BigFix Remote Control インストール・ガイド

目次

第 1 章. Remote Controlインストール・ガイド

Remote Control を使用すると、何千もの PC およびサーバーをリモートでサポートし、制御することができます。サポートおよび制御は、エンタープライズ・スケールで、中央の場所から、または直接、P2P モードで行うことができます。

Remote Control 管理 Web インターフェースを使用して、ネットワーク上の任意のロケーションから、リモート・デスクトップの表示および制御 (キーボードやマウスを含む) を行います。チャット、ファイル転送、リモートでのユーザーの誘導、 さまざまなユーザーおよびターゲット・グループに適用するポリシーの管理、その他多くの機能を利用できます。これらの機能により、 管理者のデスクトップから効率的かつ効果的にユーザーの問題を分析することができ、技術者を派遣するコストを省き、電話でのユーザーからの説明に頼る必要もなくなります。Remote Control を使用すると、セッションの強化された中央ロギングとビデオ・キャプチャー、およびデータ・ストリーム全体の暗号化に対応した堅固な機能によって、サポートの質が向上し、柔軟性が高まり、セキュリティーが強化されます。

対象読者

本書は、Remote Control をインストールおよび管理しようとする管理者および IT 管理者を対象としています。各コンポーネントのシステム要件について詳しく説明しているほか、 ご使用の環境に本プログラムを導入できるインストール手順についても説明しています。また、Remote Control の構成および保守についても説明しています。

バージョン

本書は、 Remote Control V10 で導入された機能について記載しています。

本書で使用される用語

次の用語は、すべて Remote Control の用語です。これらの用語は、本書全体で、Remote Control というラベルなしで随時使用されます。

- コントローラーは常に Remote Control コントローラー・アプリケーションを意味します
- ターゲットは常に Remote Control ターゲットを意味します
- サーバーは常に Remote Control サーバーを意味します
- ブローカーは常に Remote Control ブローカーを意味します
- 管理対象モードは、サーバーがデプロイされていて、ターゲットがそのサーバーに登録して状況をレポートするよう構成されるインストール済み環境を指します

Remote Control システムの概要

Remote Control システムには、以下の主要コンポーネントが含まれます。

Remote Control ターゲット

このターゲットは、Remote Control を使用してリモート側で制御する必要があるすべてのコンピューターにインストールされます。このターゲットは、コントローラーからの接続要求を listen します。また、ブローカーを使用することで、インターネット経由でターゲットとのリモート・コントロール・セッションを開始することもできます。

イントラネットの外部に存在するターゲットを構成して、そのターゲットの詳細をサーバーに登録することができます。これらのターゲットとのセッションは、サーバー・ポリシーによって管理されます。これらのターゲットをデプロイするには、**Managed** プロパティーを「Yes」に設定する必要があります。また、**ServerURL プロパティー**と **BrokerList** プロパティーも構成する必要があります。ターゲットの詳細をサーバーに送信しないようにターゲットを構成することもできます。これらのターゲットは、未登録ターゲットとして分類されます。ターゲット・ソフトウェアをインストールして、**Managed** プロパティーを *No* に設定します。**BrokerList** プロパティーも設定する必要があります。また、オンデマンド・ターゲット機能を使用して、ターゲット・ソフトウェアが事前にインストールされていないコンピューターとのリモート・コントロール・セッションを開始することもできます。オンデマンド・セッションの管理にはサーバー・ポリシーが使用されます。ターゲット・ソフトウェアはセッションの最後に削除されます。

Remote Control コントローラー

Fixlet を使用するか、P2P セッションで使用するために提供されているインストーラーを使用して、コントローラーをインストールできます。また、リモート・コントロール・サーバーまたは Remote Control コンソールからコンテキスト起動することもできます。どのような場合でも、コントローラーを使用することで、リモート・コントロール・ターゲットがインストールされているリモート・コンピューターをユーザーが制御できるようにすることができます。コントローラーには、コントローラー・ユーザーが使用できる、リモート・コントロール、ガイダンス、チャット、ファイル転送、コラボレーションその他の多数のアクションへのインターフェースが備わっています。

Remote Control Server

管理対象モードで動作して、Remote Control サーバーの URL を指すように構成されているすべてのインストール済みターゲットを管理する Web アプリケーション。既存の WebSphere® サーバーにインストールするか、組み込みバージョンの WebSphere® とともにインストーラー・パッケージを使用してインストールすることができます。このサーバーは、デフォルトで HTTP または HTTPS 接続を listen します。組み込みの WebSphere® オプションでインストールされると、WebSphere® はポート 80 および 443 で listen します。既存の WebSphere® サーバー上にデプロイすると、Remote Control サーバーはポート 9080 および 9443 で listen します。そのサーバーにはデータベース・サーバーが必要です。サポートされているオプションは、組み込み Derby (PoC デプロイメントの場合のみ)、DB2®、SQL Server、および Oracle です。また、Active Directory や Tivoli Directory Server など、LDAPv3 サーバーからのユーザーとグループのデータが同期および認証されるように構成することもできます。このデプロイメント・シナリオのネットワーキング特性はピアツーピアと同じです。このため、すべてのコントローラーとすべてのターゲットとの間には、直接的な TCP 接続が必要です。ただし、Remote Control サーバーでは中央集中型のより詳細なポリシー制御方法を使用できます。この方法では、リモート・コントロール・セッションを開始しようとしているユーザーによって決定されるさまざまなポリシーをターゲットで使用できます。また、サーバーは、セッションの完全な自動記録の一元的な監査と保管の機能も提供します。このシナリオでは、コントローラーはスタンドアロン・アプリケーションでは

なく、リモート・コントロール・セッションを開始するために、Remote Control サーバーの Web インターフェースから Java™ Web Start アプリケーションとして開始されます。

注: ピアツーピアと管理対象は排他モードではありません。次の方法で、Remote Control ターゲットを構成できます。

- 厳密な管理対象として。
- サーバーにアクセスできない場合に P2P モードにフェイルバックする。
- P2P モードと管理対象モードの両方のリモート・コントロール・セッションを受け入れる。

以下のコンポーネントは、管理対象モードでのみ使用できます。

Remote Control CLI ツール

CLI ツールは、ターゲット・コンポーネントの一部として常にインストールされますが、別個にインストールすることもできます。CLI は、以下のタスクを行うためのコマンド・ライン・ツールを提供します。

- 管理対象リモート・コントロール・セッションの起動をスクリプト化または統合します。
- 管理対象ターゲットがインストールされたコンピューターでリモート・コマンドを実行します。

Remote Control ゲートウェイ

セキュア・ネットワーク境界にあるコンピューターにインストールされるサービス。セキュア・ネットワーク境界では、セキュア・ネットワーク間でのトラフィック・フローが厳密に制御されます。例えば、境界にあるファイアウォールは、特定の IP アドレスとポートのペア間のトラフィックのみを許可します。このようなシナリオでは、ゲートウェイのネットワークをデプロイできます。このゲートウェイは、特定のネットワーク・ゾーン内のコントローラーから別のネットワーク・ゾーン内のターゲットへのリモート・コントロール・トラフィックについて、ルーティングとトンネリングを行います。ゲートウェイは Windows™ または Linux™ オペレーティング・システムがインストールされているコンピューターにインストールできるネイティブ・サービスです。listen するためのデフォルト・ポートはなく (ただし通常は 8881 を選択します)、複数の着信リスニング・ポートおよび発信接続について構成することができます。

Remote Control ブローカー

企業ネットワーク外 (インターネット・カフェや自宅) にあるコンピューターから到達できるようにするために、通常は DMZ 内のコンピューターにインストールされるサービス。Remote Control ブローカーは、コントローラーおよびターゲットからのインバウンド接続を受け取り、この 2 つのコンポーネント間でリモート・コントロール・セッション・データをトンネリングします。このブローカーは、Windows™ コンピューターまたは Linux™ コンピューターにインストール可能なネイティブ・サービスです。listen するためのデフォルト・ポートはありませんが、推奨オプションは 443 です。その理

由は、通常、このポートはアウトバウンド接続用に開かれており、コンテンツ・フィルターの問題が、例えば 80 の場合よりも少なくなるためです。

本書の利用方法

Remote Control を稼働させるプロセスは、ご使用のネットワーク環境および達成する目標である管理の細分性によって異なります。インストール・ガイドでは、以下の 3 つのタイプのデプロイメントに焦点を合わせています。

P2P

最も単純なシナリオであるため、小規模デプロイメントに最適です。すべてのターゲットがコントローラーからネットワークを介して見えるようになっており、コントローラー・ポリシーを中央集中的に管理する必要はありません。

イントラネット管理対象

ファイアウォールをトラバースするためにゲートウェイのデプロイメントを必要とする複雑なネットワーク・インフラストラクチャー内の場合、または厳格なポリシー制御および中央集中監査が必要である場合に最適です。

管理対象

インターネットに接しているコンピューターに少なくとも 1 つのブローカーをインストールして、コントローラーからネットワークを介して見ることができないターゲットから見えるようにするインターネット・セッションのサポートを備えています。

読みやすさや一般性のために、インストール・ガイドでは以下の制限を前提としています。

- 各 Remote Control サーバーは、サポートされるデータベース・サーバーのいずれかにアクセスできなければなりません。データベースは、サーバー・コンピューター上にローカルに配置することも、リモート側の別個のサーバーに配置することもできます。サポート対象データベース・システムは、DB2、Oracle、および MS SQL です。インストーラーで提供される組み込み Derby データベースを使用してサーバーをインストールすることも可能です。ただし、この構成は実動デプロイメントに対してはサポートされません。
- 管理対象環境で、各コントローラーは、Remote Control サーバーへの HTTP 接続または HTTPS 接続を作成できます。
- 管理対象環境で、ネットワーク内の各 Remote Control ターゲット・コンピューターは、指定ポートでのサーバー、ゲートウェイ、またはブローカーへの HTTP 接続または HTTPS 接続を作成することが可能になっている必要があります。

ご使用のネットワーク構成が該当する章のどのシナリオにも一致しない場合は、追加オプションについてサポート技術員に連絡してください。

最小管理対象 Remote Control システム (サーバーといくつかのターゲット) の初期デプロイメントは、完了するまでに約 1 時間かかります。

Remote Control インストールのいくつかのステップは、前のステップの完了に依存しています。そのため、記載されている順序で説明に従うことをお勧めします。

Remote Control の動作要件

Remote Control は、最小限のサーバー、ネットワーク、およびクライアント・リソースで効率的に動作します。クライアント・プログラムの要件は厳密なものではありません。サーバーおよびターゲットに必要なハードウェアは、管理対象であるコンピューターの数と、それらの状況更新について定義されている頻度によって異なります。

基本インストール

最も基本的なインストールには、Remote Control ターゲットとコントローラーの各コンポーネントが必要です。その 2 つのコンポーネントを使用して、ピアツーピアのリモート・コントロール・セッションを開始します。この場合、セッションのポリシーはターゲット・レベルでのみ定義されます。

ターゲットからコントローラーへの通信に使用されるポートは、インストール時に構成できます。デフォルトはポート 888 です。

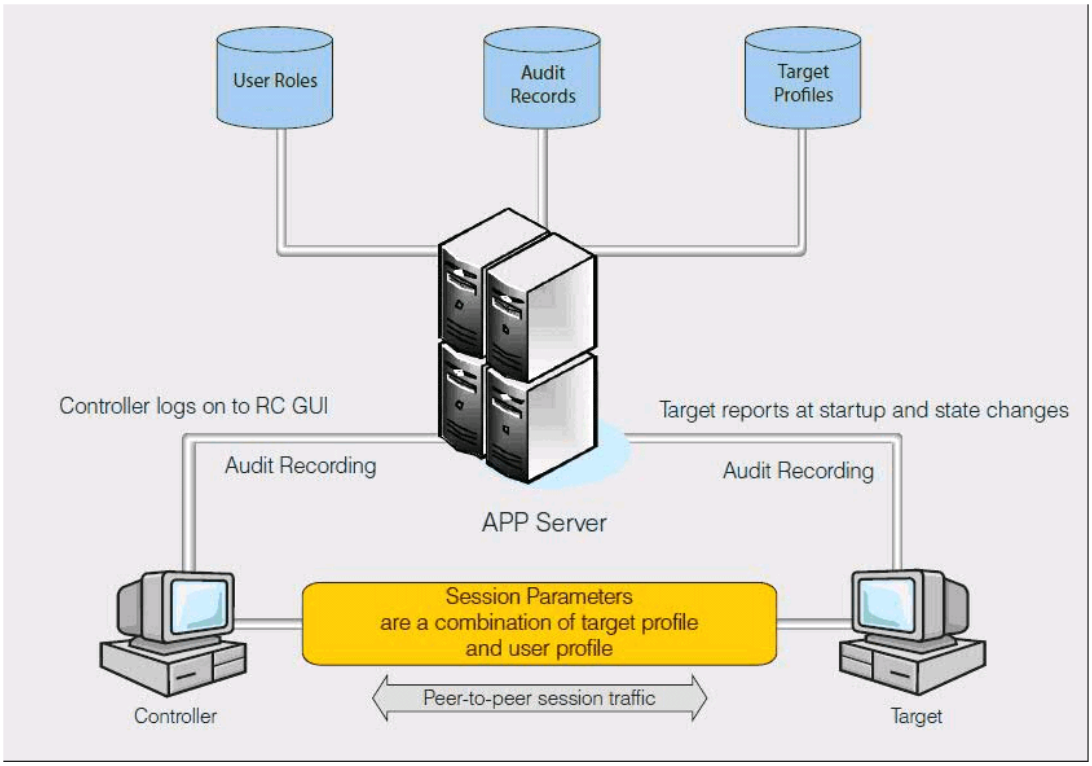
このようなインストールでは、基本的な監査情報が提供されます。この情報には、BigFix® コンソールからアクセスできます。この情報は、Windows オペレーティング・システムではアプリケーション・イベント・ログ、Linux オペレーティング・システムではシステム・ログにも保管されます。ただし、ユーザーおよびコンピューターの一元的な監査および管理が必要な場合は、サーバー・コンポーネントをインストールしてください。

サーバー・コンポーネントには、コントローラー・ユーザーが簡単にターゲットを検索できる単一のインターフェースが用意されています。また、最も頻繁にアクセスされている複数のターゲットを編成することや、それらのターゲットのセッション履歴を表示することもできます。管理対象環境で管理者が実行できる追加機能は、以下のとおりです。

- ユーザーおよびターゲットの一元管理: 類似するプロファイルを持つユーザーをグループに編成できます。Remote Control サーバー・インターフェースを使用して手動で、または LDAP からユーザーおよびグループをインポートして編成することができます。同様に、ターゲットの編成は、手動でも、ターゲットのメンバーシップ・ルールを設定してターゲットを特定のグループに自動的に割り当てることによっても可能です。ターゲットのメンバーシップ・ルールについて詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。
- ポリシーの一元管理: サーバー・インターフェースからセッションを開始すると、セッションに設定されるアクセス許可が、ターゲットおよびコントローラーのプロパティーから取り込まれます。単一のターゲットに対して、組織内のさまざまなユーザーごとに、異なるアクセス・レベルをより柔軟に定義できます。
- 監査および記録の一元的リポジトリー: 管理者は、Remote Control サーバー・インターフェースを使用して、監査情報を閲覧および調査できます。また、特定のリモート・コントロール・セッションに関連付けられた記録を表示することもできます。管理者は、既存のセッション履歴を検索できます。例えば、ユーザー ID やコンピューター名などを基準として検索することができます。

- アクセス要求の管理: 管理者は、ターゲットまたはターゲット・グループに対する一時アクセス権限を付与することや、アクセス権限のレベルを上げることができます。一時アクセス権限は、Remote Control に登録されたユーザーにも、未登録のユーザーにも付与できます。
- レポート作成機能

図 1. 基本インストールの環境



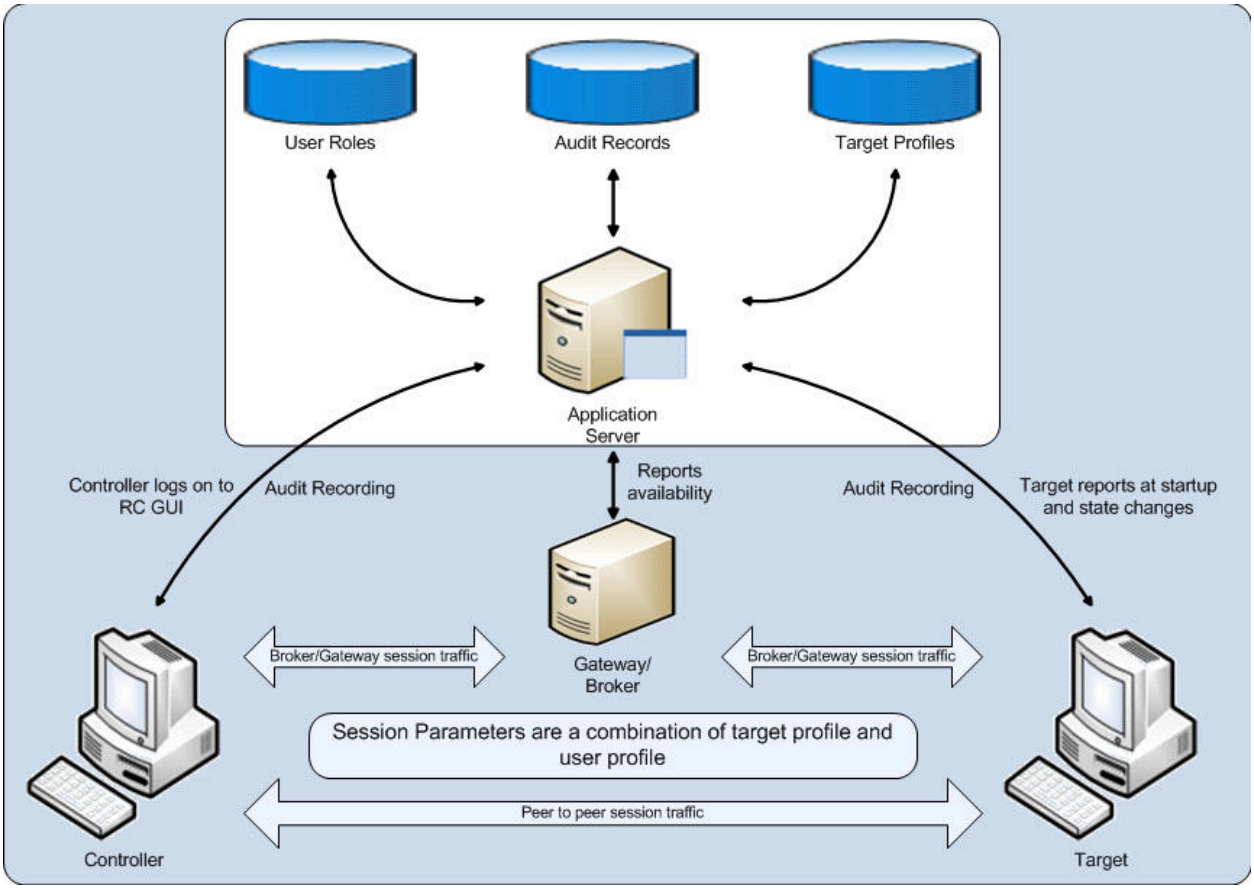
注: 管理対象環境では、コントローラー・コンポーネントをインストールする必要はありません。リモート・コントロール・セッションは、Remote Control サーバー・インターフェースからコンテキストに応じて起動されますまた、管理対象環境で、スタンドアロン・コントローラー・コンピューターからのピアツーピア・リモート・コントロール要求を受け入れるよう、ターゲット・コンポーネントを構成することもできます。ターゲットのインストールについて詳しくは、「ターゲットのインストール」を参照してください。

ファイアウォールおよび NAT のトラバーサルに対応したインストール

環境によっては、ファイアウォールのポートを開くことで、コントローラーからターゲット、またはターゲットからサーバーへの通信を、すべてのエンドポイントについて有効にする、ということができない場合があります。ファイアウォールをトラバースするには、ゲートウェイとして機能する単一のマシンからのトラフィック、またはそのコンピューターへのトラフィックを有効にする方が妥当です。

ネットワークにゲートウェイ・コンポーネントを戦略的にインストールすることで、別々のネットワークにターゲットとコントローラーとの間、またはターゲットとサーバーとの間のトラフィックを有効にすることができます。ま

た、このコンポーネントをプロキシー・サーバーとして使用して、ターゲットの状況の更新をリモート・コントロール・サーバーに転送することもできます。



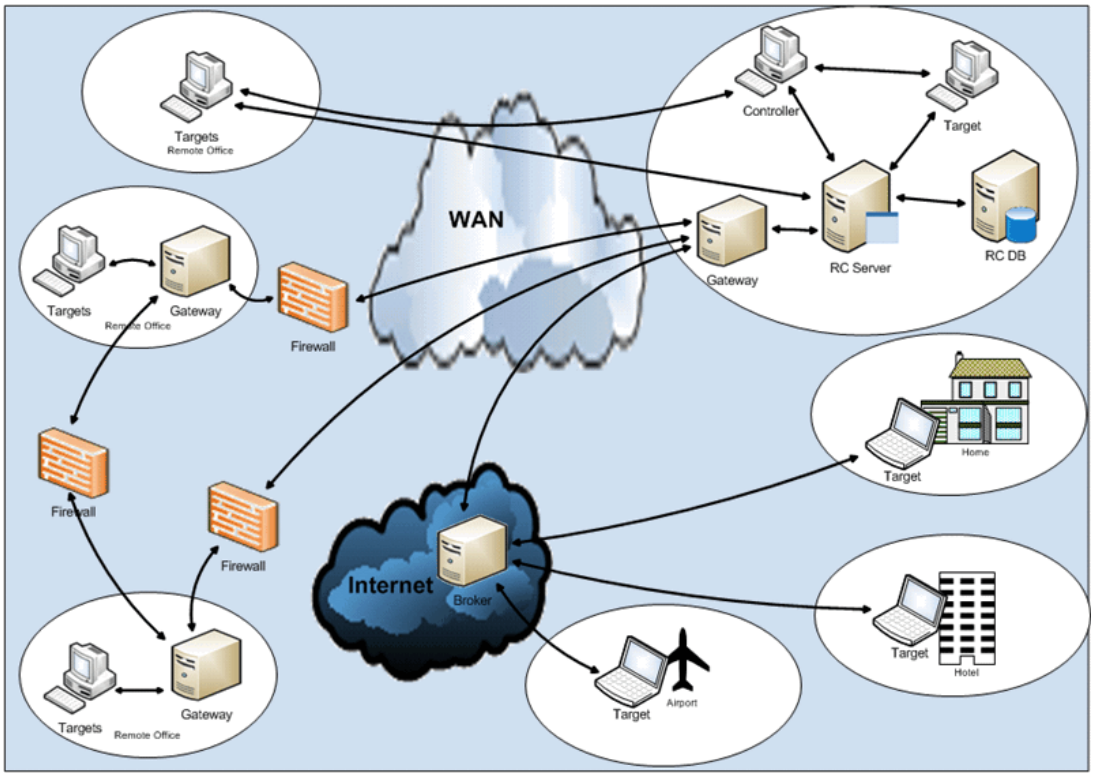
インターネット経由のリモート・コントロール・セッションに対応したインストール

サポートの必要なターゲットが、ネットワーク経由で見ることができない、インターネット上のロケーションに存在していることがあります。例えば、ホテルや空港のラウンジなどです。

これらのコンピューターを対象としたリモート・コントロール・セッションを有効にするには、ブローカー・コンポーネントを使用して、ターゲットとコントローラーの間の通信を仲介します。ブローカーは DMZ 内に配置されている必要があり、またイントラネット内のサーバーへのセキュアな通信を実現するためにはゲートウェイが必要です。

このシナリオでは、コントローラー・ユーザーが、サーバーからブローカー接続を開始して、接続コードを取得できます。支援を必要とするユーザーは、ターゲット UI で該当するメニュー・オプションを使用して、接続コードを入力します。サーバーによってセッションの詳細が検証されると、セッションが接続されます。

図 2. デプロイメント環境例



サーバーの要件

サーバー・コンポーネントに必要なハードウェアは、管理対象であるコンピューターの数と、それらの状況更新について定義されている頻度によって異なります。

Remote Control は分散アーキテクチャーを採用しているため、 単一のサーバーで何十万ものコンピューターをサポートすることができます。

注: Remote Control には、DB2® v11.5および WebSphere® v8.5 のライセンスが含まれています。

Remote Control サーバーをインストールするコンピューターは、最低でも以下の機能を備えている必要があります。

最小ハードウェア要件

- クワッド・コア・プロセッサー 1 個またはデュアル・コア・プロセッサー 2 個、2.40 GHz、およびサポート対象 OS。
- 最小 4GB のメモリー。
- インストール用に最小 2 GB のストレージまたはハード・ディスク・スペース、データベースにはクライアントあたり平均 2 MB。
- サーバーの自動インストールを実行するには、800 x 600 ピクセル以上の画面解像度が必要です。

- セッションのビデオ録画を格納するための適切なスペース。録画はハード・ディスクに格納され、サイズはセッションの所要時間と画面アクティビティーによって異なります。平均すると、8 ビット・モードの 5 分間のセッションでおよそ 2 MB のスペースが使用される可能性があります。トゥルー・カラーの 24 ビット・モードの場合、録画にこれよりも多くのスペースが使用される可能性があります。
- TCP/IP をサポートするネットワーク・カード。
- サポート対象のブラウザー。

サポートされているブラウザー

検証済みのブラウザーは次のとおりです。

- Internet Explorer
- Mozilla Firefox
- Chrome
- Safari
- Edge

オペレーティング・システムのサポート

以下のオペレーティング・システムがサポートされています。

- Windows™ Server 2012
- Windows™ Server 2012 R2
- Windows™ Server 2016
- Windows™ Server 2019
- Windows™ サーバー 2022
- Red Hat Enterprise Linux™ 6.0 以降
- Red Hat Enterprise Linux™ 7.0 以降
- Red Hat Enterprise Linux™ 8.0 以降
- SUSE Linux™ Enterprise Server 10 以降
- SUSE Linux™ Enterprise Server 11 以降
- CentOS 5.0 以降
- CentOS 6.0 以降

サポートされるアーキテクチャー

- Intel™ IA®-32 (x86, x86-32 とも呼ばれます)
- Intel™ 64 または AMD64 (x64、x86-64、EM64T とも呼ばれます)

注: IA®-64 (Itanium™とも呼ばれる) プロセッサーはサポートされていません。

サポートされるデータベース

以下のデータベースがサポートされています。

- IBM DB2 11.5 仮想プロセッサー・コア (VPC)。
- Oracle 11g および 12c。

  Oracle データベースを使用する場合、Oracle 11g ドライバーを使用している場合は、trc.properties ファイルで oracle.increment.keys.off=1 を設定してください。サーバー・サービスを再起動します。

- Microsoft SQL Server 2008、2012、2014、2016、2017、2019。

  バージョンが 6.3 以上の JDBC ドライバーを使用する必要があります。古いバージョンでは、TLS1.2 または JRE8 はサポートされません。

  MS SQL データベースを使用する場合、Windows™ 認証はサポートされません。ドメイン・ユーザーを使用してログインすることはできません。混合モード認証を使用し、データベースに接続するための SQL ユーザーを作成する必要があります。

注: 少なくとも Java 8 をサポートする JDBC ドライバーを使用してください。

Derby バージョン10.13 は、Remote Control サーバーに付属しています。インストール時に Derby オプションを選択すると、Derby がローカル側にインストールされます。

注: Derby のインストールは、PoC 構成の場合のみにしてください。Derby は実稼働環境ではサポートされていません。

インストーラーを使用してサーバーをインストールするときに、WebSphere Application Server Liberty Profile バージョン 19.x.x.x もインストールされます。

サーバー環境のガイドライン

システム要件に加えて、ご使用の環境で使用するサーバー・インストールのタイプも判別する必要があります。以下の情報をガイドとして使用してください。

表 1. Remote Control サーバー・インストール・タイプ

サーバー・インストール・タイプ	インストールするコンポーネント	BigFix® コンソールを使用したインストール	インストール・ファイルを使用したインストール
1	組み込み Liberty プロファイル。組み込み Derby データベース	はい	はい
2	組み込み Liberty プロファイル (既にインストール済みの DB2®、MS SQL、または Oracle データベースを使用)	はい	はい

表 1. Remote Control サーバー・インストール・タイプ (続く)

サーバー・インストール・タイプ	インストールするコンポーネント	BigFix® コンソールを使用したインストール	インストール・ファイルを使用したインストール
3	WebSphere Application Server にアクセスするスタンドアロン Remote Control サーバー (既にインストール済みの DB2®、MS SQL、または Oracle データベースを使用)	いいえ	はい

注: サーバー・インストール・タイプ 1 および 2 は、Windows® または Linux® オペレーティング・システムを使用する場合のみ選択できます。

注: サーバー・インストール・タイプ 1 を使用するのは、PoC (概念検証) デプロイメントまたはテスト・デプロイメントの場合のみにしてください。

以下のセクションでは、環境サイズに基づいて、ガイドラインおよび推奨事項を示します。

小規模環境についてのガイドライン

ターゲットが 5,000 以下の環境では、サーバー環境のガイドラインで示したサーバー・インストール・タイプ 1 (PoC (概念検証) のみ) または 2 を使用できます。

以下の追加要件も考慮してください。

- プロセッサー: クワッド・コア・プロセッサー 1 個またはデュアル・コア・プロセッサー 2 個、2.40 GHz、およびサポート対象 OS。
- メモリー: 4 GB RAM。
- ストレージ。詳しくは、『サーバーの要件』を参照してください。
- ハートビート構成

表 2. ハートビート構成プロパティー: 小規模環境の推奨値

プロパティー `trc.properties`	値
heartbeat.timeout	60 **注:** パフォーマンスの問題がある場合は、値を 1440 (24 時間) に設定してください。例えば、レポートを多く使用する場合 (特に Derby で) です。 デフォルトは 60 (1 時間) です。
heartbeat.retry	10

プロパティー trc.properties	値
heartbeat.delay	20
heartbeat.on.wake	0
heartbeat.on.user.change	1
heartbeat.on.change	0
heartbeat.on.stop	0

注: インストール・タイプ 1 は、デモンストレーション・プロジェクトまたはパイロット・プロジェクトに適しています。インストール・タイプ 2 の方が高いパフォーマンスを発揮できるため、こうした環境の実動システムでは 2 を選択することをお勧めします。

中規模環境についてのガイドライン

環境に含まれるターゲット数が 5,000 から 75,000 までの場合、サーバー環境のガイドライン のサーバー・インストール・タイプ 2 または 3 を使用できます。パフォーマンスの点では、インストール・タイプ 2 が適しています。しかし、インストール・タイプ 3 では、インストール済みの WebSphere Application Server の管理機能も使用できます。

以下の追加要件も考慮してください。

- プロセッサー: クワッド・コア・プロセッサー 1 個またはデュアル・コア・プロセッサー 2 個、2.40 GHz。
- メモリー: 8 GB RAM。
- 記憶域: RAID 5 - 6 HDD。DB2、Oracle、もしくは MS SQL 64 ビットまたは 32 ビット。
- ハートビート構成 -

表 3. ハートビート構成プロパティー: 中規模環境の推奨値

プロパティー trc.properties	値
heartbeat.timeout	1440
heartbeat.retry	10

注: 定期的な更新を増やす必要がある特定のコンピューターのグループがある場合、それらの特定のターゲット・グループに対して、小さいハートビート・タイムアウト設定をグループ属性として適用できます。この属性のグループ・レベルでの設定について詳しくは、「*BigFix® Remote Control* 管理者ガイド」のターゲット・グループの作成方法に関する章を参照してください。

プロパティー trc.properties	値
	注: 環境に含まれるターゲット数が 75,000 に近づいている場合は、パフォーマンスを改善するために、この値を 20 に設定してください。
heartbeat.delay	20
	注: 環境に含まれるターゲット数が 75,000 に近づいている場合は、パフォーマンスを改善するために、この値を 40 に設定してください。
heartbeat.on.wake	0
heartbeat.on.user.change	1
heartbeat.on.change	0
heartbeat.on.stop	0

注: このタイプの環境では、ターゲットのデプロイメントを段階的に実行するようにしてください。デプロイメントを段階的に行うことにより、ターゲットがサーバーへの登録を試行するときに、サーバーが過負荷になることを回避できます。**RegistrationDelay** ターゲット・プロパティーには、ターゲット・コンピューターの登録操作がデプロイメントの各段階に均等に分散されるような値を設定してください。ターゲットの登録操作は、多数のコンピューターが一度に登録を試行することが回避されるよう、分散させてください。

大規模環境についてのガイドライン

環境に含まれるターゲット数が 75,000 から 225,000 までの場合、サーバー環境のガイドライン のサーバー・インストール・タイプ 3 を使用できます。

以下の追加要件も考慮してください。

WebSphere Application Server をホストするための要件

- プロセッサー: クアッド・コア・プロセッサー 2 個。 2.40 GHz、サポート対象 OS。
- メモリ: 16 GB の RAM。
- 記憶域: RAID 5 - 6 HDD。
- ハートビート構成 -

表 4. ハートビート構成プロパティー: 大規模環境の推奨値

プロパティー trc.properties	値
heartbeat.timeout	1440

プロパティー `trc.properties`	値
	注: 定期的な更新を増やす必要がある特定のコンピューターのグループがある場合、それらの特定のターゲット・グループに対して、小さいハートビート・タイムアウト設定をグループ属性として適用できます。この属性のグループ・レベルでの設定について詳しくは、「*BigFix® Remote Control* 管理者ガイド」のターゲット・グループの作成方法に関する章を参照してください。
heartbeat.retry	60
	注: 環境に含まれるターゲット数が 75,000 に近づいている場合は、パフォーマンスを改善するために、設定値を大きくしてください。
heartbeat.delay	60
	注: 環境に含まれるターゲット数が 75,000 に近づいている場合は、パフォーマンスを改善するために、設定値を大きくしてください。
heartbeat.on.wake	0
heartbeat.on.user.change	1
heartbeat.on.change	0
heartbeat.on.stop	0

- オプション: ネットワーク・カード 2 つ (ターゲット通信に 1 つ、データベース通信に 1 つ) があると、パフォーマンス・チューニングに役立つ可能性があります。

データベースをホストするための要件 (DB2®、Oracle、または MS SQL がサポート対象) は以下のとおりです。

- プロセッサー: クワッド・コア・プロセッサー 4 個、2.40 GHz。
- メモリー: データベース・サプライヤーの推奨に従う。
- 記憶域: RAID 5 - 6 HDD 146 GB

注: データベース管理者は、適切なパフォーマンスを実現するためにデータベースを調整する必要があります。

サイズの大きいレポートを使用する場合、性能低下が生じる可能性があるため、以下のガイドラインも考慮する必要があります。

- **「すべてのターゲット」**レポートがデフォルトのホーム・ページ・レポートにならないようにします。
- ターゲットが登録を試行するときにサーバーが過負荷になることを回避するため、ターゲットを段階的にデプロイするようにします。

  注: RegistrationDelay ターゲット・プロパティーには、ターゲット・コンピューターの登録操作がデプロイメントの各段階に均等に分散されるような値を設定してください。ターゲットの登録操作は、多数のコンピューターが一度に登録を試行することが回避されるよう、分散させてください。

注: LDAP を構成しており、LDAP 同期が有効な場合、同期の適切な頻度を設定してください。LDAP 構成が多数のユーザーおよびグループをインポートするようセットアップされている場合は、頻度を 24 時間に設定してください。LDAP の構成について詳しくは、LDAP の構成を参照してください。

コントローラーの要件

コントローラーは Java™ ベースのアプリケーションであり、記載の前提条件を満たす、以下のオペレーティング・システム上で実行できます。

オペレーティング・システムのサポート

以下のオペレーティング・システムがサポートされています。

- Windows™ 7
- Windows™ 8 および 8.1
- Windows™ 10
- Windows™11
- Windows™ Server 2012
- Windows™ Server 2012 R2
- Windows™ Server 2016
- Windows™ Server 2019
- Windows™ サーバー 2022
- Red Hat Enterprise Linux™ 6.0 以降
- Red Hat Enterprise Linux™ 7.0 以降
- Red Hat Enterprise Linux™ 8.0 以降
- SUSE Linux™ Enterprise Server 10 以降
- SUSE Linux™ Enterprise Server 11 以降
- SUSE Linux™ Enterprise Desktop 10 以降
- SUSE Linux™ Enterprise Desktop 11 以降
- CentOS 5.0 以降
- CentOS 6.0 以降

- macOS 10.14 Mojave
- macOS 10.14 Catalina
- macOS 11.x BigSur
- macOS 12.x Monterey

前提条件

- Oracle Java™ SE Runtime Environment 8 または IBM® Java™ SE Runtime Environment 8。

注: Oracle Java™ は、FIPS または NIST SP800-131a モードではサポートされません。このモードでは、IBM® Java™ を使用する必要があります。

ターゲットの要件

最小必要要件

Remote Control ターゲットをインストールするコンピューターは、最低でも以下の仕様を持つ必要があります。

- 1 GHz Intel™® 以上または AMD プロセッサー。
- 最低 1 ギガバイト (GB) の RAM (32 ビット) または 2 GB の RAM (64 ビット)。
- 最小 50 MB のハード・ディスク・スペース。
- セッションのビデオ録画を格納するための適切なスペース。録画はハード・ディスクに格納され、サイズはセッションの所要時間と画面アクティビティーによって異なります。平均すると、8 ビット・モードの 5 分間のセッションでおよそ 2 MB のスペースが使用される可能性があります。トゥルー・カラーの 24 ビット・モードの場合、録画にこれよりも多くのスペースが使用される可能性があります。
- ディスプレイごとの最大ディスプレイ解像度は、7680 ピクセル x 4320 ピクセルです。
- ディスプレイの最大数は、8 x 8 です。

ネットワーク要件

Remote Control をインストールする前に、以下のネットワーク要件が満たされていることを確認してください。

- ターゲット・ポート 888 (または Remote Control セッション用に構成されているその他のポート) への着信 TCP 接続をファイアウォール・ルールで許可する必要があります。
- 49152 ～ 65535 のポート上の `trc_base`、 `trc_gui`、`trc_dsp`、`trc_ft` 間のローカルホスト・ループバック・アドレス 127.0.0.1 のトラフィックを許可する必要があります。

注: アンチウィルス・ソフトウェアまたは侵入検知システム・ソフトウェアも、このトラフィックをブロックする可能性があります。

オペレーティング・システムのサポート

以下のオペレーティング・システムがサポートされています。

- Windows™ 7
- Windows™ 8 および 8.1
- Windows™ 10
- Windows™11
- Windows™ Server 2012
- Windows™ Server 2012 R2
- Windows™ Server 2016
- Windows™ Server 2019
- Windows™ サーバー 2022
- Red Hat Enterprise Linux™ 6.0 以降
- Red Hat Enterprise Linux™ 7.0 以降
- SUSE Linux™ Enterprise Server 10 以降
- SUSE Linux™ Enterprise Server 11 以降
- SUSE Linux™ Enterprise Desktop 10 以降
- SUSE Linux™ Enterprise Desktop 11 以降
- CentOS 5.0 以降
- CentOS 6.0 以降
- macOS 10.14 Mojave
- macOS 10.15 Catalina
- macOS 11.x BigSur
- macOS 12.x Monterey

注: macOS 11.1 では、モニター画面の解像度が以下のいずれかに設定されていることを確認してください。1280 x 768、1280 x 800、1280 x 1024、1360 x 768、1440 x 900、1600 x 900、1680 x 1050、1920 x 1080、または 2880 x 1800。これは、以下の画面解像度を使用すると、リモート・セッション中にコントローラーに黒い画面が表示される可能性があるためです。1400 x 1050、1768 x 992。

サポートされるアーキテクチャー

- Intel™ IA®-32 (x86, x86-32 とも呼ばれます)
- Intel™ 64 または AMD64 (x64、x86-64、EM64T とも呼ばれます)
- Apple シリコン

注: IA®-64 (Itanium™とも呼ばれる) プロセッサーはサポートされていません。

ゲートウェイの要件

Remote Control ゲートウェイのインストール先であるコンピューターは、最低でも以下のアイテムまたは仕様を備えている必要があります。

1. 最低 1 GHz の Intel® または AMD プロセッサー。
2. 最低 1 ギガバイト (GB) の RAM (32 ビット) または 2 GB の RAM (64 ビット)
3. 最小 50 MB のハード・ディスク・スペース。

オペレーティング・システムのサポート

以下のオペレーティング・システムがサポートされています。

- Windows™ Server 2012
- Windows™ Server 2012 R2
- Windows™ Server 2016
- Windows™ Server 2019
- Windows™ サーバー 2022
- Red Hat Enterprise Linux™ 6.0 以降
- Red Hat Enterprise Linux™ 7.0 以降
- Red Hat Enterprise Linux™ 8.0 以降
- SUSE Enterprise Linux™ Server 10 以降
- SUSE Enterprise Linux™ Server 11 以降
- SUSE Linux™ Enterprise Desktop 10 以降
- SUSE Linux™ Enterprise Desktop 11 以降
- CentOS 5.0 以降
- CentOS 6.0 以降

サポートされるアーキテクチャー

- Intel™ IA-32 (x86、x86-32 とも呼ばれます)
- Intel™ 64 または AMD64 (x64、x86-64、EM64T とも呼ばれます)

注: IA-64 (Itanium™とも呼ばれます) プロセッサーはサポートされていません。

ブローカーの要件

Remote Control ブローカーをインストールするコンピューターは、最低でも以下のアイテムまたは仕様を持つ必要があります。

1. 最低 1 GHz の Intel® または AMD プロセッサー。
2. 最低 1 ギガバイト (GB) の RAM (32 ビット) または 2 GB の RAM (64 ビット)
3. 最小 50 MB のハード・ディスク・スペース。
4. セッションのビデオ録画を格納するための適切なスペース。録画はハード・ディスクに一時的に格納され、サイズはセッションの所要時間と画面アクティビティーによって異なります。平均すると、8 ビット・モードの 5 分間のセッションでおよそ 2 MB のスペースが使用される可能性があります。トゥルー・カラーの 24 ビット・モードの場合、録画にこれよりも多くのスペースが使用される可能性があります。

オペレーティング・システムのサポート

以下のオペレーティング・システムがサポートされています。

- Windows™ Server 2012
- Windows™ Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows™ サーバー 2022
- Red Hat Enterprise Linux™ 6.0 以降
- Red Hat Enterprise Linux™ 7.0 以降
- Red Hat Enterprise Linux™ 8.0 以降
- SUSE Linux™ Enterprise Server 10 以降
- SUSE Linux™ Enterprise Server 11 以降
- CentOS 5.0 以降
- CentOS 6.0 以降

サポートされるアーキテクチャー

- Intel™ IA-32 (x86、x86-32 とも呼ばれます)
- Intel™ 64 または AMD64 (x64、x86-64、EM64T とも呼ばれます)

注: IA-64 (Itanium™とも呼ばれます) プロセッサーはサポートされていません。

はじめに

ここまで、Remote Control の用語、および使用可能なコンポーネントについて説明してきました。これで、インストールする必要のあるコンポーネントを特定することができます。

表 5. インストールするコンポーネントの判別

要件	ターゲット	コントローラー	サーバー	ゲートウェイ	ブローカー
他のユーザーがこのコンピューターにリモートで接続できるようにする。	はい	はい			
Remote Control コンソールを使用するか、スタンドアロン・コントローラーを起動して、他のコンピューターにリモートで接続する。	はい	はい			

表 5. インストールするコンポーネントの判別（続く）

要件	ターゲット	コントローラー	サーバー	ゲートウェイ	ブローカー
ユーザーとターゲット、およびそれらのポリシーを一元管理する。	はい	オプション *	はい		
監査および記録の一元的リポジトリーを維持する。	はい	オプション *	はい		
自社のインフラストラクチャー内のファイアウォールをトラバースする。	はい	オプション *	はい	はい	
自社のネットワーク外のターゲットに接続する。	はい	オプション *	はい	可 **	はい

* 管理対象環境では、コントローラー・ユーザーが Remote Control サーバー・インターフェースからリモート・コントロール・セッションを開始します。この方法でセッションを開始する場合は、コントローラー・コンポーネントを別個にインストールする必要はありません。Remote Control サーバー・インターフェースでは、Java Web Start コントローラー・コンソールが、コンテキストに応じて起動されます。

** ブローカー・デプロイメントでは、ゲートウェイは厳密に必要というわけではありませんが、ゲートウェイがあるとセキュリティーが向上します。

Remote Control コンポーネントのインストール

Remote Control コンポーネントは 2 とおりの方法でインストールできます。BigFix® コンソールにアクセスできる場合は、適用 Fixlet を使用してコンポーネントをインストールします。

詳しくは、*BigFix® Remote Control* コンソール・ユーザー・ガイド を参照してください。もう 1 つの方法は、コンポーネントのインストール・ファイルを使用する方法です。

インストール・ファイルはさまざまな方法で取得できます。適切な方法を選択してファイルを入手してください。各種コンポーネントのインストール時に守られる必要のある順序は、特にありません。

インストール・ファイルの入手

Remote Control コンポーネントをインストールするためにインストール・ファイルはさまざまな方法で入手できます。

HCL License & Delivery Portal

Remote Control コンポーネントをインストールするには、Flexnet Operations (HCL License & Delivery Portal) から以下のイメージを使用します。詳しくは、HCL ソフトウェアのナレッジ記事 KB0010149 を参照してください。

注:

IBM Passport Advantage® および Fix Central®は、FlexNet Operations®に置き換えられました。

表 6. Remote Control のインストールに必要な部品

部品番号	ファイル名
Windows™ オペレーティング・システム CNJ05ML - BIGFIX REM CNTRL V10 IMAGE1。	`Bigfix_Rem_Cntrl_V10_Image_1.zip`
Linux™ オペレーティング・システム CNJ06ML - BIGFIX REM CNTRL V10 IMAGE2。	`Bigfix_Rem_Cntrl_V10_Image_2.tar`
Windows™、 Linux™、macOS オペレーティング・システム CNJ07ML - BIGFIX REM CNTRL V10 IMAGE3。	`Bigfix_Rem_Cntrl_V10_Image_3.tar`

オペレーティング・システムおよびインストールするコンポーネントに応じて、必要なイメージ・ファイルを判別します。

`BIGFIX_REM_CNTRL_V10_Image_1.zip`

Windows™ オペレーティング・システム・コンポーネントのインストール・ファイルは、このイメージ・ファイルから解凍します。Windows™ オペレーティング・システム実行可能ファイルは `\windows` ディレクトリーにあります。

`BIGFIX_REM_CNTRL_V10_Image_2.tar`

Linux™ サーバー・コンポーネントのインストール・ファイルは、このイメージ・ファイルから解凍します。この `trc_server_setup.bin` のファイルは `\linux` のディレクトリーにあります。他の Linux™ コンポーネント用のインストール・ファイルにアクセスするには、`Bigfix_Rem_Cntrl_V10_Image_3.tar` ファイルを使用します。

`BIGFIX_REM_CNTRL_V10_Image_3.tar`

`BigFix_Rem_Cntrl_V10_Image_3.tar` ファイルからデータを抽出します。*platform* ご使用のオペレーティングシステムに関連する `\Disk1\InstData\`*`platform`*`\VM` ディレクトリーに移動します。追加のセットアップは、Windows™ および Linux™ システムでのみ実行できます。macOS コンポーネント用のインストール・ファイルを解凍するには、このユーティリティーを a Windows™ または Linux™ システムで実行した後、`.pkg` ファイルを macOS システムにコピーしてください。追加のセットアップ・ユーティリティーの実行について詳しくは、追加のセットアップ・ユーティリティーを使用したインストール・ファイルの解凍を参照してください。

サーバー UI からのファイルのダウンロード

Remote Control サーバーをインストールする場合は、ターゲット、コントローラー、および cli コンポーネント用のインストール・ファイルをダウンロードすることができます。コントローラーのインストール・ファイルは、 標

準のコントローラーのものです。FIPS 準拠のコントローラーのインストール・ファイルの場合は、 追加セットアップ・ユーティリティーを使用してください。

1. **「ツール」「ダウンロード」**をクリックします。
2. **「エージェント・ダウンロード」**を選択します。
3. 適切なコンポーネント・ファイルを選択します。

サーバーのインストール

Remote Control サーバーでサポートされているインストール・タイプは以下のとおりです。

表 7. サーバー・インストール・タイプ

自動インストール (詳しくは、サーバー・インストーラーを使用したインストールを参照してください)	**手動インストール (詳しくは、WebSphere Application Server バージョン 8.5.5 へのインストールWAR ファイルのデプロイを参照してください)**
Windows® オペレーティング・システムおよび Linux オペレーティング・システムで使用可能。	AIX オペレーティング・システム、Solaris オペレーティング・システム、および WebSphere Application Server 8.5 がサポートしているすべてのオペレーティング・システムで使用可能。
Derby を組み込みとしてインストールするか、既存のサポート対象データベースを使用。ローカルまたはリモート。	データベースの作成が必要、または既存のサポート対象データベースを使用可能。
すべての組み込みコンポーネントが、同じコンピューターに、ローカルにインストールされる。	データベースは、別のコンピューターにインストール可能。

注: 組み込み Derby データベースは、実動ではサポートされていません。

データベースのセットアップ

データベースをセットアップする前に、データベース・ソフトウェアをインストールして、Remote Control のデータベースを保持するインスタンスを作成します。

DB2® のセットアップ

DB2® のデータベースのセットアップを行うには、以下のステップを実行します。Windows® オペレーティング・システムを使用している場合は、ステップ 2 から開始してください。Linux® オペレーティング・システムまたは AIX® オペレーティング・システムを使用している場合は、ステップ 1 から始めてください。

1. TCP/IP を使用してリモート接続を行うための準備が DB2® およびインスタンスで完了しているどうか確認するために、以下のステップを実行します。

   a. `db2 get database manager configuration` を実行して、**svcename** の値が有効なポートになっているかどうかを確認します。

   ```
   for example 50000


   or a reference mapped to a valid port
   for example,db2c_db2inst1.
   ```

   b. 構成されたポートが、システム内の他のプロセスによって使用されていないこと、またはアプリケーション・サーバー・ホストと DB2® サーバーの間にあるファイアウォールによってブロックされていないことを確認します。

   c. `db2stop` コマンドを使用して、DB2® インスタンスを停止します。

   以下のコマンドを使用して、**DB2COMM** を tcpip に設定します。

   ```
   db2set DB2COMM=tcpip
   ```

   db2start を実行して、DB2® インスタンスを再開します。

   これで、DB2® サーバーはネットワーク全体にわたるアクセスを実行できるようになりました。
2. 以下のコマンドをインスタンス所有者として実行して、Remote Control が使用するデータベースを作成します。

   注: データベースがローカルの場合は不要です。

   ```
   db2 create db databasename using codeset UTF-8 territory requiredtrerritory
   ```

   ここで、*databasename* は、データベースに付ける必要のある名前です。このデータベース名は、構成設定で参照されている名前にする必要があります。例えば、「TRCDB」などと入力します。

   requiredtrerritory は、必要な地域です。例えば、グレートブリテン島の場合は GB です。
3. データベースの特定のユーザーが保持する必要のある特権を確認します。
   db2inst1 ユーザーは、 Remote Control データベースにアクセスするように構成するユーザーとしては使用しないでください。データベース所有者特権を持つ、DB2® の新しい特定のユーザーを作成してください。

これで、空のデータベースが作成され、使用できるようになりました。次のステップでは、WebSphere® サーバーをセットアップします (アプリケーション・サーバーのセットアップ参照)。DB2® クライアントを使用して別のホストからデータベースに接続することで、データベースが正しくセットアップされているかどうか検証することができます。詳しくは、DB2® のインフォメーション・センターを参照してください。

Oracle のセットアップ

Remote Control で使用できるよう Oracle をセットアップするには、データベースを作成してから、データベースのアクセス許可をセットアップします。

データベースの作成

Oracle Database Configuration Assistant を実行して、データベースを作成します。

Remote Control に使用する Oracle データベースを作成するには、以下のステップを実行します。

1. Oracle Database Configuration Assistant を実行します。

   Windows® システム

   操作の一例:**「スタート」「すべてのプログラム」「Oracle」「構成およびマイグレーション・ツール (Configuration and Migration Tools)」「Database Configuration Assistant」**を選択します。

   UNIX®ベースのシステム

   `$ORACLE_HOME/bin` ディレクトリーからコマンド dbca を入力します。

2. 「ようこそ」画面で**「次へ (Next)」**をクリックします。
3. **ステップ 1**:**「データベースの作成 (Create a Database)」**を選択します。「**次へ**」をクリックします。
4. **ステップ 2**: テンプレートとして**「汎用 (General Purpose)」**を選択します。「**次へ**」をクリックします。
5. **ステップ 3**:
   a. データベースの名前を指定します。例えば、「TRCDB」などと入力します。
   b. データベースを参照するときに使用する SID を指定します。例えば、「TRCDB」などと入力します。

   「**次へ**」をクリックします。
6. **ステップ 4**: 必要なデータベース管理オプションを選択します。例えば、**「データベース管理用のデータベース・コントロールを使用 (Use Database Control for Database Management)」**を選択します。「**次へ**」をクリックします。
7. **ステップ 5**: データベースのパスワードを指定し、パスワードを確認します。例えば、「dboracle」などと入力します。「**次へ**」をクリックします。
8. **ステップ 6**: データベースを保管する場所を指定します。例えば、「ファイル・システム (File System)」を選択します。「**次へ**」をクリックします。
9. **ステップ 7**: データベース・ファイルの場所を指定します。例えば、「テンプレートのデータベース・ファイルの場所を使用 (Use Database File Locations from Template)」を選択します。「**次へ**」をクリックします。
10. **ステップ 8**: データベースのリカバリー・オプションを選択します。「**次へ**」をクリックします。
11. **ステップ 9**:「データベース・コンテンツ (Database Content)」ウィンドウで、**「次へ (Next)」**をクリックします。
12. **ステップ 10**:「初期設定パラメーター (Initialization Parameters)」画面で、**「文字セット (Character Sets)」**タブを選択します。
    a. 必要を満たしたデータベースの文字セットを選択します。
    b. 「**次へ**」をクリックします。

13. Oracle 11g を使用している場合は、以下の 2 つのステップも必要です。
    a. 「セキュリティー設定 (Security Settings)」。11g の拡張されたデフォルトのセキュリティー設定を受け入れます。
    b. 「自動保守タスク (Automatic Maintenance Tasks)」。自動保守タスクを有効にします。
14. **ステップ 11**:「データベース・ストレージ」ウィンドウで、**「次へ」**をクリックします。
15. **ステップ 12**: 必要な作成オプションを選択します。「**終了**」をクリックします。
16. 確認画面で**「OK」**をクリックして、データベースの作成を開始します。

    注: 作成処理は複数の段階に分けて実行されるため、時間がかかる場合があります。

17. データベースの作成が完了したら、**「終了」**をクリックします。

Remote Control に使用する Oracle データベースが作成されます。

データベースのアクセス許可のセットアップ

Remote Control に使用する Oracle データベースを作成したら、そのデータベースのアクセス許可を構成する必要があります。

データベースのアクセス許可を構成するには、以下のステップを実行します。

1. Oracle SQL*Plus を実行します。

   Windows® システム

   例:**「スタート」 > 「プログラム」 > 「Oracle-OraHomeName」 > 「アプリケーション開発 (Application Development)」 > 「SQL Plus」**をクリックします。

   または、コマンド・プロンプトで以下のコマンドを入力します。

   sqlplusw

   データベースのユーザー名とパスワードを使用してログオンし、**「OK」**をクリックします。ユーザー名とパスワードがない場合は、データベース・システムの管理者に問い合わせてください。

   以下に例を示します。

   ユーザー名 - system

   パスワード - dboracle

   Linux® システム

   UNIX® または Windows® 端末を開き、以下の SQL*Plus コマンドを入力します。

   sqlplus *username* / *password* *@connect_identifier*

   username および *password* は、データベースへの接続に必要なデータベースの資格情報です。

connect_identifier は、特定のデータベースに必要な接続です。

例えば、「@TRCDB as SYSDBA」などと指定します。

@//*servername*:*port*/*DatabaseSID* as SYSDBA

servername は、Oracle のインストール済み環境が存在するシステムのサーバー名または IP アドレスです。

port は、Oracle のインストール済み環境が存在するシステムのポートです。

DatabaseSID は、作成したデータベースに定義された SID です。

SQL*Plus の実行可能ファイルは `$ORACLE_HOME/bin` にインストールされます。このパスは、オペレーティング・システムの PATH 環境変数に追加されます。SQL*Plus を開始するために、`$ORACLE_HOME/bin` ディレクトリーに移動することが必要になる場合があります。

2. SQL*Plus が開始され、データベースに接続されたら、必要なユーザーを作成して、アクセス許可を付与できます。ユーザーを作成してアクセス許可を付与する方法は 2 種類あります。適切な方法を選択してユーザーを作成してください。

Oracle 内でユーザー ID を 1 つ作成して、これを Remote Control へのログオンにも使用する

単一のユーザーを作成します。ユーザー ID は Asset とする必要があります。このユーザー ID を使用するのは、Remote Control です。これにより、データベースを作成し、データベースにログオンし、データベースを使用します。

以下のコマンドを実行して、ユーザー ASSET を作成します。

a. connect SYS/PASSWORD@DATABASE AS SYSDBA;

   ここで、*PASSWORD* は、Oracle のデフォルトのユーザー・パスワードです。

   また、*DATABASE* は、データベースの作成時に定義したデータベース名です。例えば、TRCBD などです。

b. CREATE USER ASSET IDENTIFIED BY PASSWORD DEFAULT TABLESPACE users TEMPORARY TABLESPACE temp;

   注: PASSWORD は、ユーザー ASSET の必要に応じた内容に変更できます。

c. GRANT UNLIMITED TABLESPACE TO ASSET;
d. GRANT CONNECT TO ASSET;
e. GRANT CREATE INDEXTYPE TO ASSET;
f. GRANT CREATE SEQUENCE TO ASSET;
g. GRANT CREATE TABLE TO ASSET;
h. GRANT CREATE TRIGGER TO ASSET;

i. GRANT CREATE INDEXTYPE TO ASSET;
j. GRANT CREATE PROCEDURE TO ASSET;
k. GRANT CREATE VIEW TO ASSET;
l. GRANT ANALYZE ANY TO ASSET;

Remote Control にログオンするために、別個のユーザー ID を作成する

2 つのユーザーを作成します。ユーザー 1 の ID は Asset とする必要があります。このユーザーは特定のアクセス許可を持たず、スキーマ名としてのみ使用されます。ユーザー 2 はメインのユーザーであり、任意の ID を付けることができます。このユーザーを使用するのは、Remote Control です。これにより、データベースを作成し、データベースにログオンし、データベースを使用します。アシスタント・ツールを使用して、ユーザー TRCDBU を作成します。

ユーザー TRCDBU に必要なアクセス許可を作成するには、以下のステップを実行します。

a. GRANT UNLIMITED TABLESPACE TO ASSET;
b. GRANT UNLIMITED TABLESPACE TO TRCDBU;
c. GRANT ALTER ANY INDEX TO TRCDBU ;
d. GRANT ALTER ANY INDEXTYPE TO TRCDBU ;
e. GRANT ALTER ANY PROCEDURE TO TRCDBU ;
f. GRANT ALTER ANY SEQUENCE TO TRCDBU ;
g. GRANT ALTER ANY TABLE TO TRCDBU ;
h. GRANT ALTER ANY TRIGGER TO TRCDBU ;
i. GRANT COMMENT ANY TABLE TO TRCDBU ;
j. GRANT CREATE ANY INDEX TO TRCDBU ;
k. GRANT CREATE ANY INDEXTYPE TO TRCDBU ;
l. GRANT CREATE ANY SEQUENCE TO TRCDBU ;
m. GRANT CREATE ANY TABLE TO TRCDBU ;
n. GRANT CREATE ANY TRIGGER TO TRCDBU ;
o. GRANT CREATE INDEXTYPE TO TRCDBU ;
p. GRANT CREATE PROCEDURE TO TRCDBU ;
q. GRANT CREATE SEQUENCE TO TRCDBU ;
r. GRANT CREATE TABLE TO TRCDBU ;
s. GRANT CREATE TRIGGER TO TRCDBU ;
t. GRANT CREATE VIEW TO TRCDBU ;
u. GRANT DELETE ANY TABLE TO TRCDBU ;
v. GRANT INSERT ANY TABLE TO TRCDBU;
w. GRANT DROP ANY INDEX TO TRCDBU ;
x. GRANT DROP ANY INDEXTYPE TO TRCDBU ;
y. GRANT DROP ANY PROCEDURE TO TRCDBU ;
z. GRANT DROP ANY SEQUENCE TO TRCDBU ;
aa. GRANT DROP ANY TABLE TO TRCDBU ;
ab. GRANT DROP ANY TRIGGER TO TRCDBU ;
ac. GRANT EXECUTE ANY INDEXTYPE TO TRCDBU ;

ad. GRANT EXECUTE ANY LIBRARY TO TRCDBU ;
ae. GRANT EXECUTE ANY TYPE TO TRCDBU ;
af. GRANT SELECT ANY SEQUENCE TO TRCDBU ;
ag. GRANT SELECT ANY TABLE TO TRCDBU ;
ah. GRANT UNLIMITED TABLESPACE TO TRCDBU ;
ai. GRANT UPDATE ANY TABLE TO TRCDBU;
aj. GRANT ANALYZE ANY TO TRCDBU;

MS SQL のセットアップ

Remote Control で使用できるよう MS SQL をセットアップするには、データベースを作成してから、データベースのアクセス許可をセットアップします。

データベースの作成

MS SQL Management Studio を使用して、以下のステップを実行します。

1. **「接続」**をクリックします。
2. **サーバー・ツリー**を右クリックし、**「プロパティ」**をクリックします。
3. **「セキュリティ」**を選択します。
4. SQL Server と認証モードが選択されていることを確認します。
5. **サーバー・ツリー**を展開します。
6. **「データベース」**を右クリックします。
7. **「新しいデータベースを作成する」**を選択します。
8. データベースの名前を入力します。例えば、「TRCDB」などと入力します。「**OK**」をクリックします。

データベースのデフォルトの所有者は、ユーザー *sa* (システム管理者) です。Remote Control で使用するデータベースの所有者となる新規ユーザーを作成します。

データベースのアクセス許可

デフォルトのシステム管理者は、データベースの所有者であるため、データベースを使用するために必要なアクセス許可を保持しています。新規ユーザーを作成し、そのユーザーをデータベースの所有者に割り当てた場合は、そのユーザーも必要なアクセス許可を保持しています。

サーバー・インストーラーを使用したインストール

Remote Control サーバー・インストーラーは、Windows™ オペレーティング・システム、Red Hat Linux™ オペレーティング・システム、および SUSE Linux™ オペレーティング・システムで使用できます。以下のいずれかのコンポーネント設定を備えた、完全に機能する自己完結型のサーバーがインストールされます。

- WebSphere® Application Server Liberty Profile バージョン および Derby データベースを備えた Remote Control サーバー。
- WebSphere® Application Server Liberty Profile バージョン および以下のいずれかのデータベースを備えた Remote Control サーバー。
    - IBM DB2 11.5 仮想プロセッサー・コア (VPC)。
    - Oracle 11g および 12c。

      Oracle データベースを使用する場合、Oracle 11g ドライバーを使用している場合は、trc.properties ファイルで oracle.increment.keys.off=1 を設定してください。サーバー・サービスを再起動します。
    - Microsoft SQL Server 2008、2012、2014、2016、2017、2019。

      バージョンが 6.3 以上の JDBC ドライバーを使用する必要があります。古いバージョンでは、TLS1.2 または JRE8 はサポートされません。

      MS SQL データベースを使用する場合、Windows™ 認証はサポートされません。ドメイン・ユーザーを使用してログインすることはできません。混合モード認証を使用し、データベースに接続するための SQL ユーザーを作成する必要があります。

インストールされるコンポーネントのサポート対象バージョンについて詳しくは、サーバーの要件を参照してください。

注: インストールを終了するには、 随時**「キャンセル」**をクリックします。

おおよそのインストール時間

- インストーラーでのオプションの指定: 5 〜 10 分。
- ソフトウェアのインストール: 5 分。

1. インストーラーを使用するときは、画面解像度 1024 x 768 ピクセル以上をお勧めします。
2. Linux™ オペレーティング・システムの場合は、オペレーティング・システムをインストールして構成するときに **libstdc++.so.5** をインストールする必要があります。このパッケージがインストールされていない場合は、パッケージ **compat-libstdc++-33** (**libstdc++.so.5** が含まれている) をインストールすることができます。

注:

- コンソール・モード・インストールはサポートされていません。
- サーバー・インストールのファイル・コピー・フェーズ中:
    - 既存のインストールのバックアップ・コピーが保存されます。アップグレードするインストール済み環境に問題が発生した場合に、この機能が役立ちます。
    - 次のディレクトリーが存在している場合は削除されます。

[INSTALLDIR]/trcserver.bak.

- 現在のサーバーのインストール [INSTALLDIR]/wlp/usr/servers/trcserver は、名前が変更されるか、[INSTALLDIR]/trcserver.bak に移動されます。

このバックアップ・ディレクトリーにアクセスして、前のインストールのすべての内容を復元またはリカバリーできます。

Remote Control サーバー・アプリケーションをインストールするには、 以下の手順を実行します。

1. ご使用のオペレーティング・システムに該当するサーバー・インストール・ファイルを実行します。

   Windows™ システム

   trc_server_setup.exe

   Linux™ システム

   trc_server_setup.bin

   インストール・ファイルを入手するには、インストール・ファイルの入手を参照してください。
2. 言語を選択して、**「OK」**をクリックします。
3. **「概要」**ウィンドウで **「次へ」**をクリックします。
4. クリックして IBM® および IBM® 以外のご使用条件に同意し、**「次へ」**をクリックします。
5. デフォルトの場所を受け入れるか、**「選択」**をクリックしてインストール・ファイルの場所を定義し、**「次へ」**をクリックします。

   注: WebSphere® Application Server は、名前に非英語文字が含まれているディレクトリーにはインストールできません。このインストールでは、組み込みバージョンの WebSphere® Application Server がインストールされます。そのため、インストール・ファイルの宛先として、名前に非英語文字が含まれないものを選択してください。

6. データベースを選択し、**「次へ」**をクリックします。

   注: アプリケーションには Derby が組み込まれており、Derby が選択された場合にローカル環境にインストールされます。DB2® または Oracle を使用するには、それらをインストールし、データベース・インスタンスを作成してから、Remote Control をインストールする必要があります。

7. 選択したデータベースに応じてオプションを入力し、**「次へ」**をクリックします。

   Derby

   a. データベースの名前を指定し、**「次へ」**をクリックします。例えば、TRCDB です。

      注: 既存のデータベースを使用する場合は、データベースを除去することを選択できます。

DB2®

データベース・サーバー

データベース・サーバーの IP アドレスまたはホスト名。

注: DB2® がローカルにインストールされている場合、127.0.0.1を使用できます。DB2® がリモート・システムにインストールされている場合は、リモート・システムの IP アドレスを入力します。

Port (ポート)

DB2® がインストールされているポート。

注:

a. Windows™® システムの場合、デフォルト・ポートは 50000 です。Linux™ システムの場合、デフォルト・ポートは 50001 です。
b. リモート DB2® インストールは、タイプ 4 接続に制限されます。ローカル・インストールではタイプ 2 または 4 を使用できます。タイプ 2 接続ではポート値を 0 に設定します。

管理者ユーザー ID

データベースにログオンするときに使用する管理者ユーザー ID を指定します。このユーザー ID は、データベースへの管理アクセス権限を持っている必要があります。

「データベースの作成」を選択する場合は、ユーザー ID が DB2® に対する管理者権限を持っている必要があります。

管理者パスワード

データベースに接続するための管理者パスワードを指定します。

データベース名

データベースの名前を指定します。例えば、`TRCDB` です。

注: リモート・データベースを使用する場合は、リモート・システムに作成したデータベースの名前を入力します。

db2jcc.jar ファイルのディレクトリー・パス (Directory path to db2jcc.jar file)

DB2® JAR ファイル、`db2jcc.jar`、 および `db2jcc_license.jar` へのパスを指定します。

注: リモート・データベースを使用する場合は、DB2® の JAR ファイルの格納先ドライブをリモート・システムで共有します。その共有ドライブのロケーションを入力します。

データベースの作成

DB2® がローカル (127.0.0.1) にインストールされている場合は、インストール中にブランク・データベースを作成することを選択できます。既存のローカル・データベースを除去して新規データベースを作成することも選択できます。

注: リモート・データベースを使用する場合は、データベースの作成とデータベースの除去のいずれも選択しないでください。

データベースをインストールするパス (Path for database install)

データベースをインストールできる場所のパスを指定します。インストール済み環境がローカルであり、データベースの作成を選択した場合は、指定された管理ユーザーが適切な権限を持っていなければなりません。Windows™ システムでは db2admin ユーザーを使用します。Linux™ システムでは、ユーザーがグループ db2grp1 のメンバーであることが必要です。

注:

Linux™ システム

管理ユーザー ID が読み取り権限および書き込み権限を持つディレクトリーを指定します。

Windows™ システム

ドライブ名を指定します。

Oracle

データベース・サーバー

ご使用のデータベース・サーバーの IP アドレスまたはホスト名。ローカルに Oracle がインストールされている場合は、127.0.0.1 を使用できます。Oracle がリモート・システムにインストールされている場合は、リモート・システムの IP アドレスを入力します。

ポート\n

Oracle がインストールされているポート。

管理者ユーザー ID

データベースにログオンするときに使用する管理者ユーザー ID を指定します。このユーザー ID は、データベースへの管理アクセス権限を持っている必要があります。

注: Oracle のインストール済み環境では、 **asset** というユーザーが存在していなければなりません。このユーザー ID をここで使用することも、既存または新規のユーザーを使用することもできます。

管理者パスワード

データベースに接続するための管理者パスワードを指定します。

データベース名

データベースの名前を指定します。この名前は、`tnsnames.ora` 内の名前ではなく、サーバーでの SID 名です。例えば、`TRCDB` です。

Oracle Java JDBC ライブラリーのディレクトリー・パス (Directory path to the oracle Java JDBC library)

oracle Java™ JDBC ライブラリーへのパスを指定します。ロケーションは、Oracle サーバーのインストール済み環境から取得するか、Oracle Web サイトからダウンロードできます。例えば、 `c:\oracle\ora92\jdbc\lib\ojdbc14.jar`

MSSQL

データベース・サーバー

データベース・サーバーの IP アドレスまたはホスト名。

注: MS SQL が Windows™ システム上にローカルにインストールされている場合のみ、127.0.0.1 を使用できます。

ポート\n

MS SQL がインストールされているポート。

管理者ユーザー ID

データベースにログオンするときに使用する管理者ユーザー ID を指定します。このユーザー ID は、データベースに対する管理アクセス権限を持っている必要があります。

管理者パスワード

データベースに接続するための管理者パスワードを指定します。

データベース名

データベースの名前を指定します。例えば、`TRCDB` です。

MS JDBC Java ファイルのディレクトリー・パス (Directory path to the MS JDBC Java files)

MS JDBC Java ファイルへのパスを指定します。使用している MS SQL データベースのバージョンに応じて、`mssql-jdbc-X.X.X.jre8.jar` ファイルを使用する必要があります。

同じサーバーにインストール済みの場合、データベースの作成を選択

MS SQL がローカル環境にインストールされている場合は、データベースを作成することを選択できます。

ローカルにインストール済みのデータベースを除去

「データベース名」に入力した名前のデータベースが既に存在するが、そのデータベースを使用しない場合に選択します。

ローカルの場合、データベースを作成するパスを選択します

データベースのインストール・パスを指定します。インストール済み環境がローカルであり、データベースの作成を選択した場合は、管理ユーザーがこの処理を行うための適切な権限を持っていなければなりません。

Linux™ システム。

管理ユーザー ID が読み取り権限および書き込み権限を持つディレクトリーを指定します。

Windows™ システム。

既存のディレクトリーを指定します。

8. Web サーバーのパラメーターを指定し、**「次へ」**をクリックします。

ターゲットで強制的に HTTPS を使用 (Force targets to use HTTPS)

ターゲット・ソフトウェアが HTTPS URL を使用してサーバーと通信する場合、このオプションを選択します。`trc.properties` ファイル内の **enforce.secure.endpoint.callhome** プロパティーと **enforce.secure.endpoint.upload** プロパティーも *true* に設定されています。新規インストールではこのチェック・ボックスはデフォルトで選択されています。

HTTPS によるログオンおよび Web ポータルへのアクセスを有効にする **enforce.secure.web.access**、 **enforce.secure.weblogon**、および **enforce.secure.alllogon** プロパティーは、どれを選択するかにかかわらず、すべてデフォルトで *True* に設定されています。これらのプロパティーについて詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

注: HTTPS を使用する場合は、サーバー名に完全修飾ドメイン名を使用する必要があります。

「セキュア登録トークンを使用してターゲットを登録する」

セキュア・ターゲット登録機能を有効にするにはこのオプションを選択します。この機能により、無許可のターゲットは Remote Control サーバーに登録できなくなります。新規インストールではこのチェック・ボックスはデフォルトで選択されています。**「https を使用するようにターゲットに強制」**オプションも選択されていることを確認してください。セキュア登録について詳しくは、セキュア・ターゲット登録の有効化を参照してください。

データをサーバーにアップロードします。

Remote Control サーバーの完全修飾名。例えば、 `trcserver.example.com`

注: 必ず完全修飾名を入力してください。この名前は、ターゲットが初めてサーバーと接続した後にターゲットに渡される URL を `trc.properties` ファイル内に作成するときに使用されます。完全修飾名が誤っていると、 ターゲットが次にサーバーに接続するときに正常に接続できない可能性があります。

「URL の Web パス」

サーバー URL の Web パスを指定します。例えば、`/trc` です。

WebSphere 上のサーバー・ポート (デフォルト 80)

サーバーのポートを指定します。

SSL ポート (デフォルト 443)

SSL のポートを指定します。

「管理者の電子メール」

管理者の電子メール・アドレスを指定します。例えば、`admin@company.com` です。

注: 電子メール機能を使用するには、メール・サーバーをインストールする必要があります。Remote Control サーバーをインストールした後に、`trc.properties` ファイルを編集します。このプロパティー・ファイルの編集について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

「FIPS を有効にする」

サーバーで FIPS 準拠を有効にするには、このオプションを選択します。FIPS 準拠の有効化について詳しくは、Remote Control での連邦情報処理標準 (FIPS 140-2) 準拠を参照してください。

NIST SP800-131A 準拠を有効にする (FIPS を有効にする)

サーバーで NIST SP800-131A 準拠を有効にするには、このオプションを選択します。NIST SP800-131A 準拠の有効化について詳しくは、Remote Control における NIST SP800-131A 準拠を参照してください。

9. SSL 証明書のオプションを選択し、**「次へ」**をクリックします。証明書の構成は `ssl.xml` ファイルに保管されます。

自動生成された証明書ストアの使用

インストーラーによって生成された自己署名証明書を使用するには、このオプションを選択します。

注: 以下のオプションが有効でない場合は、**「自動生成された証明書ストアの使用」**をクリックしてこれらのオプションを有効にしてください。

既存の証明書ストアの上書き。

自己署名証明書ストアが既に保存されている場合、保存された証明書ストアが新しい証明書によって上書きされます。このオプションはデフォルト・オプションです。

新規または以前に生成された証明書ストアのパスワード。

自己署名証明書の新規パスワードを入力します。上書きを選択しない場合は、既存の自動生成された証明書ストアのパスワードを入力してください。空白のままにすると、デフォルトのパスワード **TrCWebAS** がパスワードとして保存されます。パスワードには、最低 6 文字を指定する必要があります。

既存の証明書ストアの選択

既に保存されている既存の証明書ストアを使用するには、このオプションを選択します。

既存の証明書ストアのロケーションを選択 (Select existing certificate store location.)

「選択」をクリックして、該当する証明書ストアを参照します。証明書ストアを選択します。ファイル拡張子は `.jks` または `.p12` です。

既存の証明書ストアを使用する場合、その証明書ストアはインストール時にインストール・ディレクトリーにコピーされません。サーバーのソフトウェア・インスタンスは、指定された証明書ストアのロケーションを指します。したがって、サーバーのインストールを開始する前に、サーバー上の適切なロケーションに証明書ストアを保存していることを確認する必要があります。証明書ストアは、削除されないロケーションに格納する必要があります。そのため、このファイルを *`[installdir]`*`\wlp` ディレクトリーやそのサブディレクトリーに保存しないでください。インストールの最後に証明書ストアを削除しないでください。

サーバー・インストール・ディレクトリーから保存済みの自動生成された証明書ストアを選択すると、警告が表示されます。このファイルをインストール時に削除されないロケーションにコピーするには、**「ファイルのコピー」**を選択します。この証明書ストア・ファイルが正常にコピーされない場合、そのファイルを別のロケーションに手動でコピーする必要があります。**「選択」**をクリックし、ファイルの新しいロケーションを選択します。

「デフォルトの復元」をクリックして、フィールドの値を元の値にリセットします。

証明書ストアのパスワードを入力 (Enter the certificate store password.)

証明書ストアのパスワードを入力します。

10. シングル・サインオン (SSO) を構成するためのオプションを選択して、**「次へ」**をクリックします。SSO の構成は 、 `sso.xml` ファイルに保管されます。

    SSO の有効化 (Enable SSO)

    シングル・サインオン (SSO) を有効にするには、このオプションを選択します。構成を続行するには、ID プロバイダー (IdP) から SAML メタデータ XML ファイルと、使用されているハッシュ・アルゴリズム(SHA-1 または SHA-256) を取得する必要があります。

    メタデータ XML ファイル (Metadata XML file)

    「選択」をクリックして、IdP から取得した SAML メタデータ XML ファイルを選択します。

    SAML メッセージの署名に使用するアルゴリズム (Algorithm used to sign SAML messages)

    ID プロバイダー (IdP) とこのサービス・プロバイダー、つまり BigFix® Remote Control サーバー の間の通信でメッセージに署名するために使用する署名アルゴリズム (SHA-1 または SHA-256) を選択します。

    拡張パラメーター (Advanced parameters) (オプション)

    その他の構成オプションを入力します。属性名を*[keyword]="[keyword-value]*" 形式でスペース区切りリストに追加します。ここで *[keyword]* は、属性名、は *[keyword-value]* 属性値です。

    SAML データを強制的に再生成します (IdP を使用して再登録する必要があります)。

    SSO を最初に有効にしたときに、新しいデフォルトの SAML 証明書鍵ストアが作成されています。今後のアップグレードでは、新しいデフォルトの証明書鍵ストアを作成するための再生成オプションを選択できます。現在の鍵ストアは削除され、新しい鍵ストアが保存されます。このオプションを選択する場合、サーバーの再始動後に SP と IdP の間の接続を再確立する必要があります。

11. 製品アイコンを表示する場所を選択します。
    「その他」を選択する場合は、**「選択」**をクリックして場所を指定します。

    注: Linux™ を使用する場合、製品アイコンは機能しません。

12. **「概要」**ペインで、**「インストール」**をクリックします。
13. SSO を有効にすることを選択した場合、**「重要」**というラベルが付いたペインが表示されます。URL と情報を書き留め、**「次へ」**をクリックします。
14. **「完了」**をクリックしてインストールを完了します。

Remote Control サーバー・ソフトウェアが一連のプロパティー・ファイルとともにインストールされます。これらのファイルを編集して環境を構成することができます。

注:

1. 必ず `trc.properties` ファイルの **URL** プロパティーに Remote Control サーバーの正しい URL が指定されていることを確認してください。このプロパティーが使用されるのは、ターゲットがサーバーと接続するとき、およびリモート・ターゲット・インストール中にサーバーを判別する目的のためです。URL プロパティー値が誤っていると、リモート・ターゲットが正常にサーバーと接続できません。そのため、ターゲットとのリモート・コントロール・セッションを開始するときに問題が発生する可能性があります。
2. サーバーの IP アドレスが変更される場合はいつでも、必ず `trc.properties` の URL プロパティーを更新してください。ターゲットはこのプロパティーが変更されるまで古い IP アドレスに接続を試みるため、サーバー・サービスを再始動してください。

WebSphere Application Server バージョン 8.5.5 へのインストールWAR ファイルのデプロイ

前提条件のセクションで説明したとおり、Remote Control 用のデータベースを作成する必要があります。データベースを作成したら、そのデータベースを WebSphere® データ・ソースに追加します。

アプリケーション・サーバーのセットアップ

WebSphere プロファイルは、パスにスペースを含まないフォルダーに作成する必要があります。そのようにしない場合、アプリケーションの WAR ファイルのデプロイ時にリカバリー不能な問題が発生する可能性があります。

WebSphere Integrated Solution Console を使用して、アプリケーション・サーバーを構成します。

Integrated Solution Console にアクセスするには、以下のステップを実行します。

1. ブラウザーで、以下を入力します。

```
https://[server : port]/ibm/console
where server is the IPaddress or name for the application server machine
for example localhost or 192.0.2.0
and port is the port that the server is listening on.
```

   WebSphere Application Server 管理コンソールのデフォルトのポートは 9060 です。
2. WebSphere のインストール時に定義した ID とパスワードを使用してログオンします。

DB2®configuration

DB2 データベースの認証データの作成

Remote Control DB2 データベースに接続するための認証データの作成

データベース接続に使用する資格情報を設定して、JAAS-J2C 認証データに新規エントリーとして追加する必要があります。

エントリーを作成するには、以下のステップを実行します。

1. **「セキュリティー」>「グローバル・セキュリティー」**をクリックします。
2. 画面右側の**Java™「Java 認証・承認サービス (JAAS)」**を展開します。
3. **「J2C 認証データ」**をクリックします。
4. **「新規」**をクリックして新規エントリーを追加します。
5. 以下の情報を指定します。

   別名

   認証別名としての名前を指定します。

   ユーザー ID

   DB2® のインストール時に定義したユーザー ID を入力します。以下のいずれかのユーザーを指定できます。
   - 特定のユーザーを作成した場合は、TRCDB データベースにアクセスするための権限を持つユーザー。
   - DB2® の所有者インスタンスである **db2admin** (Windows® システムの場合) および **db2inst1** (UNIX® / Linux® システムの場合)。

   パスワード

   DB2® のインストール時に定義したパスワードを入力します。

6. 「**OK**」をクリックします。
7. **「保存」**をクリックします。

WebSphere 変数の検証

JDBC プロバイダーは、WebSphere®環境変数を使用して、JDBC ドライバー JAR ファイルへのパスを定義します。

- db2jcc.jar
- db2jcc-javax.jar
- db2jcc-license_cu.jar
- db2jcc4.jar. (使用可能な場合)

以下のステップを実行して、正しい値が定義されているかどうか検証します。

1. **「環境」 / WebSphere®「変数」** を選択します。
2. **「DB2UNIVERSAL_JDBC_DRIVER_PATH」** をクリックして、この変数が DB2® ライブラリーを指していることを確認します。

   ローカル DB2® データベース

   DB2® データベースをローカルにインストールした場合のファイルの場所は以下のとおりです。

   Windows® システム

   ```
   \Program Files\ibm\sqllib\java
   ```

Linux® システム

```
/opt/ibm/db2/VERSION/java
 where VERSION is the DB2 version number
for example: /opt/ibm/db2/V8.1/java
```

リモート DB2® データベース

リモートの DB2® データベースを使用する場合は、リモート・システムからローカル・システム上のロケーションに JAR ファイルをコピーして、このロケーションをローカル・ファイルのパスとして指定する必要があります。

3. 「**OK**」をクリックします。
4. **「保存」**をクリックします。

DB2 データ・ソースの作成

JDBC プロバイダーが正しく構成されていることを確認したら、その JDBC プロバイダーを使用して、Remote Control のデータ・ソースを作成する必要があります。

データ・ソースを作成するには、以下のステップを実行します。

1. **「リソース」「JDBC」「データ・ソース」**を選択します。
2. ドロップダウン・メニューから、ノードとサーバーを含む有効範囲を選択します。
   例えば、ノードは TEST-2008Node02、サーバーは server1 などです。
3. 「**新規**」をクリックします。
4. データ・ソース情報を指定します。

   a. 基本的なデータ・ソース情報を入力します。

   データ・ソース名

   データ・ソースの名前を指定します。必要を満たした任意の名前を指定できます。

   JNDI 名

   これは「jdbc/trcdb」に設定する必要があります。

   注: この名前が変更された場合は、**common.properties** ファイルも変更する必要があります。

   b. JDBC プロバイダーを選択します。

   データ・ソースでは、WebSphere で事前定義されている DB2 用ユニバーサル JDBC プロバイダーが使用されます。

i. **DB2 ユニバーサル JDBC ドライバー・プロバイダー (DB2 universal JDBC Driver provider)** が使用可能な場合は、リストから**「既存 JDBC プロバイダーを選択」**を選択します。これが使用できない場合は、**「新規 JDBC プロバイダーの作成」**をクリックします。
ii. データベース・タイプのリストで、**「DB2」**を選択します。
iii. **「DB2 ユニバーサル JDBC ドライバー・プロバイダー (DB2 universal JDBC Driver provider)」**を選択します。
iv. **「実装タイプ」**リストから、**「接続プール・データ・ソース」**を選択します。
v. 「**次へ**」をクリックします。
vi. デフォルト値を受け入れ、**「次へ」**をクリックします。

c. データ・ソースのデータベース固有のプロパティーを入力します。

ドライバー・タイプ

リストから 4 を選択します。

データベース名

これは **db2 create db** コマンドの実行時に使用した名前です。

サーバー名

これには DB2® のインストール先サーバーの IP またはホスト名を設定します。DB2 がローカルにインストールされている場合は、localhost を使用できます。

ポート番号

これには DB2® でリモート接続用に構成されたポートを設定します。

「**次へ**」をクリックします。

d. セキュリティー別名をセットアップします。
i. **「コンポーネント管理の認証別名」**リストで、「*your node*/DB2」を選択します。ここで、*your node* は、以前に DB2 用に作成したノードです。
ii. 他のリストでは、デフォルトの「なし」を受け入れます。
iii. 「**次へ**」をクリックします。

e. 要約を確認し、**「終了」**をクリックします。

5. 構成変更を保存するには、**「保存」**をクリックします。

データ・ソースを作成し、プロファイルへの変更を保存したら、データ・ソースが正しく構成されているかどうかテストします。データ・ソースのリストからデータ・ソースを選択し、「テスト接続」をクリックします。接続が成功すると、確認メッセージが表示されます。Remote Control は有効なデータ・ソースがなければ機能しないため、テストでエラーが発生した場合は、インストールを続行する前に修正する必要があります。

Oracle の構成

Oracle データベースの認証データの作成

データベース接続に使用する資格情報を設定して、JAAS-J2C 認証データに新規エントリーとして追加する必要があります。

エントリーを作成するには、以下のステップを実行します。

1. **「セキュリティー」 > 「グローバル・セキュリティー」**をクリックする。
2. 画面右側の**Java™「Java 認証・承認サービス (JAAS)」**を展開します。
3. **「J2C 認証データ」**をクリックします。
4. 新規エントリーを追加するには、**「新規」**をクリックします。
5. 以下の情報を指定します。

   別名

   認証別名としての名前を指定します。

   ユーザー ID

   Oracle データベースの作成時に定義した ID を入力します。これはアクセス許可の作成対象となったユーザーです。

   パスワード

   Oracle のインストール時に定義したパスワードを入力します。
6. 「**OK**」をクリックします。
7. **「保存」**をクリックします。

Oracle の JDBC プロバイダーの作成

Oracle データベースへのアクセスを確立するには、Oracle アクセス用の JDBC プロバイダーを作成する必要があります。

JDBC プロバイダーを作成するには、以下のステップを実行します。

1. **「リソース」 > 「JDBC」 > 「JDBC プロバイダー」を選択します**。
2. 「有効範囲」を選択し、ノードおよびサーバーを含む有効範囲を選択します。
3. 「**新規**」をクリックします。
4. JDBC プロバイダー情報を指定します。

   データベース・タイプ

   「Oracle」に設定します。

   プロバイダー・タイプ

   「Oracle JDBC ドライバー (Oracle JDBC Driver)」に設定します。

   実装タイプ

   「接続プール」データ・ソースに設定します。
5. 「**次へ**」をクリックします。

6. クラス・パスは既に `${ORACLE_JDBC_DRIVER_PATH}/ojdbc6.jar` として事前設定されています。JAR ファイルの `${ORACLE_JDBC_DRIVER_PATH}` のディレクトリー・ロケーションが正しく設定されている必要があります。これは、Oracle サーバーのインストール済み環境から取得するか、Oracle Web サイトからダウンロードできます。例えば、`C:\app\Administrator\product\11.2.0\dbhome_1\jdbc\lib` です。「**次へ**」をクリックします。
7. 「**終了**」をクリックします。
8. **「保存」**をクリックします。

WebSphere 変数の検証

JDBC プロバイダーは、WebSphere®環境変数を使用して、JDBC ドライバー JAR ファイルへのパスを定義します。以下のステップを実行して、正しい値が定義されているかどうか検証します。

1. **「環境」 / WebSphere®「変数」** を選択します。
2. **「ORACLE_JDBC_DRIVER_PATH」**をクリックします。
   次に、この変数が『Oracle の JDBC プロバイダーの作成』セクションのステップ 6 で選択したディレクトリー・ロケーションを指していることを確認します。
3. 「**OK**」をクリックします。
4. **「保存」**をクリックします。

Oracle データ・ソースの作成

JDBC プロバイダーが正しく構成されていることを確認したら、その JDBC プロバイダーを使用して、Remote Control のデータ・ソースを作成する必要があります。

データ・ソースを作成するには、以下のステップを実行します。

1. **「リソース」「JDBC」「データ・ソース」**を選択します。
2. ノードおよびサーバーを含む有効範囲を選択します。
3. 「**新規**」をクリックします。
4. データ・ソース情報を指定します。

   a. データ・ソース情報を指定します。

   データ・ソース名

   データ・ソースの名前を指定します。必要を満たした任意の名前を指定できます。

   JNDI 名

   これは 「jdbc/trcdb」 に設定する必要があります。

   注: この名前が変更された場合は、**common.properties** ファイルにも追加の変更を加える必要があります。

「**次へ**」をクリックします。

b. JDBC プロバイダーを選択します。

「既存 JDBC プロバイダーを選択」をクリックして、**「Oracle JDBC ドライバー (Oracle JDBC Driver)」**を選択します。「次へ」をクリックします。

c. データ・ソースのデータベース固有のプロパティーを入力します。

URL

url=jdbc:oracle:thin@*dbserver*:1521:*SID*

ここで、*dbserver* は、サーバーの IP アドレスです。

SID Oracle データベースの SID です。

データ・ストアのヘルパー・クラス名

デフォルトのデータ・ストアのヘルパー・クラス名である**「Oracle 11g データ・ストア・ヘルパー (Oracle 11g.data store helper)」**を受け入れます。

残りのデフォルト選択値を受け入れ、**「次へ」**をクリックします。

d. セキュリティー別名をセットアップします。

i. **「コンポーネント管理の認証別名」**を選択し、以前に Oracle 用に作成した別名を選択します。
ii. 他のリストでは、デフォルトの**「なし」**を受け入れます。
iii. 「**次へ**」をクリックします。

e. 要約画面で、**「終了」**をクリックしてデータ・ソースを作成します。

5. **「保存」**をクリックします。

新規作成したデータ・ソースを選択して**「テスト」**をクリックすると、接続をテストできます。

MS SQL の構成

認証データの作成

データベース接続に使用する資格情報を設定して、JAAS-J2C 認証データに新規エントリーとして追加する必要があります。

エントリーを作成するには、以下のステップを実行します。

1. **「セキュリティー」>「グローバル・セキュリティー」**をクリックします。
2. 右側の **Java™「認証・承認サービス」**を展開します。
3. **「J2C 認証データ」**をクリックします。
4. 新規エントリーを追加するには、**「新規」**をクリックします。
5. 以下の情報を指定します。

別名

認証別名としての名前を指定します。

ユーザー ID

MS SQL のインストール時に定義した ID を入力します。これはアクセス許可の作成対象となったユーザーです。デフォルトは **sa** です。

パスワード

MS SQL のインストール時に定義したパスワードを入力します。

6. 「**OK**」をクリックします。
7. **「保存」**をクリックします。

JDBC プロバイダーの作成

MS SQL データベースへのアクセスを確立するには、MS SQL アクセス用の JDBC プロバイダーを作成する必要があります。

JDBC プロバイダーを作成するには、以下のステップを実行します。

1. **「リソース」 > 「JDBC」 > 「JDBC プロバイダー」を選択します。**
2. 「有効範囲」を選択し、ノードおよびサーバーを含む有効範囲を選択します。
3. 「**新規**」をクリックします。
4. JDBC プロバイダー情報を指定します。

   データベース・タイプ

   「SQL Server」に設定します。

   プロバイダー・タイプ

   「Microsoft JDBC ドライバー (Microsoft JDBC Driver)」に設定します。
5. 「接続プール」データ・ソースを選択します。
6. 「**次へ**」をクリックします。
7. JAR ファイルのパスを受け入れるには、**「次へ」**をクリックします。
8. 「**終了**」をクリックします。
9. **「保存」**をクリックします。

WebSphere 変数の検証

JDBC プロバイダーは、WebSphere®環境変数を使用して、JDBC ドライバー JAR ファイルへのパスを定義します。正しい JDBC ドライバー・ソフトウェアを Microsoft からダウンロードする必要があります。推奨されるバージョンは以下のとおりです。

Microsoft JDBC Driver 4.0 for SQL Server - sqljdbc_4.0.2206.100_enu.exe

この SQL Server JDBC ドライバーをダウンロードして、サーバーのルート・ドライブにコピーします。次に、このファイルを実行してドライバーを解凍します。`sqljdbc4.jar` ファイルが以下のディレクトリー構造に解凍されます。

C:*extract_path*\sqljdbc_4.0\enu\

ここで、 *extract_path*は、ファイルを解凍したときに選択したディレクトリーです。

注: このパスにスペースを含めることはできません。

以下のステップを実行して、正しい値が定義されているかどうか検証します。

1. **「環境」 / WebSphere®「変数」** を選択します。
2. **「MICROSOFT_JDBC_DRIVER_PATH」**をクリックして、この変数が解凍した Microsoft SQL Server JDBC ドライバーである sqljdcb4.jar ファイルを指していることを確認します。
3. 「**OK**」をクリックします。
4. **「保存」**をクリックします。

MS SQL データ・ソースの作成

JDBC プロバイダーが正しく構成されていることを確認したら、その JDBC プロバイダーを使用して、Remote Control のデータ・ソースを作成する必要があります。

データ・ソースを作成するには、以下のステップを実行します。

1. **「リソース」「JDBC」「データ・ソース」**を選択します。
2. ノードおよびサーバーを含む有効範囲を選択します。
3. 「**新規**」をクリックします。
4. データ・ソース情報を指定します。

    a. 基本的なデータ・ソース情報を入力します。

    データ・ソース名

    データ・ソースの名前を指定します。必要を満たした任意の名前を指定できます。

    JNDI 名

    これは**「jdbc/trcdb」**に設定する必要があります。

    注: この名前を変更する場合は、WAR ファイルのデプロイ後に、`common.properties` ファイルの **datasource.context** プロパティーを変更する必要があります。正しい値を設定したら、ファイルを保存して、Websphere 管理コンソールからアプリケーションを再始動します。

    b. JDBC プロバイダーを選択します。

「Microsoft SQL Server JDBC ドライバー (Microsoft SQL Server JDBC Driver)」、または必要な JDBC プロバイダーを選択します。「**次へ**」をクリックします。

c. データ・ソースのデータベース固有のプロパティーを入力します。

データベース名

これは MS SQL データベースの作成時に使用した名前です。

ポート番号

MS SQL のインストール時に使用したポート。デフォルトは 1433 です。

サーバー名

これには MS SQL のインストール済み環境を含むサーバーの IP またはホスト名を設定します。MS SQL がローカルにインストールされている場合は、localhost を使用できます。

d. セキュリティー別名をセットアップします。

i. **「コンポーネント管理の認証別名」**を選択し、以前に MS SQL 用に作成した別名を選択します。

ii. 他のリストでは、デフォルトの**「なし」**を受け入れます。

iii. 「**次へ**」をクリックします。

e. 要約画面で、**「終了」**をクリックしてデータ・ソースを作成します。

5. **「保存」**をクリックします。

Remote Control アプリケーションのデプロイ

アプリケーション・サーバーのインストールとセットアップが完了したら、Remote Control のアプリケーション・コードを WebSphere® サーバーにデプロイします。これには、`trc.war` ファイルが必要です (追加のセットアップ・ユーティリティーを使用してサーバーのインストール・メディアを解凍すると入手できます)。

注:

1. このタイプのインストールでは、ヒープ・サイズを 512 MB 以上に設定する必要があります。

サーバー・アプリケーションをデプロイするには、以下のステップを実行します。

1. 追加のセットアップ・ユーティリティーを使用して、`trc.war` ファイルを解凍します。必要なファイルとこのユーティリティーの実行について詳しくは、コンポーネント・インストール・ファイルを解凍するためのユーティリティーを参照してください。
2. WebSphere 管理コンソールで、以下のステップを実行します。

a. **「アプリケーション」 > 「新規アプリケーション」**を選択します。

b. **「新規エンタープライズ・アプリケーション」**をクリックします。

c. 「参照」をクリックし、ローカルまたはリモートのファイル・システム内の **trc.war** ファイルのパスを入力します。「**次へ**」をクリックします。

d. **「アプリケーション・インストールの準備」**画面で、**「ファスト・パス」**を選択します。**「次へ」** をクリックします。

e. **ステップ 1: インストールオプション**
デフォルト・オプションをそのまま使用することができます。アプリケーション名は、役割の内容をより明確に表すものに変更することができますが、スペースが含まれないようにする必要があります。「**次へ**」をクリックします。

f. **ステップ 2: サーバーへのモジュールのマップ**
サーバーへのデフォルトの関連付けをそのまま使用します。「**次へ**」をクリックします。

g. **ステップ 3: Web モジュール用の仮想ホストをマップ**
デフォルト・ホスト (仮想ホスト) へのデフォルトの関連付けを変更できます。「**次へ**」をクリックします。

h. ステップ 4
コンテキスト・ルートとして `/trc` を使用してください。これを使用しない場合は、`trc.properties` ファイルで、さらに変更を加える必要があります。「**次へ**」をクリックします。

i. ステップ 5
Remote Control アプリケーションのインストールを続行する前に、選択したデプロイメント設定の要約が表示されます。

「完了」をクリックします。

インストールの進行中は状況ページが表示され、インストールが完了するとその結果が表示されます。

j. **「保存」**をクリックしてマスター構成に保存します。

Remote Control アプリケーションが、デプロイメント・プロセスの「インストール・オプション (Installation options)」ステップで入力した記述名を使用して、エンタープライズ・アプリケーションのリストに表示されます。アプリケーションを開始する前に、`trc properties` ファイルをカスタマイズし、デフォルト値を変更することができます。このプロパティー・ファイルは、アプリケーションと共にデプロイされ、WebSphere 内の `installedApps` ディレクトリーにあります。このファイル内のプロパティーについて詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

注: ターゲットが正しいサーバーに接続されるよう、**trc.properties** ファイルの**「URL」**フィールドに、正しいサーバー IP アドレスまたはサーバー名が設定されていることを確認してください。HTTPS を使用する場合は、URL プロパティーに設定されたホスト名または IP アドレスが、サーバーにインストールされた SSL 証明書の **CN** フィールドの値と正確に一致している必要があります。

BigFix コンソールからのインストール

BigFix® コンソールを使用すると、サーバー・インストール・タスクを作成および実行することでサーバーをインストールできます。詳しくは、「*BigFix® Remote Control* コンソール・ユーザー・ガイド」と、ターゲットおよびサーバー構成の管理に関する章を参照してください。

ターゲットのインストール

Remote Control ターゲットは、リモート側で制御する必要のあるすべてのコンピューターにインストールできます。また、これを使用し、ブローカーを使用してインターネット接続を行って、インターネットを介してリモート・コントロール・セッションを開始することもできます。

Remote Control では、2 とおりの方法でターゲット・コンポーネントをインストールできます。BigFix® コンソールにアクセスできる場合は、適用 Fixlet を使用してターゲットをデプロイします。詳しくは、*BigFix® Remote Control* コンソール・ユーザー・ガイド を参照してください。あるいは、Remote Control ターゲットのインストール・ファイルを使用します。

Windows™ ターゲットのインストール

この `trc_target_setup.exe` ファイルは、Remote Control ターゲット・コンポーネントを Windows™ システムにインストールするために必要です。

Windows™ コンポーネントのインストール・ファイルの入手方法について詳しくは、「Remote Control コンポーネントのインストール」を参照してください。適切な方法を選択してファイルを入手してください。

1. `trc_target_setup.exe` ファイルを実行する。
2. 「ようこそ」画面で**「次へ」**をクリックします。
3. 使用許諾契約に合意します。**「次へ」**をクリックします。
4. インストール・ファイルのデフォルトの場所を受け入れるか、**「変更」**をクリックして別の場所を選択します。
5. ターゲットの接続先となる Remote Control サーバーのホスト名を指定します。
   例えば、`trcserver.example.com` です。

注: サーバーのインストール時に HTTPS を使用することを選択した場合は、**「セキュア接続 (https) を使用」**を選択します。

6. セキュア・ターゲット登録の場合は、**「サーバーのアドレス」**ウィンドウに **Registration** トークンを入力するか貼り付けます。
   必ず**「セキュア接続 (https) を使用」**も選択してください。セキュア・ターゲット登録について詳しくは、セキュア・ターゲット登録用のトークンの追加を参照してください。
7. 詳細設定を行う場合は、**「詳細設定」**をクリックします。

   サーバー・ポート

   このポートは、サーバーのインストール時に**「Web サーバー上のサーバー・ポート」**パラメーターとして入力した値と一致している必要があります。

   サーバー・コンテキスト

   サーバー・コンテキストは、サーバーに接続するための URL の一部として使用されます。これは、サーバーのインストール時に **「Web サーバーのパラメーター」**画面の**「URL のパス (Path to URL)」**フィールドで「/」の後ろに入力した値と一致している必要があります。

   FIPS 認定の暗号プロバイダーの使用

   ターゲットで FIPS 準拠を有効にするには、このオプションを選択します。FIPS 準拠の有効化について詳しくは、ターゲットでの FIPS 準拠の有効化を参照してください。

   NIST SP800-131A 準拠性を使用可能にする (FIPS を使用可能にする) (Enable NIST SP800-131A compliance (Enables FIPS))

   ターゲットで NIST SP800-131A 準拠を有効にするには、このオプションを選択します。NIST SP800-131A 準拠の有効化について詳しくは、Remote Control における NIST SP800-131A 準拠を参照してください。

8. 「**次へ**」をクリックします。
9. プロキシー・サーバーを使用しない場合は、**「プロキシー設定」**画面で**「次へ」**をクリックします。
   - プロキシーを使用するには、**「プロキシー・サーバーまたは Remote Control ゲートウェイを使用します」**を選択します。
     a. プロキシー・サーバーの IP アドレスまたはホスト名を入力します。
     b. プロキシー・サーバーが listen しているポートを入力します。
     c. HTTP プロキシーを使用するのか、Remote Control ゲートウェイを使用するのかを選択します。
     d. プロキシー・サーバーで認証が必要な場合は、**「プロキシーは認証が必要です」**を選択します。プロキシー・サーバーに対する認証に ID およびパスワードを入力します。ターゲットの始動時にユーザー ID およびパスワードは自動的に暗号化されます。パスフレーズの自動暗号化について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

        注: ユーザー ID およびパスワードが暗号化された後にターゲット・インストーラーを再実行して**「変更」**を選択すると、ユーザー ID のフィールドに暗号化されたユーザー ID とパスワードの組み合わせが表示されます。パスワード・フィールドは空のままです。

     e. 「**次へ**」をクリックします。

10. 着信リモート・コントロール・セッションの listen に使用するポート値を受け入れるか、変更します。**「次へ」**をクリックします。

注: ご使用のオペレーティング・システムに、ファイアウォール、アンチウィルス、侵入検知システムがデフォルトでインストールされている場合があります。詳しくは、『ターゲットの要件』を参照してください。

11. P2P モードへのフェイルオーバーを有効にするには、以下のいずれかのオプションを選択します。

サーバーの状況によらない

サーバーが使用可能かどうかに関係なく、コントローラーとこのターゲットとの間に直接、P2P セッションを確立できます。**「P2P」**ポリシーをクリックして、P2P セッション中にターゲットで使用するローカル・ポリシーを設定します。**「次へ」**をクリックして、P2P ポリシー画面を移動します。

サーバーのダウン時またはアクセス不能時のみ

サーバーがダウンしているか、ターゲットがサーバーに接続できない場合にのみ、P2P セッションを確立できます。**「P2P」**ポリシーをクリックして、P2P セッション中にターゲットで使用するローカル・ポリシーを設定します。**「次へ」**をクリックして、P2P ポリシー画面を移動します。

なし

コントローラーとこのターゲットとの間に直接 P2P セッションを確立することはできません。このオプションを選択した場合は、ステップ 12 から続行してください。

ピアツーピア・ポリシー

定義およびプロパティーの詳細については、ターゲットの構成で設定可能なプロパティーを参照してください。

セッション・ポリシー・オプション

表 8. セッション・ポリシー・オプション

インストール・ オプション	ターゲット・プロパティー	デフォルト値
アクティブ	AllowActive	選択済み。
ガイダンス	AllowGuidance	選択済み。
モニター	AllowMonitor	選択済み。
高品質カラーを使用可能にする	EnableTrueColor	未選択
カラー品質のロック	LockColorDepth	未選択
デスクトップ・バックグラウンドの除去	RemoveBackground	未選択

インストール・ オプション	ターゲット・プロパティー	デフォルト値
スクリーン・セーバーがアクティブな場合にスクリーン・セーバーの更新を停止する (Stop screen saver updates when screen saver is active)	NoScreenSaver	未選択

ポリシー・オプション

表 9. ポリシーの説明 -

インストーラー画面の名前	ターゲット・プロパティー	これがデフォルト値です。
チャットの無効化	DisableChat	未選択
チャット メッセージの保存	AutoSaveChat	未選択
ターゲットからコントローラーへのファイル転送を使用不可にする	DisableFilePull	未選択
コントローラーからターゲットへのファイル転送を使用不可にする	DisableFilePush	未選択
クリップボード転送の無効化	DisableClipboard	未選択
「ローカル記録機能の許可」	AllowRecording	選択済み。
コラボレーションの許可	AllowCollaboration	選択済み。
セッション・ハンドオーバーの許可 (Allow session handover)	AllowHandover	選択済み。
既存セッションの切断要求を許可する (Allow requests to disconnect existing session)	AllowForceDisconnect	未選択
切断猶予時間 (Disconnect grace time)	ForceDisconnectTimeout	45
アプリケーション・イベント・ログに対する監査	AuditToSystem	選択済み。

セキュリティー・ポリシー

表 10. セキュリティー・ポリシー

インストーラー画面の名前	ターゲット・プロパティー	デフォルト値
Windows ログオンを使用した認証	CheckUserLogin	選択済み。
「これらの Windows グループのメンバーである必要があります」	CheckUserGroup	説明を参照してください。
プライバシーの保護	AllowPrivacy	選択済み。

インストーラー画面の名前	ターゲット・プロパティー	デフォルト値
「入力ロックの許可」	AllowInputLock	選択済み。
セッションの開始時にプライバシーを使用可能にする	EnablePrivacy	未選択
セッションの開始時に入力ロックを使用可能にする	EnableInputLock	未選択
画面上のセッション通知の有効化	EnableOSSN	未選択
パニック・キーの無効化	DisablePanicKey	未選択
一定時間操作がなかったことによるタイムアウト	IdleTimeout	360

ユーザー確認ポリシー

表 11. ユーザー確認ポリシー

インストーラー画面の名前	ターゲット・プロパティー	デフォルト値
テークオーバー・セッション	ConfirmTakeOver	選択済み。
セッション・モードを変更	ConfirmModeChange	選択済み。
ファイルの転送	ConfirmFileTransfer	選択済み。
システム情報	ConfirmSysInfo	選択済み。
ローカル記録	ConfirmRecording	選択済み。
コラボレーション	ConfirmCollaboration	選択済み。
ユーザーの受け入れ猶予時間	AcceptanceGraceTime	45
確認要求のタイムアウト時も続行	AcceptanceProceed	未選択
ユーザーがログオンしていないときは、ユーザーの受け入れのプロンプトを表示しない	AutoWinLogon	選択済み。
ウィンドウの非表示を使用可能にする	HideWindows	未選択

セッション・スクリプト

表 12. セッション・スクリプト・ポリシー

インストーラー画面の名前	ターゲット・プロパティー	デフォルト値
セッション前に実行するスクリプト	RunPreScript	未選択
セッション後に実行するスクリプト	RunPostScript	未選択
スクリプトの失敗時にセッションを続行する	ProceedOnScriptFail	未選択

追加機能

仮想スマート・カード・リーダー・ドライバーをインストールするには、**「仮想スマート・カード・リーダー用のデバイス・ドライバーをインストール (Install device driver for Virtual Smart Card Reader)」**を選択します。スマート・カード・リーダー・ドライバーについて詳しくは、ターゲットへのスマート・カード認証のサポートのためのドライバーのインストールを参照してください。

12. **「インストール」**をクリックしてインストールを開始します。
13. インストールが完了したら、**「完了」**をクリックします。

Linux™ ターゲットのインストール

Linux™ コンピューターにターゲット・コンポーネントをインストールするには、 Remote Control インストール・ファイルで提供される RPM ファイルを使用します。

注: ブローカー・コンポーネントのインストール・パッケージは、32 ビット・バージョンの以下のライブラリーに依存しています。**glibc libgcc**、**libblkid**、**libstdc++**。

`trc-target-10.x.x.i386.rpm` ファイルを使用して、Linux™ にターゲット・コンポーネントをインストールします。ここで、10.x.xは、インストールするバージョンです。Linux™ コンポーネントのインストール・ファイルの入手方法について詳しくは、「 インストール・ファイルの入手 」を参照してください。適切な方法を選択してファイルを入手してください。

デフォルトのターゲット RPM ファイルをインストールします。インストール後にターゲットを構成します。

RPM ファイルをインストールするには、以下のコマンドを実行して、インストールするバージョンに固有のファイルを使用します。例えば、 rpm -ivh trc-target-10.x.x.i386.rpm

ターゲットがインストールされたら、`/etc/trc_target.properties` ファイルを編集することによって、ターゲットのプロパティーを構成します。ターゲットのプロパティーおよびその定義について詳しくは、ターゲットの構成で設定可能なプロパティーを参照してください。

BigFix® Remote Control Target for macOS のインストール

BigFix® Remote Control Target for macOS はさまざまな方法でインストールできます。`trc_target.pkg` ファイルを使用して、このアプリケーションを在席モードまたは無人モードでインストールします。また、BigFix® コンソールで Fixlet® を使用してこのターゲットをインストールすることもできます。

BigFix® Remote Control Target for macOSコンポーネントのインストール・ファイルの取得方法については、「BigFix® Remote Control コンポーネントのインストール」を参照してください。適切な方法を選択してファイルを入手してください。

BigFix® コンソールからの BigFix® Remote Control Target for macOS のインストール

BigFix® コンソールで Fixlet® を使用して BigFix® Remote Control Target for macOS コンポーネントをインストールできます。デプロイメント Fixlet® は、「システム・ライフサイクル」ドメインの Remote Control サイトで入手できます。

注: 管理対象モードを選択するためのオプション (サーバー URL とセキュア登録トークンを求めるプロンプトが出されるオプション) は、管理対象モードが BigFix® Remote Control Target for macOS ではサポートされないために使用できません。

BigFix® Remote Control Target for macOS ターゲット・コンポーネントをインストールするには、以下のステップを実行します。

1. **「システム・ライフサイクル」**ドメイン内で、**「Remote Control の設定」 > 「Remote Control」**を展開します。
2. **「デプロイメント」**ノードを展開します。
3. **「macOS」**を選択します。
4. **「BigFix® Remote Control Target for macOS のデプロイ 」**を選択します。
5. **「タスク」**ペインで、説明を確認し、**「アクション」**ボックス内の指示に従ってタスクを開始します。
6. **「アクションの実行」**ペインの**「対象」**タブで、BigFix® Remote Control Target for macOS コンポーネントをデプロイするコンピューターを決定するための関連オプションを選択します。
7. 「**OK**」をクリックします。
   概要画面にタスクの進行状況が表示され、タスクが完了すると状況が**「完了」**に設定されます。

.pkg ファイルを使用した BigFix® Remote Control Target for macOS のインストール

`trc_target.pkg` ファイルを使用して、BigFix® Remote Control Target for macOS をインストールすることができます。

`pkg` ファイルはパスポート・アドバンテージから、または Remote Control サーバーの UI から取得できます。詳しくは、『インストール・ファイルの入手』を参照してください。`pkg` ファイルがある場合は、次の 2 つのインストール方式を使用できます。在席モードと無人モード

また、ターゲットのインストール時にカスタム構成設定を適用することもできます。構成値は `trc_target.cfg` ファイル内に設定します。このファイルを作成し、カスタム値を追加します。このファイルを、BigFix® Remote Control Target for macOS のインストール先のコンピューターにコピーします。`trc_target.cfg` ファイルを `trc_target.pkg` ファイルと同じディレクトリーにコピーします。

構成設定がターゲットとともにインストールされます。ターゲットの構成は、`/Library/Preferences/com.bigfix.remotecontrol.target.plist` にインストールされています。

ブローカー・セッションをサポートするようにターゲットを構成するには、**BrokerList** プロパティーを構成し、信頼証明書を提示する必要があります。信頼証明書を含む `broker.certs` ファイルを、`trc_target.pkg` ファイルと同じディレクトリーに入れます。このパッケージは `broker.certs` ファイルを次の場所にインストールします

`/Library/Application Support/com.bigfix.remotecontrol.target/TrustStore`.

`.cfg` ファイル内で設定できるターゲット・プロパティーについて詳しくは、「ターゲットの構成で設定可能なプロパティー」を参照してください。

カスタム構成を適用しない場合、ターゲットではそのインストール時に組み込み済みの構成設定が使用されます。

BigFix® Remote Control Target for macOS をインストールする際のインストール方式を選択します。

在席モード:

1. `trc_target.pkg` ファイルをダブルクリックします。
2. **「続行」**をクリックします。
3. **「インストール」**をクリックして起動ディスクにインストールします。システムに複数のディスクがある場合は、ターゲットのインストール先ディスクを選択できます。**「インストール場所の変更 (Change Install Location)」**をクリックしてインストール先ディスクを選択します。
4. 管理者権限を持つユーザーの場合は、プロンプトが出されたらパスワードを入力します。そうでない場合は、有効な管理者 ID とパスワードを入力します。**「ソフトウェアのインストール (Install Software)」**をクリックします。
5. インストールが完了したら、**「閉じる」**をクリックします。

無人モード:

1. **「ターミナル」**ウィンドウを開き、次のコマンドを入力します。

   sudo installer -pkg "/[path]/trc_target.pkg" -target /

   ここで *[path]* は、`.pkg` ファイルへのパスです。

.pkg ファイルをインストールしたら、`Remote Control Target.app` を開いてターゲットを開始します。

ターゲットのカスタム・インストールの実行

パラメーターを使用してターゲット・ソフトウェアをインストールするには、Remote Control ターゲットのカスタム・インストールを実行します。インストールは複数の方法で実行できます。

無人およびサイレント

ユーザーによる操作は不要で、ユーザーには UI ダイアログも進行状況表示バーも表示されません。

無人

ユーザーによる操作は不要で、インストール進行状況表示バーがユーザーに表示されます。

在席

完全なインストール UI が表示され、ユーザーの操作が必要です。

インストール設定をカスタマイズできます。インストール時にターゲットを特定のグループに割り当てることも可能です。

Windows® システムでのターゲット・カスタム・インストールの実行

Windows® オペレーティング・システムでターゲット・ソフトウェアをインストールするには、`trc_target_setup.exe` ファイルを使用します。

このファイルの入手について詳しくは、インストール・ファイルの入手を参照してください。

ターゲットをインストールするには、以下のステップを実行します。

1. `TRC` というフォルダーをルート・ドライブに作成します。
2. `trc_target_setup.exe` を TRC にコピーします。
3. コマンド・プロンプト・ウィンドウを開き、TRC に移動します。
4. `DIR` と入力し、当該 exe ファイルがこのフォルダーにあることを確認します。
5. ターゲットをインストールするには、以下のコマンドを 1 行に入力します。

```
trc_target_setup.exe /s /v"/qn [INSTALLPARAMETER1][INSTALLPARAMETER2]...[INSTALLPARAMETERX]"
```

インストールをカスタマイズするには、以下のインストール・パラメーターを使用します。

注: 値の検証は実行されないため、正しい値がパラメーターに割り当てられていることを確認してください。

/s

サイレント・インストールを指示します。

/v"

/v に付加されるストリングには、インストールを実行するソフトウェアである `msiexec.exe` のパラメーターが含まれます。

/qn

進行状況ウィンドウも UI もない、サイレントおよび無人インストールを実行します。

/qn の代わりに、以下のパラメーターを使用することもできます。

/qb

基本 UI と小さな進行状況表示バーがある無人インストールをする場合。

/qr

縮小された UI 進行状況表示バーを大きなウィンドウ内に表示する無人インストールをする場合。

/qf

完全な UI のある在席インストールをする場合。

TRC_SERVER_HOSTNAME

サーバーのホスト名または IP アドレス。このプロパティーは必須です。デフォルト値は *<blank>* です。

例えば、`TRC_SERVER_HOSTNAME=trc.myserver.com` です。

TRC_SERVER_CONTEXT

このパラメーター値は、サーバー URL 内のパスの最後の部分と一致する必要があります。デフォルト値は *trc* です。

例えば、`TRC_SERVER_CONTEXT=trc` です。

TRC_SERVER_PORT

サーバーが標準外ポートで稼働する場合は、ポート番号を指定します。デフォルト値は 80 です。

例えば、`TRC_SERVER_PORT=8080` です。

TRC_SERVER_PROTOCOL

プレーン HTTP とセキュア HTTPS プロトコルから選びます。有効値は http および https です。デフォルト値は http です。

例えば、`TRC_SERVER_PROTOCOL=http` です。

TRC_PROXY_HOSTNAME

プロキシー・サーバーのホスト名または IP アドレス (使用している場合)。デフォルト値は *<blank>* です。

例えば、`TRC_PROXY_HOSTNAME=proxy.company.com` です。

TRC_PROXY_PORT

プロキシー・サーバーのポート番号。デフォルト値は *<blank>* です。

例えば、`TRC_PROXY_PORT=8080` です。

TRC_PROXY_USER_ID

プロキシーに認証が必要な場合のユーザー ID。デフォルト値は *<blank>* です。ターゲットの開始時に、ユーザー ID とパスワードは自動的に暗号化されます (**DISABLEAUTOMATICPASSPHRASEENCRYPTION** が *Yes* に設定されている場合を除く)。パスフレーズの自動的な暗号化について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

例えば、`TRC_PROXY_USER_ID=proxyuser` です。

TRC_PROXY_PASSWORD

プロキシーに認証が必要な場合のパスワード。デフォルト値は *<blank>* です。ターゲットの開始時に、ユーザー ID とパスワードは自動的に暗号化されます (**DISABLEAUTOMATICPASSPHRASEENCRYPTION** が *Yes* に設定されている場合を除く)。パス

フレーズの自動的な暗号化について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

`TRC_PROXY_PASSWORD=v264xmpt`.

TRC_PROXY_AUTH_B64

ユーザー ID およびパスワード。フォーマットは `user: password` です。Base64 でエンコードされます。ユーザー ID およびパスワード・プロパティーはオーバーライドされます。パスワードを簡単に表示できないようにする場合は、このパラメーターを使用します。Base64 は暗号化ではありません。デフォルト値は *<blank>* です。

例えば、 `TRC_PROXY_AUTH_B64=cHJveHl1c2VyOnYyNjR4bXB0`

ターゲットの開始時に、ユーザー ID とパスワードは自動的に暗号化されます (**DISABLEAUTOMATICPASSPHRASEENCRYPTION** が *Yes* に設定されている場合を除く)。パスフレーズの自動的な暗号化について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

TRC_TARGET_PORT

ターゲットを標準外ポートで実行する場合は、使用するポート番号を指定します。デフォルト値は 888 です。

例えば、`TRC_TARGET_PORT=888` です。

TRC_SERVER_HEARTBEAT_RETRY

サーバーが応答しないときに、ターゲットがサーバーにハートビートを再送するまでの待機時間 (分単位)。デフォルト値は 10 です。

例えば、`TRC_SERVER_HEARTBEAT_RETRY=1` です。

TRC_ACCESSIBILITY

アクセシビリティー対応の UI を有効にします。デフォルト値は *No* です。Windows® オペレーティング・システムで使用できます。

GROUP_LABEL

ターゲットが割り当てられるグループの名前。この機能を有効にするには、`trc.properties` ファイルを編集して、*allow.target.group.override = true* を設定します。このプロパティー・ファイルの編集について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。デフォルト値は *DefaultTargetGroup* です。

注:

a. ターゲットが Remote Control サーバーで既に登録されている場合は、GROUP_LABEL パラメーターは破棄されます。
b. サーバー上で既に定義されているターゲット・グループを指定する必要があります。

例えば、`GROUP_LABEL=NewTargetGroup` です。

INSTALLDIR

このパラメーターは、ターゲット・ソフトウェアのインストール先ディレクトリーを指定するために使用します。

例えば、`INSTALLDIR= c:\trc\target` です。

ALLOWP2P

このパラメーターは、サーバーの状況に関係なく、P2P 接続を有効にするために使用します。デフォルト値は *No* です。

ALLOWP2PFAILOVER

このパラメーターは、サーバーがダウンしているか、サーバーに到達できない場合に、P2P モードへのフェイルオーバーを有効にするために使用します。デフォルト値は *No* です。

AUDITTOSYSTEM

このパラメーターは、監査目的でターゲット・アプリケーション・イベント・ログに P2P セッション・イベントを記録するために使用します。デフォルト値は *No* です。

AUTOSAVECHAT

このパラメーターは、ターゲット上のファイルにチャット・ウィンドウのコンテンツを保存するために使用します。デフォルト値は *No* です。

AUTOWINLOGON

ユーザーがターゲットにログオンしていない場合に、セッションを開始できるようにするかどうかを決定します。デフォルト値は *Yes* です。

CHECKUSERGROUP

コントローラー・ユーザーは、リストされているグループのメンバーである必要があります。デフォルト値は、Windows® システムでは `BUILTIN\Administrators`、 Linux® システムでは `wheel` です。

CHECKUSERLOGIN

コントローラー・ユーザーが**「接続のオープン」**ウィンドウでセッション・タイプを選択したときに、ログイン・ウィンドウを表示するかどうかを決定します。デフォルト値は *Yes* です。

CONFIRMFILETRANSFER

コントローラー・ユーザーが P2P セッションでターゲットのファイルをコントローラーに転送する前にユーザー確認ウィンドウを表示するかどうかを決定します。デフォルト値は *Yes* です。

CONFIRMMODECHANGE

リモート・コントロール・セッション中にコントローラー・ユーザーが別のセッション・モードを選択した場合に、ユーザー確認ウィンドウを表示するかどうかを決定します。デフォルト値は *Yes* です。

CONFIRMSYSINFO

コントローラー・ユーザーがターゲット・システム情報の表示を要求した場合にユーザー確認ウィンドウを表示するかどうかを決定します。デフォルト値は *Yes* です。

CONFIRMTAKEOVER

P2P セッションが要求された場合にユーザー確認ウィンドウを表示するかどうかを決定します。デフォルト値は *Yes* です。

DISABLEAUTOMATICPASSPHRASEENCRYPTION

ターゲットの開始時に、プロキシー認証のユーザー ID とパスワードを自動的に暗号化するかどうかを決定します。デフォルト値は *No* です。パスフレーズの自動的な暗号化について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

DISABLECHAT

ターゲットとのチャット・セッションを開始し、P2P セッション中にコントローラー・ユーザーともチャットすることができるかどうかを決定します。デフォルト値は *No* です。

DISABLECLIPBOARD

P2P セッション中にクリップボード転送メニューを使用可能にするかどうかを決定します。デフォルト値は *No* です。

DISABLEFILEPULL

P2P セッション中にターゲットからコントローラーにファイルを転送できるかどうかを決定します。

DISABLEFILEPUSH

P2P セッション中にコントローラーからターゲットにファイルを転送できるかどうかを決定します。デフォルト値は *No* です。

FIPSCOMPLIANCE

すべての暗号機能について、FIPS 認定の暗号プロバイダーの使用を有効にします。デフォルト値は *No* です。

SP800131ACOMPLIANCE

すべての暗号機能について、NIST SP800-131A 準拠のアルゴリズムと鍵強度の使用を有効にします。デフォルト値は *No* です。

HTTPSSTRICTVALIDATION

ターゲットが、システムのトラストストアを使用してサーバーへの HTTPS 接続を確認するかどうかを決定します。デフォルト値は *No* です。

LOGLEVEL

ロギング・レベルを設定します。ロギング・レベルによって、エントリーのタイプと、ターゲット・ログ・ファイルに追加される情報量が決定されます。有効な値は 0、1、2、または 4 のいずれかです。ただし、**LOGLEVEL=4** は IBM ソフトウェア・サポートからの要請があった場合にのみ使用してください。デフォルト値は 2 です。

例えば、`LOGLEVEL=2` です。

LOGROTATION

古いログ・ファイルが上書きされるようになるまでの期間を制御します。**「毎日」**、**「毎週」**、または **「毎月」** のいずれかに設定します。デフォルト値は Weekly です。

例えば、`LOGROTATION=Monthly` です。

値 Disabled を使用して、ログのローテーションを無効にすることもできます。

LOGROLLOVER

新しいログ・ファイルが開始されるまでの期間を制御します。この期間は LOGROTATION 期間より短くなければならないため、すべての組み合わせが有効とは限りません。LOGROLLOVER を無効にすることはできません。**「毎日」** または **「毎時」** に設定します。デフォルト値は Daily です。

例えば、`LOGROLLOVER=Daily` です。

VSC

仮想スマート・カード・リーダーのデバイス・ドライバーをインストールする場合に、このパラメーターを使用します。ドライバーをインストールするには、パラメーターのリストに **VSC=1** を追加します。

注: パラメーターのリスト内に、パラメーターの値ではなく、**VSC** が存在するかどうかによって、ドライバーをインストールするかどうかが決定されます。パラメーターのリストに **VSC= n** が指定されている場合、ドライバーがインストールされます。パラメーターのリストに **VSC** が指定されていない場合、ドライバーはインストールされません。**VSC** には、任意の値を指定することができます。ただし、推奨値は **VSC=1** です。

サイレント・インストール中に仮想スマート・カード・リーダーのデバイス・ドライバーをインストールする方法について詳しくは、「サイレント・インストールの実行による仮想スマート・カード・リーダー・ドライバーのインストール」を参照してください。

REGISTRATIONTOKEN

このパラメーターを使用して、ターゲットに対して登録トークンを提供します。このトークンは、ターゲットが最初にサーバーに接続するときに、サーバーでターゲットを認証するために使用されます。このプロパティーの値は登録トークンに設定されます。サイレント・インス

トールの実行によるセキュアな登録トークンを使用したターゲットのインストールについて詳しくは、セキュア登録トークンを伴うターゲットのサイレント・インストールの実行を参照してください。

注: ターゲットの既存のインストール済み環境についてのパラメーターを再構成する場合は、**REINSTALL=ALL** パラメーターを使用します。ただし、ターゲットのアップグレード時にこのパラメーターを使用した場合、このパラメーターは無視されます。

例えば、コマンド・ラインで、以下のコマンドを入力することができます。

trc_target_setup.exe /s /v"/qn REINSTALL=ALL"

ターゲット構成を変更してアップグレードを適用する場合は、以下のステップを実行します。

1. ターゲット・ソフトウェアの新しいバージョンを使用して、サイレント・インストールを実行します。パラメーターは使用しないでください。パラメーターを指定した場合、ターゲットはアップグレードされますが、指定したパラメーターは無視され、更新されません。
2. `REINSTALL=ALL` と任意の新しいパラメーターを指定して、サイレント再インストールを実行します。

オーバーライドするパラメーターを指定することもできます。

例えば、ターゲット・ポートを 2222 に変更するには、以下のコマンドを入力します。

trc_target_setup.exe /s /v"/qn TRC_TARGET_PORT=2222 REINSTALL=ALL"

注: インストール中にヘルプ・オプションを表示するには、コマンド・ラインで以下のコマンドを入力します。 trc_target_setup.exe --help

コントローラーのインストール

Remote Control コントローラーをローカル・システムにインストールして、P2P モードが有効な場合にターゲットに直接接続するために使用できます。

Remote Control では、2 とおりの方法でコントローラー・コンポーネントをインストールすることができます。BigFix® コンソールにアクセスできる場合は、適用 Fixlet® を使用してコントローラーを導入します。詳しくは、Remote Control コンポーネントのデプロイ を参照してください。*BigFix® Remote Control* コンソール・ユーザー・ガイドもう 1 つの方法は、Remote Control コントローラーのインストール・ファイルを使用する方法です。

Windows™ システムでのコントローラーのインストール

この `trc_controller_setup.exe` ファイルは、コントローラー・コンポーネントを Windows™ システムにインストールするために必要です。

Windows™ システムのコンポーネントのインストール・ファイルの入手方法について詳しくは、「Remote Control コンポーネントのインストール」を参照してください。適切な方法を選択してファイルを入手してください。

1. `trc_controller_setup.exe` ファイルを実行する。
2. ファイルのダウンロード・ウィンドウで、**「実行」**または**「保存」**を選択します。

実行

「実行」を選択してインストール・ウィザードを開始します。

a. ようこそ画面で**「次へ」**をクリックします。
b. 使用許諾契約に同意し、**「次へ」**をクリックします。
c. インストール・ファイルの場所を受け入れるか変更し、**「次へ」**をクリックします。
d. **「インストール」**をクリックします。
e. 「**終了**」をクリックします。

注: 既にコントローラー・ソフトウェアがシステムにインストールされている場合は、変更、修復、または削除のオプションを選択できます。

保存\n

「保存」を選択して、`trc_controller_setup.exe` ファイルを選択した場所に保存します。このファイルを実行して、コントローラーをインストールします。

コントローラーが、デフォルトの場所 `\Program Files\BigFix\Remote Control\Controller` またはインストール中に選択した場所にインストールされます。

Linux™ コントローラーのインストール

`trc-controller-10.x.x.noarch.rpm` ファイルと `trc-controller-jre-10.x.x.i386.rpm` ファイルを使用して、 コントローラー・コンポーネントを Linux™ にインストールします。ここで、*10.x.x* はインストールするバージョンに該当します。 Linux™ コンポーネントのインストール・ファイルの入手方法について詳しくは、「Remote Control コンポーネントのインストール 」を参照してください。適切な方法を選択してファイルを入手してください。

Linux™ では、2 つのモード、FIPS 準拠コントローラーまたは標準コントローラーのいずれかで、コントローラーをインストールできます。

コントローラーをインストールするための該当するコマンドを入力します。ここで、*10.x.x* はインストールするバージョンに該当します。 となります。

- 標準コントローラーの場合

```
#rpm -ivh ~/BigFix/Tivoli_Remote_Control/RCTarget/trc-controller-10.x.x.noarch.rpm
```

- FIPS 準拠コントローラーの場合は、以下の両方のコマンドを実行して、標準コントローラーと FIPS 準拠 JRE をインストールします。

  #rpm -ivh ~/BigFix/Tivoli_Remote_Control/RCTarget/trc-controller-10.x.x.noarch.rpm

  #rpm -ivh ~/BigFix/Tivoli_Remote_Control/RCTarget/trc-controller-jre-10.x.x.i386.rpm

注: 標準コントローラーのインストールは、システムにインストールされている代替の JRE を使用して、`trc-controller-10.x.x.noarch.rpm` ファイルで実行できます。コントローラーを FIPS 準拠にする場合は、`trc-controller-jre-10.x.x.i386.rpm` ファイルもインストールする必要があります。コントローラーを FIPS モードで実行する予定がない場合でも、`trc-controller-jre-10.x.x.i386.rpm` ファイルをインストールすることができます。

コントローラーがインストールされると、そのコントローラーをアプリケーション・リストから開始することができます。

BigFix® Remote Control Controller for macOS のインストール

BigFix® Remote Control Controller for macOS はさまざまな方法でインストールできます。`trc_controller.pkg` ファイルを使用してこのアプリケーションをインストールできます。また、BigFix® コンソールで Fixlet® を使用してこのコントローラーをインストールすることもできます。

BigFix® Remote Control Controller for macOS コンポーネントのインストール・ファイルの取得方法については、インストール・ファイルの入手を参照してください。適切な方法を選択してファイルを入手してください。

BigFix® コンソールからの BigFix® Remote Control Controller for macOS のインストール

BigFix® コンソールで Fixlet® を使用して BigFix® Remote Control Controller for macOS コンポーネントをインストールできます。デプロイメント Fixlet® は、「システム・ライフサイクル」ドメインの Remote Control サイトで入手できます。

1. **「システム・ライフサイクル」**ドメイン内で、**「Remote Control の設定」** > **「Remote Control」**を展開します。
2. **「デプロイメント」**ノードを展開します。
3. **「macOS」**を選択します。
4. **「BigFix® Remote Control Controller for macOS のデプロイ 」**を選択します。
5. **「タスク」**ペインで、説明を確認し、**「アクション」**ボックス内の指示に従ってタスクを開始します。
6. **「アクションの実行」**ペインの**「対象」**タブで、BigFix® Remote Control Controller for macOS コンポーネントをデプロイするコンピューターを決定するための関連オプションを選択します。
7. 「**OK**」をクリックします。
   概要画面にタスクの進行状況が表示され、タスクが完了すると状況が**「完了」**に設定されます。

BigFix® Remote Control Controller for macOS のインストール

`trc_controller.pkg` ファイルを使用して、BigFix® Remote Control Controller for macOS をインストールすることができます。

`pkg` ファイルはパスポート・アドバンテージから、または Remote Control サーバーの UI から取得できます。詳しくは、『インストール・ファイルの入手』を参照してください。このコントローラーをインストールするには、以下の手順を実行します。

1. `trc_controller.pkg` ファイルをダブルクリックします。
2. **「続行」**をクリックします。
3. **「インストール」**をクリックして起動ディスクにインストールします。システムに複数のディスクがある場合は、コントローラーのインストール先ディスクを選択できます。**「インストール場所の変更 (Change Install Location)」**をクリックしてインストール先ディスクを選択します。
4. 管理者権限を持つユーザーの場合は、プロンプトが出されたらパスワードを入力します。そうでない場合は、有効な管理者 ID とパスワードを入力します。**「ソフトウェアのインストール (Install Software)」**をクリックします。
5. インストールが完了したら、**「閉じる」**をクリックします。

.pkg ファイルをインストールしたら、`Remote Control Controller.app` を開いてターゲットを開始します。

その他のサポートされるオペレーティング・システムでのコントローラーのインストール

Windows™ オペレーティング・システム、Linux™、AIX®、Solaris (SPARC) 以外のサポートされるオペレーティング・システムを使用している場合は、追加セットアップ・ユーティリティーを使用してコントローラー・ファイルを解凍します。その後、コントローラーを実行するシステムに、必要なファイルをコピーします。追加セットアップ・ユーティリティーは Windows™、Linux™、AIX®、または Solaris (SPARC) システムで実行する必要があります。追加のセットアップ・ユーティリティー・ファイルの入手について詳しくは、Remote Control コンポーネントのインストールを参照してください。

注: 他のサポートされるオペレーティング・システムでコントローラーを実行するには、 サポートされるバージョンの Java™ がインストールされていることを確認してください。『コントローラーの要件』を参照してください。

コントローラーをインストールするには、以下の手順を実行します。

1. インストール・ファイルを解凍した後、`RCController` ディレクトリーに移動します。
2. コントローラーを実行するシステムにファイル `trc_console.zip` をコピーします。
3. `trc_console.zip` ファイルからファイルを解凍します。
4. 以下のコマンドを入力してコントローラーを実行します。

   ```
   java -jar TRCConsole.jar
   ```

事前構成済みコントローラー・コンポーネントのインストール

コントローラー・コンポーネントのインストール時にカスタム構成設定を適用することもできます。

コントローラーの事前構成は、無人インストールの場合に便利です。構成ファイルに構成ファイル値を設定して、そのファイルをコントローラーをインストールするコンピューターにコピーできます。構成設定が、コントローラーとともにインストールされます。構成値は `trc_controller.cfg` ファイル内に設定します。このファイルを作成してカスタム値を追加するか、またはデフォルトの構成ファイルを編集できます。事前構成を適用しない場合、 コントローラー・コンポーネントのインストール時にデフォルトの構成ファイルがインストールされます。

`trc_controller.cfg` のプロパティー値はグローバルであり、コントローラーを実行するすべてのユーザーで同じ値になります。ただし、ユーザーがローカル構成を作成することはできます。コントローラーを実行してグローバル値をオーバーライドすると、ユーザーのローカル構成の値が使用されます。グローバルのプロパティー値を施行するため、ユーザーがコントローラー UI の**構成ウィンドウ**でプロパティーを編集できないように、プロパティーを mandatory に設定できます。必須のグローバル・プロパティーは、ローカル・プロパティーをオーバーライドします。

必須プロパティーを設定するには、以下の手順を実行します。

1. `trc_controller.cfg` ファイルを開きます。
2. プロパティー名をコピーし、末尾に *.mandatory = true* を追加します。

   例えば、**「アドレス履歴を使用可能にする」**プロパティーを必須にして**構成ウィンドウ**で編集できないようにするには、以下のようにします。

   enable.address.history=false enable.address.history.mandatory=true
3. ファイルを保存します。

`trc_controller.cfg` ファイルを保存した後、コントローラーをインストールします。

Windows™ オペレーティング・システム・インストール用のコントローラーの事前構成

1. `trc_controller.cfg` ファイルを `trc_controller_setup.exe` または `trc_controller.msi file` と同じディレクトリーにコピーします。
2. コントローラーのインストール・ファイルを実行します。

コントローラーが構成済みの設定とともにインストールされます。

注: コントローラーの事前構成は、Linux™ オペレーティング・システムでのインストールではサポートされていません。必要な場合、ソース `.rpm` ファイルを変更して、コントローラー `.rpm` ファイルを再作成できます。

デフォルトの構成ファイルのコンテンツを利用してカスタム構成ファイルを作成し、独自の値を設定します。

fips.compliance=false sp800131a.compliance=false enable.address.history=true enable.user.history=false enable.domain.history=true history.max.items=20 tool01.ToolName = Control Panel tool01.ToolCommand

= [SystemFolder]\\control.exe tool01.ToolParameters = tool01.ToolUser = tool02.ToolName = Command Prompt tool02.ToolCommand = [SystemFolder]\\cmd.exe tool02.ToolParameters = tool02.ToolUser = tool03.ToolName = Administrator Command Prompt tool03.ToolCommand = [SystemFolder]\\cmd.exe tool03.ToolParameters = tool03.ToolUser = admin tool04.ToolName = Task Manager tool04.ToolCommand = [SystemFolder]\\taskmgr.exe tool04.ToolParameters = tool04.ToolUser = tool05.ToolName = Windows™ Explorer tool05.ToolCommand = [WindowsFolder]\\explorer.exe tool05.ToolParameters = tool05.ToolUser = tool06.ToolName=Terminal tool06.ToolCommand=/usr/bin/gnome-terminal tool06.ToolParameters = tool06.ToolUser = tool07.ToolName=Control Panel tool07.ToolCommand=/usr/bin/gnome-control-center tool07.ToolParameters = tool07.ToolUser = tool08.ToolName= tool08.ToolCommand= tool08.ToolParameters = tool08.ToolUser = tool09.ToolName= tool09.ToolCommand= tool09.ToolParameters = tool09.ToolUser = tool10.ToolName= tool10.ToolCommand= tool10.ToolParameters = tool10.ToolUser = # Custom keys # example.KeySequenceName = Inject F1 # example.KeySequenceValue = [F1] # # サポートされているキーコードのリストについては、ユーザーガイドを参照してください key01.KeySequenceName = key01.KeySequenceValue = key02.KeySequenceName = key02.KeySequenceValue = key03.KeySequenceName = key03.KeySequenceValue =

コマンド・ライン・ツールをインストールします。

コマンド・ライン・ツールを使用すると、コマンド・ラインからリモート・コントロール・セッションを開始したり、ターゲット・ユーザーによる操作なしにターゲット・システムでコマンドを実行したりすることができます。コマンドは、 BigFix® Remote Control サーバー ・インターフェースを使用せずにターゲットに接続する場合や、 複数のコマンドを自動的に実行するスクリプトの一部として使用する場合に便利です。このコマンド・ライン・ツールは、Windows™ オペレーティング・システムおよび Linux™ オペレーティング・システムでの実行でのみ使用可能です。

Remote Control では、2 とおりの方法でコマンド・ライン・ツールをインストールすることができます。BigFix® コンソールにアクセスできる場合は、適用 Fixlet を使用してツールをデプロイします。これらのコンポーネントのデプロイについて詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。もう 1 つの方法は、Remote Control コントローラーのインストール・ファイルを使用する方法です。

Windows™ システムでの CLI ツールのインストール

この `trc_cli_setup.exe` ファイルは、コントローラー・コンポーネントを Windows™ システムにインストールするために必要です。

Windows™ コンポーネントのインストール・ファイルの入手方法について詳しくは、「 Remote Control コンポーネントのインストール 」を参照してください。適切な方法を選択してファイルを入手してください。

1. `trc_cli_setup.exe` ファイルを実行する。
2. ファイルのダウンロード・ウィンドウで、**「実行」** または**「保存」**を選択します。

   実行

   「実行」 を選択してインストールを開始します。
   a. 「ようこそ」画面で**「次へ」**をクリックします。
   b. 使用許諾契約に同意し、**「次へ」**をクリックします。

c. インストール・ファイルの場所を受け入れるか変更し、**「次へ」**をクリックします。
d. サーバー・アドレスの画面で、以下の情報を入力して **「次へ」** をクリックします。

サーバーホスト名。

Remote Control サーバーの IP アドレスまたはサーバー名を入力します。

セキュア接続 (https) を使用

サーバーへの接続にセキュア接続を使用するには、https を選択します。

詳細設定

追加の構成設定を行うには、**「詳細設定」** をクリックします。

サーバー・ポート

サーバーが listen するポート番号を入力します。

サーバー・コンテキスト

サーバー・コンテキストの値を入力します。例: `trc`

FIPS 認定の暗号プロバイダーの使用

FIPS 準拠のツールをインストールするには、**「FIPS 認定の暗号プロバイダーの使用」**を選択します。

NIST SP800-131A 準拠性を使用可能にする (FIPS を使用可能にする) (Enable NIST SP800-131A compliance (Enables FIPS))

NIST SP800-131A 準拠のツールをインストールするには、**「NIST SP800-131A 準拠を有効にする (FIPS を有効にする) (Enable NIST SP800-131A compliance (Enables FIPS))」**を選択します。

e. プロキシー・サーバーを使用しない場合は、**「プロキシー設定」**パネルで**「次へ」**をクリックします。
- プロキシーを使用している場合は、**「プロキシー・サーバーまたは Remote Control ゲートウェイを使用します」**を選択します。関連する情報を入力します。
  i. プロキシー・サーバーの IP アドレスまたはホスト名を入力します。
  ii. プロキシー・サーバーが listen しているポートを入力します。
  iii. **「HTTP プロキシーを使用します」**または**「Remote Control ゲートウェイを使用します」**を選択します。
  iv. **「プロキシーは認証が必要です」**を選択し、プロキシー・サーバーに対する認証のためのユーザー ID およびパスワードを入力します。ターゲットの始動時にユーザー ID およびパスワードは自動的に暗号化されます。パスフレーズの自動暗号化について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

注: CLI がターゲットなしで独立してインストールされる場合、および CLI が標準のユーザーによって実行される場合は、CLI はプロキシー資格情報を自動的に暗号化できません。ターゲットのパッケージに含まれている CLI を使用する場合は、プロキシー資格情報がターゲットによって自動的に暗号化されます。レジストリーまたは構成ファイル内の設定を編集した後、ターゲットを再始動する必要があります。独立型の CLI ツールを使用する場合は、Windows オペレーティング・システムの**管理者のコマンド・プロンプト**から、あるいは Linux に root としてログインしたときに、CLI を一度実行する必要があります。

v. 「**次へ**」をクリックします。

f. デフォルトのポートを受け入れるか、値を入力し、**「次へ」** をクリックします。

g. **「インストール」**をクリックします。

h. 「**終了**」をクリックします。

保存\n

「保存」を選択して、`trc_cli_setup.exe` ファイルを特定の場所に保存します。

注: この実行可能ファイルを実行して、コマンド・ライン・ソフトウェアをインストールします。

以下の実行可能ファイルが、選択されたディレクトリー内にあります。

`wrc.exe`

このツールを使用して、ターゲットとのリモート・コントロール・セッションを開始します。

`wrcmdpcr.exe`

このツールを使用して、ターゲットでコマンドを実行し、 そのコマンドからの出力をコマンド発行元のコンピューターに表示します。

コマンド・ライン・ツールの使用について詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

での CLI ツールのインストール Linux™

Linux™ コンピューターに CLI ツールをインストールするには、Remote Control インストール・ファイルで提供される RPM ファイルを使用します。

注: ブローカー・コンポーネントのインストール・パッケージは、32 ビット・バージョンの以下のライブラリーに依存しています。**glibc libgcc**、**libblkid**、**libstdc++**。

`trc-cli-10.x.x.i386.rpm` ファイルを使用して、 Linux™ に CLI ツールをインストールします。ここで、*10.x.x* はインストールするバージョンに該当します。 Linux™コンポーネントのインストール・ファイルの入手方法について詳しくは、「Remote Control コンポーネントのインストール」を参照してください。適切な方法を選択してファイルを入手してください。

注: `trc-target` RPM ファイルがインストールされている場合、ターゲットには既に CLI コマンドが組み込まれているため、`trc-cli` RPM ファイルをインストールする必要は必要ありません。これらのコマンドの使用について詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

1. 以下のコマンドを入力して、コマンド・ライン・ソフトウェアをインストールします。
   ここで、*10.x.x* はインストールするバージョンに該当します。

   ```
   $ rpm -ivh ~/BigFix/Tivoli_Remote_Control/RCTarget/trc-cli-10.x.x.i386.rpm
   ```

2. インストールが完了したら、`/etc/trc_target.properties` ファイルを編集し、構成を設定します。
   - **ServerURL** の値を、ご使用の BigFix® Remote Control サーバー のホスト名または IP アドレスに設定します。
   - FIPS 準拠の場合は、**FIPSCompliance** の値を Yes に設定します。
   - NIST SP800-131a 準拠の場合、*SP800131ACompliance* の値を yes に設定します。
3. ファイルを保存します。

これらのコマンドの使用について詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

Remote Control でのゲートウェイ・サポートのインストール

ターゲット、コントローラー、およびサーバーが、相互に直接接続できない別々のネットワーク上にある場合は、ゲートウェイ・サポートをインストールし、構成することができます。

Remote Control では、2 とおりの方法でゲートウェイ・サポートをインストールすることができます。BigFix® コンソールにアクセスできる場合は、適用 Fixlet を使用してゲートウェイ・サポートをデプロイします。詳しくは、BigFix® Remote Control コンソール・ユーザー・ガイド を参照してください。別の方法として、Remote Control ゲートウェイ・サポートのインストール・ファイルを使用することもできます。

Windows ゲートウェイ・サポートのインストール

Windows オペレーティング・システムにゲートウェイ・サポートをインストールするには、`trc_gateway_setup.exe` ファイルが必要です。Windows ゲートウェイ・サポート・ファイルの入手方法について詳しくは、Remote Control コンポーネントのインストールを参照してください。適切な方法を選択してファイルを入手してください。

注: ゲートウェイ・サポートは、サイレント・インストールを実行することでユーザー対話を行わずにインストールすることもできます。サイレント・インストールについて詳しくは、サイレント・インストールによる ゲートウェイ・サポートのインストールを参照してください。

ゲートウェイ・サポートをインストールするには、以下の手順を実行します。

1. `trc_gateway_setup.exe` ファイルを実行する。
2. 「ようこそ」画面で**「次へ」**をクリックします。
3. インストール先を受け入れるか変更し、**「次へ」**をクリックします。
4. **「インストール」**をクリックします。
5. インストールが完了したら、**「完了」**をクリックします。

ゲートウェイ・サポートをインストールしたら、ご使用の環境向けに構成する必要があります。ゲートウェイ・サポートの構成について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

サイレント・インストールによる ゲートウェイ・サポートのインストール

サイレント・インストールの実行によって Windows® システムにゲートウェイ・サポートをインストールするには、以下のステップを実行します。

1. `TRC` というフォルダーをルート・ドライブに作成します。
2. `trc_gateway_setup.exe` ファイルを `TRC` にコピーします。
3. コマンド・プロンプト・ウィンドウを開き、`TRC` に移動します。
4. 以下のコマンドをすべて 1 行で入力します。

```
trc_gateway_setup.exe /s /v"/qn"
```

/s

サイレント・インストールを指示します。

/v"

/v に付加されるストリングには、インストールを実行するソフトウェアである `msiexec.exe` のパラメーターが含まれます。

/qn

進行状況ウィンドウを表示せずにサイレント・インストールを実行します。

ゲートウェイ・サポートの構成について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

Linux™ ゲートウェイ・サポートのインストール

Linux™ コンピューターにゲートウェイ・サポートをインストールするには、Remote Control インストール・ファイルで提供される RPM ファイルを使用します。

注: ブローカー・コンポーネントのインストール・パッケージは、32 ビット・バージョンの以下のライブラリーに依存しています。**glibc libgcc**、**libblkid**、**libstdc++**。

`trc-gateway-10.x.x.i386.rpm` ファイルを使用して、Linux™ にゲートウェイ・サポートをインストールします。ここで、*10.x.x* はインストールするバージョンです。Linux™ ゲートウェイ・サポート・ファイルの入手について詳しくは、「Remote Control コンポーネントのインストール」を参照してください。適切な方法を選択してファイルを入手してください。

ゲートウェイ・サポートをインストールするには、コマンド・プロンプトに以下のコマンドを入力します。ここで、*10.x.x* はインストールするバージョンです。

```
$ rpm -ivh trc-gateway-10.x.x.i386.rpm
```

ゲートウェイ・サポートをインストールしたら、ご使用の環境向けに構成します。ゲートウェイ・サポートの構成について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

ブローカー・サポートのインストール

コントローラーからターゲット・コンピューターに直接アクセスできず、インターネット経由で接続する場合は、コントローラーをターゲット・コンピューターに接続するコンピューターにブローカー・サポートをインストールする必要があります。

Remote Control では、2 とおりの方法でブローカー・サポートをインストールすることができます。BigFix® コンソールにアクセスできる場合は、適用 Fixlet を使用してブローカー・サポートを導入します。詳しくは、*BigFix® Remote Control* コンソール・ユーザー・ガイド を参照してください。もう 1 つの方法は、Remote Control ブローカーのインストール・ファイルを使用する方法です。

Windows™ ブローカー・サポートのインストール

Remote Control のブローカー・インストール・ファイルは実行可能ファイルであり、Windows™ コンピューターにブローカー・サポートをインストールするために使用できます。

Windows™ システムにブローカー・サポートをインストールするには、`trc_broker_setup.exe` ファイルが必要です。Windows™ ブローカー・サポート・ファイルの入手方法について詳しくは、「Remote Control コンポーネントのインストール」を参照してください。適切な方法を選択してファイルを入手してください。

Windows™ コンピューターにブローカー・サポートをインストールするには、以下の手順を実行します。

1. `trc_broker_setup.exe` ファイルを実行する。
2. 「ようこそ」画面で**「次へ」**をクリックします。
3. 使用許諾書条件に同意し、**「次へ」**をクリックします。
4. デフォルトの場所を受け入れるか、インストール先フォルダーを変更します。「**次へ**」をクリックします。

   デフォルトの場所は次のとおりです。 `\Program Files\BigFix\Remote Control\Broker`

5. **「インストール」**をクリックします。
6. 「**終了**」をクリックします。

以下のファイルが *[working dir]*`\Broker` ディレクトリーにインストールされます。ここで *[working dir]* は、ブローカー・サポートのインストール先 Windows™ オペレーティング・システムのバージョンによって決まります。

例えば、`\Documents and Settings\All Users\Application Data\BigFix\Remote Control` です。

- `trc_broker.properties`
- `TRCICB-computername-day.log` ここで、*computername* はブローカーのインストール先システムのコンピューター名であり、*day* はブローカーをインストールした曜日です。

Remote Control- インターネット接続ブローカー・サービスが登録され、開始されていることを確認してください。

Linux™ ブローカー・サポートのインストール

Linux™ コンピューターにブローカー・サポートをインストールするには、Remote Control インストール・ファイルで提供される RPM ファイルを使用します。

注: ブローカー・コンポーネントのインストール・パッケージは、32 ビット・バージョンの以下のライブラリーに依存しています。**glibc libgcc**、**libblkid**、**libstdc++**。

`trc-broker-10.x.x.i386.rpm` ファイルを使用して、Linux™ にブローカー・サポートをインストールします。ここで、*10.x.x* はインストールするバージョンです。Linux™ コンポーネントのインストール・ファイルの入手方法について詳しくは、「Remote Control コンポーネントのインストール」を参照してください。適切な方法を選択してファイルを入手してください。

コマンド・プロンプトに以下のコマンドを入力して、ブローカー・ソフトウェアをインストールします。ここで、*10.x.x* はインストールするバージョンです。

```
rpm -ivh trc-broker-10.x.x.i386.rpm
```

以下のファイルが、`/opt/bigfix/trc/broker` ディレクトリーにインストールされます。

- libcrypto.so.1.0.0
- libssl.so.1.0.0
- trc_icb
- ライセンス・ディレクトリー

`trc_broker.properties` ファイルが、`/etc` ディレクトリーにインストールされます。

ブローカー・サポートをインストールしたら、`trc_broker.properties` ファイルを編集してブローカー・プロパティーを構成します。

コンポーネント・インストール・ファイルを解凍するためのユーティリティー

Remote Control には、各コンポーネントに必要なインストール・ファイルを解凍するために使用できるユーティリティーが用意されています。

`BigFix_Rem_Cntrl_V914_Image_3.tar` ファイルからデータを抽出します。*platform* ご使用のオペレーティングシステムに関連する `\Disk1\InstData\platform\VM` ディレクトリーに移動します。ユーティリティーは、`trc_additional_setup.exe` または `trc_additional_setup.bin` ファイルを使用してのみ実行できます。その他のサポート対象オペレーティング・システム用のインストール・ファイルを解凍するには、例えば macOS の場合であれば、 `trc_additional_setup` のいずれかのファイルを実行してインストール・ファイルを解凍した後、 `.pkg` ファイルを macOS システムにコピーしてください。

追加のセットアップ・ユーティリティーを実行するために使用するファイルは、以下のとおりです。

Windows® システム

`trc_additional_setup.exe`

Linux® システム

`trc_additional_setup.bin`

`BigFix_Rem_Cntrl_V914_Image_3.tar` ファイルの入手方法について詳しくは、「インストール・ファイルの入手」を参照してください。

以下のコンポーネント・インストール・ファイルを解凍できます。

- サーバー・インストール・メディア: これらのファイルを使用して、サーバーの手動インストールを実行します。`trc.war` ファイルと手順が解凍されます。
- ターゲット・インストール・メディア:
  - Windows パッケージ (`.exe` および `.msi`)
  - Linux パッケージ (`.rpm`)
  - macOS パッケージ (.pkg)
- コントローラー・インストール・メディア:
  - Windows パッケージ (`.exe` および `.msi`)
  - Linux パッケージ (`.rpm`)
  - macOS パッケージ (.pkg)
- コマンド行インターフェース・インストール・メディア:
  - Windows パッケージ (`.exe` および `.msi`)
  - Linux パッケージ (`.rpm`)
- ゲートウェイ・インストール・メディア:
  - Windows パッケージ (`.exe` および `.msi`)
  - Linux パッケージ (`.rpm`)
- インターネット接続ブローカー・インストール・メディア:

- Windows パッケージ (`.exe` および `.msi`)
- Linux パッケージ (`.rpm`)

追加のセットアップ・ユーティリティーを使用したインストール・ファイルの解凍

追加セットアップ・ユーティリティーを実行するには、以下の手順を実行します。

1. ご使用のオペレーティング・システムに該当する `trc_additional_setup` ファイルを実行します。このファイルは、`BigFix_Rem_Cntrl_V914_Image_3.tar` ファイルから解凍したファイル構造内から実行する必要があります。使用するファイルについて詳しくは、コンポーネント・インストール・ファイルを解凍するためのユーティリティーを参照してください。
2. 言語を選択して、**「OK」**をクリックします。
3. ご使用条件に同意し、**「次へ」**をクリックします。
4. 必要なファイルを解凍しないオプションをクリアします。必要なオプションのみが選択された状態にしてある必要があります。
   a. サーバー・インストール・メディア: サーバーのインストールに必要なファイルを解凍する場合に選択します。
   b. ターゲット・インストール・メディア: ターゲットのインストールに必要なファイルを解凍する場合に選択します。
   c. コントローラー・インストール・メディア: コントローラーのインストールに必要なファイルを解凍する場合に選択します。
   d. コマンド・ライン・インターフェース・インストール・メディア: コマンド・ライン・インターフェースの実行に必要なファイルを解凍する場合に選択します。
   e. ゲートウェイ・インストール・メディア: ゲートウェイ・サポートのインストールに必要なファイルを解凍する場合に選択します。
   f. インターネット接続ブローカー・インストール・メディア: ブローカー・サポートのインストールに必要なファイルを解凍する場合に選択します。
5. 「**次へ**」をクリックします。
6. インストール・フォルダーを受け入れるか変更します。「**次へ**」をクリックします。
7. 要約画面で、**「インストール」**をクリックします。
8. 完了したら、**「完了」**をクリックします。
9. 選択したインストール・フォルダーに移動します。

インストール・ファイルが以下のディレクトリーに配置されます。

- `RCServer` - サーバー・インストール・ファイル `trc.war`。
- `RCTarget` - ターゲットのインストール・ファイル。
- `RCController` - コントローラーのインストール・ファイル。
- `RCCLI` - コマンド・ライン・ツールのインストール・ファイル。
- `RCGateway` - ゲートウェイのインストール・ファイル。
- `RCBroker` - ブローカーのインストール・ファイル。

セキュア・ターゲット登録の有効化

無許可のターゲットが Remote Control サーバーに登録されないよう、セキュア登録機能を有効にし、トークンを使用してターゲットを認証できます。

セキュア登録機能は、インストーラー・プログラムを使用する場合、Remote Control サーバーの新規インストール時にデフォルトで有効になります。サーバーをインストールした後に、サーバーで登録トークンを作成し、ターゲットのインストール時にそのトークンを使用します。セキュア登録機能について、およびトークンの作成方法について詳しくは、「」*BigFix® Remote Control* 管理者ガイド の「**セキュア・ターゲット登録**」の章を参照してください。

サーバーでのセキュア・ターゲット認証の有効化

BigFix® Remote Control サーバー には、ターゲットのセキュア登録を有効にするためのインストール・オプションが用意されています。

この機能を有効にすると、サーバーはターゲットによって送信されたセキュア登録トークンがサーバー上の既存のトークンと一致するか検証します。トークンが有効であれば、ターゲットはサーバーに登録され、サーバーからエンドポイント・トークンを受け取ります。ターゲットは、サーバーに接続するたびにエンドポイント・トークンをサーバーに送信します。

注: データベースに既存のターゲットがあり、セキュア登録機能を有効にした場合、既存のターゲットは、エンドポイント・トークンがないためにサーバーに正常に接続できません。そのため、既存のターゲットが引き続きサーバーに接続できるよう、有効なセキュア登録トークンを作成または使用し、そのトークンを指定して既存のターゲットを再インストールする必要があります。

サーバー・インストーラー・プログラムの実行時におけるセキュア登録の有効化

インストーラー・プログラムを使用してサーバーをインストールするときに、セキュア・ターゲット登録機能を有効にすることができます。この機能は、サーバーの新規インストール時にデフォルトで有効になります。

セキュア登録機能を有効にするには、以下のステップを実行します。

1. サーバー・インストーラーを使用したインストールのインストール手順に従います。
2. **「Web サーバーのパラメーター」**ウィンドウで、**「https を使用するようにターゲットに強制」**が選択されていることを確認します。
3. **「セキュア登録トークンを使用してターゲットを登録する」**を選択します。
4. インストールを完了します。

サーバーをインストールし、セキュア・ターゲット登録機能を有効にしたら、登録トークンを作成します。登録トークンの作成について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

サーバーのインストール後のセキュア・ターゲット登録の有効化

サーバーのインストール後に、`trc.properties` ファイルのプロパティーを編集してセキュア・ターゲット登録機能を有効にすることができます。

サーバーのインストール後にセキュア登録機能を有効にするには、以下のステップを実行します。

1. サーバーの UI で、**「アドミニストレーター」 > 「プロパティー・ファイルを編集」**を選択します。
2. リストから `trc.properties` を選択します。
3. **rc.enforce.secure.registration** を `true` に設定します。

   enforce.secure.endpoint.callhome プロパティーと **enforce.secure.endpoint.upload** プロパティーも `true` に設定されていることを確認します。
4. 「**送信**」をクリックします。
5. **「アドミニストレーター」 > 「アプリケーションをリセット」**をクリックします。

プロパティー・ファイルを手動で編集してこのプロパティーを true に設定することもできます。このファイルを編集したら、サーバーを再始動します。プロパティー・ファイルは、以下のディレクトリーにあります。

Windows® システム

[*installdir*]\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes

installdir は、BigFix® Remote Control サーバー がインストールされているディレクトリーです。例えば、以下のようにします。

```
C:\Program Files\BigFix\TRC\server\wlp\usr\servers\trcserver
\apps\TRCAPP.ear\trc.war\WEB-INF\classes
```

Linux® システム

[*installdir*]/wlp/usr/servers/trcserver/apps/TRCAPP.ear/trc.war/WEB-INF/classes

installdir は、BigFix® Remote Control サーバー がインストールされているディレクトリーです。例えば、以下のようにします。

```
/opt/BigFix/TRC/server/wlp/usr/servers/trcserver/apps/TRCAPP.ear
/trc.war/WEB-INF/classes
```

セキュア・ターゲット登録用のトークンの追加

BigFix® Remote Control ターゲットには、セキュア登録トークンを追加するためのインストール・オプションが用意されています。BigFix® コンソールで Fixlet を実行してトークンを追加することもできます。

このトークンを使用して、無許可のターゲットが Remote Control サーバーに登録されないようにします。サーバーでトークンを作成し、ターゲットのインストール時にそのトークンを使用します。サーバーでは必ずセキュア登録機能も有効にしてください。

ターゲットは、最初にサーバーに接続するときにセキュア登録トークンをサーバーに送信します。サーバーはトークンがサーバー上の既存のトークンと一致するか確認します。トークンが有効であれば、ターゲットはサーバーに登録され、サーバーからエンドポイント・トークンを受け取ります。

注:

ターゲットは、サーバーへのセキュア接続を使用する場合にのみ、サーバーへのコール・ホームにトークンを含めます。ターゲットがサーバーへの接続に使用するサーバー URL の先頭は HTTPS になっていなければなりません。

Windows™ システムへのターゲットのインストール時におけるセキュア登録トークンの追加

Windows™ システムでは、さまざまな方法でセキュア登録トークンを追加できます。

- ターゲット・インストーラー・プログラムを使用してトークンを追加する。
- コマンド・ラインからターゲットのインストールを実行してトークンを追加する。
- ターゲットをインストール後に変更する。

セキュア登録トークンを使用したターゲット・インストーラーの実行

ターゲット・コンポーネントをインストールする場合、BigFix® Remote Control ターゲット・インストーラーを使用してターゲットにセキュア登録トークンを渡します。ターゲットは、サーバーに初めて接続するときに、そのトークンを使用してサーバーで認証を受けます。

トークンを使用してターゲット・インストーラーを実行するには、以下のステップを実行します。

1. Windows ターゲットのインストールのインストール手順に従います。
2. **「サーバーのアドレス」**ウィンドウで、セキュア・ターゲット登録用にトークンを**「セキュア登録トークン (Secure registration token)」**フィールドに入力するか貼り付けます。
   必ず**「セキュア接続 (https) を使用」**も選択してください。セキュア・ターゲット登録について詳しくは、セキュア・ターゲット登録用のトークンの追加を参照してください。
3. インストールを完了します。

セキュア登録トークンを伴うターゲットのサイレント・インストールの実行

Remote Control ターゲットの新規サイレント・インストールを実行する際に、セキュア登録トークンとともにターゲットをインストールします。

ターゲットのカスタム・インストールの実行について詳しくは、「*BigFix® Remote Control* インストール・ガイド」を参照してください。

ターゲット・コンポーネントとトークンをインストールするには、次のコマンドを 1 行で実行します。

trc_target_setup.exe /s /v"/qn REGISTRATIONTOKEN=*xxxxxxxxxxx* TRC_SERVER_HOSTNAME=*yyyyyyyyyyyyy*"

xxxxxxxxxxx はトークンに置き換え、*yyyyyyyyyyyyy* は Remote Control サーバーのホスト名に置き換えます。

ターゲットのアップグレード時におけるサイレント・インストールの実行について詳しくは、セキュア登録トークンを使用したターゲットのアップグレードを参照してください。

ターゲットのインストール後のセキュア登録トークンの追加

ターゲット・コンポーネントをインストールしていてセキュア登録トークンをインストールしていない場合は、ターゲットを変更してトークンを追加できます。

トークンの追加方式を選択します。

インストーラー・プログラムを実行してトークンを追加する場合は、以下のステップを実行します。

1. **「コントロール パネル」**に移動します。例えば、**「スタート」「コントロール パネル」「プログラム」「プログラムと機能」**に進みます。
2. **Remote Control「-Target」**を右クリックします。
3. **「変更」**を選択します。
4. **「プログラム保守」**ウィンドウで、**「変更」**を選択します。
5. **「サーバーのアドレス」**ウィンドウが表示されるまで、**「次へ」**をクリックします。
6. トークンを**「セキュア登録トークン (Secure registration token)」**フィールドに入力するか貼り付けます。必ず**「セキュア接続 (https) を使用」**も選択してください。
7. **「インストール」**をクリックします。
8. **「終了」**をクリックします。

ターゲット・レジストリーを編集してトークンを追加する場合は、以下のステップを実行します。

1. ターゲットレジストリを編集して、次の場所に移動します `HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\Remote Control\Target`

   注: 64 ビット・システムでは、すべての 32 ビット・レジストリー・キーは **WOW6432Node** キーの下にあります。例えば、 `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BigFix\Remote Control\Target`

2. **RegistrationToken** を右クリックします。
3. **「変更」**をクリックします。
4. トークンを入力するか貼り付けます。
5. ターゲットを再始動します。

セキュア登録トークンを使用したターゲットのアップグレード

セキュア登録トークンを使用して Remote Control ターゲットをアップグレードします。

アップグレード・プロセスでは 2 つのステップを行う必要があります。最初にターゲットをアップグレードし、次にトークンを使用してインストールを実行する必要があります。

- インストーラーによってトークンを使用してターゲットをアップグレードするには、以下のステップを実行します。

  1. `trc_target_setup.exe` ファイルを実行する。
  2. 自動アップグレードに対して**「はい」**を選択します。
  3. 「**次へ**」をクリックします。
     「使用中のファイル」ウィンドウが表示されたら、**「OK」**をクリックします。
  4. 「**終了**」をクリックします。
  5. トークンを追加するには、ターゲットのインストール後のセキュア登録トークンの追加のステップを実行します。

- サイレント・インストールを実行し、トークンを使用してターゲットをアップグレードする場合は、以下のステップを実行します。

  1. コマンド・プロンプトに、trc_target_setup.exe /s /v"/qn" と入力して、ターゲットをアップグレードします。
  2. トークンの実行を追加するにはtrc_target_setup.exe /s /v"/qn REGISTRATIONTOKEN=xxxxxx REINSTALL=ALL"

     xxxxxx は、作成して保存したトークンに置き換えます。

Linux™ システムへのターゲットのインストール時における登録トークンの追加

Linux™ システムでは、ターゲットのインストール後に `/etc/trc_target.properties` ファイルを編集してセキュア・ターゲット認証用の登録トークンを追加できます。

Linux ターゲットにセキュア登録トークンを追加するには、ターゲットのインストール後に以下のステップを実行します。Linux システムへのターゲットのインストールについて詳しくは、Linux ターゲットのインストールを参照してください。

1. `/etc/trc_target.properties` ファイルを編集します。
2. 登録トークンのプロパティーを追加し、そのプロパティーを登録トークンの値に設定します。**RegistrationToken** = *xxxxxxxxxxxxxxx* と設定します。*xxxxxxxxxxxxxxx* はトークン・データに置き換えます。例えば、6386e21f-4316-460b-b339-deb3d132f3c7 とします。
3. ファイルを保存します。
4. ターゲット・サービスを再起動します。詳しくは、『Linux コンポーネントの開始、停止、または再起動』を参照してください。

ターゲットへのスマート・カード認証のサポートのためのドライバーのインストール

BigFix® Remote Control ターゲットには、仮想スマート・カード・リーダー・ドライバーをインストールするためのインストール・オプションがあります。BigFix® コンソールから Fixlet を実行することによって、ドライバーをインストールすることもできます。

リモート認証でスマート・カードを使用できるようにする場合、あるいはターゲット・コンピューターに対してアクションを実行する場合は、仮想スマート・カード・リーダー用のデバイス・ドライバーが必要です。

リモート・コントロール・セッション中に、ターゲットは仮想カード・リーダーを作成します。コントローラー・ユーザーは、使用しているシステム上にある物理カード・リーダーを選択し、これを仮想カード・リーダーに接続して、ターゲット・システムがスマート・カードにアクセスできるようにします。セッション中に、Windows から仮想カード・リーダーに要求が出されると、ターゲットはその要求をコントローラー・システム上の物理カード・リーダーにリダイレクトします。

セッション中のスマート・カード機能の使用について詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

仮想スマート・カード・リーダーのデバイス・ドライバーは、Windows 7 以降、および Windows Server 2008 R2 以降でのみサポートされます。

注: Windows 7 または Windows Server 2008 R2 でドライバーをインストールする場合は、ターゲット上に以下の更新をインストールする必要がある場合があります。

KB2921916

「Windows 7 または Windows Server 2008 R2 にドライバーをインストールする際に、「信頼していない発行元」ダイアログ・ボックスが表示される」という問題を解決するための Microsoft 修正プログラム。

KB3033929

Windows 7 for x64-Based Systems 用セキュリティー更新プログラム。

インストーラーを使用した仮想スマート・カード・リーダー・ドライバーのインストール

ターゲット・コンポーネントのインストール時に、BigFix® Remote Control ターゲット のインストーラーを使用して、仮想スマート・カード・リーダー用のデバイス・ドライバーをインストールします。既にターゲット・コンポーネントがインストールされているシステムで、インストーラーを使用してドライバーをインストールすることもできます。

ターゲットのインストール後にドライバーを追加する方法について詳しくは、インストーラーを使用した仮想スマート・カード・リーダー・ドライバーの追加または削除を参照してください。

ターゲット・ソフトウェアおよび仮想スマート・カード・リーダー用のデバイス・ドライバーをインストールするには、以下の手順を実行します。

1. Windows ターゲットのインストールの手順に従います。
2. **「追加機能 (Additional features)」**ウィンドウで、**「仮想スマート・カード・リーダー用のデバイス・ドライバーをインストール (Install device driver for Virtual Smart Card Reader)」**を選択します。

スマート・カード認証が要求された場合にターゲットが自動的にドライバーを有効にすることができるように、ドライバーのインストール後に証明書をインストールする必要があります。Fixlet の実行による証明書のインストールについて詳しくは、「*BigFix® Remote Control* コンソール・ユーザー・ガイド」を参照してください。証明書をダウンロードして手動でインストールすることもできます。詳しくは、「*BigFix® Remote Control* コンソール・ユーザー・ガイド」を参照してください。

インストーラーを使用した仮想スマート・カード・リーダー・ドライバーの追加または削除

ターゲット・コンポーネントをインストールした後、インストーラーを使用して仮想スマート・カード・リーダー用のデバイス・ドライバーを追加または削除することができます。

ターゲット・コンポーネントをインストールしていてデバイス・ドライバーをインストールしていない場合、ターゲットを変更して、ドライバーを追加することができます。ドライバーを追加するには、以下の手順を実行します。

1. **「コントロール パネル」**に移動します。例えば、**「スタート」「コントロール パネル」「プログラム」「プログラムと機能」**に進みます。
2. **Remote Control「-Target」**を右クリックします。
3. **「変更」**を選択します。
4. **「プログラム保守」**ウィンドウで、**「変更」**を選択します。
5. **「追加機能」**ウィンドウが表示されるまで、**「次へ」**をクリックします。
6. **「仮想スマート・カード・リーダー用のデバイス・ドライバーをインストール (Install device driver for Virtual Smart Card Reader)」**を選択します。**「次へ」**をクリックします。
7. **「インストール」**をクリックします。
8. **「終了」**をクリックします。

リモート・コントロール・セッション中にスマート・カード認証が要求された場合、ターゲットは自動的にドライバーを有効にすることができます。ドライバーを削除するには、同じ手順を使用します。ステップ 6 では、**「仮想スマート・カード・リーダー用のデバイス・ドライバーをインストール (Install device driver for Virtual Smart Card Reader)」**をクリアします。

スマート・カード認証が要求された場合にターゲットが自動的にドライバーを有効にすることができるように、ドライバーのインストール後に証明書をインストールする必要があります。Fixlet の実行による証明書のインストールについて詳しくは、「*BigFix® Remote Control* コンソール・ユーザー・ガイド」を参照してください。証明書をダウンロードして手動でインストールすることもできます。詳しくは、「*BigFix® Remote Control* コンソール・ユーザー・ガイド」を参照してください。

サイレント・インストールの実行による仮想スマート・カード・リーダー・ドライバーのインストール

Remote Control ターゲットのサイレント・インストールの実行時に、仮想スマート・カード・リーダー用のデバイス・ドライバーをインストールします。

ターゲット・コンポーネントがインストールされていないコンピューターでサイレント・インストールを実行するときにドライバーをインストールすることができます。インストール済みのターゲットでドライバーを追加または削除することもできます。ターゲットのカスタム・インストールの実行について詳しくは、ターゲットのカスタム・インストールの実行を参照してください。

- ターゲット・コンポーネントおよび仮想スマート・カード・リーダー用のデバイス・ドライバーをインストールするには、次のコマンドを実行します。

  trc_target_setup.exe /s /v"/qn VSC=1"

- インストール済みのターゲットにドライバーを追加するには、次のコマンドを実行します。

  trc_target_setup.exe /s /v"/qn ADDLOCAL=vsc REINSTALL=service"

- インストール済みのターゲットからドライバーを削除するには、次のコマンドを実行します。

  trc_target_setup.exe /s /v"/qn REMOVE=vsc REINSTALL=service"

スマート・カード認証が要求された場合にターゲットが自動的にドライバーを有効にすることができるように、ドライバーのインストール後に証明書をインストールする必要があります。Fixlet の実行による証明書のインストールについて詳しくは、「*BigFix® Remote Control* コンソール・ユーザー・ガイド」を参照してください。証明書をダウンロードして手動でインストールすることもできます。詳しくは、「*BigFix® Remote Control* コンソール・ユーザー・ガイド」を参照してください。

ターゲットのアップグレード時の仮想スマート・カード・リーダー・ドライバーのインストール

Remote Control ターゲットのアップグレード時に仮想スマート・カード・リーダー用のデバイス・ドライバーをインストールします。

- インストーラーを使用してターゲットをアップグレードするときにドライバーをインストールするには、以下の手順を実行します。

  1. `trc_target_setup.exe` ファイルを実行する。
  2. 自動アップグレードに対して**「はい」**を選択します。
  3. 「**次へ**」をクリックします。
     「使用中のファイル」ウィンドウが表示されたら、**「OK」**をクリックします。

4. 「**終了**」をクリックします。

5. ドライバーをインストールするには、インストーラーを使用した仮想スマート・カード・リーダー・ドライバーの追加または削除に記載されている手順を実行します。

- サイレント・インストールを実行してアップグレードするときにドライバーをインストールするには、以下の手順を実行します。
  1. コマンド・プロンプトに、trc_target_setup.exe /s /v"/qn" と入力して、ターゲットをアップグレードします。
  2. ドライバーを追加するには、trc_target_setup.exe /s /v"/qn ADDLOCAL=vsc REINSTALL=service" を実行します。

スマート・カード認証が要求された場合にターゲットが自動的にドライバーを有効にすることができるように、ドライバーのインストール後に証明書をインストールする必要があります。Fixlet の実行による証明書のインストールについて詳しくは、「*BigFix® Remote Control* コンソール・ユーザー・ガイド」を参照してください。証明書をダウンロードして手動でインストールすることもできます。詳しくは、「*BigFix® Remote Control* コンソール・ユーザー・ガイド」を参照してください。

Fixlet の実行による仮想スマート・カード・リーダー・ドライバーおよび証明書のインストール

BigFix® コンソールで Fixlet を実行して、仮想スマート・カード・リーダー用のデバイス・ドライバーを証明書と一緒にインストールします。

ターゲットをインストールした後に、Fixlet を実行してドライバーおよび証明書をインストールすることができます。ドライバーおよび証明書をインストールするには、以下の手順を実行します。

1. **Remote Control**サイトで、**「デプロイメント」**ノードをクリックします。
2. **「Remote Control 仮想スマート・カード・リーダー・ドライバーバージョン10.0.0.23 および証明書をインストール」**タスクを選択します。
3. **「説明」**タブの情報を確認します。
4. **「アクション」**フィールドの説明に従い、ドライバーをインストールします。

スマート・カード認証に必要なデバイス・ドライバーおよび証明書がインストールされます。これで、リモート・コントロール・セッション中にコントローラー・ユーザーがシステム上の物理カード・リーダーを選択すると、ターゲットは仮想カード・リーダーを作成できるようになります。

注: Fixlet の実行中にエラーが報告される場合、ターゲットのインストール・ディレクトリーにある `VSCDriverInstall.log` ファイルをデバッグのために使用してください。

の実行による証明書のインストール Fixlet®

Fixlet® を使用して、仮想スマート・カード・リーダー用のデバイス・ドライバーに必要な証明書をインストールします。

Fixlet® を実行することによって、証明書をドライバーと一緒にインストールすることができます。ただし、**「Remote Control - 仮想スマート・カード・リーダーのドライバー状況」**分析の結果に、デバイス・ドライバーはコンピューターにインストールされていて証明書は存在していないことが示される場合、Fixlet® を実行して証明書をインストールすることができます。証明書をインストールするには、以下の手順を実行します。

1. **Remote Control**サイトで、**「デプロイメント」**ノードをクリックします。
2. **「仮想スマート・カード・リーダー・ドライバー・バージョン 10.0.0.23 の Remote Control 証明書をインストールする」**タスクを選択します。
3. **「説明」**タブの情報を確認します。
4. **「アクション」**フィールドの説明に従い、ドライバーをインストールします。

スマート・カード認証に必要な証明書がインストールされます。**「Remote Control - 仮想スマート・カード・リーダーのドライバー状況」**分析について詳しくは、『スマート・カード・サポートが有効になっているかどうかの判別』を参照してください。

注: Fixlet® の実行中にエラーが報告される場合、ターゲットのインストール・ディレクトリーにある `VSCCertsInstall.log` ファイルをデバッグのために使用してください。

仮想スマート・カード・リーダー用の証明書のダウンロード

仮想スマート・カード・リーダー用のデバイス・ドライバーに必要な証明書をダウンロードして、手動でインストールすることができます。例えば、Active Directory グループ・ポリシーを使用します。

証明書のダウンロードは複数の方法で実行できます。証明書をダウンロードする方法を選択してください。

- BigFix® コンソールの Remote Control サイトからのファイルのダウンロード:
    1. **「デプロイメント」**ノードをクリックして、**「Remote Control 仮想スマート・カード・リーダー・ドライバー・バージョン 10.0.0.23 および証明書をインストールする」**タスクを選択します。
    2. **「説明」**タブを選択します。
    3. **「説明」**フィールドの説明に従い、証明書をダウンロードします。
    4. `vsc_certs_1020.zip` ファイルを保存します。
    5. `.zip` ファイルから証明書ファイルを解凍します。
- インストール・メディアからの証明書ファイルの解凍:
    1. イメージ・ファイルにアクセスします。イメージ・ファイルについて詳しくは、インストール・ファイルの入手を参照してください。
    2. `BigFix_Rem_Cntrl_V10xx_Image_1.zip` ファイルをダウンロードします。ここで、*10xx* はインストールされているバージョンに対応します。
    3. `.zip` ファイルの `\Windows` ディレクトリーから、証明書ファイルを解凍します。

証明書をインストールするときに、`HCL_America_Inc-sha256.crt` ファイルを Trusted Publishers ストアにインストールする必要があります。`TrustedRoot.crt` ファイルおよび `DigiCertCA-sha256.crt` ファイルを Trusted Root Certificate Authorities ストアにインストールします。

コンポーネント・サービスの管理

Remote Control コンポーネントをインストールした後、これらのコンポーネントの構成を変更する場合は、コンポーネント・サービスを停止、開始、または再始動できます。

ご使用のオペレーティング・システムに該当するセクションに記載されたステップを実行してください。

Windows™ コンポーネントの開始、停止、または再起動

Remote ControlWindows™ コンポーネントの開始、停止、または再起動は、コントロール・パネルから実行できます。

Remote Control Windows™ コンポーネントを管理するには、以下の手順を実行します。

1. **「コントロール パネル」**で、**「管理ツール」「サービス」**を選択します。
2. 該当するサービスを強調表示します。

   サーバー・サービス

   Remote Control- サーバー

   ターゲット・サービス

   Remote Control- ターゲット

   ゲートウェイ・サービス

   Remote Control- ゲートウェイ

   ブローカー・サービス

   Remote Control- インターネット接続ブローカー
3. サービスに対するアクションを選択するための適切な方法を選択します。
   右クリックして、**「開始」**、**「停止」**、または**「再起動」**を選択するか、左側のリストから、**「開始」**,**「停止」**または**「再起動」**を選択します。

Linux™ コンポーネントの開始、停止、または再起動

Remote ControlLinux™ コンポーネントの開始、停止、または再起動は、コントロール・パネルから実行できます。

コンポーネントを管理するには、使用している Linux™ のバージョンに応じて、以下のいずれかのコマンドを使用します。

- `/sbin/service component action`
- `/etc/init.d/component action`

ここで、*component* は、管理対象のコンポーネント・サービス、*action* は、開始、停止、または再起動です。

サーバー

例えば、サーバー・サービスを開始します。

- `/sbin/service trcserver start`
- `/etc/init.d/trcserver start`

ターゲット

例えば、ターゲット・サービスを停止します。

- `/sbin/service trctarget stop`
- `/etc/init.d/trctarget stop`

ゲートウェイ

例えば、ゲートウェイ・サービスを再始動します。

- `/sbin/service trcgateway restart`
- `/etc/init.d/trcgateway restart`

ブローカー

例えば、ブローカー・サービスを再起動します。

- `/sbin/service trcbroker restart`
- `/etc/init.d/trcbroker restart`

電子メールの有効化

電子メール機能を使用するには、電子メール・サーバーのインストールとセットアップを行う必要があります。例えば、パスワードを忘れた場合や、レポートをエクスポートして電子メールで送信する目的、または特定のターゲットへのアクセスを要求する目的のためです。

電子メール機能を有効にするには、以下の手順を実行します。

1. 有効な管理者 ID およびパスワードを使用して、Remote Control サーバーにログオンします。
2. **「アドミニストレーター」 > 「プロパティー・ファイルを編集」**をクリックします。
3. **trc.properties** を選択します。
4. 以下の変数を編集します。

   email.enabled

   true に設定して電子メールを有効にします。

   SMTP.server

   使用するメール・サーバーのアドレスに設定します。

   SMTP.authentication

   true または false に設定します。SMTP の ID とパスワードによる認証を行う場合は true に設定します。

   SMTP.userid

SMTP サーバーのユーザー ID。

SMTP.password

SMTP サーバーのパスワード。

5. 「**送信**」をクリックします。

電子メール機能が有効になります。

LDAP の構成

Remote Control は、Lightweight Directory Access Protocol バージョン 3 のサポートを提供します。LDAP を使用すると、Remote Control データベースに対するユーザーおよびその関連グループ・メンバーシップの認証および統合を有効にすることができます。

LDAP 認証に必要なすべての構成情報は、`ldap.properties` ファイルにあります。構成を実行する前に、前提条件に関する情報を取得する必要があります。この情報によって、構成プロセスが単純化されます。

- Active Directory サーバーとの接続を確立するために Remote Control が使用するユーザー名およびパスワード。このユーザー名には、ディレクトリー・ツリーから必要なすべての情報を読み取るために必要な権限が割り当てられていなければなりません。
- Remote Control とともに使用する Active Directory サーバーの完全修飾サーバー・ホスト名または IP アドレス。
- エンタープライズ・シナリオでは、2 次バックアップ LDAP サーバーも Remote Control 内で構成されます。

LDAP 同期の設定

LDAP 認証を有効にするには、LDAP サーバーとの同期も有効にする必要があります。同期を有効にするには、`common.properties`ファイルと `ldap.properties` ファイルの値を編集します。

LDAP 認証の基本構成を行うには、以下の手順を実行します。

1. **「アドミニストレーター」 > 「プロパティー・ファイルを編集」**をクリックします。
2. `common.properties` ファイルを編集中であることを確認した上で、以下のプロパティーを編集します。

authentication.LDAP

LDAP 認証を有効または無効にします。

True

LDAP ユーザー認証が有効です。

注: Active Directory と同期するときに毎回ユーザーおよびユーザー・グループが Remote Control データベースから削除された後、Active Directory からインポートされます。そのため、LDAP を有効にした場合

は、新しいユーザーおよび新しいユーザー・グループを Remote Control ではなく、Active Directory で作成する必要があります。

False

LDAP ユーザー認証が無効です。ユーザーは、Remote Control データベースと照合して認証されます。

```
authentication.LDAP=true
```

authentication.LDAP.config

LDAP 構成プロパティーが入っているファイルを定義します。

```
authentication.LDAP.config=ldap.properties
```

sync.ldap

Active Directory のユーザーおよびグループを Remote Control データベースと同期させます。値が true の場合は同期し、false の場合は同期しません。

True

LDAP サーバーは、LDAP 内で加えられた変更を反映させるために、Remote Control データベースと同期化されます。

False

同期化は行われません。同期が無効な場合は、手動でユーザーを Remote Control データベースにインポートする必要があります。そのようにしないと、ユーザーは Remote Control サーバーにログオンできません。リモート・コントロール・セッションの確立に必要な関連アクセス許可をユーザーに割り当てられるように、それらのユーザーが Remote Control データベースに存在しなければなりません。

注: 同期は、スケジュールされたタスクを実行することによって行われます。このタスクでは、LDAP サーバーから LDAP 情報をプルし、ユーザーまたはグループの情報に加えられた変更によってデータベースを更新します。`trc.properties` ファイル内の 2 つの属性により、スケジューラーがスケジュール済みタスクの有無を検査する時間間隔が定義されます。

scheduled.interval

スケジュール済みタスクの有無をサーバーが検査する頻度。検査間隔を時間単位の数で表したものです。デフォルトでは 60 分です。

注: この値を変更した場合は、 サーバー・サービスを再始動して新しい値を有効にする必要があります。

sync.LDAP.task_run_time

定時同期を実行する必要がある時刻を指定するために使用します。これは scheduled.interval の代替設定です。可能な値: HH:MM:SS の形式による時刻の 24 時間表記。例えば、午前 2 時に同期を実行する場合は「02:00:00」とします。

注:

- usingsync.LDAP.task_run_time を使用する場合は、LDAP 同期がタスク・スケジューラーのコンテキスト内で行われるため、実際のタスク実行時間が scheduled.interval 設定の影響を受けます。実際の実行時間は sync.LDAP.task_run_time から sync.LDAP.task_run_time + scheduled.interval にスパンできます。
- 定時同期を使用するには、サーバーを再起動する必要があります。

scheduled.interval.period

スケジュールされたタスクがあるかどうかサーバーが検査する頻度を指定するためにスケジュール間隔とともに使用する時間の単位。デフォルトは minutes です。

scheduled.interval 属性は、デフォルトとして 60 に設定され、**scheduled.interval.period** は minutes に設定されます。つまり、サーバーはスケジュール済みタスクの有無を 60 分ごとに調べます。ユーザーまたはグループに対する変更を正確に反映させるためには、**scheduled.interval** 属性をこれより低い値に設定して、 同期の頻度を高くしてください。

3. **「送信」**をクリックします。

接続情報の検証

パラメーターを使用して、Remote Control がどのように LDAP サーバーに接続するかを定義します。接続は、Remote Control にインポートされたユーザーおよびグループの情報を LDAP サーバーに照会するために使用されます。

`ldap.properties` ファイルを変更しても、**「アドミニストレーター」**、**「アプリケーションをリセット」**を選択するまで、変更内容は有効になりません。何度も再起動したり長時間停止したりするのを避けるために、 構成プロセス全体の補助として LDAP ブラウザーと **LDAP 構成ユーティリティー**を使用します。

LDAP ブラウザーを使用して接続情報を検査するには、完全修飾ホスト名と信任状情報を入力することにより、LDAP サーバー・プロファイルを定義します。最初に LDAP ブラウザーを開くときに、新しいプロファイルの詳細情報を指定します。

プロファイルには以下の情報を組み込むことができます。

ホスト

優先される LDAP サーバーのホスト名または FQDN。

ポート\n

ディレクトリーとの通信に使用されるポート。通常はポート 389 ですが、ご使用の環境が子ドメインを含む場合は、代わりにポート 3268 を使用する必要があります。ポート 3268 は、子ドメインを収容するグローバル・カタログを指します。

ベース DN

サーバーにバインドするためのルート・ポイント。例えば、`DC=mydomain,DC=mycompany,DC=com` です。

情報を入力すると、Active Directory ツリーのルートで使用可能な属性名と値が LDAP ブラウザーに表示されます。

接続が確立されたら、LDAP ブラウザーで使用した情報と同じ情報を使用して `ldap.properties`ファイルのパラメーターを設定します。

- **「アドミニストレーター」 > 「プロパティー・ファイルを編集」**をクリックします。
- リストから **ldap.properties** を選択します。
- 変更が完了したら、**「送信」**をクリックします。

変更を有効にするために、アプリケーションをリセットする必要があります。**「アドミニストレーター」 > 「アプリケーションをリセット」**をクリックするか、サーバー・サービスを再起動します。

プロパティー・ファイルは、BigFix® Remote Control サーバー 上でそのファイルを見つけることによって、手動で編集することもできます。ファイルはディレクトリー `[installdir]wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes` にあります。 *installdir* は、BigFix® Remote Control サーバー がインストールされているディレクトリーです。例えば、 `C:\Program Files (x86)\BigFix\TRC\server\wlp\usr\servers\trcserver \apps\TRCAPP.ear\trc.war\WEB-INF\classes`

注: Remote Control にはデフォルトの `ldap.properties` ファイルが用意されており、 多くの拡張構成オプションがコメント化されています。オプションを有効にするには、ファイルを手動で編集する必要があります。

注: BigFix® Remote Control サーバー は、1 つのグローバル・カタログのみを管理できます。これは、異なるドメインのドメイン・コントローラーを同じ BigFix® Remote Control サーバー で管理できないことを意味します。

サーバー構成で指定されたフォレストには含まれないドメインに属するユーザーは、同じ BigFix® Remote Control サーバー のユーザーに追加できません。

接続資格情報の構成

LDAP サーバーに接続するための有効な資格情報を設定するには、 以下のプロパティーを使用します。

注: これらの資格情報を使用して LDAP ブラウザーに正常に接続できることを確認し、 資格情報が有効であることを検証してください。

1. `ldap.properties` ファイルを編集します。
2. 以下のプロパティーを構成します。

ldap.connectionName

読み取り専用 LDAP 接続に対する認証に使用されるユーザー名。設定しない場合は匿名で接続します。例えば、`administrator@mydomain.mycompany.com` です。

ldap.connectionPassword

読み取り専用 LDAP 接続の確立に使用されるパスワード。パスワードは、ここにプレーン・テキストで入力することも、 暗号化することもできます。パスワードを暗号化するには、LDAP ウィザードを使用します。詳しくは、 『LDAP ウィザードを使用した LDAP プロパティーの構成』を参照してください。

ldap.connectionPasswordEncrypted

True

LDAP パスワードは暗号化されます。

False

LDAP パスワードは暗号化されず、プレーン・テキストとして入力されます。

ldap.connectionURL

LDAP 接続の確立に使用されるディレクトリー URL。LDAP サーバーの URL を入力します。

```
ldap://myldapserver.mydomain.mycompany.com
```

接続セキュリティーの設定

以下のプロパティーは、LDAP サーバーへの接続で使用するセキュリティーのレベルを定義します。以下のパラメーターを `simple` に設定すると、Remote Control サーバーがほとんどの Active Directory サーバーと通信できるようになります。

ldap.security_authentication

使用するセキュリティー・レベルを指定します。値は、以下のいずれかのストリングに設定できます。none、simple、strong このプロパティーが指定されていない場合は、 振る舞いはサービス・プロバイダーによって決定されます。

```
ldap.security_athentication=simple
```

ほとんどの LDAP サーバーは単純なプレーン・テキストによるログインをサポートしていますが、一部の Active Directory 管理者はセキュア接続を必要とします。Remote Control は、Active Directory サーバーに対する 2 つのタイプのセキュア接続をサポートしています。**SASL** (DIGEST-MD5) または **SSL** です。また、Active Directory サーバーへ接続できない場合、以下のエラーが `trc.log` に出力されます。

```
LDAP Authentication.exception[LDAP: error code 8 - 00002028: LdapErr: DSID-0C09018A,
comment: The server requires binds to turn on integrity checking if SSL\TLS are not
already active on the connection, data 0, vece ]
```

この場合は、Remote Control を SASL 接続用または SSL 接続用に構成する必要があります。

SASL (Simple Authentication and Security Layer)

以下のパラメーターは、LDAP サーバーへの接続を機密保護機能のあるものにするための SASL の使用に関連しています。SASL を使用しない場合は、これらのパラメーターを編集しないでください。これらのパラメーターはコメント化してください。以下の値は、テスト環境で SASL を使用する Active Directory に接続するように Remote Control を構成するために使用されます。お客様の会社に合った正しい値を取得するには、お客様の組織の Active Directory サポート・チームに問い合わせてください。

ldap.security_authentication

使用するセキュリティー・レベルを指定します。このプロパティーが指定されていない場合は、 振る舞いはサービス・プロバイダーによって決定されます。SSL を使用している場合は、この値を simple に設定します。SASL を使用しているる場合は、この値を SASL メカニズムの DIGEST-MD5 に設定します。

```
ldap.security_authentication= DIGEST-MD5
```

ldap.connectionRealm

ユーザー ID およびパスワードが存在するレルムの名前。

```
ldap.connectionRealm= mydomain.mycompany.com
```

ldap.connectionQop

この値は、以下のいずれかです。

- auth = 認証のみ
- auth-int = 認証、およびシグニチャーを使用した整合性検査
- auth-conf = (SASL のみ) 認証、およびシグニチャーと暗号化を使用した整合性と機密性の検査。

```
ldap.connectionQop= auth-conf
```

ldap.connectionMaxbuf

auth-int または *auth-conf* を使用する場合にサーバーが受信可能な最大のバッファーのサイズを示す数値。The default is 65536.

```
ldap.connectionMaxbuf= 16384
```

ldap.connectionStrength

接続の強度は低、中、高のいずれかにできます。

```
ldap.connectionStrength= high
```

SSL (Secure Socket Layer)

以下のパラメーターは、Active Directory サーバーに接続するための SSL の使用を定義します。SSL を使用するには、ルート CA の公開鍵証明書鍵ストアを Remote Control サーバーにインストールする必要があります。SSL を使用しない場合は、`ldap.properties` ファイルのパラメーターをコメント化して構いません。

ldap.security_protocol

使用するセキュリティー・プロトコルを指定します。値は、サービス・プロバイダーによって決定される文字列です。例えば ssl などです。このプロパティーが指定されていない場合は、 振る舞いはサービス・プロバイダーによって決定されます。

```
ldap.security_protocol =ssl
```

ldap.ssl_keyStore

鍵ストア・ファイルの場所を入力します。

```
ldap.ssl_keyStore=PathOfKeyStoreFile
```

ldap.ssl_keyStorePassword

鍵ストア・パスワードの場所を入力します。

```
ldap.ssl_keyStorePassword=KeystorePassword
```

ユーザー認証プロパティーの設定

ユーザーの認証

ユーザーが Remote Control サーバーへのログオンを試行した際にユーザーがどのように認証されるかを定義するには、以下のプロパティーを使用します。以下のセクションを構成するには、各パラメーターの説明に従って LDAP ブラウザーを使用し、 正しい設定を導き出してください。

ldap.digest

LDAP が使用するダイジェスト・アルゴリズム。値は SHA、MD2、または MD5 に限ります。デフォルトは cleartext です。LDAP サーバーがパスワードを戻す場合、Remote Control はダイジェスト・アルゴリズムを使用してユーザーが入力したパスワードを暗号化し、これを、LDAP サーバーから受け取ったパスワードと比較します。LDAP サーバーからパスワードが返されない場合、Remote Control は、エンド・ユーザーが指定したユーザー名およびパスワードを使用して LDAP での認証を行います。

```
ldap.digest=SHA
```

ldap.userid

ldap.userid は、Remote Control データベースの **userid** フィールドにマップされるユーザー ID が含まれる LDAP 属性です。このとき、**userPrincipalPattern** プロパティーは、Active Directory 認証のために *@domainname* (UPN サフィックス) が追加されるかどうかを認識する必要があります。

sAMAccountName

sAMAaccount は、ログオンのユーザー ID のみの部分 (UPN サフィックスなし) を使用する目的で使用します。

userPrincipalName

すべてのログオンで強制的に完全なユーザー・プリンシパル名を使用させるには、userPrincipalName を使用します。

注: ユーザー ID に無効な文字が含まれないことが保証されるように、**ldap.userid** はこの値に設定することをお勧めします。例えば、アポストロフィが無効文字の例です。

ldap.userid は、`ldap.properties` ファイル内の他の構成値に関連します。

例えば ldap.userid を userPrincipalName に設定した場合、ユーザーは完全な ID で Remote Control にログオンする必要があります。例えば、`awilson@example.com` です。

- **ldap.userSearch** 変数は、(userPrincipalName={0}) になります。
- **ldap.principalPattern** は、{0} になります。

sAMAccountName を使用するように ldap.userid を設定した場合、ユーザーは ID のユーザー ID 部分のみで Remote Control にログオンする必要があります。例えば、awilson を使用します。完全修飾名が付加されるように、以下のパラメーターを設定する必要があります。

次に例を示します。

- **ldap.userSearch** 変数は、(userPrincipalName={0}@mydomain.mycompany.com) になります。

  ユーザー awilson@example.com の場合、**ldap.userSearch** 変数は (userPrincipalName={0}) になります。

- **ldap.principalPattern** は、{0}@mydomain.mycompany.com になります。

  ユーザー awilson@example.com の場合、**ldap.principalPattern** は `{0}@example.com` になります

ldap.userPassword

ユーザー・パスワードが含まれている、ユーザーのディレクトリー・エントリー内の LDAP 属性の名前。Active Directory では、password がこの属性のデフォルト名です。

```
ldap.userPassword=password
```

ldap.userEmail

ユーザーの電子メールが含まれている、ユーザーのディレクトリー・エントリー内の LDAP 属性の名前。

注: ldap.userEmail プロパティーをヌル値にすることはできません。Active Directory ツリーに電子メール情報が含まれていない場合は、別の属性を使用する必要があります。例えば、**ldap.userEmail** を **userPrincipalName** に設定できます。

ldap.userRealm

ユーザー認証に使用するレルム名。この設定はオプションであり、ほとんどの構成の場合はコメント化して構いません (`ldap.properties` ファイルにあります)。

```
ldap.userRealm=users.company.domain.com
```

ldap.principalPattern

LDAP 認証を使用するためのユーザー・プリンシパルの作成用パターン。LDAP サーバーによって、電子メール・アドレス (`userid@domain.com` など) が要求される場合や、ユーザー ID のみが要求される場合があります。文字列「{0}」は、ログイン画面で入力されたユーザーのユーザー ID で置換されます。

ユーザー・ディレクトリー・エントリーの検索

エンド・ユーザー情報を検出するために使用可能な方式には、Active Directory ツリー内の開始点を定義し、Remote Control がツリー全体を再帰的に検索してユーザー ID を探し出せるようにすることが含まれます。ほとんどの Active Directory の実装では、ユーザーが Active Directory ツリー内の複数のロケーションに分散されているのが普通なので、この方式が好まれます。この方式は、ユーザー情報がツリーの 1 つのブランチの下に入っているが、部門別つまりブランチの下で分けられている場合に特に便利です。

注: LDAP を使用可能にした場合は、 新しいユーザーと新しいユーザー・グループを Remote Control では**なく**、Active Directory で作成する必要があることに注意してください。理由は、Active Directory と同期するときに毎回ユーザーおよびユーザー・グループが Remote Control データベースから削除された後、再度 Active Directory からインポートされるためです。

再帰的検索を使用するには、以下のパラメーターを構成します。

ldap.userBase

検索条件に合致するユーザーを検索するための基本 LDAP ディレクトリー・エントリー。指定しない場合は、 検索ベースがディレクトリー・コンテキストの最上位エレメントになります。

```
for example OU=mylocation,DC=mycompany,DC=com
```

OU 構造内をより深くたどって、 特定の組織単位内のみを検索するように選択することで、検索を詳細化できます。 例えば Users という OU の場合は、以下のようにプロパティー値を設定します。

```
ldap.userBase=OU=Users,ou=mylocation,dc=mydomain,dc=mycompany,dc=com
```

これにより、Users OU (および ldap.groupSubtree が true に設定されている場合は Users OU に属するすべての OU) 内のみで基準に合致するユーザーを検索するよう Remote Control に指示が出されます。

ldap.userSearch

Active Directory ユーザーを Remote Control にインポートするために使用する LDAP 照会を定義します。定義する照会では、 検索条件に合致するユーザーのみが Remote Control にインポートされるように結果をフィルターに掛ける必要があります。デフォルト値は以下のとおりです。

(objectClass=user)

この場合は、 このユーザー・ベース内のユーザー・オブジェクトであるすべてのオブジェクトでユーザーが検索されます。つまり、すべての Active Directory ユーザーが Remote Control にインポートされます。

注: 上記を使用する場合、 環境によっては何千ものユーザーが含まれていることがあるため、 必要なユーザーのみをインポートするフィルターを作成することが重要です。検索条件に合致し、**ldap.groupSearch** フィルターを通して Remote Control にインポートされたグループのメンバーであるユーザーのみがインポート対象ユーザーになるように制限するには、**ldap.userInGroup** プロパティーを true に設定する必要があります。また、ユーザーは、グループ検索で返される関連グループにインポートされるだけではなく、**DefaultGroup** にもインポートされるので注意してください。**ldap.userInGroup** を false に設定すると、グループ・メンバーシップに関係なく、検索条件に一致するすべてのユーザーがインポートされます。

このため、より複雑な照会を使用することで、検索をさらに詳細化することができます。例えば、以下の値を設定したとします。

```
ldap.groupBase=(OU=mylocation.DC=mycompany.DC=com)
Ldap.userSearch: (&(objectClass=user)(|(memberOf=CN=Department1,OU=GROUPS,
OU=mylocation,DC=mycompany,DC=com) (memberOf=CN=Department3,OU=GROUPS,
OU=mylocation,DC=mycompany,DC=com))(name={0}))
```

3 つのグループ Department1、Department2、および Department3 が定義されている場合は、上記の照会により、オブジェクト・クラス user として定義され、Department1 グループまたは Department3 グループのメンバーであるすべてのユーザーが認証され、 インポートされます。Department2 のユーザーは Remote Control にログオンできません。

(&(name={0}) を末尾に追加することで、name 属性をログインに使用することを指定しています。ldap.userid としてどの属性を指定した場合でも、この値が一致する必要があります。

ldap.userSubtree

ユーザーのディレクトリー項目の userBase 属性で指定されたエレメントのサブツリーを再帰的に検索する場合は、この値を true に設定します。デフォルト値の false では最上位のみが検索されます (非再帰的検索)。userPattern 式を使用する場合は無視されます。

```
ldap.userSubtree=true
```

Active Directory グループのインポート

Active Directory と統合することの最大の利点の 1 つは、既存の Active Directory グループを使用できることです。Active Directory グループをインポートした後に、管理者は各グループのアクセス許可を定義する必要があります。グループ・メンバーシップは本質的に Active Directory によって処理されます。Active Directory グループをインポートするには、`ldap.properties` ファイルで以下のプロパティーを構成します。

ldap.groupName

グループ検索に使用される LDAP 属性名。

```
ldap.groupName=cn    OR   ldap.groupName=name
```

ldap.groupDescription

グループの説明を取得するために使用される LDAP 属性名。これはデフォルトで description に設定されます。

```
ldap.groupDescription=description
```

ldap.groupNameTrim

true または false に設定します。Remote Control データベースにインポートするグループの名前を 64 文字までに制限します。推奨値は false です。

ldap.groupMembers

指定された検索の結果として返されるグループのメンバーを検出するために使用される LDAP 属性名。デフォルト値は member です。

```
ldapgroupMembers=member
```

ldap.groupSubtree

true に設定すると、Remote Control が、**ldap.groupBase** パラメーターで指定されたエレメントのサブツリー全体を再帰的にたどって、ユーザーに関連付けられたグループを検索します。指定しない場合は、デフォルト値の false により、最上位のみが検索されます。再帰的な検索は実行されません。True または False (デフォルト) です。

ldap.groupBase

同期するグループの検索を開始する基本 LDAP ディレクトリー・エントリー。指定しない場合は、 デフォルトでディレクトリー・コンテキストの最上位エレメントが使用されます。

```
for example OU=mylocation,DC=mycompany,DC=com
```

検索を詳細化して OU 構造内をより深くたどるには、特定の組織単位内のみで検索を開始することを選択します。例えば、Test という OU を使用します。プロパティーを以下の値に設定します。

```
OU=Test,OU=mylocation,DC=mycompany,DC=com
```

そのため、 Remote Control は、Test OU (および **ldap.groupSubtree** が true に設定されている場合は Test OU に属するすべての OU) 内のみで基準に合致するグループを検索します。

ldap.groupSearch

AD グループを Remote Control にインポートするために使用される LDAP 照会を定義します。定義される照会では、結果をフィルターに掛け、必要なグループのみが Remote Control にインポートされるようにする必要があります。

`ldap.groupSearch=(objectClass=group)`

ldap.groupBase プロパティーで指定された OU に存在するすべての AD グループを Remote Control にインポートします。環境によっては、何千というグループが存在する可能性があります。

`ldap.groupSearch=(&(objectClass=group)(cn=*SMS*))`

cn 属性に SMS を含んでいるグループをすべてインポートします。例えば、*visio-sms-users* です。

`ldap.groupSearch=(&(objectClass=group)(cn=admins))`

admin の名前が付いたすべてのグループをインポートします。

`ldap.groupSearch=(&(objectClass=group)(cn=admins*))`

名前に admins というテキストを含むすべてのグループをインポートします。例えば、administrators、server-administrators です。

ldap.groupMembers

指定された検索の結果として返されるグループのメンバーを検出するために使用される LDAP 属性名。デフォルト値は member です。

これらの照会をテストするには、LDAP ブラウザーのディレクトリー検索オプションか、または Remote Control サーバー UI 内の LDAP 構成ユーティリティーを使用します。

接続のテスト

`common.properties` ファイルおよび `ldap.properties` ファイルを更新した場合は、**「アドミニストレーター」 > 「アプリケーションをリセット」**を選択して Remote Control アプリケーションをリセットしてください。

サービスが再始動したら、Active Directory のユーザー ID とパスワードを使用して、Remote Control サーバーにログオンします。LDAP プロパティー・ファイル内の項目が正しい場合は、正常に認証され、ログオンできます。

BigFix® Remote Control サーバー は、LDAP に直接接続します。そのため、LDAP パスワードの変更が、`ldap.properties` ファイル内で設定されている LDAP サーバーと同期されている場合に限り、LDAP 内でのパスワード変更は直ちに有効になります。

注: BigFix® Remote Control サーバー ・アプリケーション内のデフォルトの ADMIN ユーザー ID は、LDAP 認証が有効かどうかにかかわらず、常に BigFix® Remote Control サーバー と照合して認証されま

す。BigFix® Remote Control サーバー と LDAP の間に接続の問題がある場合、ADMIN ユーザーは常にログオンできます。

`ldap.properties` ファイル内にエラーがある場合は、ログオンが失敗したことを示すメッセージが表示されます。ユーザー名が無効であるかパスワードが誤っていることを示すメッセージが**ログオン**画面に表示されます。

失敗の原因を判別するには、`trc.log` ファイルを調べます。サーバー UI を使用してアプリケーション・ログを表示します。

- BigFix® Remote Control サーバー の UI で、**「アドミニストレーター」 > 「アプリケーション・ログを表示」**をクリックします。
- **CTRL+END** をクリックして、ファイルの末尾に移動します。

以下の一般的なエラーを表示することができます。これらのエラーは、BigFix® Remote Control サーバー と Active Directory の間の初期接続の作成に関する問題があったことを示しています。

AcceptSecurityContext エラー、データ 525

ユーザー名が無効のときに返されます。

AcceptSecurityContext エラー、データ 52e (AcceptSecurityContext error, data 52e)

ユーザー名は有効であるがパスワードまたは資格情報が無効な場合に返されます。記載されているように、他のほとんどのエラーの表示を抑止します。

AcceptSecurityContext エラー、データ 530

ログオンの失敗: アカウント・ログオン時間制限違反。有効なユーザー名およびパスワードの資格情報が入力された場合にのみ表示されます。

AcceptSecurityContext エラー、データ 531

ログオン失敗: このユーザーはこのコンピューターへのログオンが許可されていません。有効なユーザー名およびパスワードの資格情報が入力された場合にのみ表示されます。

AcceptSecurityContext エラー、データ 532

ログオンの失敗: 指定されたアカウントのパスワードは有効期限が切れています。有効なユーザー名およびパスワードの資格情報が入力された場合にのみ表示されます。

AcceptSecurityContext エラー、データ 533

ログオンの失敗: アカウントは現在無効になっています。有効なユーザー名およびパスワードの資格情報が入力された場合にのみ表示されます。

AcceptSecurityContext エラー、データ 701

ユーザーのアカウントの有効期限が切れています。有効なユーザー名およびパスワードの資格情報が入力された場合にのみ表示されます。

AcceptSecurityContext エラー、データ 773

ユーザーが初めてログオンする前に、ユーザーのパスワードを変更する必要があります。有効なユーザー名およびパスワードの資格情報が入力された場合にのみ表示されます。

AcceptSecurityContext エラー、データ 775 (AcceptSecurityContext error, data 775)

参照されたアカウントはロックアウトされており、ログオンできません。無効なパスワードが入力された場合でも表示されます。

LDAP Authentication.exceptionmyserver.mydomain.com:389

ldap.connectionURL で指定された名前のサーバーに到達できない場合に表示されます。

グループがインポートされたことの確認

正常に認証されて Remote Control サーバーにログオンしたら、**「ユーザー・グループ」 > 「すべてのユーザー・グループ」**をクリックし、Active Directory から正しいグループがインポートされていることを確認します。

グループが Remote Control にインポートされたら、新しくインポートされたグループのアクセス許可を定義してください。

グループがインポートされたことの確認

正常に認証されて Remote Control サーバーにログオンしたら、**「ユーザー・グループ」 > 「すべてのユーザー・グループ」**をクリックし、Active Directory から正しいグループがインポートされていることを確認します。

グループが Remote Control にインポートされたら、新しくインポートされたグループのアクセス許可を定義してください。

接続のテスト

`common.properties` ファイルおよび `ldap.properties` ファイルを更新した場合は、**「アドミニストレーター」 > 「アプリケーションをリセット」**を選択して Remote Control アプリケーションをリセットしてください。

サービスが再始動したら、Active Directory のユーザー ID とパスワードを使用して、Remote Control サーバーにログオンします。LDAP プロパティー・ファイル内の項目が正しい場合は、正常に認証され、ログオンできます。

BigFix® Remote Control サーバー は、LDAP に直接接続します。そのため、LDAP パスワードの変更が、`ldap.properties` ファイル内で設定されている LDAP サーバーと同期されている場合に限り、LDAP 内でのパスワード変更は直ちに有効になります。

注: BigFix® Remote Control サーバー ・アプリケーション内のデフォルトの ADMIN ユーザー ID は、LDAP 認証が有効かどうかにかかわらず、常に BigFix® Remote Control サーバー と照合して認証されます。BigFix® Remote Control サーバー と LDAP の間に接続の問題がある場合、ADMIN ユーザーは常にログオンできます。

`ldap.properties` ファイル内にエラーがある場合は、ログオンが失敗したことを示すメッセージが表示されます。ユーザー名が無効であるかパスワードが誤っていることを示すメッセージが**ログオン**画面に表示されます。

失敗の原因を判別するには、`trc.log` ファイルを調べます。サーバー UI を使用してアプリケーション・ログを表示します。

- BigFix® Remote Control サーバー の UI で、**「アドミニストレーター」 > 「アプリケーション・ログを表示」**をクリックします。
- **CTRL+END** をクリックして、ファイルの末尾に移動します。

以下の一般的なエラーを表示することができます。これらのエラーは、BigFix® Remote Control サーバー と Active Directory の間の初期接続の作成に関する問題があったことを示しています。

AcceptSecurityContext エラー、データ 525

ユーザー名が無効のときに返されます。

AcceptSecurityContext エラー、データ 52e (AcceptSecurityContext error, data 52e)

ユーザー名は有効であるがパスワードまたは資格情報が無効な場合に返されます。記載されているように、他のほとんどのエラーの表示を抑止します。

AcceptSecurityContext エラー、データ 530

ログオンの失敗: アカウント・ログオン時間制限違反。有効なユーザー名およびパスワードの資格情報が入力された場合にのみ表示されます。

AcceptSecurityContext エラー、データ 531

ログオン失敗: このユーザーはこのコンピューターへのログオンが許可されていません。有効なユーザー名およびパスワードの資格情報が入力された場合にのみ表示されます。

AcceptSecurityContext エラー、データ 532

ログオンの失敗: 指定されたアカウントのパスワードは有効期限が切れています。有効なユーザー名およびパスワードの資格情報が入力された場合にのみ表示されます。

AcceptSecurityContext エラー、データ 533

ログオンの失敗: アカウントは現在無効になっています。有効なユーザー名およびパスワードの資格情報が入力された場合にのみ表示されます。

AcceptSecurityContext エラー、データ 701

ユーザーのアカウントの有効期限が切れています。有効なユーザー名およびパスワードの資格情報が入力された場合にのみ表示されます。

AcceptSecurityContext エラー、データ 773

ユーザーが初めてログオンする前に、ユーザーのパスワードを変更する必要があります。有効なユーザー名およびパスワードの資格情報が入力された場合にのみ表示されます。

AcceptSecurityContext エラー、データ 775 (AcceptSecurityContext error, data 775)

参照されたアカウントはロックアウトされており、ログオンできません。無効なパスワードが入力された場合でも表示されます。

LDAP Authentication.exceptionmyserver.mydomain.com:389

ldap.connectionURL で指定された名前のサーバーに到達できない場合に表示されます。

Active Directory グループのインポート

Active Directory と統合することの最大の利点の 1 つは、既存の Active Directory グループを使用できることです。Active Directory グループをインポートした後に、管理者は各グループのアクセス許可を定義する必要があります。グループ・メンバーシップは本質的に Active Directory によって処理されます。Active Directory グループをインポートするには、`ldap.properties` ファイルで以下のプロパティーを構成します。

ldap.groupName

グループ検索に使用される LDAP 属性名。

```
ldap.groupName=cn    OR   ldap.groupName=name
```

ldap.groupDescription

グループの説明を取得するために使用される LDAP 属性名。これはデフォルトで description に設定されます。

```
ldap.groupDescription=description
```

ldap.groupNameTrim

true または false に設定します。Remote Control データベースにインポートするグループの名前を 64 文字までに制限します。推奨値は false です。

ldap.groupMembers

指定された検索の結果として返されるグループのメンバーを検出するために使用される LDAP 属性名。デフォルト値は member です。

```
ldapgroupMembers=member
```

ldap.groupSubtree

true に設定すると、Remote Control が、**ldap.groupBase** パラメーターで指定されたエレメントのサブツリー全体を再帰的にたどって、ユーザーに関連付けられたグループを検索します。指定しない場合は、デフォルト値の false により、最上位のみが検索されます。再帰的な検索は実行されません。True または False (デフォルト) です。

ldap.groupBase

同期するグループの検索を開始する基本 LDAP ディレクトリー・エントリー。指定しない場合は、 デフォルトでディレクトリー・コンテキストの最上位エレメントが使用されます。

```
for example OU=mylocation,DC=mycompany,DC=com
```

検索を詳細化して OU 構造内をより深くたどるには、特定の組織単位内のみで検索を開始することを選択します。例えば、Test という OU を使用します。プロパティーを以下の値に設定します。

```
OU=Test,OU=mylocation,DC=mycompany,DC=com
```

そのため、 Remote Control は、Test OU (および **ldap.groupSubtree** が true に設定されている場合は Test OU に属するすべての OU) 内のみで基準に合致するグループを検索します。

ldap.groupSearch

AD グループを Remote Control にインポートするために使用される LDAP 照会を定義します。定義される照会では、結果をフィルターに掛け、必要なグループのみが Remote Control にインポートされるようにする必要があります。

`ldap.groupSearch=(objectClass=group)`

ldap.groupBase プロパティーで指定された OU に存在するすべての AD グループを Remote Control にインポートします。環境によっては、何千というグループが存在する可能性があります。

`ldap.groupSearch=(&(objectClass=group)(cn=*SMS*))`

cn 属性に SMS を含んでいるグループをすべてインポートします。例えば、*visio-sms-users* です。

`ldap.groupSearch=(&(objectClass=group)(cn=admins))`

admin の名前が付いたすべてのグループをインポートします。

`ldap.groupSearch=(&(objectClass=group)(cn=admins*))`

名前に admins というテキストを含むすべてのグループをインポートします。例えば、administrators、server-administrators です。

ldap.groupMembers

指定された検索の結果として返されるグループのメンバーを検出するために使用される LDAP 属性名。デフォルト値は member です。

これらの照会をテストするには、LDAP ブラウザーのディレクトリー検索オプションか、または Remote Control サーバー UI 内の LDAP 構成ユーティリティーを使用します。

ユーザー認証プロパティーの設定

ユーザーの認証

ユーザーが Remote Control サーバーへのログオンを試行した際にユーザーがどのように認証されるかを定義するには、以下のプロパティーを使用します。以下のセクションを構成するには、各パラメーターの説明に従って LDAP ブラウザーを使用し、 正しい設定を導き出してください。

ldap.digest

LDAP が使用するダイジェスト・アルゴリズム。値は SHA、MD2、または MD5 に限ります。デフォルトは cleartext です。LDAP サーバーがパスワードを戻す場合、Remote Control はダイジェスト・アルゴリズムを使用してユーザーが入力したパスワードを暗号化し、これを、LDAP サーバーから受け取ったパスワードと比較します。LDAP サーバーからパスワードが返されない場合、Remote Control は、エンド・ユーザーが指定したユーザー名およびパスワードを使用して LDAP での認証を行います。

```
ldap.digest=SHA
```

ldap.userid

ldap.userid は、Remote Control データベースの **userid** フィールドにマップされるユーザー ID が含まれる LDAP 属性です。このとき、**userPrincipalPattern** プロパティーは、Active Directory 認証のために *@domainname* (UPN サフィックス) が追加されるかどうかを認識する必要があります。

sAMAccountName

sAMAaccount は、ログオンのユーザー ID のみの部分 (UPN サフィックスなし) を使用する目的で使用します。

userPrincipalName

すべてのログオンで強制的に完全なユーザー・プリンシパル名を使用させるには、userPrincipalName を使用します。

注: ユーザー ID に無効な文字が含まれないことが保証されるように、**ldap.userid** はこの値に設定することをお勧めします。例えば、アポストロフィが無効文字の例です。

ldap.userid は、`ldap.properties` ファイル内の他の構成値に関連します。

例えば ldap.userid を userPrincipalName に設定した場合、ユーザーは完全な ID で Remote Control にログオンする必要があります。例えば、`awilson@example.com` です。

- **ldap.userSearch** 変数は、(userPrincipalName={0}) になります。
- **ldap.principalPattern** は、{0} になります。

sAMAccountName を使用するように ldap.userid を設定した場合、ユーザーは ID のユーザー ID 部分のみで Remote Control にログオンする必要があります。例えば、awilson を使用します。完全修飾名が付加されるように、以下のパラメーターを設定する必要があります。

次に例を示します。

- **ldap.userSearch** 変数は、(userPrincipalName={0}@mydomain.mycompany.com) になります。

  ユーザー awilson@example.com の場合、**ldap.userSearch** 変数は (userPrincipalName={0}) になります。

- **ldap.principalPattern** は、{0}@mydomain.mycompany.com になります。

  ユーザー awilson@example.com の場合、**ldap.principalPattern** は `{0}@example.com` になります

ldap.userPassword

ユーザー・パスワードが含まれている、ユーザーのディレクトリー・エントリー内の LDAP 属性の名前。Active Directory では、password がこの属性のデフォルト名です。

```
ldap.userPassword=password
```

ldap.userEmail

ユーザーの電子メールが含まれている、ユーザーのディレクトリー・エントリー内の LDAP 属性の名前。

注: ldap.userEmail プロパティーをヌル値にすることはできません。Active Directory ツリーに電子メール情報が含まれていない場合は、別の属性を使用する必要があります。例えば、**ldap.userEmail** を **userPrincipalName** に設定できます。

ldap.userRealm

ユーザー認証に使用するレルム名。この設定はオプションであり、ほとんどの構成の場合はコメント化して構いません (`ldap.properties` ファイルにあります)。

```
ldap.userRealm=users.company.domain.com
```

ldap.principalPattern

LDAP 認証を使用するためのユーザー・プリンシパルの作成用パターン。LDAP サーバーによって、電子メール・アドレス (`userid@domain.com` など) が要求される場合や、ユーザー ID のみが要求される場合があります。文字列「{0}」は、ログイン画面で入力されたユーザーのユーザー ID で置換されます。

ユーザー・ディレクトリー・エントリーの検索

エンド・ユーザー情報を検出するために使用可能な方式には、Active Directory ツリー内の開始点を定義し、Remote Control がツリー全体を再帰的に検索してユーザー ID を探し出せるようにすることが含まれます。ほとんどの Active Directory の実装では、ユーザーが Active Directory ツリー内の複数のロケーションに分散されているのが普通なので、この方式が好まれます。この方式は、ユーザー情報がツリーの 1 つのブランチの下に入っているが、部門別つまりブランチの下で分けられている場合に特に便利です。

注: LDAP を使用可能にした場合は、 新しいユーザーと新しいユーザー・グループを Remote Control では**なく**、Active Directory で作成する必要があることに注意してください。理由は、Active Directory と同期するときに毎回ユーザーおよびユーザー・グループが Remote Control データベースから削除された後、再度 Active Directory からインポートされるためです。

再帰的検索を使用するには、以下のパラメーターを構成します。

ldap.userBase

検索条件に合致するユーザーを検索するための基本 LDAP ディレクトリー・エントリー。指定しない場合は、 検索ベースがディレクトリー・コンテキストの最上位エレメントになります。

```
for example OU=mylocation,DC=mycompany,DC=com
```

OU 構造内をより深くたどって、 特定の組織単位内のみを検索するように選択することで、検索を詳細化できます。 例えば Users という OU の場合は、以下のようにプロパティー値を設定します。

```
ldap.userBase=OU=Users,ou=mylocation,dc=mydomain,dc=mycompany,dc=com
```

これにより、Users OU (および ldap.groupSubtree が true に設定されている場合は Users OU に属するすべての OU) 内のみで基準に合致するユーザーを検索するよう Remote Control に指示が出されます。

ldap.userSearch

Active Directory ユーザーを Remote Control にインポートするために使用する LDAP 照会を定義します。定義する照会では、 検索条件に合致するユーザーのみが Remote Control にインポートされるように結果をフィルターに掛ける必要があります。デフォルト値は以下のとおりです。

(objectClass=user)

この場合は、 このユーザー・ベース内のユーザー・オブジェクトであるすべてのオブジェクトでユーザーが検索されます。つまり、すべての Active Directory ユーザーが Remote Control にインポートされます。

注: 上記を使用する場合、 環境によっては何千ものユーザーが含まれていることがあるため、 必要なユーザーのみをインポートするフィルターを作成することが重要です。検索条件に合致し、**ldap.groupSearch** フィルターを通して Remote Control にインポートされたグループのメンバーであるユーザーのみがインポート対象ユーザーになるように制限するには、**ldap.userInGroup** プロパティーを true に設定する必要があります。また、ユーザーは、グループ検索で返される関連グループにインポートされるだけではなく、**DefaultGroup** にもインポートされるので注意してください。**ldap.userInGroup** を false に設定すると、グループ・メンバーシップに関係なく、検索条件に一致するすべてのユーザーがインポートされます。

このため、より複雑な照会を使用することで、検索をさらに詳細化することができます。例えば、以下の値を設定したとします。

```
ldap.groupBase=(OU=mylocation.DC=mycompany.DC=com)
Ldap.userSearch: (&(objectClass=user)(|(memberOf=CN=Department1,OU=GROUPS,
OU=mylocation,DC=mycompany,DC=com) (memberOf=CN=Department3,OU=GROUPS,
OU=mylocation,DC=mycompany,DC=com))(name={0}))
```

3 つのグループ Department1、Department2、および Department3 が定義されている場合は、上記の照会により、オブジェクト・クラス user として定義され、Department1 グループまたは Department3 グループのメンバーであるすべてのユーザーが認証され、 インポートされます。Department2 のユーザーは Remote Control にログオンできません。

(&(name={0}) を末尾に追加することで、name 属性をログインに使用することを指定しています。ldap.userid としてどの属性を指定した場合でも、この値が一致する必要があります。

ldap.userSubtree

ユーザーのディレクトリー項目の userBase 属性で指定されたエレメントのサブツリーを再帰的に検索する場合は、この値を true に設定します。デフォルト値の false では最上位のみが検索されます (非再帰的検索)。userPattern 式を使用する場合は無視されます。

```
ldap.userSubtree=true
```

接続セキュリティーの設定

以下のプロパティーは、LDAP サーバーへの接続で使用するセキュリティーのレベルを定義します。以下のパラメーターを `simple` に設定すると、Remote Control サーバーがほとんどの Active Directory サーバーと通信できるようになります。

ldap.security_authentication

使用するセキュリティー・レベルを指定します。値は、以下のいずれかのストリングに設定できます。none、simple、strong このプロパティーが指定されていない場合は、 振る舞いはサービス・プロバイダーによって決定されます。

```
ldap.security_athentication=simple
```

ほとんどの LDAP サーバーは単純なプレーン・テキストによるログインをサポートしていますが、一部の Active Directory 管理者はセキュア接続を必要とします。Remote Control は、Active Directory サーバーに対する 2 つのタイプのセキュア接続をサポートしています。**SASL** (DIGEST-MD5) または **SSL** です。また、Active Directory サーバーへ接続できない場合、以下のエラーが `trc.log` に出力されます。

```
LDAP Authentication.exception[LDAP: error code 8 - 00002028: LdapErr: DSID-0C09018A,
comment: The server requires binds to turn on integrity checking if SSL\TLS are not
already active on the connection, data 0, vece ]
```

この場合は、Remote Control を SASL 接続用または SSL 接続用に構成する必要があります。

SASL (Simple Authentication and Security Layer)

以下のパラメーターは、LDAP サーバーへの接続を機密保護機能のあるものにするための SASL の使用に関連しています。SASL を使用しない場合は、これらのパラメーターを編集しないでください。これらのパラメーターはコメント化してください。以下の値は、テスト環境で SASL を使用する Active Directory に接続するように Remote Control を構成するために使用されます。お客様の会社に合った正しい値を取得するには、お客様の組織の Active Directory サポート・チームに問い合わせてください。

ldap.security_authentication

使用するセキュリティー・レベルを指定します。このプロパティーが指定されていない場合は、 振る舞いはサービス・プロバイダーによって決定されます。SSL を使用している場合は、この値を simple に設定します。SASL を使用しているる場合は、この値を SASL メカニズムの DIGEST-MD5 に設定します。

```
ldap.security_authentication= DIGEST-MD5
```

ldap.connectionRealm

ユーザー ID およびパスワードが存在するレルムの名前。

```
ldap.connectionRealm= mydomain.mycompany.com
```

ldap.connectionQop

この値は、以下のいずれかです。

- auth = 認証のみ
- auth-int = 認証、およびシグニチャーを使用した整合性検査
- auth-conf = (SASL のみ) 認証、およびシグニチャーと暗号化を使用した整合性と機密性の検査。

```
ldap.connectionQop= auth-conf
```

ldap.connectionMaxbuf

auth-int または *auth-conf* を使用する場合にサーバーが受信可能な最大のバッファーのサイズを示す数値。The default is 65536.

```
ldap.connectionMaxbuf= 16384
```

ldap.connectionStrength

接続の強度は低、中、高のいずれかにできます。

```
ldap.connectionStrength= high
```

SSL (Secure Socket Layer)

以下のパラメーターは、Active Directory サーバーに接続するための SSL の使用を定義します。SSL を使用するには、ルート CA の公開鍵証明書鍵ストアを Remote Control サーバーにインストールする必要があります。SSL を使用しない場合は、`ldap.properties` ファイルのパラメーターをコメント化して構いません。

ldap.security_protocol

使用するセキュリティー・プロトコルを指定します。値は、サービス・プロバイダーによって決定される文字列です。例えば ssl などです。このプロパティーが指定されていない場合は、 振る舞いはサービス・プロバイダーによって決定されます。

```
ldap.security_protocol =ssl
```

ldap.ssl_keyStore

鍵ストア・ファイルの場所を入力します。

```
ldap.ssl_keyStore=PathOfKeyStoreFile
```

ldap.ssl_keyStorePassword

鍵ストア・パスワードの場所を入力します。

```
ldap.ssl_keyStorePassword=KeystorePassword
```

接続資格情報の構成

LDAP サーバーに接続するための有効な資格情報を設定するには、 以下のプロパティーを使用します。

注: これらの資格情報を使用して LDAP ブラウザーに正常に接続できることを確認し、 資格情報が有効であることを検証してください。

1. `ldap.properties` ファイルを編集します。
2. 以下のプロパティーを構成します。

ldap.connectionName

読み取り専用 LDAP 接続に対する認証に使用されるユーザー名。設定しない場合は匿名で接続します。例えば、`administrator@mydomain.mycompany.com` です。

ldap.connectionPassword

読み取り専用 LDAP 接続の確立に使用されるパスワード。パスワードは、ここにプレーン・テキストで入力することも、 暗号化することもできます。パスワードを暗号化するには、LDAP ウィザードを使用します。詳しくは、 『LDAP ウィザードを使用した LDAP プロパティーの構成』を参照してください。

ldap.connectionPasswordEncrypted

True

LDAP パスワードは暗号化されます。

False

LDAP パスワードは暗号化されず、プレーン・テキストとして入力されます。

ldap.connectionURL

LDAP 接続の確立に使用されるディレクトリー URL。LDAP サーバーの URL を入力します。

```
ldap://myldapserver.mydomain.mycompany.com
```

接続情報の検証

パラメーターを使用して、Remote Control がどのように LDAP サーバーに接続するかを定義します。接続は、Remote Control にインポートされたユーザーおよびグループの情報を LDAP サーバーに照会するために使用されます。

`ldap.properties` ファイルを変更しても、 **「アドミニストレーター」**、**「アプリケーションをリセット」**を選択するまで、変更内容は有効になりません。何度も再起動したり長時間停止したりするのを避けるために、 構成プロセス全体の補助として LDAP ブラウザーと **LDAP 構成ユーティリティー**を使用します。

LDAP ブラウザーを使用して接続情報を検査するには、完全修飾ホスト名と信任状情報を入力することにより、LDAP サーバー・プロファイルを定義します。最初に LDAP ブラウザーを開くときに、新しいプロファイルの詳細情報を指定します。

プロファイルには以下の情報を組み込むことができます。

ホスト

優先される LDAP サーバーのホスト名または FQDN。

ポート\n

ディレクトリーとの通信に使用されるポート。通常はポート 389 ですが、ご使用の環境が子ドメインを含む場合は、代わりにポート 3268 を使用する必要があります。ポート 3268 は、子ドメインを収容するグローバル・カタログを指します。

ベース DN

サーバーにバインドするためのルート・ポイント。例えば、`DC=mydomain,DC=mycompany,DC=com` です。

情報を入力すると、Active Directory ツリーのルートで使用可能な属性名と値が LDAP ブラウザーに表示されます。

接続が確立されたら、LDAP ブラウザーで使用した情報と同じ情報を使用して `ldap.properties`ファイルのパラメーターを設定します。

- **「アドミニストレーター」 > 「プロパティー・ファイルを編集」**をクリックします。
- リストから **ldap.properties** を選択します。
- 変更が完了したら、**「送信」**をクリックします。

変更を有効にするために、アプリケーションをリセットする必要があります。**「アドミニストレーター」 > 「アプリケーションをリセット」**をクリックするか、サーバー・サービスを再起動します。

プロパティー・ファイルは、BigFix® Remote Control サーバー 上でそのファイルを見つけることによって、手動で編集することもできます。ファイルはディレクトリー `[installdir]wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes` にあります。 *installdir* は、BigFix® Remote Control サーバー がインストールされているディレクトリーです。例えば、 `C:\Program Files (x86)\BigFix\TRC\server\wlp\usr\servers\trcserver \apps\TRCAPP.ear\trc.war\WEB-INF\classes`

注: Remote Control にはデフォルトの `ldap.properties` ファイルが用意されており、 多くの拡張構成オプションがコメント化されています。オプションを有効にするには、ファイルを手動で編集する必要があります。

注: BigFix® Remote Control サーバー は、1 つのグローバル・カタログのみを管理できます。これは、異なるドメインのドメイン・コントローラーを同じ BigFix® Remote Control サーバー で管理できないことを意味します。

サーバー構成で指定されたフォレストには含まれないドメインに属するユーザーは、同じ BigFix® Remote Control サーバー のユーザーに追加できません。

LDAP 同期の設定

LDAP 認証を有効にするには、LDAP サーバーとの同期も有効にする必要があります。同期を有効にするには、`common.properties`ファイルと `ldap.properties` ファイルの値を編集します。

LDAP 認証の基本構成を行うには、以下の手順を実行します。

1. **「アドミニストレーター」 > 「プロパティー・ファイルを編集」**をクリックします。
2. `common.properties` ファイルを編集中であることを確認した上で、以下のプロパティーを編集します。

authentication.LDAP

LDAP 認証を有効または無効にします。

True

LDAP ユーザー認証が有効です。

注: Active Directory と同期するときに毎回ユーザーおよびユーザー・グループが Remote Control データベースから削除された後、Active Directory からインポートされます。そのため、LDAP を有効にした場合は、新しいユーザーおよび新しいユーザー・グループを Remote Control ではなく、Active Directory で作成する必要があります。

False

LDAP ユーザー認証が無効です。ユーザーは、Remote Control データベースと照合して認証されます。

```
authentication.LDAP=true
```

authentication.LDAP.config

LDAP 構成プロパティーが入っているファイルを定義します。

```
authentication.LDAP.config=ldap.properties
```

sync.ldap

Active Directory のユーザーおよびグループを Remote Control データベースと同期させます。値が true の場合は同期し、false の場合は同期しません。

True

LDAP サーバーは、LDAP 内で加えられた変更を反映させるために、Remote Control データベースと同期化されます。

False

同期化は行われません。同期が無効な場合は、手動でユーザーを Remote Control データベースにインポートする必要があります。そのようにしないと、ユーザーは Remote Control サーバーにログオンできません。リモート・コントロール・

セッションの確立に必要な関連アクセス許可をユーザーに割り当てられるように、それらのユーザーが Remote Control データベースに存在しなければなりません。

注: 同期は、スケジュールされたタスクを実行することによって行われます。このタスクでは、LDAP サーバーから LDAP 情報をプルし、ユーザーまたはグループの情報に加えられた変更によってデータベースを更新します。`trc.properties` ファイル内の 2 つの属性により、スケジューラーがスケジュール済みタスクの有無を検査する時間間隔が定義されます。

scheduled.interval

スケジュール済みタスクの有無をサーバーが検査する頻度。検査間隔を時間単位の数で表したものです。デフォルトでは 60 分です。

注: この値を変更した場合は、 サーバー・サービスを再始動して新しい値を有効にする必要があります。

sync.LDAP.task_run_time

定時同期を実行する必要がある時刻を指定するために使用します。これは scheduled.interval の代替設定です。可能な値: HH:MM:SS の形式による時刻の 24 時間表記。例えば、午前 2 時に同期を実行する場合は「02:00:00」とします。

注:

- usingsync.LDAP.task_run_time を使用する場合は、LDAP 同期がタスク・スケジューラーのコンテキスト内で行われるため、実際のタスク実行時間が scheduled.interval 設定の影響を受けます。実際の実行時間は sync.LDAP.task_run_time から sync.LDAP.task_run_time + scheduled.interval にスパンできます。
- 定時同期を使用するには、サーバーを再起動する必要があります。

scheduled.interval.period

スケジュールされたタスクがあるかどうかサーバーが検査する頻度を指定するためにスケジュール間隔とともに使用する時間の単位。デフォルトは minutes です。

scheduled.interval 属性は、デフォルトとして 60 に設定され、**scheduled.interval.period** は minutes に設定されます。つまり、サーバーはスケジュール済みタスクの有無を 60 分ごとに調べます。ユーザーまたはグループに対する

変更を正確に反映させるためには、**scheduled.interval** 属性をこれより低い値に設定して、 同期の頻度を高くしてください。

3. **「送信」**をクリックします。

Remote Control での連邦情報処理標準 (FIPS 140-2) 準拠

米国連邦情報処理標準 140-2 (FIPS 140-2) は、IT ソフトウェアで使用する暗号モジュールのセキュリティー標準を規定する暗号機能検証プログラムです。

FIPS 140-2 モードで構成されている場合、 Remote Control は以下の FIPS 140-2 承認暗号モジュールを使用します。

IBM Java JCE FIPS 140-2 暗号モジュール (IBMJCEFIPS) は、多くの FIPS 承認暗号化操作をサポートするスケーラブルで多目的な暗号モジュールです。このモジュールは、Remote Control サーバー (すべてのバージョン) とバージョン 10.0.0.0518 までの Remote Control コントローラー (Windows および Linux のみ) で使用されます。この暗号モジュールの証明書番号は #2715 で、NIST の Web サイト (https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2715) に掲載されています。

BC-FJA (Bouncy Castle FIPS Java API) (BCFIPS) は、純粋な Java で実装された FIPS 承認アルゴリズムの包括的なスイートです。このモジュールは、バージョン 10.0.0.0600 以降の Remote Control コントローラー (Windows、Linux、MacOS) で使用されます。この暗号モジュールの証明書番号は #3514 で、NIST の Web サイト (https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3514) に掲載されています。

OpenSSL FIPS オブジェクト・モジュールは、汎用の暗号モジュールです。このモジュールは、Remote Control ターゲット、ブローカー、およびその他のネイティブ・コンポーネントで使用されます。この暗号モジュールの証明書番号は #1747 で、NIST の Web サイト (https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/1747) に掲載されています。

ターゲットでの FIPS 準拠の有効化

スタンドアロン WebSphere Application Server を使用したサーバーのインストールを実行するときの FIPS 準拠の有効化

BigFix® Remote Control サーバー は、WebSphere® のセキュア HTTP 通信が提供するミドルウェア・インフラストラクチャーを使用します。そのため、手動による BigFix® Remote Control サーバー のインストール用に FIPSを有効にするには、FIPS 準拠モードに対応するように WebSphere® を構成する必要があります。`common.properties` 構成ファイル内の設定を通じて BigFix® Remote Control サーバー を構成する必要もあります。

手動インストールの場合に FIPS 準拠を有効にするには、以下の手順を実行します。

1. WebSphere の構成

   注: MS SQL データベースを使用する場合、現在は IBM® JRE および IBM® JSSE プロバイダーを使用して IBM® WebSphere® において FIPS モードで実行することはできません。MS SQL の場合、IBM® WebSphere で FIPS が有効でなければ、これらのオプションを使用できます。

2. 有効な管理者 ID およびパスワードを使用して、BigFix® Remote Control サーバー にログオンします。
3. **「アドミニストレーター」 > 「プロパティー・ファイルを編集」**をクリックします。
4. `common.properties` ファイルで、**FIPS.compliance** を true に設定します。
5. 「**送信**」をクリックします。
6. **「アドミニストレーター」 > 「アプリケーションをリセット」**をクリックします。

注: WebSphere での FIPS の有効化に伴う変更によって、そのサーバー上で稼働する他のすべてのアプリケーションが影響を受けます。このため、ブラウザーのバージョンに応じて必要な場合は、それらの他のアプリケーションにアクセスするユーザーのブラウザー設定を、トランスポート層セキュリティー (TLS) をサポートするように変更する必要があります。

例えば、Internet Explorer で TLS を有効にするには、以下の手順を実行します。

- **「ツール」 「インターネット・オプション」**クリックします。
- **「詳細設定」**タブで**「TLS 1.0 の使用」**を選択します。
- **「適用」**をクリックします。
- **「OK」**をクリックします。

自動サーバー・インストール時の FIPS 準拠の有効化

サーバーのインストール中に有効にする

BigFix® Remote Control サーバー で FIPS 準拠を有効にするには、Remote Control サーバー・インストーラーを実行し、**「Web サーバーのパラメーター」**パネルで**「FIPS を有効にする」**と**「NIST SP800-131A を有効にする」**を選択します。

手動で有効にする

FIPS 準拠を有効にするには、以下の手順に従って Remote Control サーバー・インストーラーを実行する代わりに、BigFix® Remote Control サーバーで手動で構成できます。

1. 以下のディレクトリーにある `java.security` ファイルを編集します。

   Windows® システム

   %TRC_SERVER_PATH%`\java\jre\lib\security\java.security`

   ここで、*%TRC_SERVER_PATH%* は BigFix® Remote Control サーバー のインストール・ディレクトリーのパスです。

Linux® / UNIX® システム

$TRC_SERVER_PATH/java/jre/lib/security/java.security

ここで、*$TRC_SERVER_PATH* は BigFix® Remote Control サーバー のインストール・ディレクトリーのパスです。

2. *security.provider.x=* list を変更して、 以下の項目をリストの先頭に記述します。

security.provider.1=com.ibm.crypto.FIPS.provider.IBMJCEFIPS

このリストの他の項目の順序番号を、 すべての項目が連続した番号になるように修正してください。例えば、変更後のリスト全体は次のようになります。

```
security.provider.1=com.ibm.fips.jsse.IBMJSSEFIPS
security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
security.provider.4=com.ibm.crypto.provider.IBMJCE
security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.ibm.security.sasl.IBMSASL
security.provider.8=com.ibm.xml.crypto.IBMXMLCryptoProvider
security.provider.9=com.ibm.xml.enc.IBMXMLEncProvider
security.provider.10=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
security.provider.11=sun.security.provider.Sun
```

3. 以下の行を追加します。

```
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
```

4. ファイルを保存します。
5. 以下のディレクトリーにある jvm.options を編集します。

Windows® システム

%TRC_SERVER_PATH% \wlp\usr\servers\trcserver\jvm.options

ここで、*%TRC_SERVER_PATH%* は BigFix® Remote Control サーバー のインストール・ディレクトリーのパスです。

Linux® / UNIX® システム

$TRC_SERVER_PATH/wlp/usr/servers/trcserver/jvm.options

ここで、*$TRC_SERVER_PATH* は BigFix® Remote Control サーバー のインストール・ディレクトリーのパスです。

6. 以下の行を追加します。

```
-Dcom.ibm.jsse2.usefipsprovider=true
-Dcom.ibm.jsse2.sp800-131=strict
-Dcom.ibm.jsse2.overrideDefaultTLS=true
```

7. ファイルを保存します。
8. 有効な管理者 ID およびパスワードを使用して、BigFix® Remote Control サーバー にログオンします。
9. **「アドミニストレーター」 > 「プロパティー・ファイルを編集」**をクリックします。
10. `common.properties` ファイルで、**FIPS.compliance** を true に設定します。
11. 「**送信**」をクリックします。
12. **「アドミニストレーター」 > 「アプリケーションをリセット」**をクリックします。サーバー・サービスを再起動します。
13. サーバー・サービスを再起動します。

以下の手順を実行することで、BigFix® Remote Control サーバー が FIPS に対応するように構成されているかどうか確認します。

- **「アドミニストレーター」 > 「現在のサーバー状況を表示」**をクリックします。

以下のフィールドで、FIPS 準拠が有効であることが示されます。

- FIPS モードが使用可能になりました: このフィールドの値は、`common.properties` ファイルの **FIPS.compliance** プロパティーによって決定されます。
- JVM が FIPS 用に構成されました: このフィールドの値は、JVM および `java.security` ファイルにリストされたセキュリティー・プロバイダーの構成によって決定されます。

トラブルシューティング:

- **ブラウザーまたはコントローラーと Remote Control サーバーの接続に失敗することがある**

  サーバーが FIPS モードで動作するように構成されていて、`messages.log` ファイル `java.lang.NullPointerException com.ibm.ws.channel.ssl.internal.SSLConnectionLink 238` に次の例外がある場合、 ブラウザーまたはコントローラーと Remote Control サーバーの接続に失敗する可能性があります。

  これは、IBM Java 8.0.6.26 の採用による副作用です。問題が解決しない場合は、次の手順を実行します。

  1. Remote Control サーバーを停止します。
  2. `..\TRC\java\jre\lib\security\java.security` ファイルを開き、`RSAPSS` 値を `jdk.tls.disabledAlgorithms` の最後のエントリーとして追加します。

     更新されたプロパティー・リストは、以下のようになります。

```
jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA, DH keySize < 1024, DESede,
 \ EC keySize < 224, 3DES_EDE_CBC, anon, NULL, DES_CBC, RSAPSS
```

3. Remote Control サーバーを開始します。

- **ブローカー・セッションへの参加操作に失敗することがある**

  セカンダリー・コントローラーがプライマリー・コントローラーに接続し、FIPS モードで動作するように環境が構成されている場合、ブローカー・セッションへの参加操作に失敗する可能性があります。プライマリー・コントローラーは、`messages.log` ファイルに次のような例外を表示する場合があります。

  ```
  SEVERE - The connection was refused with pkt type [260]
  ```

  これは、IBM Java 8.0.6.26 の採用による副作用です。問題が解決しない場合は、次の手順を実行します。

  `..\Controller\jre\lib\security\java.security` ファイルを開き、`RSAPSS` 値を `jdk.tls.disabledAlgorithms` の最後のエントリーとして追加します。更新されたプロパティー・リストは、以下のようになります。

  ```
  jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA, DH keySize < 1024, DESede, \ EC
   keySize < 224, 3DES_EDE_CBC, anon, NULL, DES_CBC, RSAPSS
  ```

- **サーバーが FIPS モードで動作するように構成されている場合、サーバー Web インターフェースを介したセッション記録の再生が開始されず、エラー・メッセージが表示されないことがある**

  これは、IBM Java 8.0.6.26 の採用による副作用です。問題が解決しない場合は、次の手順を実行します。

  1. サーバーから提供された `TRCPlayer.trcjws` ファイルを保存します。
  2. ファイルを編集し、行 `<argument>--forcefips</argument>` を削除します。
  3. ファイルを保存し、`TRCPlayer.trcjws` ファイルをクリックして実行します。

コントローラーでの FIPS 準拠の有効化

Remote Control コントローラーは Java™ アプリケーションであり、FIPS 準拠を有効にする場合は FIPS 認証の暗号プロバイダーが必要です。FIPS 準拠モードでは、Remote Control コントローラーは、WINDOWS、Linux、MacOS 上の IBM Semeru Runtime Open Edition JRE で BC-FJA (Bouncy Castle FIPS Java API) をサポートします。

Remote Control バージョン 10.0 0 Update 6 (ビルド番号 0612 以上) 以降、コントローラーのインストール・パッケージには、BC-FJA (Bouncy Castle FIPS Java API) FIPS 認定の暗号プロバイダーと IBM® Semeru Runtime Open Edition JRE が含まれています。コントローラーがオンデマンド・モードで管理されるサーバーから起動されると、FIPS 準拠は `.trcjws` 開始ファイルの設定によって制御されます。

注: ピアツーピア・セッションを確立するためにコントローラーをローカル環境で実行している場合にのみ必要です。

ピアツーピア・モードで動作しているときにコントローラーで FIPS 準拠を設定するには、以下のようにローカル構成を更新します。

コントローラーがインストールされているシステムで、`trc_controller.cfg` ファイルを編集します。

Windows® システム

`[controller install dir]\trc_controller.cfg`

ここで *[controller install dir]* は、コントローラーのインストール時に選択したインストール・ディレクトリーです。

Linux® / UNIX® システム

`/opt/bigfix/trc/controller/trc_controller.cfg`

fips.compliance プロパティーを True に設定し、ファイルを保存します。

リモート・コントロール・セッション中に以下の手順を実行することで、コントローラーが FIPS に対応するように構成されているかどうか確認します。

- コントローラーのウィンドウで**「コントローラー・ツール」 > 「セッション情報の表示」**をクリックします。

ターゲットでの FIPS 準拠の有効化

Remote Control ターゲットには FIPS 対応の OpenSSL ライブラリーが含まれています。FIPS 準拠は、インストール時に有効にするか、ターゲット・レジストリーの編集 (Windows® システムの場合) または構成ファイルの変更 (Linux® システムの場合) によって有効にすることができます。

ターゲットのインストールについて詳しくは、「BigFix® Remote Control インストール・ガイド」を参照してください。

ターゲット・ユーザー・インターフェースを使用して適切なオプションを選択し、 ターゲットが FIPS モードであることを確認します。

- Remote Control- ターゲット・ユーザー・インターフェースで、**「アクション」 メニュー > 「接続情報」**をクリックします。
- システム通知域の **Remote Control** アイコンにマウス・カーソルを移動します。

Windows™ ターゲットでの FIPS 準拠の有効化

Windows™ システムでは、ターゲットで FIPS 準拠を有効にする方法として、インストール時に行う方法と、インストール後にターゲットのレジストリーを編集する方法の 2 つがあります。

ターゲット・インストーラーを使用した FIPS 準拠の有効化

以下の手順を実行することによって、 インストール中に FIPS 準拠ターゲット・プロパティーを有効にします。

1. ターゲット・インストーラーの**「サーバーのアドレス」**パネルで、 **「詳細設定」**をクリックします。
2. **「FIPS 認定の暗号プロバイダーの使用」**および**「セキュア接続 (https) を使用」**を選択します。以降のターゲット・インストール処理を続けます。

サイレント・インストールの実行

ターゲットのサイレント・インストールを実行する場合は、 インストール・コマンドを実行し、**FIPSCOMPLIANCE** プロパティーを使用してターゲットで FIPS を有効にします。サイレント・インストールの実行について詳しくは、Windows システムでのターゲット・カスタム・インストールの実行を参照してください。

FIPS モードを有効にする場合は、 以下のプロパティーを使用します。

- TRC_SERVER_PROTOCOL=https
- TRC_SERVER_PORT=443
- FIPSCOMPLIANCE=yes

例えば、以下のようになります。 trc_target_setup.exe /s /v"/qn TRC_SERVER_HOSTNAME=yourserver TRC_SERVER_PROTOCOL=https TRC_SERVER_PORT=443 FIPSCOMPLIANCE=yes"

ここで、***yourserver*** はご使用の BigFix® Remote Control サーバー のホスト名または IP アドレスです。

ターゲットのインストール後の FIPS 準拠の有効化

Remote Control ターゲットをインストールした後に、 ターゲットのレジストリーを編集することで FIPS 準拠を有効にすることができます。FIPS 準拠を有効にするには、以下の手順を実行します。

1. コマンド・プロンプト・ウィンドウで regedit コマンドを実行します。
2. Windows™ レジストリーで `HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\Remote Control\Target`の手順を実行します。
3. **「FIPSCompliance」**を右クリックして**「変更」**を選択します。
4. **「値のデータ」**フィールドに yes と入力し、**「OK」**をクリックします。
5. ターゲット・サービスを再起動します。
   ターゲット・サービスの再始動について詳しくは、コンポーネント・サービスの管理を参照してください。
   ご使用のオペレーティング・システムに該当するセクションに記載されたステップを実行してください。

Linux® または UNIX® ベースのオペレーティング・システムでの FIPS 準拠の有効化

Remote Control ターゲットをインストールした後に、`trc_target.properties` ファイルを編集することで FIPS 準拠を有効にすることができます。FIPS 準拠を有効にするには、以下の手順を実行します。

1. `/etc/trc_target.properties` ファイルを編集します。
2. *FIPSCompliance* の値を「YES」に設定し、ファイルを保存します。
3. ターゲット・サービスを再起動します。
   ターゲット・サービスの再始動について詳しくは、コンポーネント・サービスの管理を参照してください。ご使用のオペレーティング・システムに該当するセクションに記載されたステップを実行してください。

ゲートウェイでの FIPS 準拠の有効化

ゲートウェイ・コンポーネントで FIPS 準拠を有効にするには、ゲートウェイ・サポートのインストール時に作成されるゲートウェイ構成ファイルを編集します。

この `trc_gateway.properties` のファイルは以下のディレクトリーにあります。

Windows™ システム

```
\Documents and Settings\All Users\Application Data\BigFix\Remote Control
\Gateway
```

または `\ProgramData\BigFix\Remote Control\Gateway`

Linux™ システム

```
/etc
```

FIPS 準拠を有効にするには、以下の手順を実行します。

1. `trc_gateway.properties` ファイルを編集します。
2. **FIPSCompliance = Yes** を設定します。
3. ファイルを保存します。
4. ゲートウェイ・サービスを再起動します。
   ゲートウェイ・サービスの再始動について詳しくは、コンポーネント・サービスの管理を参照してください。ご使用のオペレーティング・システムに該当するセクションに記載されたステップを実行してください。

ブローカーでの FIPS 準拠の有効化

ブローカー・コンポーネントで FIPS 準拠を有効にするには、ブローカー・サポートのインストール時に作成されるブローカー構成ファイルを編集します。

この `trc_broker.properties` のファイルは以下のディレクトリーにあります。

Windows® システム

```
\Documents and Settings\All Users\Application Data\BigFix\Remote Control
\broker.
```

または `\ProgramData\BigFix\Remote Control\broker`

Linux® システム

```
/etc
```

FIPS 準拠を有効にするには、以下の手順を実行します。

1. `trc_broker.properties` ファイルを編集します。
2. **FIPSCompliance = Yes** を設定します。
3. ファイルを保存します。
4. ブローカー・サービスを再起動します。
   ブローカー・サービスの再始動について詳しくは、コンポーネント・サービスの管理を参照してください。
   ご使用のオペレーティング・システムに該当するセクションに記載されたステップを実行してください。

Remote Control における NIST SP800-131A 準拠

Remote Control バージョン 10.0.0 コンポーネントは、NIST SP800-131A 準拠に対応するように構成できます。

米国連邦情報・技術局 (NIST) Special Publications (SP) 800-131A 標準は、アルゴリズムを強化し、暗号鍵の長さを増やすことによって、セキュリティーを改善します。

以下の前提条件が必要です。

- すべての鍵の鍵セキュリティー強度が 112 ビット以上であることを確認します。RSA 鍵は 2048 ビット以上でなければなりません。
- すべての証明書が、新しい鍵強度を使用して作成されていることを確認します。2048 ビットよりも短い鍵を使用する RSA 証明書は、2048 ビット以上の鍵を使用する証明書に置き換える必要があります。
- すべての証明書が、許可された署名アルゴリズム (SHA-2 以上) で署名されていることを確認します。

NIST SP800-131A 準拠を有効にすると、セキュア接続を提供するために TLSv1.2 プロトコルが使用されます。そのため、ブラウザーに互換性のあることを確認する必要があります。

表 13. TLSv1.2 に対するブラウザーの互換性
以下の表に、TLSv1.2 と互換性のあるサポート対象ブラウザー・バージョンに関する情報を示します。

	TLSv1.2 がサポート対象でないバージョン	TLSv1.2 がサポート対象のバージョン (デフォルトで使用不可)	TLSv1.2 がサポート対象のバージョン (デフォルトで使用可能)
Internet Explorer	Windows™ XP および Windows™ Vista オペレーティング・システムの全 IE バージョン (IE6、IE7、IE8、IE9)	Windows™ 7 および Windows™ 8 オペレーティング・システムの IE8、IE9、IE10。	Windows™ 7 オペレーティング・システム以降の IE11
Firefox	<24	24	>24

NIST SP800-131A に準拠するには、暗号プロバイダーが FIPS 140-2 認定のものであることも求められます。SP800-131A 準拠が有効な場合、FIPS 140-2 準拠は (設定で使用不可になっている場合でも) 自動的に有効になります。

NIST SP800-131A 準拠を有効にする場合は、すべてのコンポーネントを構成する必要があります。以前のバージョンのコンポーネントとの互換性はありません。

注: Oracle の JVM では NIST SP800-131A はサポートされません。そのため、NIST のサポートの利点を活用するには、スタンドアロンのコントローラー・コンポーネントをインストールする必要があります。

サーバーでの NIST SP800-131A 準拠の有効化

Remote Control サーバーでは、インストール中にサーバー・インストーラー・プログラムを使用しているときに、NIST SP800-131A 準拠を有効化できます。また、NIST 準拠はインストール後にも有効化できます。BigFix® Remote Control サーバー を手動でインストールする場合に NIST SP800-131A 準拠を有効にするには、BigFix® Remote Control サーバー と WebSphere® を構成する必要があります。

サーバーのインストール中の NIST SP800-131A 準拠の有効化

インストール中に NIST SP800-131A 準拠を有効にするには、サーバー・インストーラーを使用したインストールの説明に従って操作します。インストール中に、**「Web サーバーのパラメーター」**ペインで、**「NIST SP800-131A 準拠を有効にする (FIPS を有効にする) (Enable NIST SP800-131A compliance (Enables FIPS))」**を選択します。

スタンドアロン WebSphere Application Server を使用したサーバーのインストールを実行するときの NIST SP800-131A 準拠の有効化

BigFix® Remote Control サーバー は、WebSphere® のセキュア HTTP 通信が提供するミドルウェア・インフラストラクチャーを使用します。このため、BigFix® Remote Control サーバー を手動でインストールする場合に NIST SP800-131A 準拠を有効にするには、BigFix® Remote Control サーバー と WebSphere® を構成する必要があります。

サーバーを手動でインストールする場合に NIST SP800-131A 準拠を有効にするには、サーバーのインストール後に以下の手順を実行します。

1. WebSphere の構成

   WebSphere®で NIST SP800-131A を有効にする方法については、「IBM WebSphere®」の資料を参照してください 。ご使用の WebSphere® のバージョンに該当する説明に従って操作してください。
2. 有効な管理者 ID およびパスワードを使用して、BigFix® Remote Control サーバー にログオンします。
3. **「アドミニストレーター」 > 「プロパティー・ファイルを編集」**をクリックします。
4. `common.properties`ファイルで 、**sp800131a.compliancea**を true に設定します。
5. 「**送信**」をクリックします。
6. **「アドミニストレーター」 > 「アプリケーションをリセット」**をクリックします。
7. サーバー・サービスを再起動します。
   サーバー・サービスの再始動について詳しくは、コンポーネント・サービスの管理を参照してください。ご使用のオペレーティング・システムに該当するセクションに記載されたステップを実行してください。

注: WebSphere® での NIST SP800-131A の有効化に伴う変更によって、そのサーバー上で稼働する他のすべてのアプリケーションが影響を受けます。このため、それらの他のアプリケーションにアクセスするユーザーのブラウザー設定を、トランスポート層セキュリティー (TLS) をサポートするように変更する必要があります。

Internet Explorer で TLS を有効にするには、以下の手順を実行します。

- **「ツール」 「インターネット・オプション」**クリックします。
- **「詳細設定」**タブで**「TLS 1.2 の使用」**を選択します。
- 「**適用**」をクリックします。
- 「**OK**」をクリックします。

Firefox で TLS を有効にするには、以下の手順を実行します。

- ブラウザーで**「about:config」**ページに移動します。
- **「細心の注意を払って使用する」**をクリックします。
- 検索フィールドで **security.tls.version.max** を検索します。
- 値を 3 に設定します。

サーバーのインストール後の NIST SP800-131A 準拠の有効化

インストーラー・プログラムを使用してサーバーをインストールした後、いくつかの方法で NIST SP800-131A 準拠を有効にすることができます。

ただし、まだ FIPS を有効にしていない場合は、最初に FIPS を有効にする必要があります。サーバーのインストール後に FIPS を有効にする方法について詳しくは、自動サーバー・インストール時の FIPS 準拠の有効化を参照してください。

また、NIST をサポートするための前提条件に確実に従うことにより、サーバー証明書の準拠性を確保することも必要です。証明書の前提条件について詳しくは、Remote Control における NIST SP800-131A 準拠を参照してください。

BigFix® Remote Control サーバー の自動インストール後に NIST SP800-131A 準拠を有効にするには、以下の手順を実行します。

1. 適切な方法を選択して NIST 構成を有効にしてください。

   オプション 1

   a. サーバーのインストール・ディレクトリー内にある tools ディレクトリーに移動します。
   b. オペレーティング・システムに応じて `trcsetup.cmd` または `trcsetup.sh` ファイルを編集します。

c. `ssl.cmd` または `ssl.sh` ファイルを呼び出す行で、**trc** の前にある 0 を 1 に変更します。また、このコマンドの末尾にある 0 も 1 に変更します。例えば、以下のようにします。

変更前のコマンドは次のようになります。

```
...\tools\ssl.cmd" "C:\Program Files (x86)\BigFix\TRC\server"
 1 0 "C:\" "%CERTSTOREPW%" "servername.localnet" 0 trc
  "%CERSTOREPWSELF%" "TrC" "0"
```

変更後のコマンドは次のようになります。

```
...\tools\ssl.cmd" "C:\Program Files (x86)\BigFix\TRC\server"
 1 0 "C:\" "%CERTSTOREPW%" "servername.localnet" 1 trc
  "%CERSTOREPWSELF%" "TrC" "1"
```

d. ファイルを保存します。

e. 同じディレクトリーで、オペレーティング・システムに応じて `tmem.sh` または `tmem.cmd` を編集します。

f. **NIST800=1**の値を設定します。**FIPSON=1**の値を設定します (まだ設定されていない場合)。

g. 以下のコマンドを実行します。

```
trcsetup userid password certpassword
```

ここで、*userid* および *password* は、データベース接続資格情報であり、*certpassword* は使用する認証ファイルのパスワードです。

注: Derby にはデータベース資格情報はないため、資格情報としてユーザー ID およびパスワードが使用されます。Derby を使用している場合は、以下のコマンドを入力します。

```
trcsetup userid password certpassword
```

オプション 2 - 一時的な NIST 構成

注: このオプションで設定された構成変更は、 `trcsetup` ファイルまたは `tmem` ファイルを再実行すると上書きされます。

a. `[installdir]\wlp\usr\servers\trcserver` ディレクトリー内の `ssl.xml` ファイルを編集します。

ここで、

[installdir]

サーバーのインストール・ディレクトリーです。

b. **sslProtocol="TLSv1.2"** を行 **ssl id="defaultSSLConfig"** に追加します。例えば、以下のようにします。

```
<server>
<ssl id="defaultSSLConfig" sslProtocol="TLSv1.2"
/>
<keystore id="defaultKeyStore" password="TrCWebAS"
/>
</server>
```

c. `ssl.xml` ファイルを保存します。
d. 同じディレクトリーで、`jvm.options` ファイルを編集します。
e. **-Dcom.ibm.jsse2.sp800-131=strict** および **-Dcom.ibm.jsse2.overrideDefaultTLS=true** という行を追加します。
f. ファイルを保存します。

2. 有効な管理者 ID およびパスワードを使用して、BigFix® Remote Control サーバー にログオンします。
3. **「アドミニストレーター」 > 「プロパティー・ファイルを編集」**をクリックします。
4. `common.properties`ファイルで 、**sp800131a.compliancea**を true に設定します。
5. 「**送信**」をクリックします。
6. **「アドミニストレーター」 > 「アプリケーションをリセット」**をクリックします。サーバー・サービスを再起動します。
   サーバー・サービスの再始動について詳しくは、コンポーネント・サービスの管理を参照してください。ご使用のオペレーティング・システムに該当するセクションに記載されたステップを実行してください。

以下の手順を実行することで、BigFix® Remote Control サーバー が NIST SP800-131A に対応するように構成されているかどうか確認します。

- **「アドミニストレーター」 > 「現在のサーバー状況を表示」**をクリックします。

以下のフィールドで、NIST SP800-131A 準拠が有効であることが示されます。

- NIST SP800-131A モードが使用可能になりました
- JVM が NIST SP800-131A モード用に構成されました

コントローラーでの NIST SP800-131A 準拠の有効化

Windows® オペレーティング・システムおよび Linux® (Intel®) オペレーティング・システム用の IBM® JRE は Remote Control に組み込まれており、 コントローラー・ソフトウェアをインストールするときにインストールされます。

Windows® システムを使用する場合、JRE はコントローラー・パッケージ `trc_controller_setup.exe` および `trc_controller.msi` に入っています。Linux®システムの場合、JRE はパッケージ `trc-controller-jre-10.x.x.i386.rpm`に含まれています。ここで、10.x.x はインストールするバージョンです。これらのパッケージは、IBM® FIPS 認定の暗号プロバイダーと NIST SP800-131A が有効にされた状態で事前構成されている

IBM® Java™ Run-time Environment をインストールします。これらのパッケージは、MIME タイプ `application/x-trc-jws` および `*.trcjws` ファイルのファイル関連付けも登録します。

リモート・コントロール・セッション時にコントローラーが FIPS モードと NIST SP800-131A モードのどちらで接続されているか確認するには、**「コントローラー・ツール」 > 「セッション情報の表示」をクリックします**。暗号化は、FIPS モードが有効な場合は AES FIPS に設定され、NIST モードが有効な場合は TLSv1.2 に設定されます。

スタンドアロン・コントローラーでの NIST SP800-131A 準拠の有効化

スタンドアロン・コントローラーをインストールした後に、プロパティー・ファイルを編集して、NIST SP800-131A 準拠を有効化できます。

P2P リモート・コントロール・セッションを開始するために、コントローラー・コンポーネントをローカルにインストールする場合は、`trc_controller.cfg` ファイルを編集して、NIST SP800-131A 準拠を有効にする必要があります。NIST SP800-131A 準拠を有効にするには、以下の手順を実行します。

1. コントローラーがインストールされているシステムで、`trc_controller.cfg` ファイルを編集します。

   Windows® システム

   [controller install dir]\trc_controller.cfg

   ここで *[controller install dir]* は、コントローラーのインストール時に選択したインストール・ディレクトリーです。

   Linux® システム

   `opt/Bigfix/trc/controller/trc_controller.cfg`

2. **sp800131a.compliance** を true に設定します。
3. ファイルを保存します。

NIST SP800-131A が有効になっている場合の MS SQL データベース用の証明書の作成

NIST SP800-131A 準拠を有効にしているときに MS SQL データベースを使用する場合、証明書を作成する必要があります。

証明書を生成するために、IBM® 鍵管理ツールを使用できます。組み込みコンポーネントを含む Remote Control サーバーがインストールされていて、かつコントローラー・コンポーネントがインストールされている場合、IBM® 鍵管理ツールにアクセスできます。このツールは、IBM® WebSphere® Application Server によっても提供されます。

注: 鍵サイズが 4096 以上の証明書を作成するには、制限ポリシー・ファイルの `local_policy.jar` および `US_export_policy.jar` を上書きする必要があります。

以下のディレクトリーに移動して、`local_policy.jar` および `US_export_policy.jar` のファイルをコピーします。

Windows™ システム

`TRC\server\java\demo\jce\policy-files\unrestricted`

Linux™ システム

`TRC/server/java/demo/jce/policy-files/unrestricted`

以下のファイルを、コピーした JAR ファイルに置き換えます。

Windows™ システム

`TRC\server\java\jre\lib\security\local_policy.jar`

`TRC\server\java\jre\lib\security\US_export_policy.jar`

Linux™ システム

`TRC/server/java/jre/lib/security/local_policy.jar`

`TRC/server/java/jre/lib/security/US_export_policy.jar`

証明書を作成してインストールするには、以下の手順を実行します。

1. サポートされているいずれかのバージョンの MS SQL Server および最新のパッチをインストールします。最小要件は、MS SQL Server 2012 Service Pack 3 です。
2. 自己署名証明書を使用して鍵ストアを作成します。

    a. コマンド・ライン・ウィンドウを開きます。

    b. 以下のいずれかのディレクトリーに移動して、鍵ツールを実行します。

    組み込みコンポーネントとともにインストールされた Remote Control サーバー

    Remote Control サーバーのインストール・ディレクトリーに移動します。

    WebSphere® アプリケーションサーバーがインストールされている場合

    WebSphere® Application Server のインストール・ディレクトリーに移動します。

    コントローラー・コンポーネントがインストールされている場合

    `...\Controller\jre` ディレクトリーへ移動します。例えば、以下のようにします。

    Windows™ システム。

    `C:\Program Files\BigFix\Remote Control\Controller\jre`

    Linux™ システム。

    `/opt/bigfix/trc/controller/jre`

    c. `bin` ディレクトリーに移動する。

    d. ご使用のオペレーティング・システムに該当する `ikeyman` ファイルを実行します。

    Windows™ システム

    `ikeyman.bat`

Linux™ システム

```
ikeyman.sh
```

e. **「鍵データベース・ファイル」「新規」**を選択します。

f. **鍵データベース・タイプ**として**「PKCS12」**を選択します。

g. **「参照」**をクリックして、鍵ストアを保管する場所に移動します。

h. ファイルのファイル名を入力して、**「保存」**をクリックします。

i. 「**OK**」をクリックします。

j. 鍵ストアを保護するためのパスワードを入力して確認し、**「OK」**をクリックします。

k. **「作成」「新規自己署名証明書 (New Self-Signed Certificate)」**を選択します。

l. **「鍵ラベル (Key Label)」**の名前を入力します。
例えば、サーバーのホスト名を入力します。

m. **「バージョンのX509 V3**を選択します。

n. **「鍵サイズ」**の値を選択します。
NIST SP800-131A 準拠の推奨値は 2048 以上です。

o. **「署名アルゴリズム (Signature Algorithm)」**として**「SHA256WithRSA」**を選択します。

p. **「共通名」**を入力します。
サーバーの DNS ホスト名に設定します。
例: `trcserver.example.com`

q. 必要に応じて、追加のオプション情報を入力します。

r. **有効期間**を入力します。
証明書を有効にする日数を設定します。デフォルトは 365 日です。

s. **「サブジェクト代替名 (Subject Alternative Names)」**、**「DNS 名」**オプションをサーバーの DNS ホスト名に設定します。

t. 「**OK**」をクリックします。

3. 証明書ストアをデータベース・サーバーに追加します。

a. コマンド・ラインで、`mmc.exe` を実行します。

b. 証明書スナップインを追加します。

i. **「ファイル」 > 「スナップインの追加と削除」**を選択します。
ii. **「証明書」**スナップインを選択し、**「追加」**をクリックします。
iii. **「コンピューター・アカウント」** を選択し、**「次へ」**をクリックします。

iv. **「ローカル・コンピューター」**オプションが選択されていることを確認し、**「完了」**をクリックします。
v. 「**OK**」をクリックします。

c. 証明書をインポートします。
i. **「コンソール 1」**ウィンドウで、**「コンソール・ルート」 > 「証明書」に進みます**。
ii. **「証明書」**を右クリックし、**「すべてのタスク」 > 「インポート」**を選択します。
iii. **「ようこそ」**ウィンドウで**「次へ」**をクリックします。
iv. **「参照」**をクリックして作成した証明書ストアを選択します。
v. 「**次へ**」をクリックします。
vi. 証明書ストアのパスワードを入力し、**「次へ」**をクリックします。
vii. **「証明書をすべて次のストアに配置する」**が選択されていること、および**「証明書ストア」**が**「個人用」**に設定されていることを確認します。「**次へ**」をクリックします。
viii. 「**終了**」をクリックします。

4. 秘密鍵を管理します。
a. 証明書ファイルを右クリックし、**「すべてのタスク」 > 「秘密キーの管理」**を選択します。
b. 「**追加**」をクリックします。
c. **「名前の確認」**をクリックして、**「MSSQLSERVER」**を選択し、**「OK」**をクリックします。
d. **「ユーザーとグループの選択」**ウィンドウで **「OK」**をクリックします。
e. **MSSQLSERVER** の許可を**「権限」**ウィンドウで設定し、**「OK」**をクリックします。例えば、読み取り専用のオプションに対して「**読み取り**を**許可**」を選択します。
5. 構成を完了するには、SQL Server 構成マネージャーを実行します。
a. **「SQL Server ネットワークの構成」**を展開します。
b. **「MSSQLSERVER のプロトコル」**を右クリックして、**「プロパティー」**を選択します。
c. **「証明書」**タブで、インポートした証明書を選択します。
d. **「フラグ」**タブで、**「強制的に暗号化」**を「*Yes*」に設定して、**「OK」**をクリックします。
e. 「警告」ウィンドウで**「OK」**をクリックします。
f. **「SQL Server のサービス」**を選択します。
g. 右側のペインで**「SQL Server (MSSQLSERVER)」 > 「再起動」**を右クリックします。

ターゲットでの NIST SP800-131A 準拠の有効化

Remote Control ターゲットでの NIST SP800-131A 準拠の有効化は、さまざまな方法で行うことができます。インストール中にターゲットのインストール・プログラムを使用しているときに、NIST SP800-131A 準拠を有効化できます。インストール後に NIST SP800-131A 準拠を有効にするには、ターゲットのレジストリーを編集するか (Windows® システムの場合)、構成ファイルを編集します (Linux® システムの場合)。

ターゲットのユーザー・インターフェースを使用して適切なオプションを選択し、ターゲットで NIST SP800-131A 準拠が有効であることを確認します。

- Remote Control- ターゲット・ユーザー・インターフェースで、**「アクション」メニュー > 「接続情報」**をクリックします。
- システム通知域の **Remote Control** アイコンにマウス・カーソルを移動します。

Windows® ターゲットでの NIST SP800-131A 準拠の有効化

Windows オペレーティング・システムを使用している場合に、ターゲットで NIST SP800-131A 準拠を有効にするには、2 とおりの方法があります。インストール中に準拠を有効にするか、インストール後にターゲットのレジストリーを編集して準拠を有効にすることができます。

ターゲットのインストール中の NIST SP800-131A 準拠の有効化

インストール中に NIST SP800-131A 準拠のターゲット・プロパティーを有効にするには、ターゲットのインストールの説明に従って操作します。ターゲット・インストーラーの**「サーバーのアドレス」**画面で、**「詳細設定」**をクリックします。**「NIST SP800-131A 準拠を有効にする (FIPS を有効にする)」**を選択します。

ターゲットのサイレント・インストール中の NIST SP800-131A 準拠の有効化

ターゲットのサイレント・インストール中に NIST SP800-131A 準拠を有効にするには、インストール・コマンドの **SP800131A** パラメーターを使用できます。ターゲットのサイレント・インストールについて詳しくは、Windows システムでのターゲット・カスタム・インストールの実行を参照してください。

NIST SP800-131A 準拠を有効にするには、以下のパラメーターを使用します。

- TRC_SERVER_PROTOCOL=https
- TRC_SERVER_PORT=443
- SP800131A=yes

例えば、 `trc_target_setup.exe /s /v"/qn TRC_SERVER_HOSTNAME=yourserver TRC_SERVER_PROTOCOL=https TRC_SERVER_PORT=443 SP800131A=yes"`

ここで、*yourserver* は、BigFix® Remote Control サーバー のホスト名または IP アドレスです。

ターゲットのインストール後の NIST SP800-131A 準拠の有効化

Remote Control ターゲットをインストールした後に、 ターゲットのレジストリーを編集することで NIST SP800-131A 準拠を有効にすることができます。NIST SP800-131A 準拠を有効にするには、以下の手順を実行します。

1. コマンド・プロンプト・ウィンドウで regedit コマンドを実行します。
2. Windows™ レジストリーで `HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\Remote Control\Target`の手順を実行します。
   64 ビット・システムでは、32 ビット・レジストリー・キーは WOW6432Node キーの下にあります。
   例えば、`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BigFix\Remote Control\Target` です。
3. **「SP800131ACompliance」**を右クリックして**「変更」**を選択します。

4. **「値のデータ」**フィールドに yes と入力し、**「OK」**をクリックします。
5. ターゲット・サービスを再起動します。
   ターゲット・サービスの再始動について詳しくは、コンポーネント・サービスの管理を参照してください。ご使用のオペレーティング・システムに該当するセクションに記載されたステップを実行してください。

Linux® または UNIX® ベースのターゲットでの NIST SP800-131A 準拠の有効化

Remote Control ターゲットをインストールした後に、`trc_target.properties` ファイルを編集することで NIST SP800-131A 準拠を有効にすることができます。NIST SP800-131A 準拠を有効にするには、以下の手順を実行します。

1. `/etc/trc_target.properties` ファイルを編集します。
2. *SP800131ACompliance* の値を「YES」に設定し、ファイルを保存します。
3. ターゲット・サービスを再起動します。
   ターゲット・サービスの再始動について詳しくは、コンポーネント・サービスの管理を参照してください。ご使用のオペレーティング・システムに該当するセクションに記載されたステップを実行してください。

ゲートウェイでの NIST SP800-131A 準拠の有効化

ゲートウェイ・コンポーネントで NIST SP800-131A 準拠を有効化にするには、ゲートウェイ・サポートのインストール時に作成されるゲートウェイ構成ファイルを編集します。

この `trc_gateway.properties` のファイルは以下のディレクトリーにあります。

Windows™ システム

```
\Documents and Settings\All Users\Application Data\BigFix\Remote Control
\Gateway
```

または `\ProgramData\BigFix\Remote Control\Gateway`

Linux™ システム

```
/etc
```

NIST SP800-131A 準拠を有効にするには、以下の手順を実行します。

1. `trc_gateway.properties` ファイルを編集します。
2. **SP800131ACompliance = Yes** を設定します。
3. ファイルを保存します。
4. ゲートウェイ・サービスを再起動します。
   ゲートウェイ・サービスの再始動について詳しくは、コンポーネント・サービスの管理を参照してください。ご使用のオペレーティング・システムに該当するセクションに記載されたステップを実行してください。

ブローカーでの NIST SP800-131A 準拠の有効化

ブローカー・コンポーネントで NIST SP800-131A 準拠を有効にするには、ブローカー・サポートのインストール時に作成されるブローカー構成ファイルを編集します。

この `trc_broker.properties` のファイルは以下のディレクトリーにあります。

Windows® システム

```
\Documents and Settings\All Users\Application Data\BigFix\Remote Control
\broker
```

または `\ProgramData\BigFix\Remote Control\broker`

Linux® システム

```
/etc
```

NIST SP800-131A 準拠を有効にするには、以下の手順を実行します。

1. `trc_broker.properties` ファイルを編集します。
2. **SP800131ACompliance = Yes** を設定します。
3. ファイルを保存します。
4. ブローカー・サービスを再起動します。
   ブローカー・サービスの再始動について詳しくは、コンポーネント・サービスの管理を参照してください。
   ご使用のオペレーティング・システムに該当するセクションに記載されたステップを実行してください。

CLI ツールでの NIST SP800-131A 準拠の有効化

Windows オペレーティング・システムでは、インストール中に CLI ツールをインストールしているときに、NIST SP800-131A 準拠を有効化できます。Linux では、CLI ツールをインストールした後、構成ファイルを編集することで、NIST SP800-131A を有効化できます。

Windows CLI ツールのインストール時の NIST SP800-131A 準拠の有効化

コマンド・ライン・インターフェース・ツールのインストール時に NIST SP800-131A 準拠を有効にするには、Windows システムでの CLI ツールのインストールの説明に従って操作します。**「サーバーのアドレス」**画面の**「詳細設定」**をクリックし、インストール中に**「NIST SP800-131A 準拠を有効にする (FIPS を有効にする) (Enable NIST SP800-131A compliance (Enables FIPS))」**を選択します。

Linux® または UNIX® ベースのターゲットにおける CLI での NIST SP800-131A 準拠の有効化

CLI ツールをインストールした後に、`trc_target.properties` ファイルを編集することで NIST SP800-131A 準拠を有効にすることができます。NIST SP800-131A 準拠を有効にするには、以下の手順を実行します。

1. `/etc/trc_target.properties` ファイルを編集します。
2. *SP800131ACompliance* の値を yes に設定します。
3. ファイルを保存します。

サーバー・インストールの検証

サーバーのインストールが完了したら、以下のステップを実行してインストールを検証できます。

1. ブラウザー・ウィンドウで、Remote Control サーバーのアドレスを入力します。例えば、`http://yourservername/trc` *yourservername* は、ご使用の Remote Control サーバーのホスト名または IP アドレスです 。
2. Remote Control ログオン画面が表示されていることを検証します。
3. 次の管理者 ID とパスワードを使用してログオンします。- *id=admin*、*password=password*。
4. 「詳細を変更」画面で、表示された指示に従ってパスワードを変更します。

インストール・エラーからの復旧

インストール・エラーが発生した場合は、以下の章を参照して問題を特定し、対処してください。

復旧の手順

最初に以下の説明を参照して、 インストール・エラーからの復旧を支援する、ログ・ファイルなどの情報を探してください。

HCL ソフトウェア・サポートに問い合わせる必要がある場合は、以下の情報を収集してください。

- Windows™ オペレーティング・システムを使用している場合、インストール・エラーに関連するすべてのイベント・ログ。
- インストール・ログ・ファイル
- オペレーティング・システムのバージョン (すべての Service Pack を含む)
- WebSphere® Application Server、データベース・サーバー、および Java™ のバージョン。
- ハードウェアの説明
- インストール・メディアのタイプ。
- Windows™ インストールに失敗したときにアクティブだったサービス。アンチウィルス・ソフトウェアなど

発生する可能性のあるエラーに関する情報を収集するために、以下のファイルも使用できます。

`\tsetup.ini`

自動インストール中に記録された基本的な情報が書き込まれています。

`[installdir]\install.log`

内部デバッグ・メッセージが書き込まれています。

`[installdir]\inst.ini`

インストールに関するすべてのパラメーターが書き込まれています。

`[installdir]\wlp\usr\server\trcserver`

構成 XML ファイルが入っています。

`[installdir]\wlp\usr\server\trcserver\logs\messages.log`

```
[installdir]\wlp\usr\server\trcserver\logs\messages_xxxxxxx.log

[installdir]\wlp\usr\server\trcserver\logs\ffdc directory
```

インストール中のエラー

以下のトピックでは、サーバーのインストーラー・プログラムを使用する場合に、Remote Control サーバーのインストール中に発生する可能性のあるエラーに対するリカバリー・アクションについて説明します。

メモリー不足

症状

インストール中にメモリー・エラーが報告され、インストールが続行されません。

原因

インストール開始時のメモリー・チェックで、 インストールに必要な最小限のメモリーがインストール先のコンピューターにないと判別されました。

解決策

メモリーの要件について詳しくは、サーバーの要件を参照してください。

DB2® データベース・オプションの検証時の接続エラー

症状

インストール中に DB2® データベース接続エラーが報告されました。

原因

インストール中にデータベースとして DB2® を選択した場合、データベース・オプション画面で指定した情報がインストーラーによって検証されます。データベースへの接続を確立するために、ユーザー ID、パスワード、およびポートの値が使用されます。接続に失敗する場合は、エラーが報告されます。このエラーには、DB2® によって報告されるエラーも含まれます。

解決策

このエラーが報告される理由は以下のとおりです。

- データベース・オプション画面で入力した値が誤っている。前の画面に戻り、情報を確認してください。
- データベース・インスタンスが存在しない。DB2® を使用する予定の場合は、 Remote Control サーバーより前にインストールしておく必要があります。データベース・インスタンスも作成する必要があります。
- リモート・データベースに接続できない。リモート・データベースを使用している場合は、リモート・システムの IP アドレスを ping できることを確認してください。

Oracle 事前チェック

症状

インストール中に Oracle データベース接続エラーが報告されました。

原因

インストール中にデータベースとして Oracle を選択した場合、インストーラーはデータベースに接続して、データベース・オプション画面で指定された情報を検証します。接続に失敗する場合は、 エラーが報告されます。エラー・メッセージには、Oracle から返されたエラーが含まれています。

解決策

前の画面に戻り、指定した情報を使用して問題を修正してください。

例: インストール前に Oracle データベースを作成していない場合は、以下のエラーが報告されます。

```
Failed to verify userid, password, server, database and driver
file combination supplied.Please verify details and try again.
 ( Listener refused the connection with the following error:
ORA-12505. TNS:listener does not currently know of SID given in
connect descriptor
The Connection descriptor used by the client was:
127.0.0.1:1521:TRCDB
```

この場合は、インストールを取り消し、Oracle データベースを作成してから、再度 Remote Control をインストールする必要があります。

インストール・プログラムを使用してサーバーをインストールするときの libstdc++.so.5 エラー

症状

Linux® で、 以下の例外エラーが発生してサーバーのインストールが異常終了します。

```
This application has unexpectedly quit:Invocation of this Java application has caused an
InvocationTargetException. This application will now exit".
```

インストール・ログに以下のエラーが記録される場合があります。

```
java.lang.unsatisfiedlinkerror :fontmanager (libstdc++.so.5: can not open shared object file:No
such file or directory)
```

原因

必須のパッケージが欠落しています。

解決策

libstdc++.so.5 パッケージをインストールしてください。インストールするには **compat-libstdc++-33** パッケージをインストールします。 このパッケージに libstdc++.so.5 が含まれています。

インストール後のエラー

Remote Control のインストールが完了し、アプリケーション・サービスが開始していれば、ログオンすることができます。正常にログオンできない場合は、以下の情報を参照して、問題を解決してください。

- サーバー・サービスが実行されていることを確認します。

  Windows™ システム

  Windows™ サービスで、以下のサービスが開始していることを確認します。

  Remote Control-Server。

  Linux™ システム

  以下のサービスが `/etc/init.d/trcserver` または`/etc/rc.d/init.d/trcserver` で作成され、開始されます。

  注: このサーバー・タイプを手動で停止または開始するには、以下のコマンドを入力します。

  `/etc/init.d/trcserver [parameter]` ここで *parameter* は *stop*、*start* または *restart* です。

- 報告されているエラーがないかどうか、`[installdir]\wlp\usr\server\trcserver\logs` ディレクトリー内のログ・ファイルを確認します。また、サーバーのインストール・ディレクトリー内の `trc.log` ファイルを確認することもできます。
- Oracle データベースを使用している場合は、ユーザー ASSET が存在することを確認してください。

メモリー不足エラー

症状

BigFix® Remote Control サーバー の開始時にログ・ファイルにメモリー不足エラーが報告されます。ログ・ファイルには、「ヒープのインスタンス化に失敗しました」と報告されます。

原因

アプリケーションを実行するために使用可能なメモリーが不足しています。このエラーが発生した理由は、ヒープに割り振られた最大メモリーが大きすぎることです。また、実行中またはインストールされている他のアプリケーションの影響を受けている可能性があります。

インストール中に、インストーラーは Remote Control アプリケーションが使用可能 RAM の 70% までを使用するようにセットアップしようとします。Java virtual machine™ (JVM) を開始できない場合、この割合は低くなります。ただし、他のソフトウェアもインストールされている場合は、メモリー不足エラーが発生し、Remote Control のログ・ファイルに報告される場合もあります。

解決策

この問題を解決するには、付属のスクリプトを使用して、 手動でメモリー・パラメーターを低い値に設定してください。このスクリプトは、Remote Control インストール・ディレクトリーにあります。このスクリプトを使用して、メモリー・パラメーター、およびスレッド と Web 接続の数を設定します。

- `tmem.cmd` - Windows®システムの場合。
- `tmem.sh` - UNIX ベースのシステムの場合。

Remote Control のインストール・ディレクトリーから以下のコマンドを実行します。

```
tmem.cmd minmem maxmem
```

注: UNIX ベースのシステムの場合は tmem.sh を使用します。

minmem; maxmem

割り振るメモリーの最小値および最大値を設定します。

注: 32 ビットの eWAS で提供される 32 ビット Java で使用できるのは、使用可能な RAM の量にかかわらず、最大で 2.7 GB のみに制限されます。

tmem.cmd コマンドおよび tmem.sh コマンドを使用して、以下のパラメーターを調整することもできます。

maxwebconn

許可する Web 接続の数を設定します。デフォルトは 85 であり、175 まで増加することができます。

maxthreads; minthreads

許可するスレッドの最小数および最大数を設定します。最大スレッド数は 50 であり、150 まで増やすことができます。

バージョン 10.x.x でこれらのパラメーターを編集するには、以下のステップを実行します。

1. `trcsetup.cmd`または `trcsetup.sh` を編集します。
2. `memory.cmd` ファイルに対する呼び出しを含む行を編集します。例えば、 `C:\TRC\server\tools\memory.cmd 163 49 135 1`

   ここで、
   - **maxwebconn** = パラメーター 1 (163)
   - **minthreads** = パラメーター 2 (49)
   - **maxthreads**= パラメーター 3 (135)

パラメーター 4 は編集せず、値を 1 のままにしておきます。

3. 必要な値を変更します。
4. `trcsetup` ファイルを保存します。
5. 次のコマンドを入力します。

```
trcsetup userid password certpassword
```

ここで、*userid* および *password* は、データベース接続資格情報であり、*certpassword* は使用する認証ファイルのパスワードです。

注: Derby にはデータベース資格情報はないため、資格情報としてユーザー ID およびパスワードが使用されます。Derby を使用している場合は、以下のコマンドを入力します。

trcsetup userid password *certpassword*

データベース接続許可の失敗

症状

ログ・ファイルにデータベース接続許可失敗エラーが報告されます。

原因

データベース・パスワードが無効である可能性があります。

解決策

Remote Control インストール・ディレクトリーから以下のコマンドを実行することで、パスワードを変更してください。

Windows® システム。

`[installdir]\tools\tdbpasswd.cmd userid password`. ここで、*installdir* は Remote Control のインストール・ディレクトリーであり、*userid* および *password* はデータベース・ログオンの資格情報です。

UNIX ベースのシステム

`[installdir]/tools/tdbpasswd.sh userid password`. ここで、*installdir* は Remote Control のインストール・ディレクトリーであり、*userid* および *password* はデータベース・ログオンの資格情報です。

コマンドを実行して、 アプリケーションのデータベース・パスワードを変更します。コマンドを実行したら、Remote Control サービスを再起動します。

アプリケーションのウェルカム・ページが表示されない場合

症状

Remote Control サーバーの URL をブラウザーに入力しても、Remote Control サーバーのウェルカム・ページが表示されません。

原因

問題が発生した原因として、いくつかの理由が考えられます。それらはログ・ファイルに報告されています。

解決策

サーバー・インストール・ディレクトリーにある `install.log` ファイルに報告されているエラーを調べてください。

DB2® データベース・オプションの検証時の接続エラー

症状

インストール中に DB2® データベース接続エラーが報告されました。

原因

インストール中にデータベースとして DB2® を選択した場合、データベース・オプション画面で指定した情報がインストーラーによって検証されます。データベースへの接続を確立するために、ユーザー ID、パスワード、およびポートの値が使用されます。接続に失敗する場合は、エラーが報告されます。このエラーには、DB2® によって報告されるエラーも含まれます。

解決策

このエラーが報告される理由は以下のとおりです。

- データベース・オプション画面で入力した値が誤っている。前の画面に戻り、情報を確認してください。
- データベース・インスタンスが存在しない。DB2® を使用する予定の場合は、 Remote Control サーバーより前にインストールしておく必要があります。データベース・インスタンスも作成する必要があります。
- リモート・データベースに接続できない。リモート・データベースを使用している場合は、リモート・システムの IP アドレスを ping できることを確認してください。

ターゲットがサーバーに接続できない

症状

ターゲットが BigFix® Remote Control サーバー で詳細を登録および更新していません。

原因

- ターゲットにサーバーの正しい URL が設定されていません。
- サーバーへの接続に使用される URL のホスト名部分がサーバーの SSL 証明書内の共通名と一致していません。

解決策

ターゲット・ソフトウェアをインストールすると、ターゲットは、HTTP または HTTPS、およびターゲットのインストール時に定義されたサーバー URL を使用してサーバーに接続します。ただし、サーバーとターゲット間の接続を正常に確立するために注意しなければならない重要な考慮事項が 2 点あります。

- ターゲットにサーバーの正しい URL が設定されている必要があります。
- URL のホスト名部分がサーバーの SSL 証明書内の共通名に一致している必要があります。

インストール・プログラムを使用して BigFix® Remote Control サーバー をインストールする場合は、**Web サーバー・パラメーター**・ウィンドウで正しい値を指定するようにする必要があります。デフォルトでは、**「データのアップロード先サーバー」**フィールドには Windows® オペレーティング・システム設定のコンピューター名が設定されます。サーバー・インストーラー・プログラムは、このフィールドの値を使用してサーバー URL を生成します。次に、この URL が `trc.properties` ファイルの **url** プロパティーに保存され、SSL 証明書にも保存されます。そのため、インストール時に必ず正しいコンピューター名を指定してください。正しくない値を指定すると、以下の問題が発生することがあります。

ターゲットは、サーバーに初めて接続する際に、ターゲット・レジストリーまたは構成ファイルの **ServerURL** プロパティーを使用してサーバーに接続します。サーバーからターゲットへの応答には、`trc.properties` ファイルの **url** プロパティーに割り当てられているサーバー・アドレスが含まれています。ターゲットは、この URL を使用してサーバーに接続します。ターゲットに送信されたアドレスが正しくない場合、ターゲットが一度登録されるとサーバーに再度接続できなくなります。しばらく経ってから、ターゲットはオフラインとしてマークされます。このターゲットとのセッションを開始することもできません。これは、着信セッションを認証するための、正しくて有効な URL がターゲットに設定されていないからです。

サーバーの SSL 証明書内の共通名は、サーバーの IP アドレスに解決されるホスト名にする必要があります。SSL 証明書に、例えば *mytrcserver* が含まれているが、ターゲットで *mytrcserver* をサーバーの IP アドレスに変換する手段がないといった場合、ご使用の環境は正しく構成されません。正しくサポートされる唯一の名前は、DNS に登録されている完全修飾ドメイン名です。例えば、*mytrcserver.example.ibm.com* です。*mytrcserver* のみを使用するには、サーバーとターゲットが同じローカル・ネットワーク上にあり、それらで WINS が構成されている必要があります。

DNS サーバーが正しく構成されているかを確認するには、nslookup コマンドを使用して、完全なコンピューター名と IP アドレスを照会します。

例: コマンドプロンプトで、以下のコマンドを入力します。

```
C:\>nslookup

Default Server:  dns.example.ibm.com
Address:  192.0.2.0
```

```
Type in the hostname of your server

> mytrcserver.example.ibm.com
Server:  dns.example.ibm.com
Address:  192.0.2.0

Name:    mytrcserver.example.ibm.com
Address:  192.0.2.1



Type in the ip address of your server

> 192.0.2.1
Server:  dns.example.ibm.com
Address:  192.0.2.0

Name:    mytrcserver.example.ibm.com
Address:  192.0.2.1
```

サーバー・ホスト名が正しい IP アドレスに解決されていることが分かります。

データベースとして Oracle を使用する場合のエラー

症状

`java.lang.ArrayIndexOutOfBoundsException`Oracle データベースを使用しているときにエラーが報告されました。

原因

Oracle jdbc ドライバーに関する問題が存在します。

解決策

適切なオプションを選択して問題を解決します。

- Oracle 10.2g JDBC 4 ドライバーを使用します。ドライバーは、Oracle 9、10、および 11 の場合に有効です。
- Oracle 11g ドライバーを使用する場合は、`trc.properties` ファイルを手動で編集し、 プロパティー **oracle.increment.keys.off=1** を設定してください。

注: サーバー・サービスを再起動します。

FIPS 準拠モードで Microsoft® SQL データベースに接続するときのエラー

症状

FIPS 準拠モードで Microsoft® SQL データベースに接続するときのエラー

原因

IBM® JRE および IBM® JSSE プロバイダーを使用し、さらに FIPS 準拠を有効にした状態で Websphere Application Server を使用する場合は、MS SQL データベースを使用できません。

解決策

MS SQL の場合、IBM® Websphere で FIPS が有効で**なければ**、これらのオプションを使用できます。

コンポーネントのアンインストール

各種 Remote Control コンポーネントをインストールした後、それらを複数の方法でアンインストールすることができます。

サーバーのアンインストール

Remote Control サーバーを削除する場合、選択する方法は、実行されたインストールのタイプによって異なります。Remote Control インストール・プログラムを使用してサーバーをインストールした場合は、インストーラーを使用するか、「プログラムの追加と削除」を使用して、ソフトウェアをアンインストールできます。BigFix® Remote Control サーバー の手動インストールを実行した場合は、IBM® WebSphere Application Server 管理コンソールを使用して、ソフトウェアをアンインストールする必要があります。

インストーラーを使用した サーバーのアンインストール

Windows® オペレーティング・システムまたは Linux® オペレーティング・システムを使用している場合、以下の手順を使用して、Remote Control サーバー・ソフトウェアをアンインストールします。

インストーラーを使用して Remote Control サーバーをアンインストールするには、以下のステップを実行します。

1. Remote Control サーバーのインストール・ディレクトリーに移動します。
   デフォルト・ディレクトリーか、サーバーのインストール時に選択した特定のディレクトリーです。例えば、以下のようにします。

   Windows® システム

   ```
   \Program Files\BigFix\TRC\server
   ```

   Linux® システム

   ```
   /opt/BigFix/Tivoli/TRC/server
   ```

2. **「Remote Controlのアンインストール (Uninstall) - Server.exe」**をダブルクリックします。
3. **「アンインストール」**をクリックします。
4. 完了したら、**「完了」**をクリックします。

インストーラーによって作成された Remote Control の機能、ファイル、およびフォルダーが削除されます。

IBM® Websphere Application Server でのサーバー・アプリケーションのアンインストール

BigFix® Remote Control サーバー ソフトウェアの手動インストールを実行した場合は、IBM® WebSphere Application Server 管理コンソールを使用して以下のステップを実行することで、ソフトウェアをアンインストールできます。

管理コンソールにアクセスするには、以下のステップを実行します。

1. ブラウザーで、以下を入力します。

   ```
   https://[server : port]/ibm/console
   ```

   ここで *server* は、アプリケーション・サーバー・マシンの IP アドレスまたは名前 (localhost や 192.0.2.0 など) であり、*port* は、サーバーが listen するポートです。
2. WebSphere のインストール時に定義した ID とパスワードを使用してログオンします。
3. 「アプリケーション」を展開し、**「エンタープライズ・アプリケーション」**をクリックします。
4. Remote Control サーバー・アプリケーションのチェック・ボックスを選択します。
5. **「アンインストール」**をクリックします。
6. **「保存」** を選択してマスター構成に保存します。

「プログラムの追加と削除」を使用したサーバーのアンインストール

Windows® オペレーティング・システムを使用している場合、「プログラムの追加と削除」を使用して以下のステップを実行することで、サーバー・ソフトウェアをアンインストールできます。

1. **「コントロール パネル」**を開きます。
2. **「プログラムの追加と削除」**をダブルクリックします。
3. **Remote Control「- サーバー」**を選択します。
4. **「変更と削除」**をクリックします。
5. **「アンインストール」**をクリックします。
6. 完了したら、**「完了」**をクリックします。

Windows™ システムでのターゲットのアンインストール

「プログラムの追加と削除」 を使用して、Windows™ システムからターゲット・ソフトウェアを削除します。

「プログラムの追加と削除」を使用してターゲット・ソフトウェアを削除するには、以下のステップを実行します。

1. **「コントロールパネル」**を開きます。
2. **「プログラムの追加と削除」**をダブルクリックします。
3. **「IBM Remote Control - ターゲット」** を選択します。

4. 「**除去**」をクリックします。
5. プロンプトが表示されたら、**「はい」**をクリックします。

Remote Control ターゲット・ソフトウェアがシステムから削除されます。

Linux® システムでのターゲットのアンインストール

Linux® システムでターゲット・ソフトウェアを削除するには、以下のステップを実行します。

1. 以下のコマンドを実行して、インストールされている Remote Control パッケージ名を検索します。

   ```
   rpm  -qa  |grep  trc
   ```

2. 以下のコマンドを実行します。

   ```
   rpm  -e <trcpackage>
   ```

   ここで *trcpackage* は、パッケージ名です。

   ```
   For example: rpm -e trc-target
   ```

以下の手順を実行することで、ターゲットが削除されたことを確認できます。

1. ステップ 1 のコマンドを実行して、 Remote Control パッケージがインストールされていないことを確認します。
2. 以下のコマンドを実行して、実行中の Remote Control プロセスが存在しないことを確認します。

   ```
   ps  -ef  |grep  trc
   ```

以前のバージョンからのアップグレード

以下の制限は、バージョン 9.0.0、9.0.1、または 9.1.0 からバージョン 9.1.2 にアップグレードする場合は問題ではありません。

Remote Control バージョン 9.0.0 では、各種コンポーネントを正しい順序でアップグレードしないと、導入された新機能により、以前のバージョンとの互換性の問題が発生する場合があります。

この制約は、ゲートウェイ・コンポーネントとブローカー・コンポーネントがデプロイされている環境にのみ該当します。こうした環境では、サーバー・コンポーネントまたはターゲット・コンポーネントに先んじて、ブローカーとゲートウェイを更新する必要があります。ブローカーとゲートウェイのアップグレードが完了したら、ターゲットとサーバーを、(この両者の間には依存関係が存在しないため) 環境に最も適した順序でアップグレードできます。

予防措置として、すべてのプロパティー・ファイルを常にバックアップすることをお勧めします。ただし、このリリースでコントローラーをアップグレードする場合、既存のプロパティーは失われるため、プロパティー・ファイルをバックアップする必要があります。

以前のバージョンからバージョン 10 にアップグレードします

サーバーのアップグレード時に、インストーラーは、以前のバージョンのサーバーが存在し、そのサーバーインスタンスがバージョン10にアップグレードされていることを検出します。

ターゲット、ブローカー、ゲートウェイおよびコントローラーをアップグレードする場合、アップグレード・プロセスは以下のもので構成されます。

- バージョン 10 コンポーネントのインストール
- コンポーネントの構成をマイグレーション
- コンポーネントの以前のバージョンをアンインストール

注: アップグレード・プロセス中に、ブローカーの証明書は再配置されません。ブローカーのアップグレード後に、ブローカー構成内の CertificateFile パラメーターが正確であることを確認してください。

ゲートウェイ・コンポーネントのアップグレード

ゲートウェイ・コンポーネントのアップグレードは、以下のいずれかの方法を使用して実行できます。

インストール・ファイルを使用する

コンポーネントのインストール・ファイルの入手について詳しくは、インストール・ファイルの入手を参照してください。Windows システムでのインストール・ファイルを使用したゲートウェイ・サポートのインストールについて詳しくは、Windows ゲートウェイ・サポートのインストールを参照してください。Linux でのインストール・ファイルを使用したゲートウェイ・サポートのインストールについて詳しくは、Linux ゲートウェイ・サポートのインストールを参照してください。

BigFix® コンソールを使用する

BigFix® コンソール・インフラストラクチャーがインストールされている場合は、更新 Fixlet を使用してゲートウェイ・サポートをアップグレードできます。アップグレード用 Fixlet について詳しくは、「*BigFix® Remote Control* コンソール・ユーザー・ガイド」を参照してください。

ブローカー・コンポーネントのアップグレード

ブローカー・サポートのアップグレードは、以下のいずれかの方法を使用して実行できます。

インストール・ファイルを使用する

コンポーネントのインストール・ファイルの入手について詳しくは、インストール・ファイルの入手を参照してください。Windows™ システムでのインストール・ファイルを使用したブローカー・サポートのインストールについて詳しくは、「Windows ブローカー・サポートのインストール」を参照してください。Linux™ でのインストール・ファイルを使用したブローカー・サポートのインストールについて詳しくは、「Linux ブローカー・サポートのインストール」を参照してください。

BigFix® コンソールを使用する

BigFix® コンソール・インフラストラクチャーがインストールされている場合は、更新 Fixlet を使用してブローカー・サポートをアップグレードできます。アップグレード用 Fixlet について詳しくは、「*BigFix® Remote Control* コンソール・ユーザー・ガイド」を参照してください。

サーバー・コンポーネントのアップグレード

BigFix® Remote Control サーバー ソフトウェアが既にインストールされている場合は、元のインストールと同様のタイプのインストールを実行することで、コンポーネントをアップグレードします。

アップグレードを開始する前に、プロパティー・ファイルおよび記録ファイル (該当する場合) をバックアップする必要があります。また、該当する場合は、すべての証明書をバックアップします。証明書のバックアップとリストアについて詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

プロパティー・ファイル

- `common.properties`
- `ldap.properties`
- `trc.properties`
- `log4j2.properties`
- `controller.properties`

これらのファイルは、以下のディレクトリーにあります。

Windows® システム

`[InstallDir]wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes\` ここで *InstallDir* は、Remote Control サーバーのインストール・ディレクトリーです。例えば、`C:\Program Files ( x86)\BigFix\TRC\server\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes\`

Linux® システム

`[InstallDir]wlp/usr/servers/trcserver/apps/TRCAPP.ear/trc.war/WEB-INF/classes/` ここで *InstallDir* は、Remote Control サーバーのインストール・ディレクトリーです。

記録ファイル

ビデオ記録フォルダーは、**trc.properties** ファイルの **rc.recording.directory** プロパティーで定義されています。

サーバー・コンポーネントのアップグレードは、以下のいずれかの方法を使用して実行できます。

インストール・ファイルを使用する

コンポーネントのインストール・ファイルの入手について詳しくは、インストール・ファイルの入手を参照してください。インストーラーを使用したサーバーのインストールについて詳しくは、サーバー・インストーラーを使用したインストールを参照してください。

注: インストール時に、既存のプロパティー・ファイルを保持するように選択してください。データベースのドロップは選択しないでください。

WebSphere 8.5 へのサーバーのインストールについて詳しくは、WebSphere Application Server バージョン 8.5.5 へのインストールWAR ファイルのデプロイを参照してください。

BigFix® コンソールを使用する

BigFix® コンソール・インフラストラクチャーがインストールされている場合は、サーバー・インストール・タスクを作成および実行することでサーバーをアップグレードします。ウィザードを使用したサーバー構成タスクの作成について詳しくは、「*BigFix® Remote Control* コンソール・ユーザー・ガイド」を参照してください。

注: サーバー・タスクの作成時に、既存のデータベースを保持する場合は、データベースをドロップするオプションを選択しないでください。

アップグレードが完了したら、新しいバージョンがインストールされたことを確認し、新しいプロパティー・ファイルを手動で編集します。バックアップしたプロパティー・ファイル内にある値を使用して、値を更新します。該当する場合は、記録ファイルと証明書をリストアします。

ターゲット・コンポーネントのアップグレード

ターゲット・コンポーネントのアップグレードは、以下のいずれかの方法を使用して実行できます。

インストール・ファイルを使用する

コンポーネントのインストール・ファイルの入手について詳しくは、インストール・ファイルの入手を参照してください。Windows™ システムでのインストール・ファイルを使用したターゲット・コンポーネントのインストールについて詳しくは、「Windows ターゲットのインストール」を参照してください。Linux™ システムでのインストール・ファイルを使用したターゲット・コンポーネントのインストールについて詳しくは、「Linux ターゲットのインストール」を参照してください。

BigFix® コンソールを使用する

BigFix® コンソール・インフラストラクチャーがインストールされている場合は、更新 Fixlet を使用してターゲット・コンポーネントをアップグレードできます。アップグレード用 Fixlet について詳しくは、「*BigFix® Remote Control* コンソール・ユーザー・ガイド」を参照してください。

コントローラー・コンポーネントのアップグレード

コントローラー・コンポーネントのアップグレードは大規模なアップグレードです。既存のプロパティーはすべてバックアップし、新規プロパティー・ファイルに追加します。

Linux™ オペレーティング・システムを使用しており、 IBM® Endpoint Manager for Remote Control バージョン 9.0.1 以前からアップグレードする場合、`trc_controller.cfg.rpmnew` ファイルを編集します。このファイルのプロパティー値を、`trc_controller.cfg` ファイルの値と比較します。差異を `trc_controller.cfg` ファイルに取り込んで、ファイルを保存します。

コントローラー・コンポーネントのアップグレードは、以下のいずれかの方法を使用して実行できます。

インストール・ファイルを使用する

コンポーネントのインストール・ファイルの入手について詳しくは、インストール・ファイルの入手を参照してください。Windows™ システムでのインストール・ファイルを使用したコントローラー・コンポーネントのインストールについて詳しくは、「Windows システムでのコントローラーのインストール」を参照してください。Linux™ システムでのインストール・ファイルを使用したコントローラー・コンポーネントのインストールについて詳しくは、「Linux コントローラーのインストール」を参照してください。

BigFix® コンソールを使用する

BigFix® コンソール・インフラストラクチャーがインストールされている場合は、更新 Fixlet を使用してコントローラー・コンポーネントをアップグレードできます。更新 Fixlet の使用について詳しくは、「*BigFix® Remote Control* コンソール・ユーザー・ガイド」を参照してください。

ターゲット・インストール済み環境の保守

保守プログラムを使用して、BigFix® Remote Control ターゲット インストール済み環境を変更できます。

Microsoft® Windows® がインストールされたシステムで、`trc_target_setup.exe` プログラムを実行することで、保守プログラムにアクセスできます。保守プログラムにアクセスするには、以下のステップを実行します。

1. ターゲット・インストール・ディレクトリーに移動します。例えば、以下のようにします。
   `\Program Files\BigFix\Remote Control\RCTarget`
2. `trc_target_setup.exe` をダブルクリックします
3. 「ようこそ」画面で **「次へ」** をクリックします。
4. オプションを選択して **「次へ」** をクリックします。

   変更

   ターゲット・インストール画面を通過して、以前にインストールした値を変更する場合は、このオプションを選択します。

   インストール・プロパティーを変更するには、ステップ 5 から実行します。

   修復

   欠落または破損しているファイル、ショートカット、およびレジストリー項目を修正する場合は、このオプションを選択します。

   a. **「修復」** をクリックします。
   b. 「**終了**」をクリックします。

   除去\n

   ターゲット・ソフトウェアおよびそのすべての機能を削除する場合は、このオプションを選択します。

a. 「**除去**」をクリックします。
b. **「完了」**をクリックします。

ターゲットの構成で設定可能なプロパティー

ターゲット・プロパティーはインストール中またはインストール後に構成できます。構成可能なプロパティーは、ターゲット・システムのオペレーティング・システムによって決まります。ターゲット・プロパティーは、P2P セッション中に実行できるアクションを決定します。サーバー URL を設定し、**Managed** プロパティーを Yes に設定した場合、アクションは Remote Control サーバーで設定されているポリシーによって決まります。

各オペレーティング・システムで構成可能なプロパティーについて詳しくは、表 18 : プロパティーを構成できるオペレーティング・システムを参照してください。

Windows™ システム

ターゲット・プロパティーはターゲット・レジストリーに保存されます。以下のようにターゲット・レジストリーを編集してプロパティーを変更します。

1. 64 ビット・システムでは、すべての 32 ビット・レジストリー・キーは **WOW6432Node** キーの下にあります。例: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BigFix\Remote Control\Target`

   注: 32 ビット・システムでは、次に移動します。 `HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\Remote Control\Target`

2. 必要なプロパティーを右クリックして**「修正」**を選択します。
3. 必要な値を設定し、**「OK」**をクリックします。
4. ターゲット・サービスを再起動します。

Linux™ システム

ターゲット・プロパティーは、`/etc/trc_target.properties` ファイルに保存されます。インストール後にこのファイルを編集してターゲットを構成します。

1. `trc_target.properties` ファイルを編集します。
2. 必要なプロパティーを変更します。
3. ファイルを保存します。
4. ターゲット・サービスを再起動します。

macOS デバイス

ターゲットのインストール時に、`trc_target.cfg` ファイル内のプロパティーを構成できます。詳しくは、『.pkg ファイルを使用した BigFix Remote Control Target for macOS のインストール』を参照してください。ターゲット・プロパティーは、 `/Library/Preferences/com.bigfix.remotecontrol.target.plist` に保存されます。ターゲット・プロパティーを変更するには、以下の手順を実行します。

1. `Terminal.app` を開きます。
2. プロパティーを変更するには、次のコマンドを入力します。

   sudo defaults write /Library/Preferences/com.bigfix.remotecontrol.target.plist **キーワード 値**

   ここで、**Keyword** はプロパティー名、**Value** はプロパティーの値です。

   例えば、以下のようにします。

   sudo defaults write /Library/Preferences/com.bigfix.remotecontrol.target.plist LogLevel 4

3. ターゲットを再始動します。
   a. **「Remote Control ターゲット」 > 「Remote Control ターゲットの終了」**をクリックします。
   b. `Remote Control Target.app` を開きます。

ターゲット・プロパティーの定義

表 14. インストール・オプションの説明

ターゲット・プロパティー	デフォルト値	説明\n
ServerURL	ブランク	ターゲットをサーバーに登録し、サーバーから開始されるリモート・コントロール・セッションに参加させるには、次の形式で Remote Control サーバーのURLを指定します。`http://servername/trc`、ここで *servername* は、Remote Control サーバーの完全修飾名です。 例えば、 `http://trcserver.example.com/trc` **注:** サーバー URL を指定し、ターゲットをサーバーから開始されたリモート・コントロール・セッションにのみ参加させる場合は、**AllowP2P** を No に設定します。
ProxyURL	ブランク	プロキシー・サーバーのホスト名または IP アドレス (使用している場合)。
BrokerList	ブランク	ターゲットの接続先とする、ブローカーおよびそのポートのホスト名または IP アドレスのリスト。形式は **hostname1:port,hostname2:port,hostname3:port.** です。
GroupLabel	ブランク	構成の適用時にターゲットがメンバーになるターゲット・グループ名。このターゲット・グループは、Remote Control データベースに存在していなければなりません。 **注: GroupLabel** プロパティーを使用できるのは、ターゲットがまだサーバーに登録されていない場合のみです。ターゲットが既に登録されている場合は、ターゲット・グループに割り当てられません。**GroupLabel** プロパティー値を適

表 14. インストール・オプションの説明 (続く)

ターゲット・プロパティー	デフォルト値	説明\n
		用するには、サーバー上の `trc.properties` ファイルの **allow.target.group.override** プロパティーを Yes に設定する必要があります。
PortToListen	888	ターゲットが listen する TCP ポートを指定します。BigFix® Remote Control Target for macOS のデフォルト値は 8787 です。
AllowP2P	はい	P2P モードを有効にするために使用されます。このパラメーターは、サーバーの状況に関係なく、P2P 接続を有効にするために使用します。デフォルト値は No です。 **いいえ** コントローラーとこのターゲットの間に P2P セッションを確立できません。**ServerURL** が指定されている場合、ターゲットは、サーバーから開始されたリモート・コントロール・セッションにのみ参加できます。 **はい** コントローラー・ユーザーとこのターゲットの間に P2P セッションを確立できます。 **注:** このオプションが「可 (Yes)」 であり、サーバー URL が指定された場合、ターゲットは P2P セッションおよびサーバーから開始されたセッションの両方に参加できます。
AllowP2PFailover	いいえ	このパラメーターは、サーバーがダウンしているか、サーバーに到達できない場合に、P2P モードへのフェイルオーバーを有効にするために使用します。**AllowP2P** も*Yes*に設定する必要があります。デフォルト値は *No* です。 **いいえ** サーバーがダウンしているか到達不能である場合、セッションは P2P モードにフェイルオーバーされません。 **はい** サーバーがダウンしているか、サーバーに到達できない場合に、セッションが P2P モードにフェイルオーバーします。
FIPSCompliance	いいえ	このプロパティーを使用すると、すべての暗号化機能について、FIPS 準拠の暗号化サービス・プロバイダーの使用が有効になります。FIPS

表 14. インストール・オプションの説明 (続く)

ターゲット・プロパティー	デフォルト値	説明\n

		準拠の有効化について詳しくは、Remote Control での連邦情報処理標準 (FIPS 140-2) 準拠を参照してください。
		
		注: ターゲットで FIPS 準拠を有効にする場合は、インストールしたコントローラー・コンポーネントでも FIPS 準拠を有効にする必要があります。FIPS 準拠モードでは、IBM® Java™ Runtime Environment (JRE) のみがサポートされます。JRE はコントローラー・ソフトウェアのインストール時にインストールされます。コントローラーで FIPS 準拠を有効にするには、以下のステップを実行します。
		
		1. コントローラーがインストールされているシステムで、`trc_controller.cfg` ファイルを編集します。
		Windows™ システム
		`[controller installation dir]\trc_controller.cfg`
		ここで、*[controller installation dir]* はコントローラーがインストールされているディレクトリーです。
		Linux™ システム
		`opt/BigFix/trc/controller/trc_controller.cfg`
		2. **fips.compliance** プロパティーを Yes に設定し、ファイルを保存します。

SP800131ACompliance	いいえ	すべての暗号機能について NIST SP800-131A 準拠のアルゴリズムと鍵強度を使用する場合は、このオプションを選択します。NIST SP800-131A 準拠の有効化について詳しくは、Remote Control における NIST SP800-131A 準拠を参照してください。 **注:** ターゲットで NIST SP800-131A 準拠を有効にする場合は、インストールされているコントローラー・コンポーネントでも NIST SP800-131A 準拠を有効にする必要があります。IBM®Java™ NIST SP800-131A 準拠モードでは、Java Runtime Environment (JRE) のみがサポートされます。JRE はコントローラー・ソフトウェアのインストール時にインストールさ

表 14. インストール・オプションの説明 (続く)

ターゲット・プロパティー	デフォルト値	説明\n

		れます。コントローラーで NIST SP800-131A 準拠を有効にするには、以下のステップを実行します。
		1. コントローラーがインストールされているシステムで、`trc_controller.cfg` ファイルを編集します。
		Windows™ システム
		`[controller installation dir]\trc_controller.cfg`
		ここで、*[controller installation dir]* はコントローラーがインストールされているディレクトリーです。
		Linux™ システム
		`opt/BigFix/trc/controller/trc_controller.cfg`
		2. **sp800131A.compliance** プロパティーを Yes に設定し、ファイルを保存します。

アクセシビリティー	いいえ	ユーザー補助 UI を有効にするには、このオプションを選択します。**Windows** オペレーティング・システムでのみ選択可能です。
LogLevel	2	ログ・レベルによって、エントリーのタイプと、ログ・ファイルに追加される情報量が決定されます。デフォルト値は 2 です。 0 - ロギングが最小レベルに設定されます。 1 - ロギングが **ERROR** レベルに設定されます。 2 - ロギングが **INFO** レベルに設定されます。 4 - ロギングが **DEBUG** レベルに設定されます。 **注:** ログ・レベル 4 は、HCL サポートからの要請があった場合にのみ使用してください。
LogRollover	毎日	新しいログ・ファイルが開始されるまでの期間を制御します。この期間は LogRotation 期間より短くなければならないため、すべての組み合わせが有効とは限りません。LogRollover を無効にすることはできません。デフォルト値は Daily です。

表 14. インストール・オプションの説明 (続く)

ターゲット・プロパティー	デフォルト値	説明\n
		毎時 毎正時に新しいログ・ファイルを開始します。ログが頻繁に書き込まれる場合、またはログ・レベル 2 より高いレベルを使用する場合にお勧めします。 **毎日** 新しいログ・ファイルを毎日開始します。
LogRotation	週次	古いログ・ファイルが上書きされるようになるまでの期間を制御します。ログ・ローテーションは無効にすることができます。デフォルト値は Weekly です。 **毎日** 1 日経過したログ・ファイルを上書きします。LogRollover を Hourly に設定した場合は、ログ・ファイル名に 00H から 23H までのサフィックスが追加されます。 **週次** 1 週間経過したログ・ファイルを上書きします。LogRollover を Hourly に設定した場合は、ログ・ファイル名に追加されるサフィックスは曜日と時間を示します。値は Mon-00H から Sun-23H になります。LogRollover を Daily に設定した場合は、ログ・ファイル名に追加されるサフィックスは曜日を示します。値は Mon から Sun になります。 **月次** 1 か月 (01-00H から 31-23H) 経過したログ・ファイルを上書きします。LogRollover を Hourly に設定した場合は、ログ・ファイル名に追加されるサフィックスは月の日付 (数値) と時間を示します。値は 01-00H から 31-23H になります。LogRollover を Daily に設定した場合は、ログ・ファイル名に追加されるサフィックスは月の日付 (数値) を示します。値は 01 から 31 になります。 **無効** LogRotation は無効です。LogRollover を Hourly に設定した場合は、ログ・ファイル名に追加されるサフィックスは現在の日時を示します。値は *YYYY-MM-DD-hh* にすることができます。LogRollover を Daily に設定した場合

表 14. インストール・オプションの説明 (続く)

ターゲット・プロパティー	デフォルト値	説明\n
		は、ログ・ファイル名に追加されるサフィックスは現在の日付を示します。値は *YYYY-MM-DD* にすることができます。

表 15. セッション・オプションのプロパティー

ターゲット・プロパティー	デフォルト値	説明\n
AllowMonitor	はい	ターゲットがモニター P2P セッションに参加できるかどうかを決定します。開始できる各種タイプのリモート・コントロール・セッションについて詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。 **はい** ターゲットはモニター P2P セッションに参加できます。コントローラー・ウィンドウのセッション・タイプ・リストで、**「モニター」**オプションを選択できます。**「接続のオープン」**ウィンドウにも**「モニター」**オプションがリストされます。 **いいえ** ターゲットはモニター P2P セッションに参加できません。コントローラー・ウィンドウのセッション・タイプ・リストで、**「モニター」**オプションは選択できません。
AllowGuidance	はい	ターゲットがガイダンス P2P セッションに参加できるかどうかを決定します。 **はい** ターゲットはガイダンス P2P セッションに参加できます。コントローラー・ウィンドウのセッション・タイプ・リストで、**「ガイダンス」**オプションを選択できます。**「接続のオープン」**ウィンドウにも**「ガイダンス」**オプションがリストされます。 **いいえ** ターゲットはガイダンス P2P セッションに参加できません。コントローラー・ウィンドウのセッション・タイプ・リストで、**「ガイダンス」**オプションは選択できません。
AllowActive	はい	ターゲットがアクティブ P2P セッションに参加できるかどうかを決定します。

表 15. セッション・オプションのプロパティー (続く)

ターゲット・プロパティー	デフォルト値	説明\n
		はい ターゲットはアクティブ P2P セッションに参加できます。コントローラー・ウィンドウのセッション・タイプ・リストで、**「アクティブ」**オプションを選択できます。**「アクティブ」**オプションは、**「接続のオープン」**ウィンドウにも含まれます。 **いいえ** ターゲットはアクティブ P2P セッションに参加できません。コントローラー・ウィンドウのセッション・タイプ・リストで、**「アクティブ」**オプションは選択できません。
DisableChat	いいえ	ターゲットでチャット・セッションを開始し、P2P セッション中にコントローラー・ユーザーとチャットすることができるかどうかを決定します。 **はい** **「チャットのみ」** が「接続のオープン」ウィンドウで接続タイプとして選択された場合、セッションは拒否されます。セッション中、コントローラー・ウィンドウでチャット・アイコンは使用できません。 **いいえ** 「接続のオープン」ウィンドウから **「チャットのみ (Chat Only)」** セッションを開始できます。セッション中、コントローラー・ウィンドウでチャット・アイコンが使用できます。
DisableFilePull	いいえ	セッション中にターゲットからコントローラーにファイルを転送できるかどうかを決定します。 **はい** ファイルをターゲットからコントローラーに転送することはできません。 **いいえ** ファイルをターゲットからコントローラーに転送できます。
DisableFilePush	いいえ	セッション中にコントローラーからターゲットにファイルを転送できるかどうかを決定します。 **はい**

表 15. セッション・オプションのプロパティー (続く)

ターゲット・プロパティー	デフォルト値	説明\n
		ファイルをコントローラーからターゲットに転送することはできません。 **いいえ** ファイルをコントローラーからターゲットに転送できます。
DisableClipboard	いいえ	P2P セッション中にコントローラー UI でクリップボード転送メニューを使用できるようにするかどうかを決定します。メニューは、リモート・コントロール・セッション中にコントローラーとターゲットとの間でクリップボードの内容を転送する場合に使用します。 **はい** クリップボード転送メニューはセッション中に使用できず、ターゲットとの間でクリップボードの内容を転送できません。 **いいえ** セッション中、クリップボード転送メニューは使用できます。
AllowRecording	はい	コントローラー・ユーザーは、セッションのローカル記録を作成し、それを制御側のシステムに保存することができます。 **はい** コントローラー・ウィンドウで、記録オプションが使用できます。 **いいえ** コントローラー・ウィンドウで、記録オプションは使用できません。
AllowCollaboration	はい	複数のコントローラーがセッションに参加できるようにするには、このプロパティーを使用します。コントローラー・ウィンドウでコラボレーション・アイコンを使用可能にするかどうかを決定します。 **はい** コントローラー・ウィンドウで、コラボレーション・アイコンが使用できます。 **いいえ** コントローラー・ウィンドウでコラボレーション・アイコンが使用可能になりません。

表 15. セッション・オプションのプロパティー (続く)

ターゲット・プロパティー	デフォルト値	説明\n
AllowHandover	はい	コラボレーション・セッションではマスター・コントローラーがそのセッションの制御を新規コントローラーに引き渡すことができます。コラボレーション・コントロール パネルで **「ハンドオーバー」** ボタンを使用可能にするかどうかを決定します。 **はい** コラボレーション制御パネルに **「ハンドオーバー」** ボタンが表示されます。 **いいえ** コラボレーション制御パネルに **「ハンドオーバー」** ボタンは表示されません。
AllowForceDisconnect	いいえ	ターゲットに接続しようとするときに表示されるメッセージ・ウィンドウで、 **「セッションの切断」** ボタンを使用できるかどうかを決定します。**「セッションの切断」** オプションを使用すると、現行セッションを切断することができます。 **はい** メッセージ・ウィンドウに切断ボタンが表示されます。 **いいえ** メッセージ・ウィンドウに切断ボタンが表示されません。
ForceDisconnectTimeout	45	現行セッションを切断するよう求めるプロンプトにコントローラー・ユーザーが応答するのを待つ時間 (秒数)。指定された時間内に応答しない場合は、セッションから自動的に切断されます。このタイマーは、**AllowForceDisconnect** と **CheckUserLogin** が「はい」に設定されている場合のみ有効になります。デフォルト値は45です。
AutoWinLogon	はい	ユーザーがターゲットにログオンしていない場合に、セッションを開始できるようにするかどうかを決定します。 **はい** ターゲットでセッションが開始されます。 **いいえ** セッションは開始されず、以下のメッセージが表示されます。セッションを確認するためにログインしているユーザーが存在しないため、セッションは拒否されました
RunPreScript	いいえ	リモート・コントロール・セッションの開始前にユーザー定義スクリプトを実行するかどうかを決定します。このスクリプトは、セッショ

表 15. セッション・オプションのプロパティー (続く)

ターゲット・プロパティー	デフォルト値	説明\n
		ンが許可された直後で、かつコントローラー・ユーザーがターゲットにアクセスできるようになる前に実行されます。スクリプト実行の結果およびセッションの続行は,**「開始前/終了後スクリプトの失敗時も続行」** で設定される値によって決まります。 **はい** リモート・コントロール・セッションが要求されると、定義済みスクリプトは、コントローラー・ユーザーがターゲットへのアクセス権限を持つ前に実行されます。 **いいえ** セッション前にスクリプトは実行されません。 セッション前スクリプトおよびセッション後スクリプトのセットアップについて詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。
RunPostScript	いいえ	リモート・コントロール・セッションの完了後にユーザー定義スクリプトを実行するかどうかを決定します。 **はい** リモート・コントロール・セッションが終了すると、ユーザー定義スクリプトが実行されます。 **いいえ** セッション後にスクリプトは実行されません。 セッション前スクリプトおよびセッション後スクリプトのセットアップについて詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。
ProceedOnScriptFail	いいえ	前スクリプトまたは後スクリプトの実行が失敗する場合に取るアクション。正の値または 0 の場合は、前スクリプトまたは後スクリプトの実行が成功したとみなされます。負の値の場合や、スクリプトが見つからない場合、あるいは実行が 3 分以内に完了しなかった場合は、失敗とみなされます。 **はい** 前スクリプトまたは後スクリプトの実行が失敗した場合でも、セッションは続行します。 **いいえ** 前スクリプトまたは後スクリプトの実行が失敗した場合、セッションは続行されずに終了します。

表 15. セッション・オプションのプロパティー (続く)

ターゲット・プロパティー	デフォルト値	説明\n
WorkaroundW2K3RDP	いいえ	リモート・デスクトップ・コンソール・セッションの後、コンソールを自動的にリセットします。リモート・デスクトップ・ユーザーが **/admin** または **/console** のオプションを使用して Windows™ Server 2003 システムでのリモート・デスクトップ・セッションを開始する場合、ユーザーがこのリモート・デスクトップ・セッションの前後または最中にこのターゲットとのリモート・コントロール・セッションを開始すると、リモート・コントロールは表示を取り込むことができません。その結果、コントローラーにはグレイ画面が表示されます。この問題は、 Windows™ Server 2003 オペレーティング・システムの制限です。そのため、このプロパティーには、値が Yes かどうかに応じて、各リモート・デスクトップ・セッションの終了後か、またはリモート・コントロール・セッションの開始前に Windows™ セッションをリセットするという回避策が導入されています。 **0** 回避策が使用不可になります。この値はデフォルト値です。 **1** リモート・コントロール・セッションが開始したときに、セッションを自動的にリセットします。 **注:** Windows™ セッションの初期化には数分かかるため、初期化が完了するまでコントローラーのデスクトップは空白になります。セッションはリセット中であり、数分かかる可能性があることをコントローラー・ユーザーに知らせるメッセージが表示されます。 **2** リモート・デスクトップ・ユーザーがログアウトしたときに、セッションを自動的にリセットします。
EnableTrueColor	いいえ	セッションの開始時に、コントローラー・ウィンドウでターゲット・デスクトップを高品質カラーで表示するかどうかを決定します。**「カラー品質のロック」**とともに使用します。 **はい。** セッション開始時にトゥルー・カラーの 24 ビット・モードでターゲット・デスクトップが表示されます。部分的な画面更新も有効になります。

表 15. セッション・オプションのプロパティー (続く)

ターゲット・プロパティー	デフォルト値	説明\n
		いいえ セッション開始時に 8 ビット・カラー・モードでターゲット・デスクトップが表示されます。部分的な画面更新も有効になります。この値はデフォルト値です。
LockColorDepth	いいえ	リモート・コントロール・セッション開始時のカラー品質を、セッション中に変更できるかどうかを判別します。**「高品質カラーを使用可能にする」**とともに使用します。 **はい。** リモート・コントロール・セッションに対して選択された初期カラー品質はロックされ、セッション中に変更することはできません。コントローラー・ウィンドウで、**「パフォーマンス設定」**アイコンが使用不可になります。コントローラー・ユーザーは、ネットワークが低速の場合にセッションのパフォーマンスを向上させるために設定を変更することができません。 **いいえ** セッション中にカラー品質を変更することができます。コントローラー・ウィンドウで、**「パフォーマンス設定」**アイコンが使用可能になります。
RemoveBackground	いいえ	ターゲットにデスクトップ背景画像が設定されている場合は、このプロパティーを使用して、リモート・コントロール・セッション中にビューから背景を削除できます。 **はい。** リモート・コントロール・セッション中に、ターゲットのデスクトップ・バックグラウンド・イメージは表示されません。 **いいえ** リモート・コントロール・セッション中、ターゲットのデスクトップ背景画像は表示されます。
NoScreenSaver	いいえ	スクリーン・セーバーがアクティブであることが検出されたときに、ターゲットによる画面更新の送信を停止します。 **はい。** ターゲット・システムでスクリーン・セーバーがアクティブであるときに、ターゲットによる画面更新の送信が停止されます。コントローラーには、シミュレートさ

表 15. セッション・オプションのプロパティー (続く)

ターゲット・プロパティー	デフォルト値	説明\n
		れたスクリーン・セーバーが表示されて、スクリーン・セーバーがリモート・ディスプレイでアクティブになっていることがコントローラー・ユーザーに示されます。コントローラー・ユーザーは、キーを押すかマウスを動かすことによりスクリーン・セーバーを解除することができます。 **いいえ** シミュレートされたスクリーン・セーバーはセッション・ウィンドウに表示されません。ターゲット画面が通常どおり表示され、ターゲットは引き続き画面更新を送信します。
管理対象	はい	ターゲットを Remote Control サーバーに登録するかどうかを決定します。 **はい。** ターゲットは Remote Control サーバーに登録され、定期的にサーバーに接続します。 **いいえ** ターゲットは Remote Control サーバーに登録されません。ターゲットは P2P セッションにのみ参加できます。

表 16. ユーザー確認プロパティーの説明

ターゲット・プロパティー	デフォルト値	説明\n
ConfirmTakeOver	はい	リモート・コントロール・セッションが要求されたときに、ターゲットに確認ウィンドウを表示するかどうかを決定します。 **はい** ユーザー確認ウィンドウが表示され、ターゲット・ユーザーはセッションを受け入れるか、拒否することができます。 **いいえ** ユーザー確認ウィンドウは表示されずに、セッションが確立されます。
ConfirmModeChange	はい	コントローラー・ユーザーがコントローラー・ウィンドウのセッション・モード・リストから別のセッション・モードを選択した場合に、ユーザー確認ウィンドウを表示するかどうかを決定します。 **はい**

表 16. ユーザー確認プロパティーの説明 (続く)

ターゲット・プロパティー	デフォルト値	説明\n
		セッション・モードの変更が要求されるたびにユーザー確認ウィンドウが表示され、ターゲット・ユーザーは要求を受け入れるか、拒否する必要があります。 **いいえ** ユーザー確認ウィンドウは表示されず、セッション・モードは自動的に変更されます。
ConfirmFileTransfer	はい	コントローラー・ユーザーがターゲットとコントローラーの間でファイルを転送することを選択した場合に、ユーザー確認ウィンドウを表示するかどうかを決定します。 **はい** 確認ウィンドウは以下の 2 とおりの場合に表示されます。ターゲット・ユーザーは、ファイル転送を受け入れるか、拒否する必要があります。 • コントローラー・ユーザーが、コントローラー・ウィンドウの「ファイルの転送」メニューから **「ファイルをプル」** を選択した場合。ターゲット・ユーザーは、要求を受け入れた後、転送するファイルを選択する必要があります。 • コントローラー・ユーザーが、ターゲット・ウィンドウの **「アクション」** メニューから **「コントローラーへファイルを送信」** を選択した場合。 **いいえ** 要求された場合、確認ウィンドウは表示されず、ファイルは自動的にターゲットからコントローラー・システムに転送されます。
ConfirmSysInfo	はい	コントローラー・ユーザーがターゲット・システム情報の表示を要求した場合にユーザー確認ウィンドウを表示するかどうかを決定します。 **はい** コントローラー・ユーザーがコントローラー・ウィンドウの **「システム情報」** をクリックすると、ユーザー確認ウィンドウが表示されます。ターゲット・ユーザーは、要求を受け入れるか、拒否する必要があります。ターゲット・ユーザーが「受け入れ」をクリックすると、コントローラー・システムでターゲット・システム情報が別のウィンドウに表示されます。「拒否」をクリックすると、コントローラーにメッセージが表示され、システム情報は表示されません。

表 16. ユーザー確認プロパティーの説明 (続く)

ターゲット・プロパティー	デフォルト値	説明\n
		いいえ コントローラー・ユーザーがシステム情報アイコンをクリックすると、ターゲット・システム情報が自動的に表示されます。
ConfirmRecording	はい	コントローラー・ユーザーがコントローラー・ウィンドウで記録アイコンをクリックした場合に、ユーザー確認ウィンドウを表示するかどうかを決定します。 **はい** コントローラー・ユーザーがコントローラー・ウィンドウの記録アイコンをクリックすると、メッセージ・ウィンドウが表示されます。ターゲット・ユーザーが**「受け入れ」**をクリックした場合は、コントローラー・ユーザーが記録の保存ディレクトリーを選択できます。ターゲット・ユーザーが**「拒否」**をクリックした場合は、記録が拒否されたことを示すメッセージがコントローラーに表示されます。 **注:** ターゲット・ユーザーが記録要求を受け入れた後に、コントローラー・ユーザーがローカル記録を停止して再開した場合、確認ウィンドウは表示されません。 **いいえ** コントローラー・ユーザーがコントローラー・ウィンドウの記録アイコンをクリックすると、メッセージ・ウィンドウは表示されません。コントローラー・ユーザーは、記録の保存先ディレクトリーを選択できます。
ConfirmCollaboration	はい	別のコントローラー・ユーザーがターゲットとのコラボレーション・セッションへの参加を要求した場合に、ユーザー確認ウィンドウを表示するかどうかを決定します。 **はい** コラボレーション・セッションにコントローラー・ユーザーが参加しようとすると、ユーザー確認ウィンドウが表示されます。ターゲット・ユーザーは、この追加コントローラーのセッション参加許可の要求を受け入れるか、拒否する必要があります。ターゲット・ユーザーが「同意する」をクリックした場合、追加コントローラーはコラボレーション・セッションに参加します。「拒否する (refuse)」をクリックした場合は、コントローラー・システムにメッセージが表示され、追加コントローラーはコラボレーション・セッションに参加できません。 **いいえ**

表 16. ユーザー確認プロパティーの説明 (続く)

ターゲット・プロパティー	デフォルト値	説明\n
		追加コントローラーは、セッションのマスター・コントローラーに接続しようとしたときに、自動的にコラボレーション・セッションに参加します。
AcceptanceGraceTime	45	セッションの開始またはタイムアウトまでのターゲット・ユーザー応答の待ち時間 (秒数) を設定します。これは、**「着信接続の確認」**と使用します。 • 許容値は 0 から 60 です。0 に設定した場合、ターゲット・ユーザーはセッション要求への応答を求められません。 **注:** **「着信接続の確認」**が「はい」の場合、**「確認待ち時間」**には必ず 0 より大きい値を設定して、ターゲット・ユーザーが応答するのに十分な時間を設けてください。
AcceptanceProceed	いいえ	ユーザー確認ウィンドウがタイムアウトになる場合に実行されるアクションです。ターゲット・ユーザーは、**「受け入れ猶予時間」**に定義された秒数内に「受け入れ」または「拒否」をクリックしませんでした。 **はい** セッションが確立されます。 **いいえ** セッションは確立されません。
HideWindows	いいえ	**「着信接続の確認」**も「はい」に設定されているときに、ユーザー確認ウィンドウに**「ウィンドウの非表示」**チェック・ボックスを表示するかどうかを決定します。 **はい** ユーザー確認ウィンドウに**「ウィンドウの非表示」**チェック・ボックスが表示されます。 **いいえ** ユーザー確認ウィンドウに**「ウィンドウの非表示」**チェック・ボックスは表示されません。
DisableGUI_CLI	いいえ	ユーザーがコマンド・ラインを介してターゲットにアクションを送信できるようにします。 **はい** GUI コマンド・ライン・インターフェースが無効になっています。 **いいえ** GUI コマンド・ライン・インターフェースが有効になっています。

表 16. ユーザー確認プロパティーの説明 (続く)

ターゲット・プロパティー	デフォルト値	説明\n
		注: コマンド・ライン・インターフェースは、管理対象モードでのみ使用可能であり、BrokerList プロパティーが空でない場合にのみ使用できます。

表 17. セキュリティー・プロパティーの説明

ターゲット・プロパティー	デフォルト値	説明\n
CheckUserLogin	はい	**「接続のオープン」**ウィンドウでコントローラー・ユーザーがセッション・タイプ・ボタンをクリックしたときに、ログオン・ウィンドウを表示するかどうかを決定します。 **はい** ログオン・ウィンドウが表示され、コントローラー・ユーザーは有効な Windows™ オペレーティング・システム ID およびパスワードを使用してログオンする必要があります。ログオン資格情報が無効な場合、ターゲットはセッションを拒否します。 **いいえ** ログオン・ウィンドウは表示されずに、セッションが確立されます。

CheckUserGroup	説明を参照	これがデフォルト値です。
		Windows™ システム
		`BUILTIN\Administrators`
		Linux™ システム
		`wheel`
		CheckUserGroup に値が設定されている場合、認証に使用するユーザー名は、リストされているグループのうちのいずれかのグループのメンバーでなければなりません。ユーザーがメンバーではない場合、セッションは拒否されます。複数のグループを指定する場合は、セミコロンで区切る必要があります。例えば、 `wheel;trcusers`
		注: デフォルトでは、Windows™ システムの場合、管理者ユーザーのみにアクセス権限が付与されます。Linux™ システムの場合、デフォルトではどのユーザーにもアクセス権限は付与されません。この問題を解決するには、以下のいずれかのステップを実行します。

表 17. セキュリティー・プロパティーの説明 (続く)

ターゲット・プロパティー	デフォルト値	説明\n

		1. ユーザーに管理者権限も付与する場合は、それらのユーザーを Administrators グループ (Windows™ システムの場合) または wheel グループ (Linux™ システムの場合) のメンバーにします。
		2. 管理者権限を持たないユーザーについて、以下のステップを実行します。
		a. グループを作成するか、既存のグループを使用します。例えば、root として次のコマンドを実行できます。
		`groupadd trcusers`
		.
		b. ユーザーをこのグループに追加します。例えば、root として次のコマンドを実行して、**bsmith** を **trcusers** に追加します。
		`usermod -a -G trcusers <bsmith>`
		c. このグループを**「指定ユーザー・グループ」**フィールドのリストに追加します。

AuditToSystem	はい	リモート・コントロール・セッション中に実行されるアクションが、ターゲット上のアプリケーション・イベント・ログに記録されるかどうかを決定します。このファイルは、監査の目的で使用できます。 **はい** セッション中に実行された各アクションに対応するエントリーが、ターゲットのアプリケーション・イベント・ログに記録されます。 **いいえ** アプリケーション・イベント・ログにエントリーは記録されません。
AutoSaveChat	いいえ	チャット・セッション中に入力されたチャット・テキストを保存できるかどうかを決定します。 **はい** チャット・テキストは html ファイルとして保存されます。このファイルは `chat-`*`username-date`*`.html` です。*username* は、P2P セッション中にコントローラー・マシンにログオンしたユーザーの表示名です。管理対

表 17. セキュリティー・プロパティーの説明 (続く)

ターゲット・プロパティー	デフォルト値	説明\n
		象モードの場合、*username* はサーバー上のコントローラー・ユーザーの表示名です。日付は *YYYYMMDD* 形式で示します。このファイルは、ターゲットの作業ディレクトリーに保存されます。作業ディレクトリーの場所は、ターゲット・プロパティー **WorkingDir** で定義されます。例えば、Windows™ システムではこのファイルは次の場所に保存されます。 `c:\ProgramData\BigFix\Remote Control`. Linux システムではこのファイルは `/var/opt/bigfix/trc/target/` に保存されます。 Mac システムではこのファイルは `/Users/<user>/Library/Application Support/com.bigfix.remotecontrol.target` に保存されます。 **いいえ** チャット・テキストはファイルに保存されません。
EnableFileTransferSystemAccess	いいえ	ファイル転送セッションが、システム特権 (Windows) または root 特権 (Linux) を使用して、ターゲット・ファイル・システムのアクセスを許可するかどうかを決定します。このオプションは、ピアツーピア・セッションでのみ有効です。 **はい** ファイル転送セッションは、ターゲット・ファイル・システムでシステム特権 (Windows) または root 特権 (Linux) を使用します。 **いいえ** ファイル転送セッションでは、ターゲット・ファイル・システム上のログオン・ユーザーの権限が使用されます。 **注:** このオプションが No に設定されていて、ファイル転送セッション中にターゲットにログオンしたユーザーがいない場合は、エラー・メッセージが表示されます。
SessionDisconnect	いいえ	リモート・コントロール・セッションが終了したときに、ターゲット・コンピューターを自動的にロックするかどうかを決定します。指定できる値:*lock*。

表 17. セキュリティー・プロパティーの説明 (続く)

ターゲット・プロパティー	デフォルト値	説明\n
		値を *lock* に設定すると、セッションの終了時に、ターゲット・コンピューターは自動的にロックされます。このプロパティーを空白にするか、別の値に設定すると、セッションの終了時に、ターゲット・コンピューターは自動的にロックされません。
AllowPrivacy	はい	リモート・コントロール・セッション中に、コントローラー・ユーザーがターゲットのローカル入力および画面をロックできるかどうかを決定します。コントローラー・ウィンドウに**「プライバシーの有効化」**オプションを表示できるかどうかを決定します。 **はい** **「プライバシーの有効化」**オプションは、コントローラー・ウィンドウの**「ターゲット内のアクションを実行」**メニューで選択できます。 **いいえ** **「プライバシーの有効化」**オプションは、コントローラー・ウィンドウの**「ターゲット内のアクションを実行」**メニューで選択できません。
AllowInputLock	はい	このプロパティーは、**「プライバシーの保護」**と組み合わせても、単独で使用しても機能します。**「入力ロックの許可」**を使用すると、リモート・コントロール・セッション中にターゲット・ユーザーのマウスとキーボードをロックできます。 **はい** コントローラー・ウィンドウで**「ターゲット内のアクションを実行」**メニューの**「ターゲットの入力をロック」**メニュー項目が有効になります。**「ターゲットの入力をロック」**を選択すると、リモート・コントロール・セッション中、ターゲット・ユーザーのマウスとキーボードをロックします。ターゲット・ユーザーに対してはターゲット画面が引き続き表示されます。 **いいえ** コントローラー・ウィンドウで**「ターゲット内のアクションを実行」**メニューの「ターゲットの入力をロック」メニュー項目が有効になります。 **注:** セッション中に**「プライバシーの有効化」**オプションが「はい」になっていると、リモート・ユーザー入力が自動的に

表 17. セキュリティー・プロパティーの説明 (続く)

ターゲット・プロパティー	デフォルト値	説明\n
		ロックされます。入力をロックせずにプライバシーを使用可能にすることはできません。
EnablePrivacy	いいえ	すべてのセッションでローカル入力および画面をロックするかどうかを決定します。これにより、ターゲット・ユーザーは、リモート・コントロール・セッション中にターゲットで入力を含むあらゆる操作ができなくなります。 **はい** セッションが開始されると、プライバシー・ビットマップによってターゲット画面がブランクになるので、ターゲット・ユーザーはセッション中は画面を操作できなくなります。その場合でも、コントローラー・ウィンドウでは、ターゲット・デスクトップがコントローラー・ユーザーに表示されます。 **いいえ** セッションが開始されたときにターゲット画面はブランクにならず、ターゲット・ユーザーは画面を操作することができます。
EnableInputLock	いいえ	このプロパティーは、**「プライバシーの有効化」**との組み合わせで機能します。プライバシー・モードが有効な場合は、**「入力ロックの有効化」**を使用して、リモート・コントロール・セッション中、ターゲット・ユーザーがターゲット画面を表示できるようにするかどうかを決定します。 **はい** プライバシー・モードの場合、セッション中、ターゲット画面はターゲット・ユーザーに表示されますが、マウスおよびキーボードの制御はロックされます。 **いいえ** ターゲット画面はターゲット・ユーザーに表示されません。セッション中、プライバシー・ビットマップがターゲットに表示されます。また、ターゲット・ユーザーのマウスおよびキーボード入力も無効になります。 **注:「入力ロックの有効化」**を有効にするには、**「プライバシーの有効化」**に Yes を選択する必要があります。

表 17. セキュリティー・プロパティーの説明 (続く)

ターゲット・プロパティー	デフォルト値	説明\n
DisablePanicKey	いいえ	ターゲット・ユーザーが PAUSE/BREAK キーを使用してリモート・コントロール・セッションを自動的に終了できるようにするかどうかを決定します。 **はい** ターゲット・ユーザーは Pause Break キーを使用してリモート・コントロール・セッションを自動終了できません。 **いいえ** ターゲット・ユーザーは、PAUSE/BREAK キーを使用してリモート・コントロール・セッションを自動的に終了できます。
EnableOSSN	いいえ	リモート・コントロール・セッションが進行中であることを示す半透明のオーバーレイをターゲット・コンピューターに表示するかどうかを決定します。このプロパティーは、プライバシーが懸念される場合に使用します。これによりユーザーは、自分のコンピューターを誰かがリモートで表示または制御できる場合には、そのことがはっきりと通知されます。 **はい** ターゲット画面に、**Remote Control** というテキストと、進行中のリモート・コントロール・セッションのタイプを示す、半透明のオーバーレイが表示されます。`For example, Remote Control - Active Mode.` このオーバーレイはキーボードまたはマウスのアクションを妨害するものではありません。ユーザーは引き続き自分の画面を操作できます。 **いいえ** ターゲット・コンピューターにオーバーレイは表示されません。 **注:** このポリシーは、Windows™ オペレーティング・システムがインストールされているターゲットでのみサポートされます。
DisableGUI	いいえ	リモート・コントロール・セッションの開始時およびセッション中にターゲット UI を表示するかどうかを決定します。

表 17. セキュリティー・プロパティーの説明 (続く)

ターゲット・プロパティー	デフォルト値	説明\n
		注: このオプションは、ターゲットが P2P モードでインストールされ、**管理**ターゲット・プロパティが「いいえ」に設定されている場合にのみ機能します。このオプションは、サーバー URL が指定された時に、Remote Control サーバー・モードを使用してインストールされたターゲットに適用された場合は無視されます。 **はい** ターゲットにターゲット UI は表示されず、セッションが開始したことはターゲット・ユーザーには分かりません。Remote Control ターゲット・アイコンは、Windows™ システム・トレイに表示されません。 **いいえ** ターゲット UI は、セッションが開始するときにターゲットに表示され、リモート・コントロール・セッション中もターゲット・ユーザーに対して使用可能です。

プロパティーを構成できるオペレーティング・システム

表 18. プロパティーを構成できるオペレーティング・システム

プロパティー名	Windows™	Linux™	macOS
ServerURL	*	*	
ProxyURL	*	*	
BrokerList	*	*	*
GroupLabel	*	*	
PortToListen	*	*	*
AllowP2P	*	*	*
AllowP2PFailover	*	*	
FIPSCompliance	*	*	
SP800131ACompliance	*	*	
アクセシビリティー	*		
LogLevel	*	*	*
LogRollover	*	*	*

表 18. プロパティーを構成できるオペレーティング・システム (続く)

プロパティー名	Windows™	Linux™	macOS
LogRotation	*	*	*
AllowMonitor	*	*	*
AllowGuidance	*	*	*
AllowActive	*	*	*
DisableChat	*	*	*
DisableFilePull	*	*	*
DisableFilePush	*	*	*
DisableClipboard	*	*	
AllowRecording	*	*	*
AllowCollaboration	*	*	*
AllowHandover	*	*	*
AllowForceDisconnect	*	*	
ForceDisconnectTimeout	*	*	
AutoWinLogon	*	*	
RunPreScript	*	*	
RunPostScript	*	*	
ProceedOnScriptFail	*	*	
WorkaroundW2K3RDP	*		
EnableTrueColor	*	*	*
LockColorDepth	*	*	*
RemoveBackground	*		
NoScreenSaver	*		
管理対象	*	*	
ConfirmTakeOver	*	*	*
ConfirmModeChange	*	*	*
ConfirmFileTransfer	*	*	*
ConfirmSysInfo	*	*	*
ConfirmRecording	*	*	*

表 18. プロパティーを構成できるオペレーティング・システム (続く)

プロパティー名	Windows™	Linux™	macOS
ConfirmCollaboration	*	*	*
AcceptanceGraceTime	*	*	*
AcceptanceProceed	*	*	*
HideWindows	*	*	
CheckUserLogin	*	*	
CheckUserGroup	*	*	
AuditToSystem	*	*	*
AutoSaveChat	*	*	*
EnableFileTransferSystemAccess	*	*	
SessionDisconnect	*	*	
AllowPrivacy	*		
AllowInputLock	*		
EnablePrivacy	*		
EnableInputLock	*		
DisablePanicKey	*		
EnableOSSN	*		
DisableGUI	*		
DisableGUI_CLI	*	*	

Notices

This information was developed for products and services offered in the US.

HCL may not offer the products, services, or features discussed in this document in other countries. Consult your local HCL representative for information on the products and services currently available in your area. Any reference to an HCL product, program, or service is not intended to state or imply that only that HCL product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any HCL intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-HCL product, program, or service.

HCL may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

For license inquiries regarding double-byte character set (DBCS) information, contact the HCL Intellectual Property Department in your country or send inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HCL may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to HCL, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

HCL MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

索引

O

S

W

あ

い

ろ