「All Service」-「Start」で App Bridge の全サービスを起動して下さい。

5.2 スケーリング制御の Agent 監視設定引継ぎ

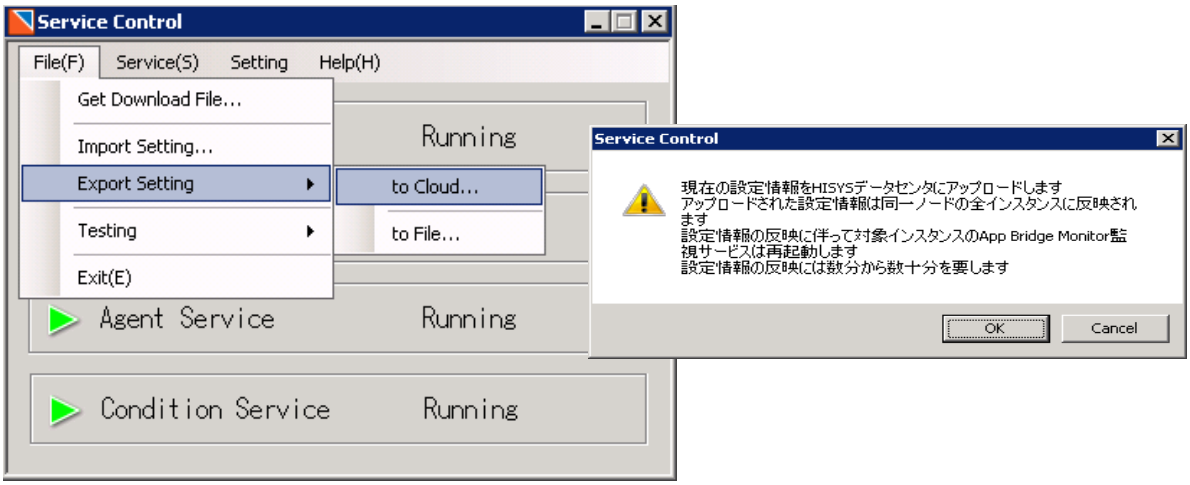
App Bridge Monitor のスケーリング制御は、App Bridge Monitor Agent がインストールされたサーバイメージから複数のサーバインスタンスを起動した際、起動されたサーバインスタンスを自動的に選別する機能です。この機能により、AWS の Auto Scaling や Azure Cloud Services などのサーバ伸縮機能に対応しています。

スケーリング制御を使用しているサーバインスタンス間では、App Bridge センタを経由した Agent 監視設定の引継ぎが可能です。

何れかのサーバインスタンスで設定変更したあと、監視設定を App Bridge センタにエクスポートすることで、同じサーバイメージから起動された他のサーバインスタンスに自動同期されます。エクスポートされた設定内容は新しく作成されたサーバインスタンスにも適用されます。



監視設定を App Bridge センタにエクスポートするためには、対象サーバに管理者権限を持ったアカウントでログインし、スタートメニューから「App Bridge Monitor」-「Service Control」を起動します。起動した Service Control のメニューから[File] - [Export Setting] - [to Cloud]をクリックします。表示されたメッセージを確認し、問題なければ[OK]をクリックします。



エクスポートされた監視設定は、同一ノード内の他サーバインスタンスに自動反映されます。監視設定の反映には数分から数十分を要します。また監視設定を反映させるため、サーバインスタンスの App Bridge Monitor 各種サービスが自動的に再起動されます。

６．監視間隔

App Bridge Monitor Windows Agent は監視結果を監視データとして App Bridge センタに送信します。監視間隔と監視データ送信間隔は以下の通りです。

監視項目	監視間隔(分)	監視データ送信間隔(分)	備考
イベントログ監視	発生都度即時	エラー判定条件に合うイベントログ発見時	
テキストログ監視	1	エラー判定条件に合致するテキストログ発見時	
CPU ビジー監視	1	15（※1）	
物理メモリ容量監視	1	15（※1）	
仮想メモリ容量監視	1	15（※1）	
ディスクビジー監視	1	15（※1）	
ディスク容量監視	5	30（※1）	
サービス監視	1	30（※2）	
プロセス監視	1	30（※3）	
SQL Server データベース容量監視	5	5	
SQL Server データベース応答監視	5	5	
Azure SQL Databases データベース容量監視	5	5	※4
Azure SQL Databases データベース応答監視	5	5	※4
ネットワークビジー監視	15	15	

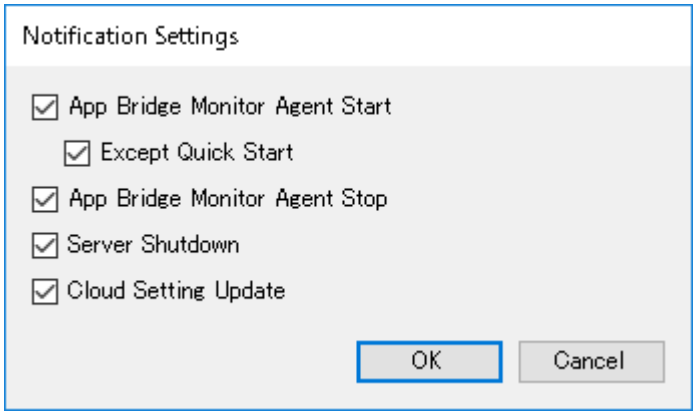
※1：エラー判定条件に該当した場合、即時送信されます
※2：ステータスの変化を検知した場合、即時送信されます
※3：プロセスの変化を検知した場合、即時送信されます
※4：以下のエラーコードがリターンされた場合、自動リトライを実施します。このため監視間隔、モニタデータ送信間隔は変動する可能性があります。
40197、40501、40544、40549、40550、40551、40552、40553、40613、20、64、233、10053、10054、10060

７．付帯機能

7.1 App Bridge イベント通知

App Bridge Monitor のイベントを監視対象とし、イベントが発生した際にエラーメッセージが送信されるように設定することができます。

Service Control のメニューから「Setting」-「Leading Service」-「Notification」を選択し、監視の必要なイベントについてチェックを入れてください。設定はサービス再起動後、有効になります。



設定項目	項目の説明	備考
App Bridge Monitor Agent Start	App Bridge Monitor のサービスが起動した際、エラーメッセージを送信します	ネットワーク障害等でイベントを通知できない場合はリトライを実施します
Except Quick Start	App Bridge Monitor のサービスが Quick 起動（※1）された場合、サービス起動時のエラーメッセージ送信を抑止します	この設定により、App Bridge Monitor のサービスが OS から起動された場合のみエラーメッセージが送信されます
App Bridge Monitor Agent Stop	App Bridge Monitor のサービスが停止した際、エラーメッセージを送信します。	ネットワーク障害等でイベントを通知できない場合があります。また、サーバシャットダウン時にはイベントは通知されません
Server Shutdown	App Bridge Monitor のサービスがサーバシャットダウンを検知した際にエラーメッセージを送信します	イベントを通知する前に OS が App Bridge Service を強制終了した場合は、イベントを通知できない場合があります
Cloud Setting Update	監視設定内容をアップデートされた時にエラーメッセージを送信します。この設定はスケーリング設定されたサーバでのみ可能です	「5.2 スケーリング制御の Agent 監視設定引継ぎ」を参照して下さい

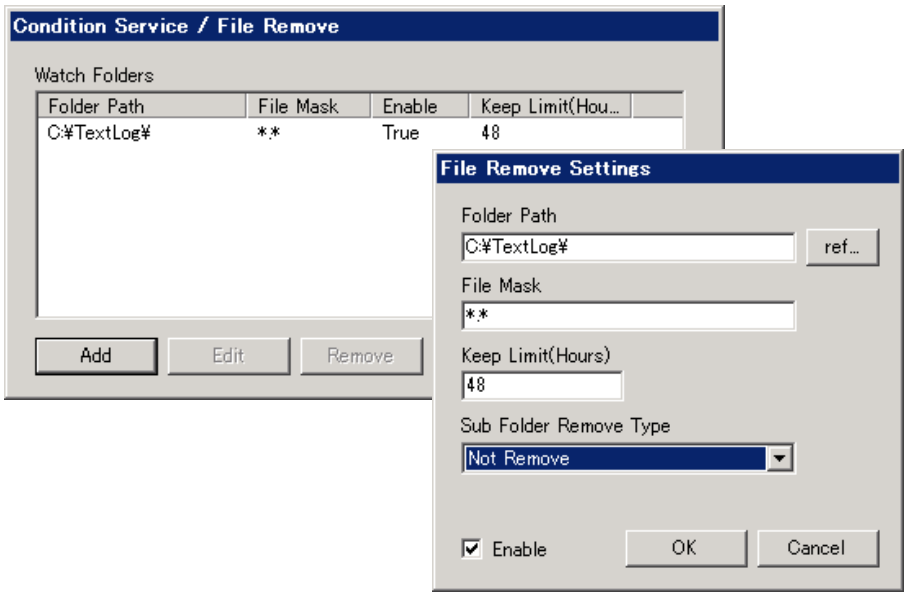
※1：通常起動では、サービス起動後、一定のインターバル（通常 60 秒）が経過してから監視処理を開始しますが、Quick 起動ではインターバルを取らず、すぐに監視処理を開始します。Service Control 等、App Bridge が提供するモジュールからサービス起動された場合、Quick 起動となります

7.2 ファイル削除の設定

コンディションサービスを使用してファイルを定期的に削除する設定です。必要に応じて設定して下さい。

7.2.1 設定方法

Service Control のメニューから「Setting」-「Condition Service」-「File Remove」を選択し、削除対象のフォルダ及びファイルを登録します。



設定項目	項目の説明	設定内容
Folder Path	削除対象となるファイルが保存されるフォルダのフルパス	
File Mask	削除対象ファイルのマスク	任意の値を設定する
Keep Limit(Hours)	ファイルの保存期間	任意の値を設定する（デフォルト：48 時間）
Sub Folder Remove Type	削除対象となるファイルが保存されるフォルダにサブフォルダがある場合の処理の選択	以下から選択します ・Not Remove サブフォルダは削除対象としない ・Remove Only Files サブフォルダのファイルを削除する ・Remove Files & Empty Folder サブフォルダのファイルを削除し、空になったサブフォルダも削除する
Enable	ファイル削除を有効とする場合チェックする	

7.2.2 リンクファイルの取り扱い

リンクファイル、シンボリックリンク、ジャンクション、ハードリンクについては、以下のとおり処理されます。

（1）リンク先がフォルダの場合

リンクの種類	フレームワークの基本動作	取得される作成日、更新日	削除時の動作
リンクファイル	リンクファイル自身を処理する	リンクファイルの情報	リンクファイルを削除する
シンボリックリンク	リンクファイルパスでリンク先フォルダを処理する	シンボリックファイルの情報	シンボリックファイルを削除する
ジャンクション	同上	ジャンクションファイルの情報	ジャンクションファイルを削除する

（2）リンク先がファイルの場合

リンクの種類	フレームワークの基本動作	取得される作成日、更新日	削除時の動作
リンクファイル	リンクファイル自身を処理する	リンクファイルの情報	リンクファイルを削除する
シンボリックリンク	リンクファイルパスでリンク先ファイルを処理する	シンボリックファイルの情報	シンボリックファイルを削除する
ハードリンク	同上	リンク先ファイルの情報	ハードリンクファイルを削除する