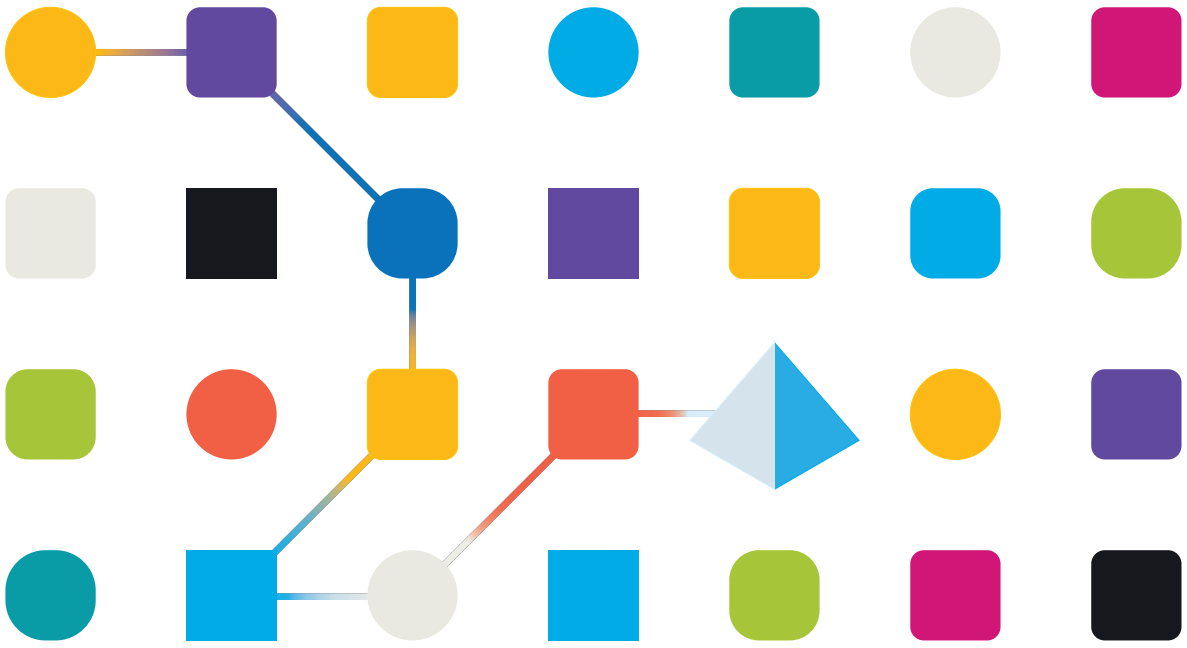
blueprism®

HubおよびInteract 4.6

プラットフォームメンテナンスガイド

Document Revision: 1.0



商標および著作権

本ガイドに記載されている情報は、Blue Prism Limitedおよび/またはその関係会社が独占的に所有する機密情報であり、権限を与えられたBlue Prism担当者の書面による同意なしに、第三者に開示してはなりません。本文書のいかなる部分も、複写機などの電子的あるいは機械的な形式や手段を問わず、Blue Prism Limitedまたはその関係会社の書面による許可を得ることなく、複製または送信してはなりません。

© Blue Prism Limited 2001 – 2023
Blue Prism、Blue Prismのロゴ、およびPrismデバイスは、Blue Prism Limitedおよびその関係会社の商標または登録商標です。All Rights Reserved.

その他のすべての商標は本文書によって確認され、各所有者のために使用されています。
Blue Prism Limitedおよびその関係会社は、本ガイドで言及する外部Webサイトの内容に関して、責任を負いません。

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom。
英国で登録：登録番号4260035。電話：+44 370 879 3000。Web：www.blueprism.com

内容

Blue Prismプラットフォームのメンテナンス概要

このガイドでは、以下を含むBlue Prism® HubおよびBlue Prism® Interactのメンテナンスのベストプラクティスについて説明します。

- SQLデータベースバックアップのメンテナンス計画の作成
- メッセージブローカーサーバーのバックアップ
- Webサーバーのバックアップと復元
- ロギング

このガイドは、Blue Prism HubとInteractに限られます。Blue Prismエンタープライズデータベースのメンテナンスに関する詳細は、「Blue Prismデータベースサーバーを保守する」を参照してください。

対象者

このガイドは、経験豊富なデータベースおよびサーバー管理者を対象としています。

SQLデータベースのメンテナンス

この情報は、あくまでもガイドとして提供されています。業界標準のベストプラクティスに従い、経験豊かなデータベース管理者のアドバイスを求めることをお勧めします。この情報は、環境全体に対する広範な影響を考慮して使用する必要があります。

次のデータベースはメンテナンスが必要です。

- InteractDB
- InteractCacheDB
- IadaDB
- AuthenticationServerDB
- HubDB
- AuditDB
- NotificationCenterDB
- LicenceManagerDB
- FileServiceDB
- EmailServiceDB
- BluePrismDecisionDB
- ImsDB
- FileServiceDB

CacheDBは、Hub 4.4からFileServiceDBに置き換えられました。

データベースメンテナンスの一般的な推奨事項

以下を行うことをお勧めします。

- すべてのデータベースに対して自動拡張を正しく設定します。推奨値は、データファイルの場合は1024MB、トランザクションログの場合は2048MBです。
- 自動拡張イベントの頻度を最小限に抑えるため、データベースのサイズの増加に合わせて自動拡張の値を再確立します。

  > ファイルの拡張率は使用せず、一定の容量を増やします。

- 過剰なトランザクションログの断片化ファイルを削除します。詳しくは、Microsoftオンラインヘルプを参照してください。
- インスタントファイルの初期化をオンにします。詳しくは、Microsoftオンラインヘルプを参照してください。
- 自動圧縮操作をオフにし、すべてのデータベースのページ検証をチェックサムに設定し、AUTO_CREATE_STATISTICSおよびAUTO_UPDATE_STATISTICSをオンにします。統計を更新するための定期的なプロセスを設けます。

  この目的のために、HubおよびInteractによってインストールされた各データベースに対して、次のT-SQLを設定できます。

```
ALTER DATABASE [ここにデータベース名] SET AUTO_CLOSE OFF
ALTER DATABASE [ここにデータベース名] SET AUTO_SHRINK OFF
ALTER DATABASE [ここにデータベース名] SET AUTO_UPDATE_STATISTICS ON
ALTER DATABASE [ここにデータベース名] SET AUTO_CREATE_STATISTICS ON
ALTER DATABASE [ここにデータベース名] SET PAGE_VERIFY CHECKSUM
```

- DBCC CHECKDBを実行する定期的なプロセスを用意します。– SQLエージェントのジョブは、システム使用率がほとんどまたは全くない時間帯に、少なくとも1日1回実行することをお勧めします。結果は、破損がないかチェックする必要があります。SQLエージェントアラートを作成して、オペレーターグループに以下のエラーを通知すると便利です。
  - 823 - ハードI/Oの破損
  - 824 - ソフトI/Oの破損
  - 825 - 読み取り/再試行の破損
  - 9100 - インデックスの破損
  - 重大度19 ~ 25のエラー
- アドホックワークロードの最適化 = オン
- バックアップ圧縮のデフォルト = オン
- バックアップチェックサムのデフォルト = オン
- 並列処理のコストしきい値 – 50から始めるといいでしょう。
- 並列化の最大レベル - SQL ServerのNUMA構成に依存しますが、単一のNUMAノードに対するコア数未満です。
- 自動終了の設定 = オン
- 最小サーバーメモリ - SQL Serverごとに異なりますが、設定する必要があります。
- 最大サーバーメモリ - SQL Serverごとに異なりますが、設定する必要があります。

ディスクレイアウトに関する推奨事項

データとトランザクションログファイル、一時データベース、バックアップには、別々のドライブを使用することをお勧めします。

メンテナンス計画を作成する

定期的なバックアップを行うためのメンテナンス計画が整っていることを確認します。SQLデータベースのバックアップには、組織が推奨するメンテナンス計画を使用します。組織にメンテナンス計画がない場合は、業界のベストプラクティスを調査し、組織のニーズに適したメンテナンス計画を選ぶことが推奨されます。

バックアップを取る

バックアップは、組織のリカバリポイント目標(RPO)とリカバリ時間目標(RTO)に基づいて設計する必要があります。

- RPO - 障害発生後にデータをリカバリできる時点。これにより、データ消失量が決定します。
- RTO - 障害発生後、データのリカバリにかかる時間。これにより、プラットフォームを使用できない時間の長さが決定します。

Blue Prismデータベースのバックアップおよびリカバリ計画を作成する際は、以下の点を考慮して実装することが重要です。

- RPOとRTOの両方を定義します。
- フルリカバリモデルを使用すると、定義したRPOとRTOに合わせて、フルバックアップ、差分バックアップ、トランザクションログバックアップを実行できます。
- すべてのバックアップの [WITH CHECKSUM] および [VERIFYONLY] オプションを使用し、バックアップが有効であり、必要に応じて復元できることを確認します。
- [WITH COMPRESSION] オプションを使用してディスク領域を節約し、データベースのバックアップとオプションの復元にかかる時間を削減します。
- バックアップおよびリカバリプロセスを文書化します。
- 定期的に復元して、バックアップの信頼性を確認してください。

これらのバックアップを実行する頻度は、組織の規模、データリスクの量や価値によって異なります。

フルバックアップは、絶対的なダウンタイム時に実行することをお勧めします。増分バックアップは、一部のデータが失われるリスクを伴うサービスを停止することなく実行できます。

インデックスの断片化を解決する

データベースインデックスの断片化により、クエリのパフォーマンスが時間の経過とともに低下します。これを防ぐには、データベースのダウンタイムが許す限り頻繁にインデックスを再構築します。また、バックアップ取得後や大量のデータ削除後にもインデックスを再構築することをお勧めします。フルバックアップを復元する必要がある場合のインデックスの断片化を最小限に抑えるために、フルデータベースバックアップを実行する前にもインデックスを再構築することをお勧めします。

インデックスの再構築や再編成のメンテナンスに推奨されるしきい値は、再編成が30%未満、再構築が30%超です。

データベースインデックスの再構築は、データベースサーバー内のジョブとして実行するようにスケジュールしたり、データベースのメンテナンス計画に追加したりできます。システムのアクティビティが低い時間帯に実行し、バックアップおよびDBCC CHECKDBメンテナンスとの重複を避けるようにスケジュールすることをお勧めします。

メッセージブローカーサーバーをバックアップする

メッセージブローカーサーバーは、RabbitMQ™を実行します。メッセージブローカーサーバーのバックアップ作成については、RabbitMQのオンラインヘルプを参照してください。

ログ

診断ロギングの目的は、アプリケーションの実行時に利用可能な情報を増やすことです。ログに記録されたエラーと警告は、エンドユーザーにすぐには明らかにならない可能性があるシステム内の障害を特定するのに役立ちます。より詳細なロギングを一時的に有効にすると、問題のトラブルシューティング時にアプリケーションがどのように動作しているかをわかりやすく図で示すことができます。

Blue PrismはNLogと呼ばれる、実績があり信頼できるライブラリを利用して、ログ情報を出力し記録します。管理者は、グローバルまたはアプリケーションの特定の領域に記録される情報量を微調整できます。

ロギングレベル

ログエントリはレベル別に分類されます。*情報*レベル以上のエントリは通常、標準として記録されます。 [デバッグ] や [*トレース*] など、より詳細な下位レベルでは、より詳細な情報が提供されますが、有効にする必要があります。

NLogは、次のレベルを定義します。

- **トレース** – 非常に詳細なログ。プロトコルペイロードなどの大量の情報が含まれることがあります。このログレベルは、通常は開発中にのみ有効になります。
- **デバッグ** – トレースよりも詳細度の低いデバッグ情報は通常、パフォーマンスに影響する可能性があるため、本番環境では有効になりません。
- **情報** – 情報メッセージ。通常は本番環境で有効になっています。
- **警告** – 警告メッセージ。通常は、復旧可能な重要でない問題、または一時的な障害に関するものです。
- **エラー** – エラーメッセージ – ほとんどの場合、これらは例外です。
- **致命的** – 非常に重大なエラー。

標準ロギング構成

ロギングレベルは、各Webサイトとサービスのインストールフォルダー内のappsettings.jsonファイル内で定義されます。デフォルトのインストールでは、これらのフォルダーはC:\\Program Files (x86)\\Blue Prism\\にあります。

Blue Prismを普通に使っている間は、自分でappsettings.jsonファイルのログ構成設定に変更を加える必要はありません。製品の問題を調査する場合は、Blue Prismカスタマーサポートから別のログ構成設定が提供されます。appsettings.jsonファイルでロギング設定を変更した場合は、サイトをIIS内で再起動する必要があります。

ロギング構成に変更を加えるとアプリケーションの性能に影響を及ぼす可能性があるため、本番環境内を修正する場合は特に注意する必要があります。

デフォルトの構成では、情報レベル以上 (警告、エラー、致命的なエラーを含む) のログエントリをログファイルに書き込みます。ログファイルは、appsettings.jsonファイルのLogsFolder設定で指定されたディレクトリに書き込まれます。通常は、./Logs_{Application}に設定されます。例 ./Logs_Hubまたは./Logs_Interact。

デフォルトでは、appsettings.jsonファイルのロギング構成設定は次のようになります。

```
"Logging": {
      "LogsFolder": "./Logs_{Application}",
      "LogLevel": {
        "Default": "Information",
        "System": "Warning",
        "Microsoft": "Warning"
      }
    },
```

ログレベルと日付に基づいて個別のログファイルが生成され、これらは、warns.2021-05-07やinfos.2021-05-07などのログファイル名に反映されます。

情報ログファイルからの行の例を次に示します。

```
[08:58:11.4549] Connect.Core.Actions.UpdateCacheAction - ウィジェットのキャッシュが更新されました
```

このテキストの形式には、以下の要素が含まれています。

- UTCの時刻 - 日付はファイル名に反映されます。
- ロガー名 – これは通常、ログエントリの起点となるクラスと名前空間を識別します。
- ログメッセージ。
- エラー情報 - 例外情報がログされている場合のみ使用可能です。完全な詳細は、ログメッセージの下の別の行に記録されます。

追加のログ構成

Blue Prismは、特定のコンポーネントによるアクティビティをキャプチャするために、適切なappsettings.jsonファイルに追加できるログ構成設定を開発しました。

LDAPのデバッグ

ロギングを構成して、HubをLDAPと同期する際に発生する可能性のあるさまざまな問題をデバッグできます。Hub UIでユーザーを同期する前に、Authentication Serverのappsettings.jsonファイルでログインを設定する必要があります。

1. サーバーで、Authentication Serverフォルダーに移動します。デフォルトでは、これはC:\Program Files (x86)\Blue Prism\にあります。
2. appsettings.jsonファイルをテキストエディターで開きます。
3. [Logging]セクションを見つけて、「`ImsServer.IntegrationServices.Services.LdapConnectionService": "Debug"`」を[LogLevel]セクションに追加し、上記の行の最後にカンマを挿入します。例:

```
"Logging": {
      "LogsFolder": "./Logs_AuthenticationServer",
      "LogLevel": {
        "Default": "Information",
        "System": "Warning",
        "Microsoft": "Warning",
        "ImsServer.IntegrationServices.Services.LdapConnectionService": "Debug"
      }
    },
```

4. ファイルを保存します。
5. IISアプリケーションプールでAuthentication Serverプールをリサイクルします。

   4.3より前のバージョンからアップグレードした場合は、IMSプールをリサイクルする必要があります。

6. IISサイトでAuthentication Serverサイトを再起動します。

これにより、Logs_AuthenticationServerディレクトリにプレフィックス「デバッグ」と適切な日付を持つファイルが作成されます。

デバッグ情報を使用して問題を解決したら、追加された行とカンマを削除してファイルを保存し、手順5と6を繰り返す必要があります。これを行わないと、ログファイルのサイズは大幅に増加し、メモリがいっぱいになる可能性があります。

ログ収集サービス

このWindowsサービスは、各Webサーバーコンポーネント(Hub、Interact、Authentication Server、Audit Service、監査サービスリスナー、Emailサービス、ログ収集サービス、IADA、Interact Remote API、SignalR、送信フォームマネージャー)から古い製品ログを削除します。このサービスは毎月7日に実行されるスケジュールとなっており、ログはC:\Program Files (x86)\Blue Prism\ArchivedLogsに移動されます。

apppsettings.json内で、アーカイブされたログフォルダーのパスとスケジューラーの日付を変更できます。C:\Program Files (x86)\Blue Prism\Log Service(デフォルト)の「ArchivedFolder」ではアーカイブパスを、「DayOfMonth」ではスケジューラーの日付を変更できます。

詳細情報

以下のリンクから、役立つ詳細情報を参照できます。

- NLog Githubリポジトリ - 基本のチュートリアル
- NLogオフィシャルWebサイト - 構成オプション

Webサーバーのメンテナンス

HubまたはInteractのWebサーバーに障害が発生した場合、再作成する必要があります。そのためには、必要なバックアップが使用可能になっていることを確認する必要があります。

バックアップ

ファイル

C:\Program Files (x86)\Blue Prismにあるファイルフォルダーを定期的にバックアップする必要があります。このフォルダーには、アプリケーションデータ、およびInteractから送信されたファイルと添付ファイルが含まれています(File Service appsettings.jsonファイルの別の場所にファイルと添付ファイルが指定されている場合を除く) 。

> これはデフォルトのインストール場所です。初回インストール時に別の場所を入力すると、ファイルフォルダーがそこに保存されます。

Interact 4.4がインストールされている場合、またはInteract 4.4からアップグレードする場合、新しいファイルはデータベースにあります。これらは、データベーススケジュールの一部としてバックアップされます。ただし、以前のバージョンのInteractからアップグレードした場合は、ファイルフォルダーのバックアップが必要です。

証明書

また、Webサーバーが使用する証明書をバックアップすることもできます。証明書の完全なリストについては、「」「Hubメンテナンスガイド」および以下の追加証明書を参照してください。

- BluePrismCloud_IMS_JWT
- BluePrismCloud_Data_Protection
- BPC_SQL_CERTIFICATE

Webサーバーの復元

既存のHubまたはInteractのWebサーバーに障害が発生した場合は、再構築する必要があります。

HubのWebサーバー

> Hubをアンインストールする前に、すべてのアプリケーションプールを停止し、インストーラーによって作成されたBPC証明書を削除することをお勧めします。

1. 既存のWebサーバーを再構築する場合は、Hubをアンインストールします。
2. Hubをインストールします。

   以下を含む、元のインストールと同じ設定を入力します。

   - Blue Prism Hubセットアップウィザードの任意のサーバーSQL接続ページで、前回のインストールで使用したものと同じ**ユーザー名**と**パスワード**を入力します。
   - Blue Prism Hubセットアップウィザードの任意のサーバーIIS設定ページで、前回のインストールで使用したものと同じ**ホスト名**と**証明書**を入力します。
3. ファイルフォルダーのバックアップコピーを、インストール場所 (例 : C:\Program Files (x86)\Blue Prism) に貼り付けます。

Interact Webサーバー

1. 既存のWebサーバーを再構築する場合は、Interactをアンインストールします。
2. Interactをインストールします。

   以下を含む、元のインストールと同じ設定を入力します。

   - Blue Prism Interactセットアップウィザードの任意の**サーバーSQL接続**ページで、前回のインストールで使用したものと同じ**ユーザー名**と**パスワード**を入力します。
   - Blue Prism Interactセットアップウィザードの任意の**サーバーIIS設定**ページで、前回のインストールで使用したものと同じ**ホスト名**と**証明書**を入力します。
3. ファイルフォルダーのバックアップコピーを、インストール場所 (例 : C:\Program Files (x86)\Blue Prism) に貼り付けます。