BigFix プラットフォーム
始めに

第 章1. 概要

BigFix は、コンプライアンス、エンドポイント、およびセキュリティーの管理について、迅速かつ直感的なソリューションを提供する製品スイートです。この製品により、組織は単一のインフラストラクチャー、単一のコンソール、および単一の種類のエージェントを使用して、物理エンドポイントと仮想エンドポイントの表示および管理を行うことができます。

BigFix は、以下の機能を提供します。

- 連続的なエンドポイント自己アセスメントおよびポリシー実施のための単一のインテリジェント・エージェント。
- 単一の管理コンソールからの、リアルタイムの可視性と制御。
- 位置、接続タイプ、または状況と関係なしに、何十万ものエンドポイントを管理。
- 正確なタイプのエンドポイント構成またはユーザーの種類を、特定アクションの目標として設定。
- 複雑性とコストの削減、正確性の改善、および生産性の向上の管理。
- パッチ管理、ソフトウェア配布、および OS デプロイメント。
- 異機種混合のプラットフォームのサポート。
- モバイル・デバイスの管理。
- 米国連邦情報・技術局 (NIST) の標準に基づく自動エンドポイント・アセスメントおよび脆弱性修復。
- マルウェアその他の脆弱性からのリアルタイム保護。
- サーバー自動化。

ビジネスと環境のニーズに応じて、このスイートに属する特定の製品のライセンスを購入し、これらの機能の一部またはすべてを選択し実装することができます。

ライセンス交付は、管理対象のエンドポイントの数およびスイートから選択された製品に応じて、1 年ごとのサブスクリプションによって行われます。

すべての製品は相互に互換性があり、BigFix コンソールを使用して、ご使用のネットワーク内のどこからでもアクセス可能です。

通常、 BigFixのインストールは次のパートから構成されています。

- BigFix プラットフォーム *(##### 4)*
- 1 つ以上のBigFix アプリケーション *(##### 8)*

製品の詳細は、以下を参照してください。

- サンプル・アーキテクチャー *(##### 12)*
- コンテンツのタイプ *(##### 13)*
- コンテンツを適用するターゲットの識別方法 *(##### 15)*

第 章2. BigFix プラットフォーム

すべての BigFix アプリケーションは、BigFix プラットフォーム上で実行されます。

BigFix のプラットフォームは、全体的な IT インフラストラクチャーの中核部分として機能する、多層構造のテクノロジー・プラットフォームです。このプラットフォームは、IT インフラストラクチャーの管理作業を管理対象デバイスそのものであるエージェントに配布する、コンテンツ駆動型の動的なメッセージングおよび管理システムです。

このプラットフォームでは、専用ネットワークまたはパブリック・ネットワークを介して、最大で 250,000 までの物理コンピューターと仮想コンピューター (サーバー・デスクトップ、ローミング・ラップトップ、携帯電話、POS 装置、現金自動預け払い機、セルフサービス・キオスクなど) を管理することができます。

このプラットフォームでサポートされるのは、Microsoft Windows、UNIX、Linux、および Mac OS です。サポートされるバージョンについては、「サーバーの要件 (（ページ）
)」を参照してください。

BigFix プラットフォームは、以下の機能および利点を備えています。

単一のインテリジェント・エージェント

10 M バイト未満の RAM で作動し、管理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する必要があります。このエージェントは、ネットワークに接続されているかどうかにかかわらず、規定されたポリシーと対比して、エンドポイントの状態を絶えず査定します。ターゲットがポリシーまたはチェックリストに準拠していないことをエージェントが検出すると、すぐにサーバーに通知し、構成済みの修復タスクを実行した後、ただちにタスクの状況および結果をサーバーに通知します。ほとんどの場合、エージェントは、ユーザーからの直接介入を一切必要としないサイレント・モードで動作します。ただし、ユーザー応答を要求する必要がある場合、このプログラムでは画面にプロンプトを表示することもできます。BigFix エージェントがインストールされたコンピューターも、######と呼ばれます。

単一のコンソール

エンドポイント保護、システム・ライフサイクル管理、セキュリティー構成および脆弱性の管理など、どのような特定のソリューションを使用する場合

でも、そのソリューションは単一のコンソールから管理されます。必要な権限を持つオペレーターであれば、コンソールを使用して、ネットワークのその他の部分に影響を与えることなく、フィックスを必要とするコンピューターのみにそれを迅速かつ容易に配布することができます。コンソール要件について詳しくは、「コンソールの要件 (#####)」を参照してください。

単一のサーバー

個々のクライアントとの間の情報の流れを調整し、その結果をデータベースに保存します。ポリシー・ベースのコンテンツを管理し、環境内のすべての装置に対してオペレーターがリアルタイム可視性を維持し、制御できるようにします。このコンテンツは *Fixlet* というメッセージで配信され、クラウド・ベースの「コンテンツ・デリバリー」サービスを使用して継続的に更新されます。ほとんどの分析、処理、および実施作業はサーバーでなくエージェントによって行われるため、単一のサーバーで最大 250.000 までのエンドポイントをサポートできます。複数のサーバーを採用すれば、高可用性を実現できます。

1 つ以上のリレー (オプション)

分散デバイスおよびポリシー・コンテンツの管理を容易にします。リレーとは、リレー・サービスを使用して拡張されたクライアントのことです。ホスト・コンピューターを保護するためのすべてのクライアント・アクションを実行し、さらに子クライアントおよび子リレー対して、コンテンツおよびソフトウェアのダウンロードを配信します。リレーを使用すると、各ネットワーク・コンピューターがサーバーに直接接続する必要がなくなるので、負荷を大幅に軽減することができます。数百のクライアントがダウンロードのために 1 台のリレーを指定することができるので、同様にサーバーに対する要求は 1 つのみになります。リレーは他のリレーにも同様に接続できるため、効率はさらに高まります。エージェントをリレーにプロモートするために要する時間は数分であり、専用のハードウェアやネットワーク構成を変更する必要はありません。

2 次サーバー (オプション)

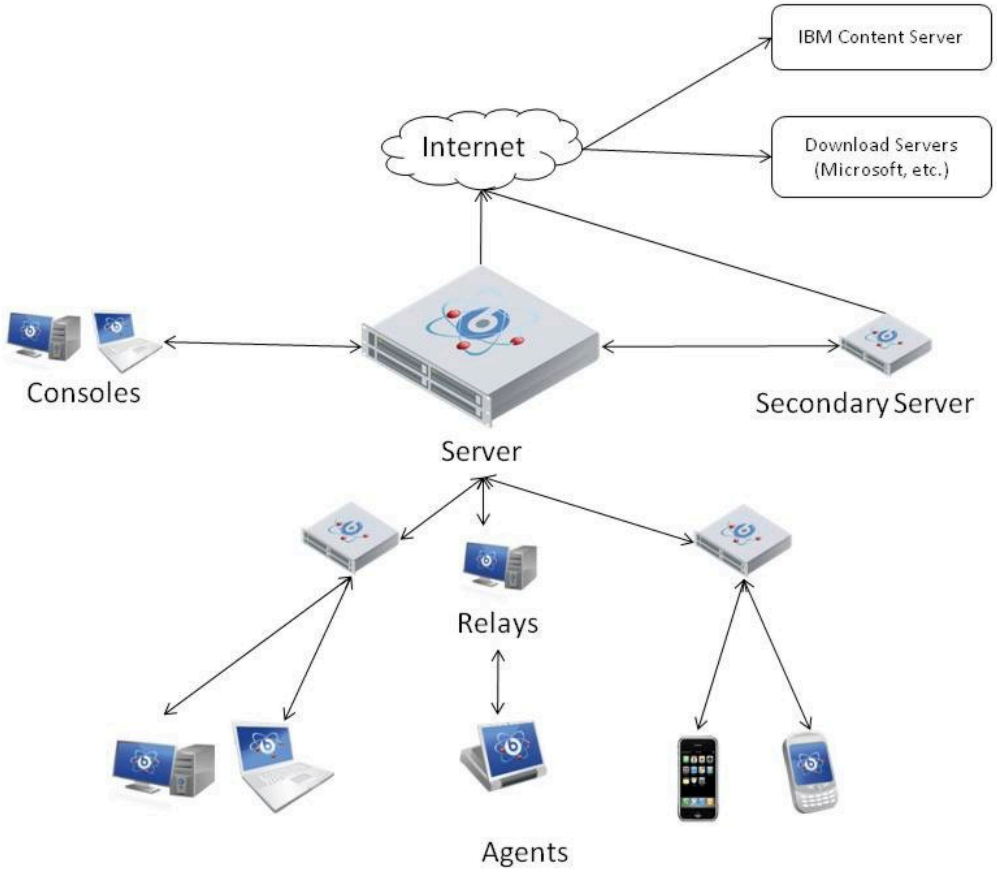
災害復旧用にサーバー情報を複製する、災害用サーバー・アーキテクチャー (DSA) サーバー。ある BigFix サーバーで障害が発生しても、他の BigFix サーバーが、元のサーバーの全機能を備えた BigFix サーバーとして自動的に引き継ぎます。

Web レポート

Web レポート・プログラムを使用すると、以下のことが可能になります。

- データのチャートやグラフを生成し、ハードコピーが得られます。
- ネットワーク内のすべての Fixlet アクティビティーの監査証跡の維持が容易になります。
- データをエクスポートして、スプレッドシートまたはデータベースでさらに操作することができます。
- 組織にインストールされている予備の BigFix サーバーからの情報を集約します。

このインターフェースは Web ブラウザーで実行され、一連のユーザーはこれを使用してコンピューターの状態を表示することができますが、これらのユーザーにこれらのコンピューターを変更する権限が付与されることはありません。


IBM Content Server
Internet
Download Servers
(Microsoft, etc.)
Consoles
Server
Secondary Server
Relays
Agents

第 章3. BigFix アプリケーション

BigFix ソリューションは、精度と生産性を高めながら、統合されたセキュリティーと運用管理、効率化および簡素化されたエンドポイント管理を提供する複数のアプリケーション製品で構成されています。

BigFix Lifecycle

このアプリケーションを使用すると、管理者は、エンドポイントの状態を正確に表示して問題を自動的に修復する、エージェント・ベースのツールを使用できるようになります。

BigFix Lifecycle には、以下のアプリケーションが含まれます。

OS Deployment

単一の一元化された場所からネットワーク全体に新規ワークステーションやサーバーを迅速にデプロイするための、統合された包括的なソリューションを提供します。

電源管理

ネットワーク内のコンピューターの消費電力設定を管理およびモニターします。また、この製品は、ダッシュボード、ウィザード、および Web レポートを使用して設定した社内の省電力ポリシーを管理および適用します。

Remote Control

適用環境内のワークステーションおよびサーバーの引き継ぎとモニターをリモートで実行します。

Server Automation

プロビジョニング・ワークフローを自動化します。サーバーやコンピューターなどのさまざまなエンドポイントにわたって、Fixlet、タスク、およびベースラインのシーケンスを自動化できます。

ソフトウェア配布

単一の一元化された場所からネットワーク全体にソフトウェアを迅速にデプロイするための、統合された包括的なソリューションを提供します。これは、コスト効率の高い運用管理機能、およびソフトウェアの配信とインストールのプロセスの可視性を提供します。

BigFix Lifecycleについて詳しくは、「ライフ・サイクルの資料」を参照してください。

BigFix Patch

このアプリケーションを使用すると、すべての分散エンドポイントに対し、自動化された単純なパッチ・プロセスを使用できるようになります。この製品は、オペレーティング・システム・パッチとソフトウェア・アプリケーション・パッチの両方を管理します。

BigFix Patchについての詳細は、「パッチ文書」を参照してください。

BigFix Compliance

このアプリケーションを使用すると、エンドポイントが保護され、修復が自動化されます。また、セキュリティー・コンプライアンス標準を満たしていることが規制機関に対して保証されます。

BigFix Complianceについての詳細は、「コンプライアンス・ドキュメント」を参照してください。

BigFix WebUI

このアプリケーションは、Web ベースのインターフェースを通じて BigFix の柔軟性と能力にアクセスすることができます。

BigFix WebUIについての詳細は、「Web UI・ドキュメント」を参照してください。

BigFix Inventory

このアプリケーションを使用すると、モニター対象のコンピューターをスキャンして、以下のことが行えます。

- インストール済みのソフトウェアを識別する。

- スキャンでディスカバーされた署名をソフトウェア・カタログと突き合わせる。
- レポートを作成する。
- その結果を、契約に定められたコストおよび資格に関する情報と比較する。

BigFix Inventoryについての詳細は、「Inventory documentation」を参照してください。

追加ライセンスを購入することにより、BigFix ソリューションに属するアプリケーションを後で必要になった際に追加することができます。購入した製品は、自動的に BigFix コンソールで使用できるようになります。ソリューションに属するアプリケーションを追加するにあたり、追加のソフトウェアをインストールしたり、新たなハードウェアを購入したりする必要はありません。Asset Discovery と Inventory のみ、新規コンポーネントのインストールを必要としますが、このインストールは BigFix 自身により行われます。

注: Asset Discovery はBigFixプラットフォームのコンポーネントの 1 つで、ご使用のネットワーク内にある管理されていない資産を識別できるようにします。

多くのお客様は、Patch などの単一のアプリケーションから使用を開始し、その後、製品ソリューションの機能全体の価値が分かり始めたら、新規ライセンスを購入して、製品を適用する範囲を拡大します。

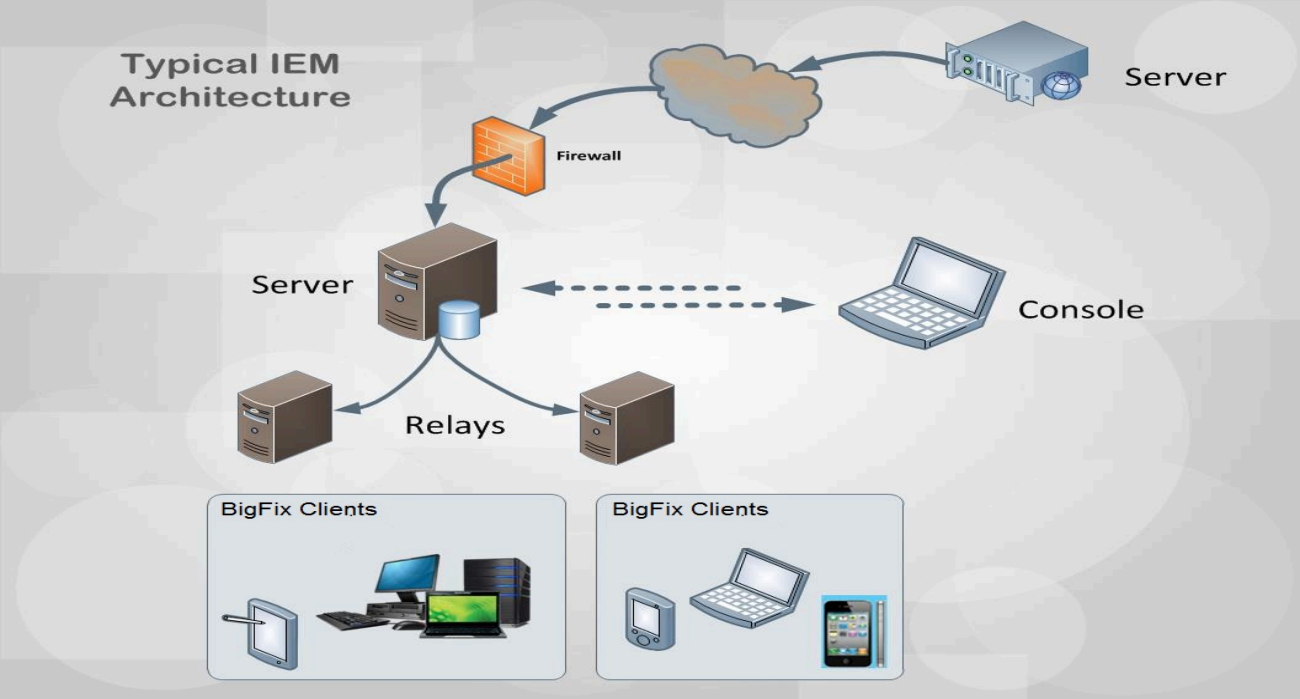
いくつかの機能は、BigFix 製品ソリューション内の複数のアプリケーションに共通しています。例えば、下の図に示すように、OS およびソフトウェア・アプリケーションのパッチを適用する機能は、Patch アプリケーションのみならず、Compliance アプリケーションおよび Lifecycle アプリケーションでも使用することができます。パッチを管理するためのこうしたライセンスは、いずれも購入が可能です。

これらのアプリケーションはすべて、エージェントでの連続的な評価と、リポジトリーからデータを取得してターゲットに送る収集プロセスを利用しています。

第 章4. サンプル・アーキテクチャー

サンプル・アーキテクチャーは、ご使用の環境の計画を立てるのに役立ちます。

標準的なインストール済み環境には、インターネットから Fixlet を収集する BigFix サーバーが少なくとも 1 つ存在します。これらのメッセージは、コンソール・オペレーターで表示したり、リレーに配信したりできます。リレーは、クライアントにデータを転送します。各クライアントはそのローカル・コンピューターを検査し、関連する Fixlet をリレーに折り返し報告します。リレーは、そのデータを圧縮してサーバーに返します。



コンソールはこのアクティビティーを監視します。サーバーに接続し、ビューを定期的に更新して、ネットワークに関する変更または新しい情報を反映させます。脆弱性が見つかった場合は、コンソール・オペレーターは該当するコンピューターを対象としてパッチやその他のフィックスを適用します。該当するすべてのコンピューターにフィックスが配信され、1 台ずつバグと脆弱性を解消していく進行状況を、ほぼリアルタイムで追跡できます。

BigFix は、遠方のオフィスに VPN を介して接続できる柔軟性があるほか、在宅勤務者や外回りの営業スタッフが、DMZ 内のファイアウォールで保護されたリレーにインターネットを介して接続することも可能にします。このシンプルな階層は拡張と深化が可能であり、実質的にあらゆるサイズのネットワークに対応することができます。

第 章5. コンテンツのタイプ

BigFix では、コンテンツに基づいています。コンテンツの総称用語は、ターゲットに配布するデータ、またはターゲットで実行する命令、またはターゲットで実行する照会を表す場合があります。

BigFix 実装環境は、以下の様々なタイプのコンテンツに基づいています。

アクション

アクションは選択されたターゲットで実行されるスクリプトです。アクションは、ポリシー違反および機密漏れの修正、構成ステップの実行、または一般に、ターゲットに対する操作やコマンドの実行のために使用されます。Fixlet、タスク、およびベースラインにはアクションが含まれ、それらの修復作業はアクションによって実行されます。

アクションについて詳しくは、アクション (（ページ）　　)を参照してください。

Fixlet

Fixlet とは、ターゲット・システムの BigFix エージェントがその状況を判断し、脆弱性やポリシー・ルールの非準拠といった問題を特定し、解決のための修正アクションを実行するために使用する指示が記述された文書のことです。

Fixlet について詳しくは、Fixlet とタスク (（ページ）　　)を参照してください。

タスク

タスクとは、ターゲット・システムの BigFix エージェントが、コマンドや構成アクティビティーをローカルで実行するために使用する指示が記述された文書のことです。

タスクについて詳しくは、Fixlet とタスク (（ページ）　　)を参照してください。

ベースライン

ベースラインは、Fixlet とタスクのデプロイメント・コンテナーです。1 つ以上のターゲットに対して、コンテンツ・セットを同時に適用する場合に使用できます。コンテンツは、ベースラインの記述で指定されたシーケンスに基づいて適用されます。例えば、ベースラインは以下を含む場合があります。

1. 製品をインストールするための Fixlet。
2. 製品を必要なレベルへアップグレードする Fixlet。
3. インストールされた製品を構成するタスク。

ベースラインがデプロイされる際、所定のシーケンスに従ってコンテンツが適用されます。

ベースラインについて詳しくは、個のベースライン (（ページ）　　)を参照してください。

分析

分析はプロパティー式のコレクションであり、オペレーターはこれを使用することで、ネットワーク上のBigFixクライアント・コンピューターの各種プロパティーを表示および要約できます。

分析について詳しくは、分析 (（ページ）　　)を参照してください。

これらのタイプのコンテンツには、BigFix コンソールからアクセスできます。BigFix スイートに属する各アプリケーションは、これらのコンテンツを使用してアクティビティーを実行します。ユーザーは、独自のニーズを満たすように、カスタム・コンテンツを作成することができます。例えば、カスタム Fixlet を作成して、独自に開発したアプリケーションにパッチを適用したり、ポリシー・ルールを適用したりすることができます。カスタム・コンテンツを作成するには、特定の許可が必要です。

コンテンツはコンテンツ・サイトにあり、適時、自動的に更新されます。利用可能なコンテンツ・サイトのセットは、購入した BigFix 製品ライセンスによって異なります。コンテンツ・サイトへのアクセスについて詳しくは、ポストインストール手順 (（ページ）　　)を参照してください。必要な許可を持っている場合は、独自のカスタム・コンテンツ・サイトを作成し、カスタム・コンテンツを収集することができます。

第 章6. コンテンツを適用するターゲットの識別方法

BigFix は、コンテンツを適用するターゲットを識別するのに役立ちます。

BigFix の主な特長の 1 つは、コンテンツの適用先となるターゲット、つまりコンテンツを必要とするコンピューターを判別する機能です。この機能は関連式を使用して実現されます。関連式はコンテンツ定義の一部であり、管理対象クライアントのハードウェアおよびソフトウェアのプロパティーを調べて、パッチや保守アクティビティーなどがそれを必要とするコンピューターのみに適用され、その他のコンピューターには適用されないようにすることを目的としています。

コンテンツを定義するには、そのコンテンツのターゲットとなる一連のコンピューターを「適用可能なコンピューター」タブで指定します。関連度の評価により、この一連のコンピューターが絞り込まれ、そのコンテンツを真に適用する必要のあるコンピューターのみが選択されます。

関連式はすべてのコンテンツ・タイプに対して同じ方法で使用されますが、以下のようにコンテンツ・タイプに応じて様々な動作がトリガーされます。

関連するアクション

この場合、アクション・スクリプト言語を使用してアクションの記述に指定された命令を実行することにより、違反が修復されます。アクションは、実行時に「アクションの実行」ダイアログでカスタマイズできる関連句を取り込みます。

関連する Fixlet

コンピューターがポリシー・ルールに準拠していない場合です。Fixlet が必要な場合、Fixlet 定義に含まれるアクションを実行して、問題を修復できます。

アクションの実行後に関連性がもう一度評価され、ぜい弱性が修復されたかどうか確認されます。

例えば、Fixlet を使用して Symantec Endpoint Protection をインストールすることができます。この Fixlet は、Symantec Endpoint Protection がインストールされていないコンピューターに関連付けられています。Fixlet がすべての該当するコンピューターにインストールされると、関連性のマークは付かなくなります。その後、「適用可能なコンピューター」タブに指定された 1 つ以上のコンピューターから Symantec Endpoint Protection がアンインストールされると、Fixlet に再び関連性のマークが付きます。

関連するタスク

コンピューターに構成標準または構成要件の違反があるか、メンテナンス・アクティビティーを実行する必要がある場合です。

例えば、タスクを使用して Symantec Endpoint Protection を始動したりします。このタスクが該当するのは、Symantec Endpoint Protection が非アクティブになっているコンピューターです。

このタスクが該当する場合、タスク定義に含まれるアクションを実行して、問題を修正することができます。アクションのすべてのステップが完了すると、タスクには、そのコンピューターには該当しないことを示すマークが付けられます。関連式が再度評価されることはありません。ベスト・プラクティスとして、アクションが正常に完了したかどうかを判別するために成功基準を使用して、修復の試みが問題の解決につながるようにすることが推奨されます。

関連するベースライン

この場合、このベースラインに含まれる 1 つ以上の Fixlet が、Fixlet の記述とベースラインの「適用可能なコンピューター」タブの両方に指定されている関連式の基準を満たす、1 つ以上のコンピューターに必要です。ベースラインの「適用可能なコンピューター」タブに何も指定されていない場合、Fixlet およびタスクの適用条件に制限は適用されません。

例えば、Windows および Linux オペレーティング・システムの Fixlet およびタスクがベースラインに含まれているものの、ベースラインの「適用可能な

コンピューター」において Windows コンピューターのみが関連すると指定されている場合、Windows に適用可能な Fixlet およびタスクのみが対象となります。

注: ベースラインにタスクが含まれる場合でも、Fixlet の動作は適用されます。

関連する分析

照会間隔に従ってプロパティー照会を実行し、結果をサーバーに送信します。この結果は BigFix コンソールに表示されます。

コンピューターが新規に収集された文書の関連性 (例えば Fixlet や分析) を評価して、結果を送信すると、その結果は BigFix コンソールに表示されます。初回の評価の後は、コンピューターは変更のみをレポートします。これは、同じ結果のレポートにネットワーク帯域幅を使用してもメリットがないためです。

関連式は、人間が読んで理解できる「Relevance Language」という専用言語で作成されます。

カスタム・コンテンツ許可を持っている場合、新規の関連式を作成したり、あるいは既存の式を変更することで、必要に応じたコンテンツが実行されるように調整することができます。オペレーターへの許可の割り当てに関する詳細は、許可されるアクティビティーと許可とのマッピング (（ページ）　　)を参照してください。

第 章7. パッチ管理のシナリオ

以下のトピックにリストされた手順に従って、新しくインストールされたBigFixサーバー上のパッチ管理アプリケーションを使用して、パッチを適用する方法を確認してください。すべての手順は BigFix コンソールから実行します。

このシナリオは、Windows オペレーティング・システムに適用されます。同じ手順に従って、他のオペレーティング・システムでもパッチを有効にして、適用することができます。

このシナリオは、以下の 2 つのパートに分かれています。

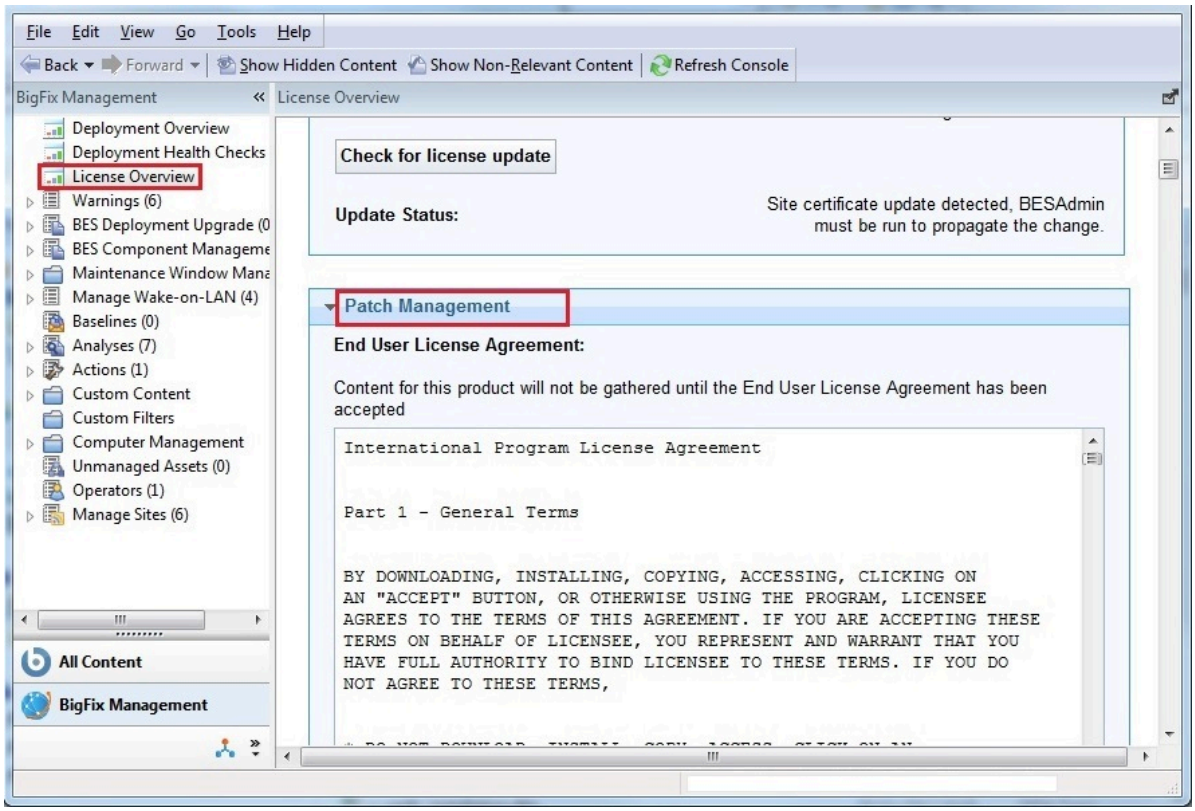
Windows パッチ用のパッチ管理の構成

インストール後に、BigFix 製品は、特定の管理サイトおよびメンテナンス・サイトをサブスクライブするように自動的にセットアップされます。これにより、それらのサイトから企業内にコンテンツが自動的に流れ込み、BigFix クライアントを実行しているすべてのコンピューターで、それらのコンテンツの関連度が評価されます。

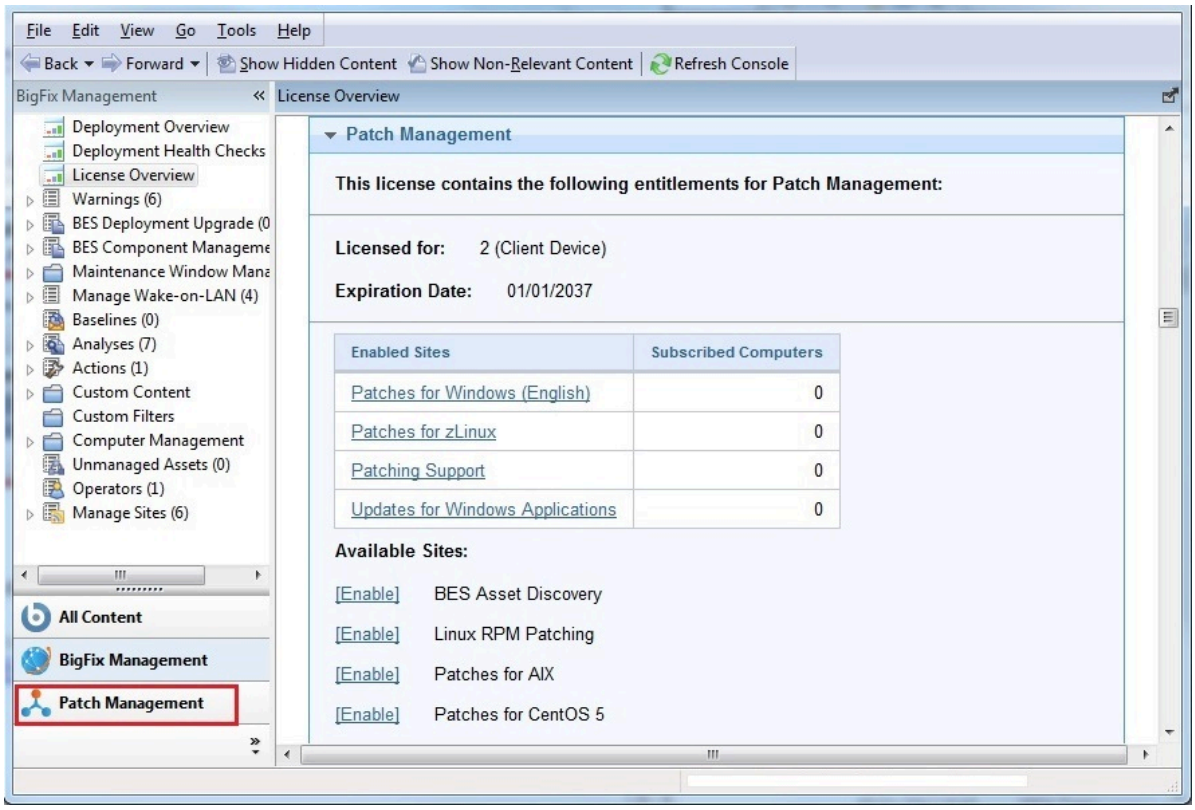
以下の手順を実行して、パッチ管理サイトをサブスクライブします。

1. 次のアイコンをダブルクリックして、BigFix コンソールを開きます。

2. **「ライセンスの概要」**ダッシュボードをクリックします。
3. 「パッチ管理」エリアまでスクロール・ダウンします。

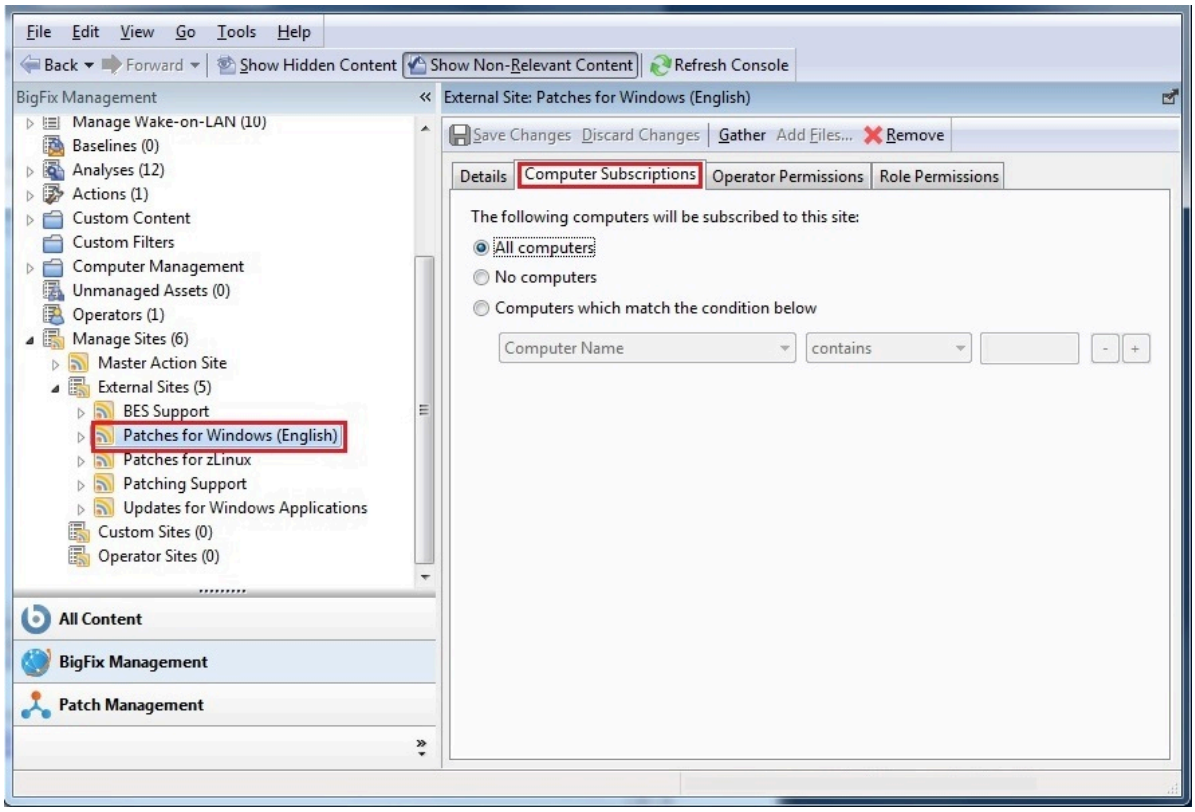


4. パッチ管理のご使用条件を読んで同意します。
5. **「利用可能なサイト」**で、**「BES Asset Discovery」**、**「Patches for Windows (英語)」**、**「パッチ・サポート」**、および**「Windows アプリケーションの更新」**の横にある**「有効化」**をクリックし、パッチ管理 Web サイトからのダウンロード・コンテンツを有効にします。



これで、パッチ管理サイトがドメイン・パネルの**「サイトを管理」**ノードにリストされます。

6. **「サイトを管理」**ノードを開いて、**「Patches for Windows (英語)」**を選択します。
7. サイト・ダイアログで、**「コンピューターのサブスクリプション」**タブをクリックしてから**「すべてのコンピューター」**を選択します。

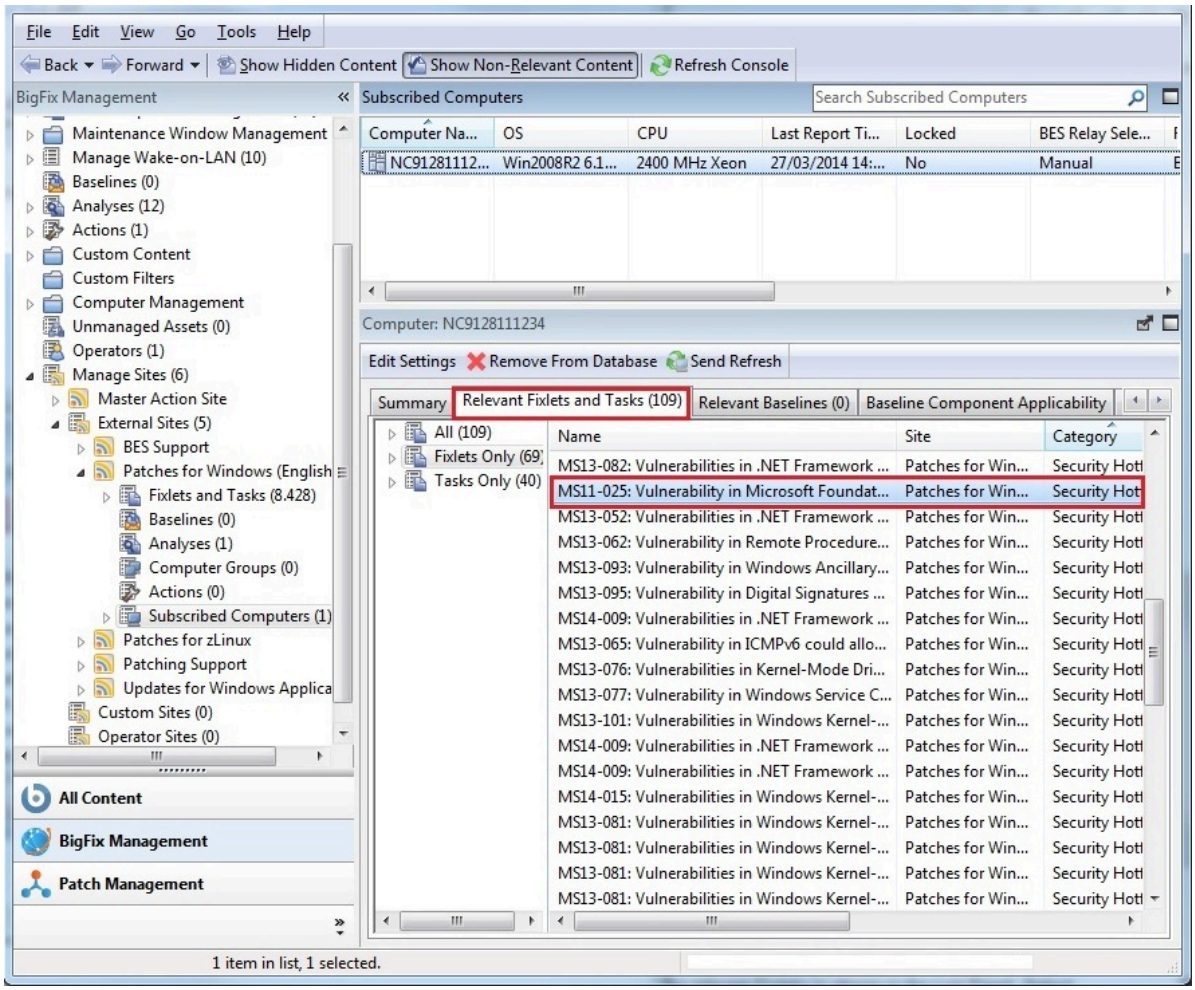


8. 収集プロセスが自動的に実行されるまで待機するか、**「収集」**をクリックして選択したサイトから使用可能なコンテンツのダウンロードを開始できます。
9. 収集プロセスが完了すると、**「Patches for Windows (英語)」**サブツリーに新規コンテンツが取り込まれます。

Windows パッチの適用

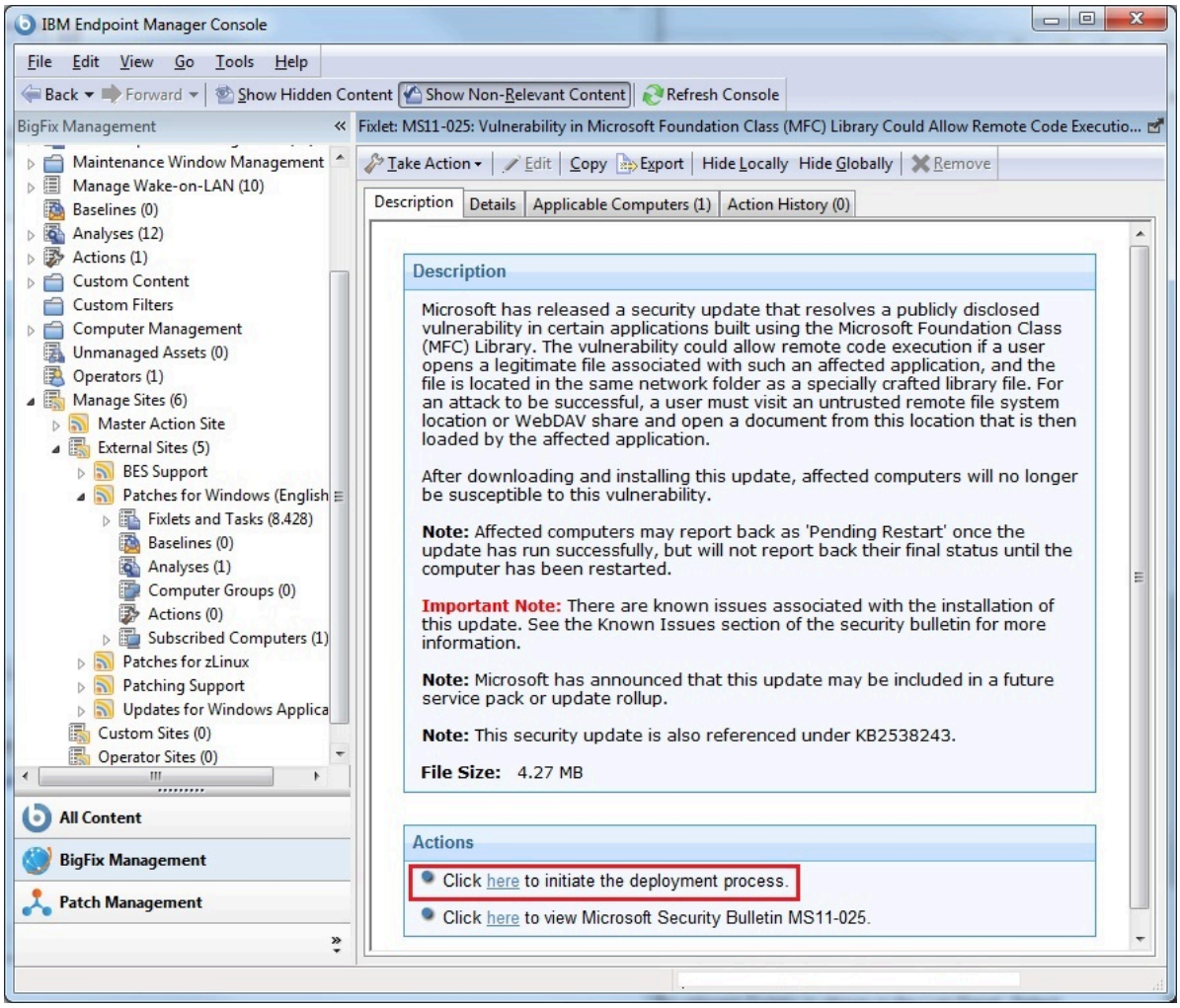
以下の手順をコンソールから実行して、Windows パッチを適用します。

1. **「Patches for Windows (英語)」**サブツリーを展開し、**「サブスクライブしたコンピューター」**をクリックします。**リスト・パネル**に、サーバー・システムにインストールされたクライアントを表すエントリーが表示されます。
2. **「関連する Fixlets とタスク」**タブを選択して、選択したクライアントに関連する Fixlets のリストを表示します。

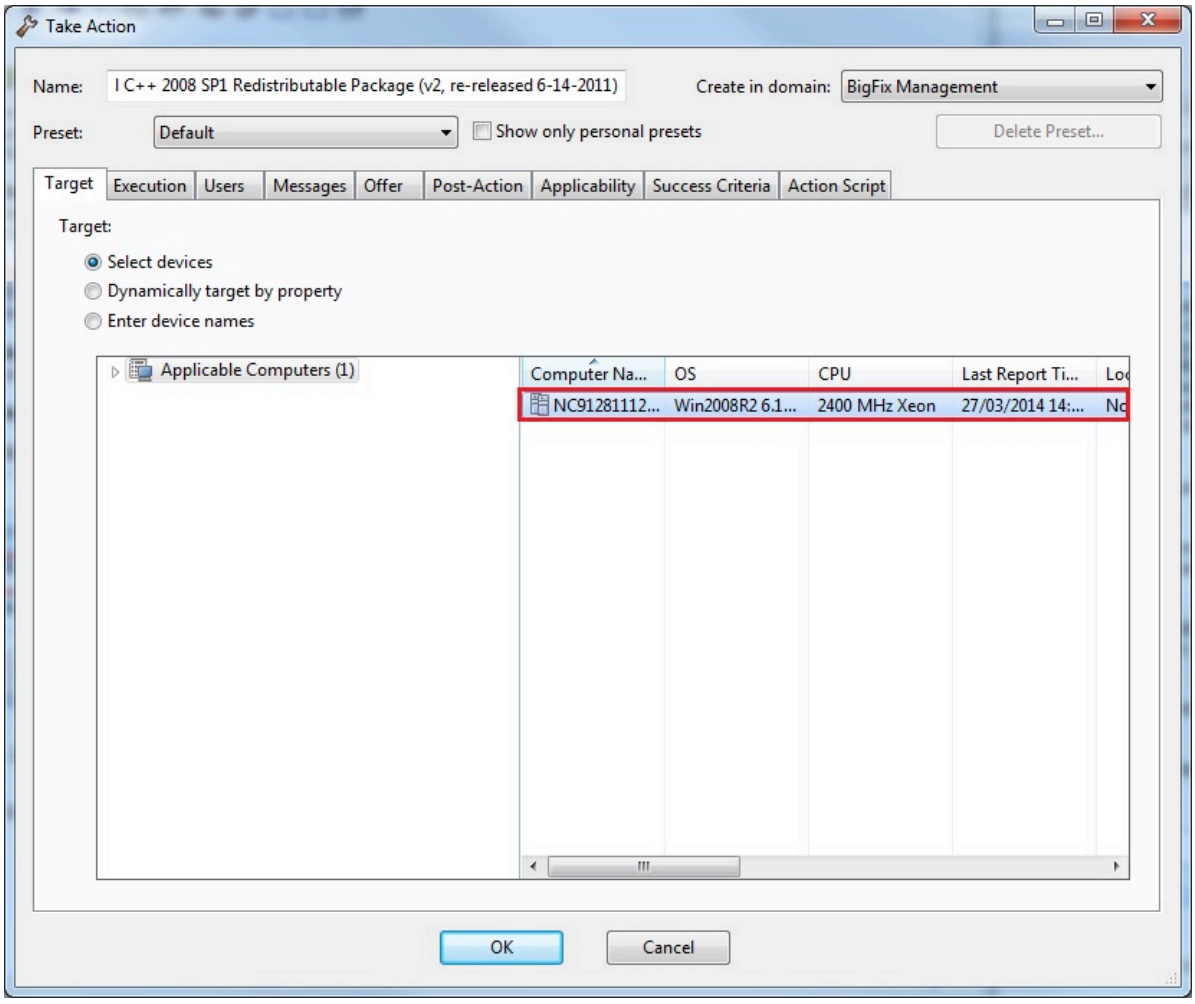


Fixlet がクライアントに関連するのは、Fixlet で参照されたコンテンツをクライアントがインストールする必要がある場合です。コンテンツをインストールする必要性については、Fixlet に指定された事前定義条件のセットを使用して、クライアント上で自動的に評価されます。

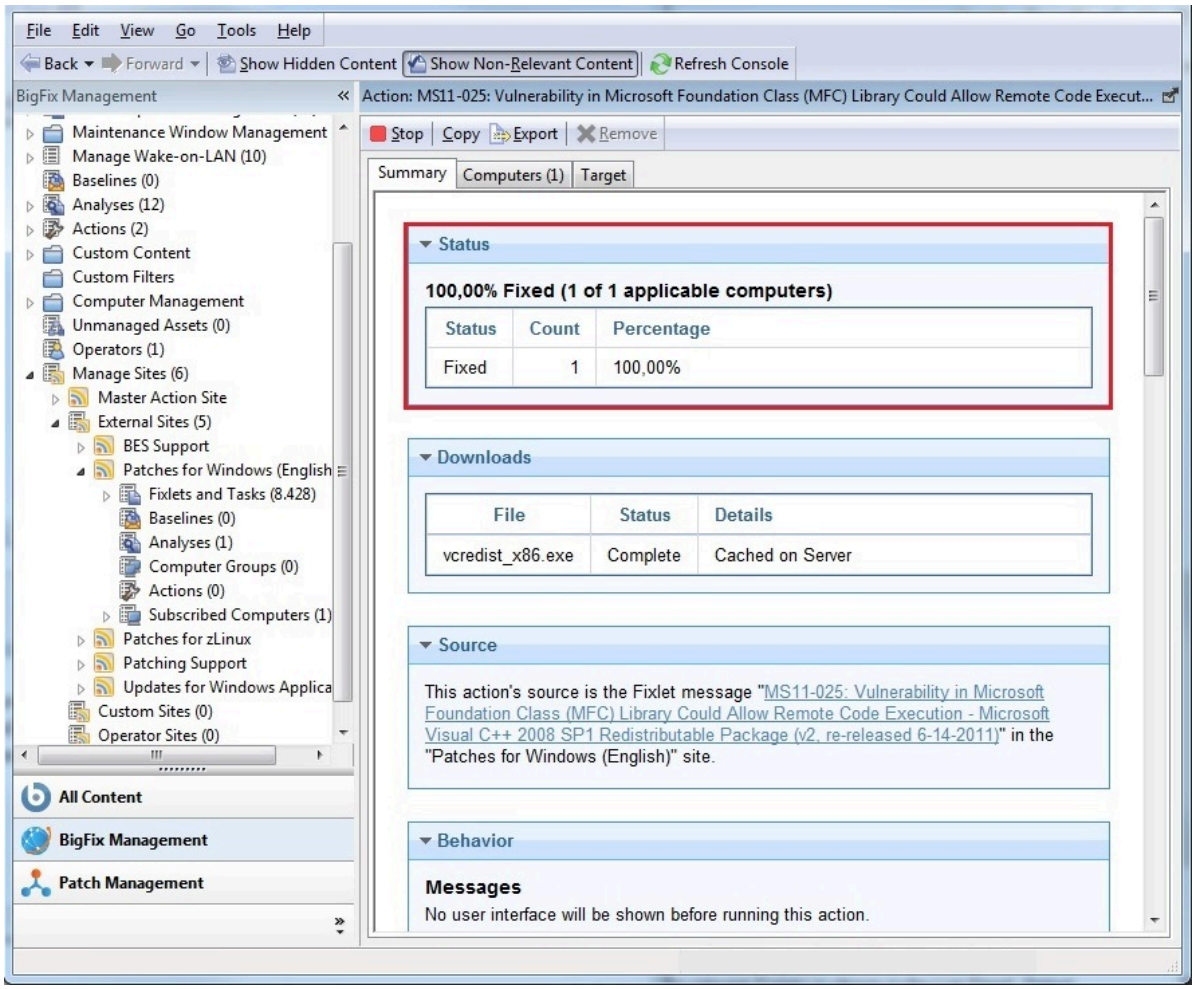
3. 「Fixlet」をダブルクリックして、Fixlet の説明にアクセスします。
4. **「アクション」**ペインで、適用プロセスの開始を選択します。



5. **「アクションの実行」**パネルが開きます。このパネルでクライアントを選択してから、**「OK」**をクリックして適用を開始します。



6. **「アクション」**パネルへ自動的にリダイレクトされます。状況ペインに、Fixlet 適用の進捗状況が表示されます。状況は**「未評価」**から**「評価中」**に変わり、クライアントの脆弱性が正常に修正されると**「修正済み」**に変わります。脆弱性の除去は、「アクション」の**「成功条件」**タブで指定された事前定義条件のセットを使用して、クライアント上で自動的に評価されます。



7. 脆弱性が除去された後は、クライアントにその Fixlet を再度適用する必要はありません。Fixlet はそのクライアントに関連がないマークが付けられます。