

BigFix Asset Discovery ユーザーズ・ガイド



Special notice

Before using this information and the product it supports, read the information in [Notices \(on page 49\)](#).

Edition notice

This edition applies to BigFix version 11 and to all subsequent releases and modifications until otherwise indicated in new editions.

第 1 章. 環境の設定

BigFix Asset Discovery の仕組みについて説明します。

エンタープライズ環境における BigFix Asset Discovery の主な用途は、以下のとおりです。

- ネットワーク資産 (IP アドレスを持つ、ルーター、プリンター、スイッチなどのデバイスおよび無線アクセス・ポイントなどを含む) の識別。
- 非管理コンピューターおよび不正コンピューター (BigFix エージェントが無効となっているコンピューターや、会社が管理していない不正コンピューターを含む) の識別。

この情報により、デバイスの種類、インストール日時、およびインストール場所に関する、ライセンス・インベントリーの重要な疑問に答えることができます。さらに、ネットワーク上の無許可の従業員コンピューター、ワイヤレス装置、または不正デバイスに関する、セキュリティ上の疑問や懸念に答えることができます。

BigFix Asset Discovery は、近くにあるコンピューターの別のエージェントがスキャンを実行するという点で、ユニークなソリューションです。これは、分散スキャンとして知られています。この方法には、以下に示すいくつかの重要なメリットがあります。

- WAN 帯域幅を節約する
- スキャンを並列に実行できるので、結果を得るのが数週間後ではなく数分後となり、非常に早くなる
- 分離サブネットを含む複雑なネットワーク構成で動作するよう容易にカスタマイズできる
- カスタマイズされたスキャン・タイプを個々のサブネットで実行できる

BigFix Asset Discovery は、Fixlet とタスクを使用して、ネットワーク内の指定されたエージェントにスキャン・ポイントをデプロイすることで動作します。その後、他の Fixlet とタスクを使用して、Nmap スキャンを好きな間隔で実行することができます。スキャン結果は自動的に BigFix サーバーに送信され、このサーバーで、データが BigFix データベースにインポートされます。これによりスキャン情報は、BigFix コンソールで「非管理資産」タブを使用して確認できます。

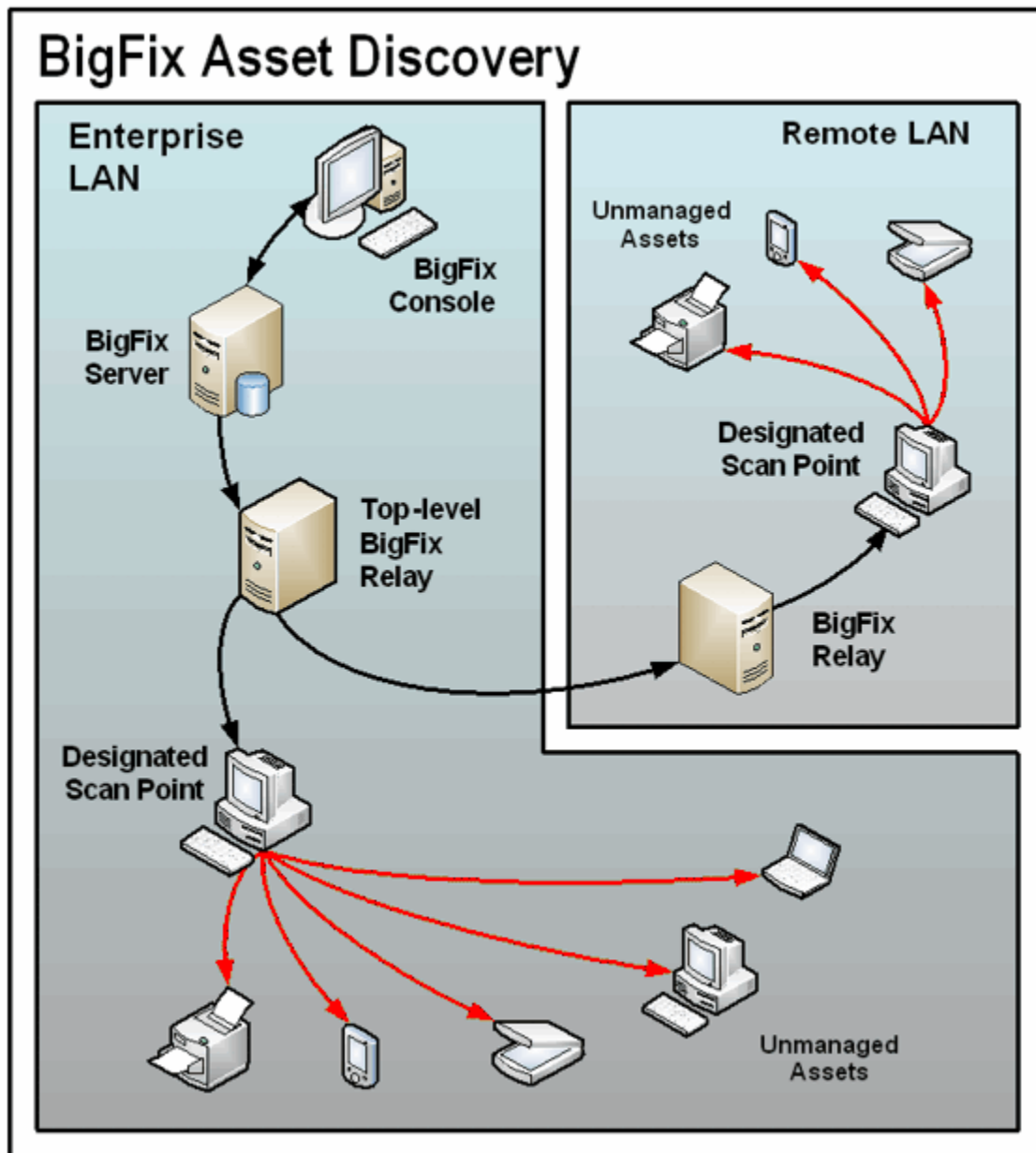


注: Linux プラットフォームでAsset Discovery Fixlet を使用するには、BES サーバー・プラグイン・サービスをインストールする必要があります。このプラグインは、BigFix サポート・サイトで入手して、インストールできます。

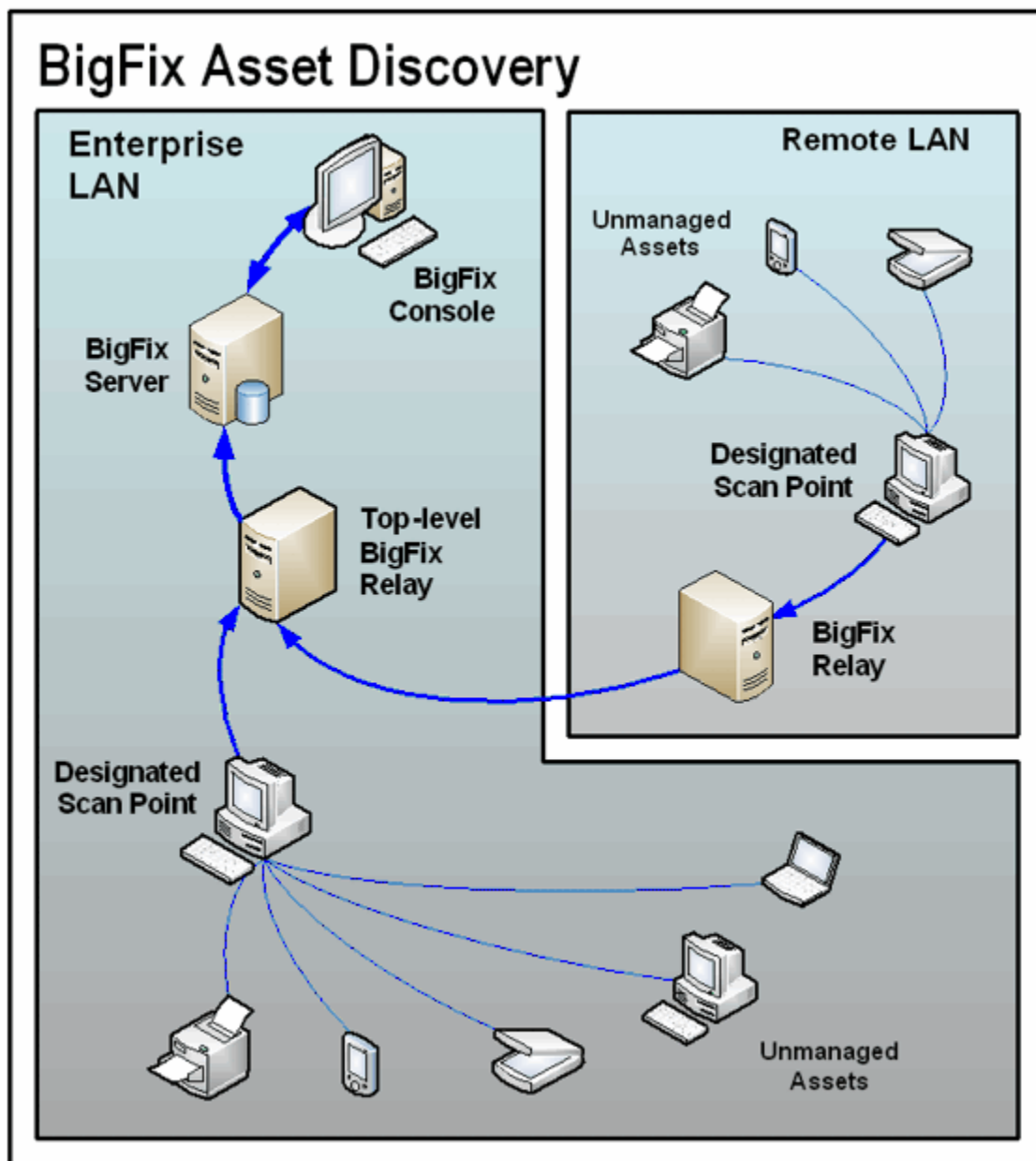
第 2 章. 概要

BigFix が資産を発見する方法と、スキャン・ポイントについての概要を説明します。

BigFix Asset Discovery は、特定のコンピューターをスキャン・ポイントとして指定することで動作します。サポートされるオペレーティング・システムを実行しているエージェントであれば、どのエージェントもスキャン・ポイントとして指定できます。これらのスキャン・ポイントは、ネットワーク内の非管理資産を照会します。次の図は、このプロセスを示したものです。



情報は、スキャン・ポイントによってこれらの非管理資産から取得され、リレーを介して、BigFix サーバー上のデータベースに送り返されます。以下のように、このデータベースから、BigFix コンソールで結果を調べることができます。



スキャン・ポイント・ハードウェア要件およびソフトウェア要件

BigFix Nmap Scan Point は、すべての Windows (x86-64)、Red Hat Enterprise Linux 7.4 以降 (x86-64)、Red Hat Enterprise Linux 8 以降 (x86-64)、Red Hat Enterprise Linux 9 以降

(x86-64)、CentOS 7、8 (x86-64)、Amazon Linux 2 (x86-64)、Amazon Linux 2023 (x86-64) など、BigFix Agent がサポートされている場所で動作します。

古い Nmap バージョンでは、BigFix Asset Discovery は 7.4 より前の Red Hat Linux 7 もサポートしています。

インストール

正常なインストールを完了するために実行するタスクについて説明します。

Asset Discovery サイトで、以下のインストール・タスクを実行します。

- お使いの BigFix サーバーで、Unmanaged Asset Importer サービスを有効にします。
- 特定のエージェントをスキャン・ポイントとして指定します。
- スキャンを実行します。



注: 「非管理資産」を表示するには、管理ツールを通してユーザーに適切な権限が設定されていなければなりません。このツールにアクセスするには、「**スタート**」>「**すべてのプログラム**」>「**BigFix Enterprise**」>「**BES 管理ツール**」をクリックします。ユーザーには、すべての非管理資産を表示する許可を付与することも、管理するスキャン・ポイントに接続されている非管理資産のみ表示する許可を付与することもできます。



注: Linux プラットフォームで Asset Discovery Fixlet を使用するには、BES サーバー・プラグイン・サービスをインストールする必要があります。このプラグインは、BigFix サポート・サイトで入手できます。

サイトのインストール

すべてのコンピューターを外部サイトに対して有効にし、サブスクライブするための手順について説明します。

BigFix コンソールを使用して、外部サイトを有効にし、すべてのコンピューターを外部サイトにサブスクライブするには、次の手順を実行します。

1. 「BigFix 管理」ドメインを開き、上部までスクロールして関連付けられたダッシュボードを表示します。
2. ライセンス・ダッシュボードで、外部サイトをクリックし、まだ外部サイトが有効になっていない場合は、サイトのリストでサイトの名前をクリックして有効にします。
3. 外部サイトのプロパティ・パネルで、「**コンピューターのサブスクリプション**」タブを選択し、「**すべてのコンピューター**」をクリックして BigFix 環境内のすべてのコンピューターを外部サイトにサブスクライブします。
4. 「**変更を保存**」をクリックして、サイト・サブスクリプション設定を保存します。

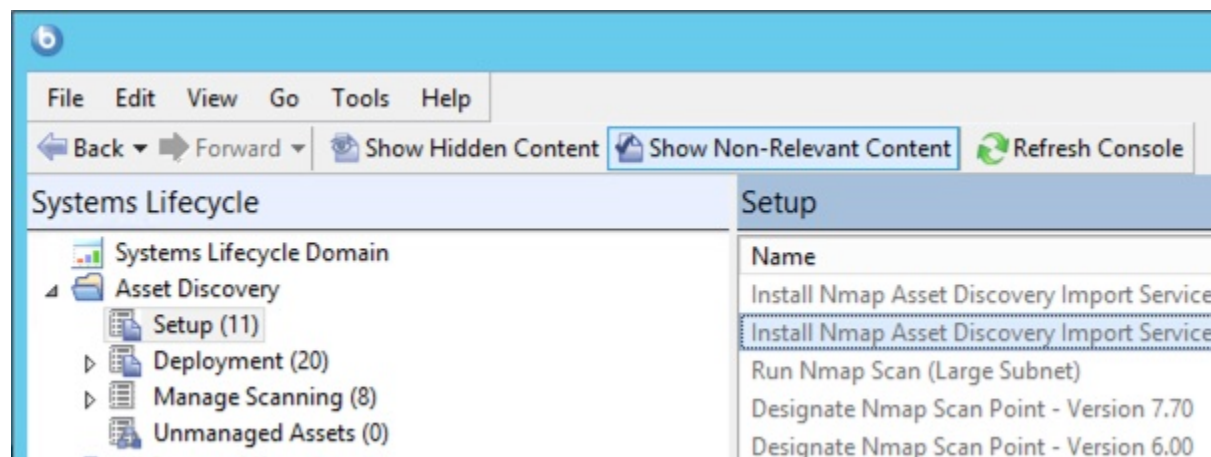
インポート・サービス・タスクのインストール

Nmap Asset Discovery インポート・サービスを BigFix サーバーにインストールする方法について説明します。

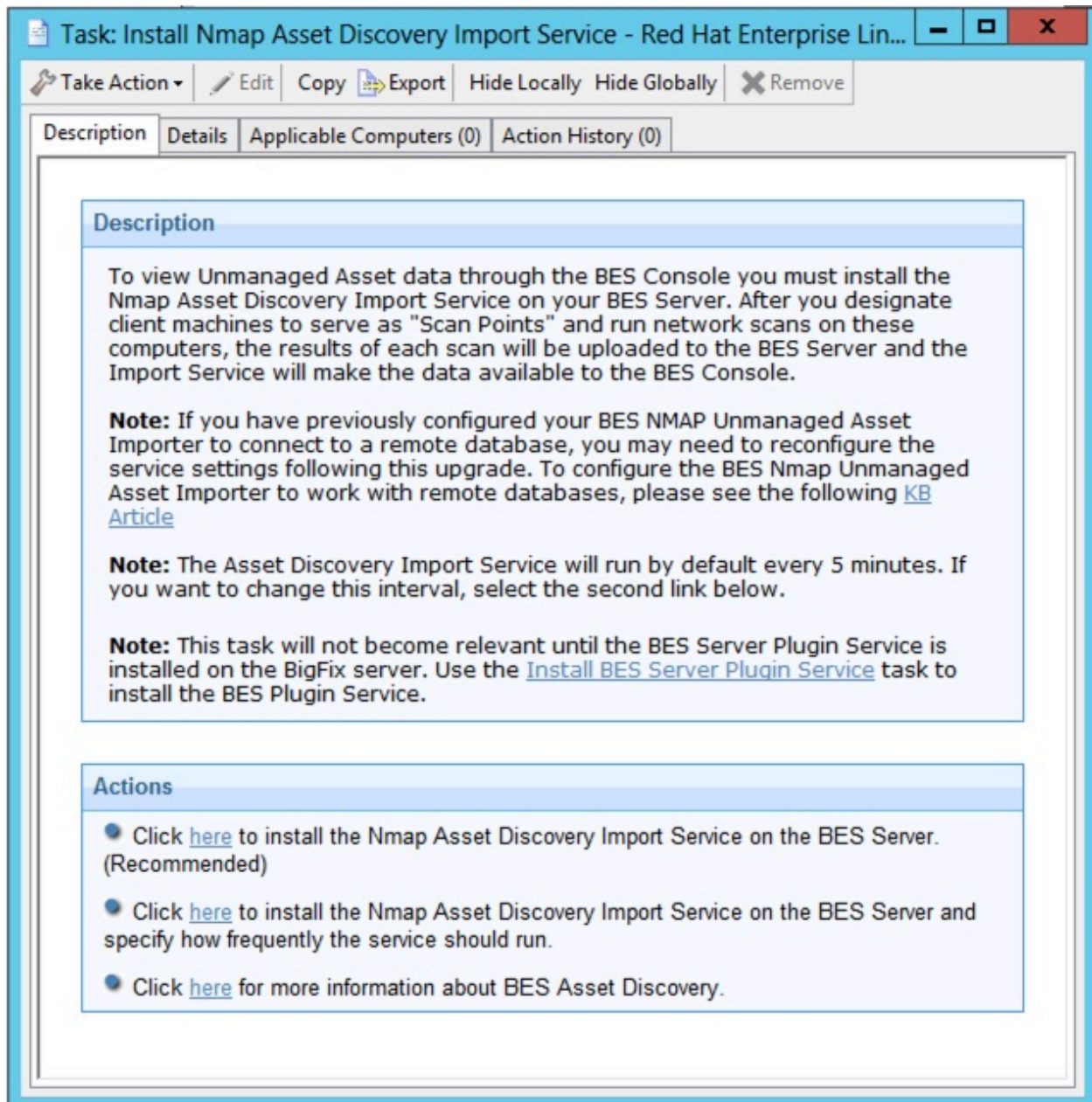


注: リモート・データベースにアクセスする場合は、NMAP インポート・サービスをドメイン・ユーザーとして実行する必要があります。これは、SQL データベースへのアクセスには標準ローカル・システムを使用することができないからです。このサービスは、リモート・データベース環境内の他の BigFix サービスと同様に構成する必要があります。

Asset Discovery ナビゲーション・ツリーの「設定」ノードを選択して、右側のパネルに「Nmap Asset Discovery インポート・サービスのインストール」タスクを見つけます。



このタスクをクリックし、ワークエリアで説明を確認します。



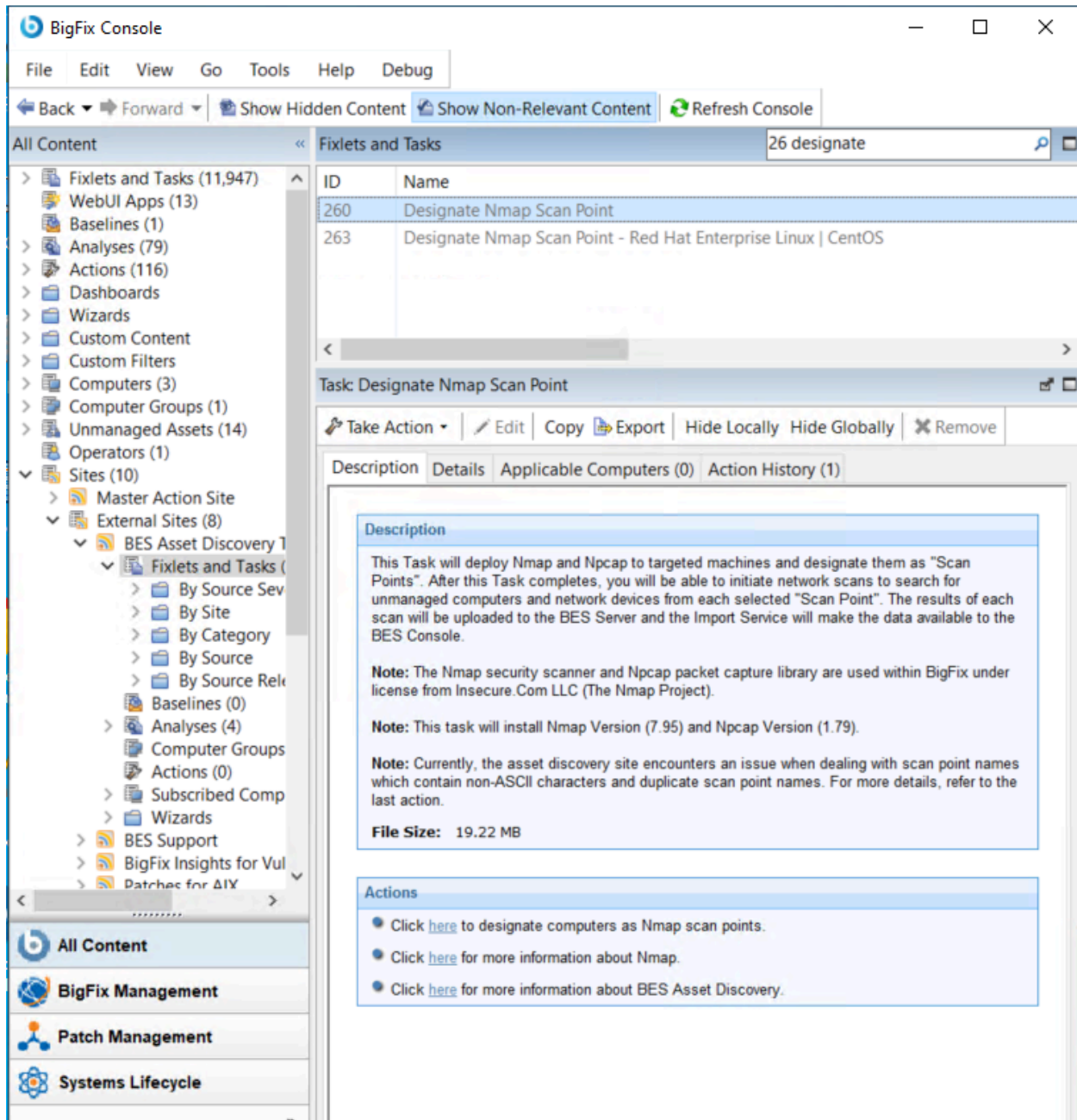
Nmap Asset Discovery インポート・サービスを BigFix サーバーにインストールするには、「アクション」ボックス内の該当するリンクをクリックします。インポート・サービスはデフォルトでは 5 分おきに実行され、BigFix サーバーに送信された新しい Nmap スキャ

ン・データがないかどうか調べられます。別の頻度を設定する場合は、2 番目のアクション・リンクを選択します。

スキャン・ポイントのインストール

スキャン・ポイントをインストールするためのアクションについて説明します。

Asset Discovery ナビゲーション・ツリーの「設定」ノードを選択して、右側のパネルに指定タスクを見つけます。



スキャン・ポイントとして指定するコンピューターは、Windows または Linux を実行していない必要があります。これらのスキャン・ポイントは、ローカル・サブネットをスキャンする起点となるハブです。

Windows の場合、「Nmap スキャン・ポイントの指定」タスクをクリックします。

「アクション」ボックスの最初のリンクをクリックして、「アクションの実行」ダイアログにアクセスします。「ターゲット」タブから、スキャン・ポイントとして指定するコンピューターを選択します。

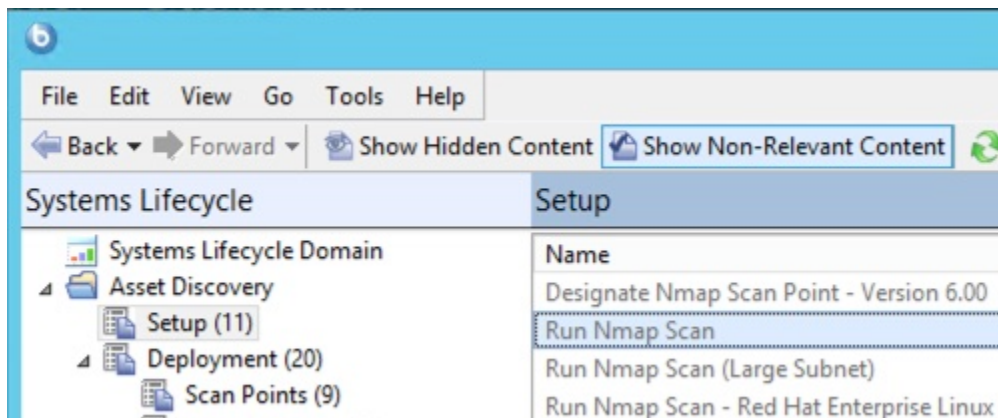
Linux の場合、「Nmap スキャン・ポイントの指定 - Red Hat Enterprise Linux」タスクをクリックします。

「アクション」ボックスの最初のリンクをクリックして、Nmap スキャン・ポイントを指定します。

スキャンの実行

非管理コンピューターと非管理ネットワーク・デバイスを検出するためのスキャンを実行する方法について説明します。

Asset Discovery ナビゲーション・ツリーの「設定」ノードを選択して、「Run Nmap Scan」で使用可能なすべてのタスクを見つけます。



ワークエリアでこのタスクが開いたら、「アクション」ボックスで、Nmap スキャンを開始するための有効なリンクの 1 つを選択します。ローカル・サブネットを指定できます。

Task: Run Nmap Scan

Take Action

Edit

Copy

Export

Hide Locally

Hide Globally

Remove

Description

Details

Applicable Computers (0)

Action History (0)

Description

This task will run an Nmap scan from the selected computers to detect unmanaged computers and network devices. Use the links below to either scan the entire local subnet or to specify a particular IP range.

Once complete, the scan data will be uploaded to the BES Server and automatically imported into the BES Server database by the Asset Discovery Import Service. You will then be able to view the results through the Unmanaged Assets report interface.

To schedule repeated scans or to specify advanced configuration options such as additional ports, timing/aggressiveness options, specific hosts to exclude, and other Nmap command line switches, use the BigFix Asset Discovery Nmap Configuration Wizard to generate a custom Nmap Scan Fixlet message.

Important Note: This task will remove client settings that were created by Nmap scans. By removing excessive old client settings, it will improve performance with the BES Client. By default, it will remove scans that were initiated over 7 days ago. To change this setting, run the task "Set Scanpoint Cleanup Configuration" (ID 34).

Note: The Nmap security scanner is used within BigFix under license from Insecure.Com LLC (The Nmap Project). For more information on Nmap, as well as advanced configuration options, visit the link below.

Note: Nmap supports CIDR-style addressing. For more details about how to specify an IP range, visit the link below.

Note: Client machines may briefly display dos and command prompt windows as a result of running the action below.

Actions

- Click [here](#) to run an Nmap scan on the local subnet.
- Click [here](#) to run an Nmap scan on a specific IP range.
- Click [here](#) to run Nmap on the last subnet scanned. This action is only valid if you have previously run an Nmap scan on the selected Scan Point(s).
- Click [here](#) for more information about Nmap.
- Click [here](#) for more information about BES Asset Discovery.

または大規模サブネットを指定できます。

Task: Run Nmap Scan (Large Subnet)

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (0) | Action History (0)

Description

This task will run an Nmap scan from the selected computers to detect unmanaged computers and network devices. Because the selected computers are connected to multiple subnets or your subnet mask indicates that you are part of a subnet with more than 1022 host addresses, you will need to specify the range of IP addresses you would like the selected "Scan Points" to scan.

Once complete, the scan data will be uploaded to the BES Server and automatically imported into the BES Server database by the Asset Discovery Import Service. You will then be able to view the results through the "Unmanaged Assets" tab of the BES Console.

To schedule repeated scans or to specify advanced configuration options such as additional ports, timing/aggressiveness options, specific hosts to exclude, and other Nmap command line switches, use the BigFix Asset Discovery Nmap Configuration Wizard to generate a custom Nmap Scan Fixlet message.

Important Note: This task will remove client settings that were created by Nmap scans. By removing excessive old client settings, it will improve performance with the BES Client. By default, it will remove scans that were initiated over 7 days ago. To change this setting, run the task "Set Scanpoint Cleanup Configuration" (ID 34).

Note: The Nmap security scanner is used within BigFix under license from Insecure.Com LLC (The Nmap Project). For more information on Nmap, as well as advanced configuration options, visit the link below.

Note: Nmap supports CIDR-style addressing. For more details about how to specify an IP range, visit the link below.

Note: Client machines may briefly display dos and command prompt windows as a result of running the action below.

Actions

- Click [here](#) to run an Nmap scan on the specified IP range.
- Click [here](#) to run Nmap on the last subnet scanned. This action is only valid if you have previously run an Nmap scan on the selected Scan Point(s).
- Click [here](#) for more information about Nmap.
- Click [here](#) for more information about BES Asset Discovery.

クラス C ネットワーク (255 個の IP アドレス) のスキャンは通常は、ご使用のネットワークに応じて、10 分から 30 分ほどかかります。Asset Discovery Nmap 設定ウィザードを使用して、Nmap スキャンをスケジュールおよび構成するための独自のカスタム・タスクを作成することもできます。

スキャン・ポイントでそのローカル・スキャンが完了すると、その結果は BigFix サーバーにアップロードされ、Importer サービスによってデータベースにインポートされます。これにより、スキャン結果が BigFix コンソールの「非管理資産」タブに表示されます。

これで、Asset Discovery サービスのインストールは完了です。

第 3 章. Asset Discovery の使用

Asset Discovery の使用方法と注意事項について

演算

スキャン・ポイント・コンピューターが取得した非管理資産に対して実行可能なアクションについて説明します。

インストールが完了すると、スキャン・ポイント・コンピューターによって取得されたすべての非管理資産情報を表示できます。

任意の時点で、「スキャン・ポイント統計」をアクティブにして、指定された Nmap スキャン・ポイントに関する情報を表示することができます。ナビゲーション・ツリーの「スキャンングを管理」ノードの下にある「スキャン・ポイント統計」をクリックします。統計は、「ステータス別」、「サイト別」、または「アクティベーション別」に表示できます。

The screenshot displays the BigFix Console interface. On the left, the 'Systems Lifecycle' tree is expanded, showing the hierarchy from 'Systems Lifecycle Domain' down to 'Scan Point Statistics (4)'. The right pane shows a table of 'Scan Point Statistics' with columns for Status, Name, Site, and Applicab. Below the table, the 'Analysis: Nmap Scan Point Statistics - Windows' is selected, showing its description and applicable computers (0).

Status	Name	Site	Applicab
Not Activated	Nmap Scan Point Statistics - Windows	BES Asset Discovery	0
Not Activated	Nmap Asset Discovery Import Service Settings	BES Asset Discovery	0
Not Activated	Nmap Scan Point Statistics - Linux	BES Asset Discovery	0
Not Activated	Scanpoint Cleanup Configuration Analysis - Windows	BES Asset Discovery	0

Analysis: Nmap Scan Point Statistics - Windows

Description

This analysis contains information regarding your designated Nmap Scan Points - Windows.

After activating this analysis, you will see the following properties for Nmap:

- Installation Time

Connected to 'localhost' as user 'BFAdmin'

スキャン・ポイント・コンピューターを解除する場合は、「インストール」ノードの「Nmap スキャン・ポイントの削除」タスクを使用します。「Nmap スキャン・ポイントの削除」タスクにアクセスするには、「インストール」ノードの下に「スキャン・ポイント」をクリックします。

The screenshot shows the BigFix Console interface. The left sidebar contains a navigation tree with the following items: All Content, BigFix Management, Patch Management, and Systems Lifecycle. The 'All Content' section is expanded, showing a list of items including Fixlets and Tasks (11,947), WebUI Apps (13), Baselines (1), Analyses (79), Actions (116), Dashboards, Wizards, Custom Content, Custom Filters, Computers (3), Computer Groups (1), Unmanaged Assets (14), Operators (1), and Sites (10). The 'Fixlets and Tasks' section is selected, and a search bar contains the text 'remove'. The main pane displays a table of tasks:

ID	Name
262	Remove Nmap Scan Point
17	Remove Nmap Scan Point - Red Hat Enterprise Linux CentOS TinyCore
2	Remove Nmap Scan Point - Version < 7.70

Below the table, the 'Task: Remove Nmap Scan Point' details are shown. The 'Description' tab is selected, displaying the following text:

This task will remove previously installed Nmap components and configuration settings from targeted machines. After deploying this Task, these computers can no longer be used to scan your network.

Note: The actions below will also remove all run statistics for Nmap from selected computers.

The 'Actions' tab is also visible, displaying the following actions:

- Click [here](#) to uninstall Nmap and Npcap.
- Click [here](#) to uninstall Nmap only.
- Click [here](#) for more information about Nmap.
- Click [here](#) for more information about BES Asset Discovery.

これにより、指定されたスキャン・ポイントから Nmap が削除され、Nmap の最新バージョンで WinPcap または Npcap も削除できます。「アクション」ボックスをクリックして、「アクションの実行」ダイアログにアクセスし、解除するスキャン・ポイント・コンピューターを選択します。非管理資産を削除するには、ナビゲーション・ツリーの一番下にある「非管理資産」をクリックします。

Nmap スキャン・ウィザードの使用

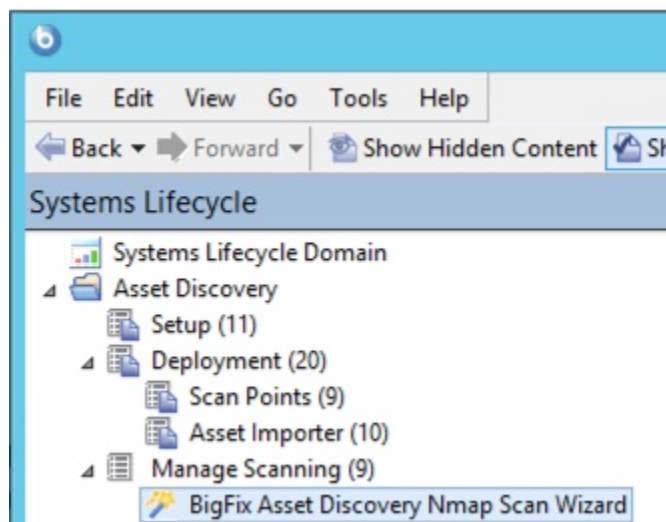
Nmap スキャナーを要件に合わせてカスタマイズする方法について説明します。

Asset Discovery Nmap スキャン・ウィザードを使用すると、Nmap スキャン・プログラムのさまざまな側面を変更できます。以前に指定したスキャン・ポイントを使用して、ネットワークの定期的な Nmap スキャンをスケジュールすることができます。



注: Nmap スキャン・プログラムを実行するには、`UnmanagedAssetImporter -NMAP` サービスがサーバー上で実行されている必要があります。


ナビゲーション・ツリーの「スキャニングを管理」ノードの下にある「スキャン・ウィザード」をクリックします。



右側にウィザードが表示されます。

BigFix Asset Discovery Nmap Scan Wizard

This wizard will enable you to schedule periodic Nmap scans of your network using previously designated "Scan Points".

Welcome to the BigFix Asset Discovery Nmap Scan Wizard.  Progress:

Please select one of the following options:


- ☒ **Scan the local subnet.**
This option is only valid if the local subnet of the Scan Point is a Class C subnet and it is only one.
- ☐ **Scan the following hosts:**
Separate multiple subnets or IP ranges with a single space (ex: 192.168.100.1-254 10.0.0.0/24).
[Nmap command line options for host specification.](#)

まず、スキャンのタイプを選択します。ローカル・サブネットをスキャンするか、特定のホストをスキャンすることができます。「次へ」をクリックします。

「ローカル・サブネットをスキャンする」を選択した場合は、次の画面で、このスキャンの固有パラメーターを設定します。ウィンドウの上部にある進行状況表示バーを確認してください。

BigFix Asset Discovery Nmap Scan Wizard

This wizard will enable you to schedule periodic Nmap scans of your network using previously designated "Scan Points".

Welcome to the BigFix Asset Discovery Nmap Scan Wizard. → **Nmap Scan Options** → Progress: 

Nmap Scan Options
For more information on what these settings mean, click [here](#).

Enter the TCP ports you want to scan. Separate each port or port range with a single space.

22 23 80 135 139 445 61616

Select the timing policy that you want. The higher the value, the more aggressive the scan. Note that more aggressive scans will induce a greater load to your network.

☐ 0 - Paranoid ☐ 1 - Sneaky ☐ 2 - Polite ☐ 3 - Normal ☒ 4 - Aggressive ☐ 5 - Insane

Run OS Detection. Selecting "Yes" will cause Nmap to try and detect operating system information.

☒ Yes ☐ No

Enable version detection. Selecting "Yes" will cause Nmap to detect services running on open ports.

☒ Yes ☐ No

List any hosts you want to exclude from this scan. Delimit multiple host addresses and/or ranges with commas (ex: 192.168.100.1-5,10,15)

Back Next Cancel

この画面では、ポートのスキャン、オペレーティング・システム検出の実行、バージョン検出の有効化、および除外するホストのリストについて設定します。必要な選択を行って、「次へ」をクリックします。

次の画面では、Nmap Configuration 設定オプションの有効化、ping オプションの選択、その他の Nmap スキャン・オプションの入力ができます。必要な選択を行って、「次へ」をクリックします。

BigFix Asset Discovery Nmap Scan Wizard

This wizard will enable you to schedule periodic Nmap scans of your network using previously designated "Scan Points".

Welcome to the BigFix Asset Discovery Nmap Scan Wizard.

Nmap Scan Options

Progress:

Enable Advanced Nmap Configuration Options.

☐ **Enable Advanced Nmap Configuration Options.**

Select ping options. By default, Nmap uses ICMP echo requests and TCP ACK pings on port 80 in parallel.

☐ -P0: Do not try to ping hosts before scanning.

☒ -PE: Use ICMP echo request packets to ping hosts.

☒ -PA: Use TCP ACK packets to ping hosts. Specify destination port below.

☐ -PS: Use TCP SYN packets to ping hosts. Specify destination port below.

Enter additional Nmap scan options. Separate each option with a space. These switches will be appended to the command line call to Nmap. [Nmap command line reference guide](#).

☐ Take this action immediately.

Back

Next

Cancel

次の画面では、Fixlet のテキスト・フィールドをカスタマイズできます。Fixlet のタイトルと説明を編集できます。すべてのテキスト・フィールドをカスタマイズしたら、「完了」をクリックして、プライベート・キーのパスワードを入力します。

BigFix Asset Discovery Nmap Scan Wizard

This wizard will enable you to schedule periodic Nmap scans of your network using previously designated "Scan Points".

Welcome to the BigFix Asset Discovery Nmap Scan Wizard.

Nmap Scan Options

Progress:

Enable Advanced Nmap Configuration Options.

Customize the text fields for this Fixlet message.

Note: If you choose to edit this page, the default title and messages will not be regenerated by the Wizard, even in the event you go back and modify previous input.

Edit the title:

Run Nmap with Custom Scan Options - Local Subnet (27/06/2019)

Edit the description:

This Fixlet message will run an Nmap scan over the local subnet of the Scan Point.


The following TCP ports will be scanned: 22 23 80 135 139 445 61616

The OS Detection option will be used.

Nmap will run service detection to probe open ports for running services.

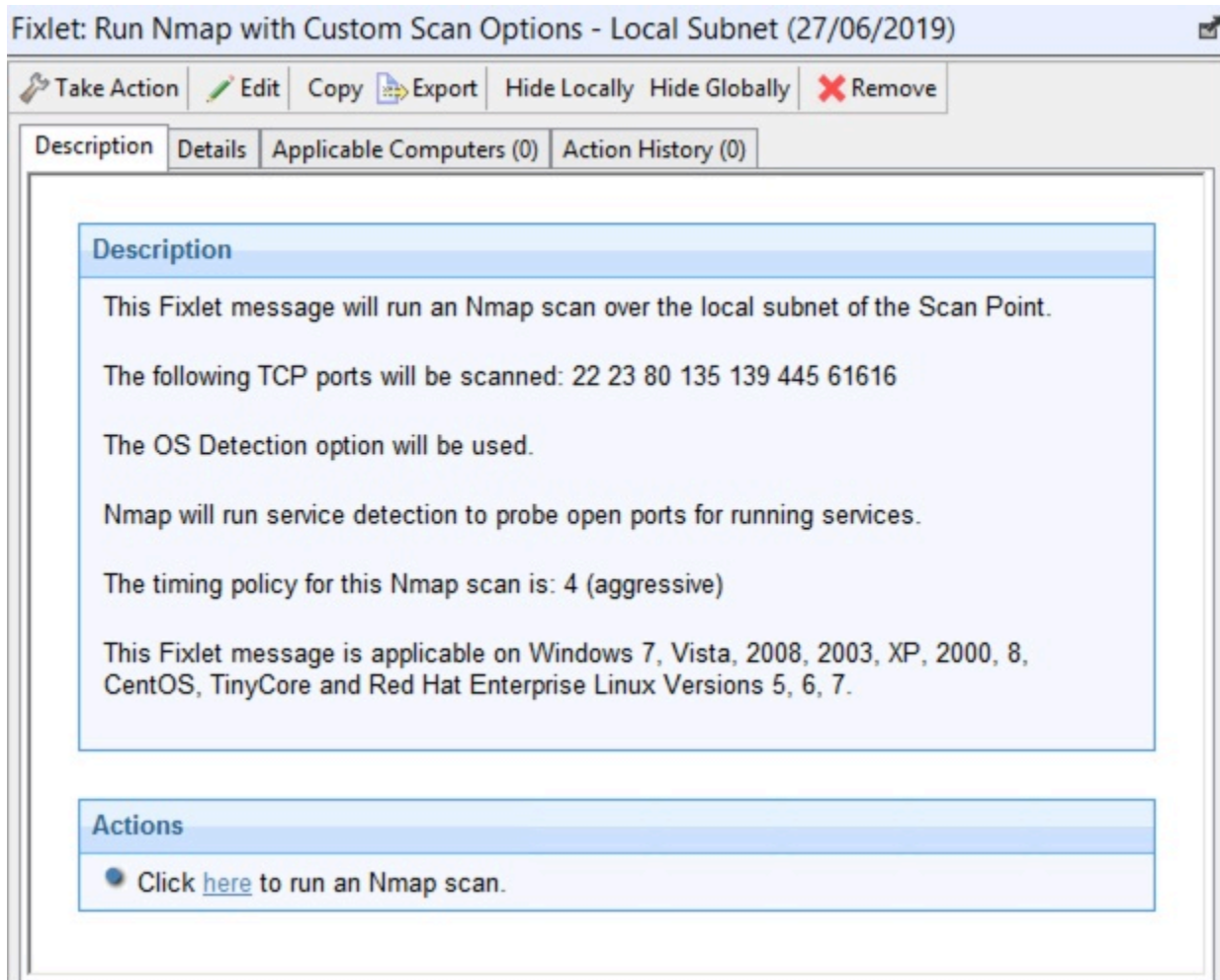
☐ Show Custom Fixlet Dialog before creating this Fixlet message.

Back

Finish 

Cancel

これにより、ウィザードで入力した固有のパラメーターおよびカスタマイズが含まれる Fixlet が表示されます。「説明」フィールドのテキストを確認し、「アクション」ボックス内の該当するリンクをクリックして、Nmap スキャンを実行します。



考慮事項

ライセンスとスキャンに関する潜在的な問題についての注意事項。

ライセンス交付

- スキャン・ポイントを指定するときは、Nmap と Npcap をインストールします。Nmap セキュリティー・スキャナーおよび Npcap パケット・キャプチャー・ライブラリーは Insecure.Com LLC のライセンスの下で BigFix 内で使用されています (The Nmap Project)。

スキャンに関する潜在的な問題

- ネットワーク・スキャンを実行すると、侵入検知システムが起動する可能性があります。この可能性を最小限に抑えるには、Nmap スキャン・モードを 0 (「Paranoid」) に設定するか、Nmap スキャンが許可されるように IDS を変更します。これにより、スキャンにかかる時間が長くなる場合があります。
- 一部のレガシー・ネットワーク・デバイス (古いネットワーク・プリンター・デバイスなど) では、ネットワーク・スキャンの実行が原因となってエラーが発生することがあります。
- ネットワーク・スキャンを実行すると、個人用ファイアウォールから、コンピューターがローカル・コンピューターをスキャンしていると通知される場合があります。Nmap スキャンを許可するように、ご使用のファイアウォールを変更してください。
- Nmap は、ウィルス・スキャン・プログラムによって、有害の恐れがあるツールとしてフラグが立てられる場合があります。ウィルス・スキャン・プログラムは、Nmap の実行を妨げないように設定してください。
- 大規模ネットワークをスキャンするように Nmap を設定した場合は、処理に数時間かかり、スキャン中にかなりの帯域幅を使用する可能性があります。デフォルトのスキャンはローカルのクラス C ネットワークであり、これは通常は高速 LAN です。WAN にまたがる大規模ネットワークをこのツールでスキャンすることはお勧めしません。
- Nmap を使用したスキャンは一般的にはいたって安全な操作ですが、対処が必要な組織固有の問題が存在する場合があります。作業に進む前に、ネットワーク・チームから適切な許可を得てください。
- スキャン・ポイント名に非 ASCII 文字を含めることはできません。非マスター・オペレーターが「スキャン・ポイント別」を実行する場合、または BigFix サーバーへのスキャン・レポートのアップロードに失敗する場合、非 ASCII 文字があると、非管理資産が見つからなくなる可能性があります。

第 4 章. Unmanaged Asset Importer - NMAP

インポーターを単体で実行するには、以下のオプションがコマンドライン引数として動作します。例えば、「UAImpoter-NMAP -debugout output.txt -file testfile.xml」です。



注: 同じ引数がクライアント設定としてまだ定義されていない場合のみ、コマンド行で指定された引数が考慮されます。それ以外の場合は、クライアント設定が使用されます。

Windows BigFix サーバー

これらのオプションは `HKLM\Software\BigFix\Enterprise Server\AssetDiscover\NMAP` の下にあります。

- "DSN"[REG_SZ]

リモート・データベースに使用される DSN。デフォルトは bes_bfenterprise です。

- "username"[REG_SZ]

SQL のユーザー名。デフォルト設定は NT 認証です。

- "password"[REG_SZ]

SQL のパスワード。デフォルト設定は NT 認証です。

- "file"[REG_SZ]

このファイルをデータベースにインポートするだけです。ファイルの形式は、

「nmap-NameOfYourChoice-1570442924」の形式にする必要があります。ここでは、「nmap」が接頭部で、「1570442924」がタイム・スタンプです。その間に任意の名前を入れます。

- "filedirectory"[REG_SZ]

このディレクトリー内のすべてのファイルをデータベースにインポートするだけです。

- "port"[REG_SZ]

BigFix クライアントを実行しながら、資産をフィルタリングによって除外する際に使用する BigFix ポート番号

- "filteroutclients"[REG_SZ]

BigFix クライアントをフィルタリングで除去するには 1 に設定、BigFix クライアントを含めるには 0 に設定します。デフォルトは 1 です。

- "serviceinterval"[REG_SZ]

資産のバッチのインポートを試行中にサービスがスリープすべき秒数。デフォルトは 300 です。

- "osfamilyclientexemptions"[REG_SZ]

os ファミリーのストリング。nmap によって、資産にこれらのファミリーの 1 つが含まれていると報告される場合、クライアントがないと見なされます。これは、デバイスがポート 52311 を listen しているため、クライアントがインストールされているとインポーターが見なす場合に役立ちます。しかし、クライアントがないのはプリンターやその他のデバイス・タイプであるため、クライアントが実行されていないことは明確です。デフォルトは「embedded;IOS;DYNIX」です。

- "usegmt"[REG_SZ]

「スキャン時刻」と「インポート時刻」をサーバーの時刻にするは 0 に設定、GMT にするには 1 に設定します。デフォルトは 0 です。

- "debugout"[REG_SZ]

このキーがファイルを指す場合、UnmanagedAssetImporter-NMAP はそのファイルにデバッグ出力を印刷します。デバッグ出力へのデフォルト・パスは "" です。

- "filteroutdownhosts"[REG_SZ]

1 に設定すると、状態が「ダウン」の資産をインポートしません。デフォルトは 1 です。

- "ignoredeletedassets"[REG_SZ]

1 の場合、削除された資産は無視され、以降のスキャンにおいて戻されません。0 の場合、削除された資産は再スキャンにおいて復元されます。デフォルトは 1 です。

Linux BigFix サーバー

これらのオプションは、besclient.config ファイルにあります。オプションの定義については、上記のセクションを参照してください。

- [Software\BigFix\EnterpriseClient\Settings\Client_AssetDiscovery_debugout]
- [Software\BigFix\EnterpriseClient\Settings\Client_AssetDiscovery_file]
- [Software\BigFix\EnterpriseClient\Settings\Client_AssetDiscovery_filedirectory]
- [Software\BigFix\EnterpriseClient\Settings\Client_AssetDiscovery_port]
- [Software\BigFix\EnterpriseClient\Settings\Client_AssetDiscovery_filteroutclients]
- [Software\BigFix\EnterpriseClient\Settings\Client_AssetDiscovery_serviceinterval]
- [Software\BigFix\EnterpriseClient\Settings\Client
_AssetDiscovery_osfamilyclientexemptions]
- [Software\BigFix\EnterpriseClient\Settings\Client_AssetDiscovery_usgmt]
- [Software\BigFix\EnterpriseClient\Settings\Client
_AssetDiscovery_filteroutdownhosts]
- [Software\BigFix\EnterpriseClient\Settings\Client
_AssetDiscovery_ignoreddeletedassets]

付録 A. よくある質問

よくある質問のリスト。

「非管理資産」はどのように識別されますか？

2つの「非管理資産」で、MAC アドレスが既知の場合、MAC が同じであれば一致となりますが、それ以外は一致となりません。2つの「非管理資産」で、MAC アドレスの1つが既知のものでなく、ホスト名が既知の場合、ホスト名が同じであれば一致となりますが、それ以外は一致となりません。両方の「非管理資産」に MAC アドレスもホスト名も無い場合、IP アドレスが同じであれば一致となりますが、それ以外は一致となりません。

スキャンを開始しましたが、結果はどこにありますか。

Asset Discovery を初めてインストールした場合は、最初にシステムをスキャンして非管理資産について報告するのに、数分かかる可能性があります。20 分経過しても BigFix コンソールに何も表示されない場合は、キーボードの F5 を押して、強制的にフル・リフレッシュを実行してください。

「非管理資産」タブは、どこに表示されるのですか。

「非管理資産」タブは、Nmap Asset Discovery インポート・サービスをインストールして初めて表示されます。インターフェースに表示されるのに数分かかる可能性があります。このタブが表示されたら、タブを開き、個々の資産をクリックして、その資産の詳細を確認することができます。

標準的なスキャンにはどのくらいの時間がかかりますか。

クラス C サブネットをスキャンすると、通常は 10 分から 30 分かかりますが、これは、ご使用のネットワークによって変わる可能性があります。より大規模なネットワークでは、スキャンの実行に数時間かかる場合があります。

帯域幅の要件はどのようになっていますか。

Nmap スキャン・プログラムは、帯域幅の問題を引き起こす可能性の低い、小さいパケットを送信します。これは、このプログラムが、高速ネットワーク上で近くにあるコンピュータをスキャンするように設計されていることが主な理由です。スキャンが完了すると、スキャン結果は BigFix サーバーにアップロードされます。通常、このファイルは比較的小さいファイルであり (一般に 10 KB から 200 KB)、スキャンされるエンドポイントの数によって異なります。1つのスキャン・ポイントで大規模ネットワークをスキャンする

と、ファイルのサイズは大きくなるがありますが、このようなスキャンは定期的にし
か実行されません。

どのくらいの頻度でスキャンを実行できますか。

Asset Discovery が正しくセットアップされている場合、ネットワークへの影響はほとん
でないため、スキャンをかなり頻繁に実行しても、問題はありません。無許可のネットワ
ーク・デバイスを検出するために、スキャンを 1 日に何度も実行してもかまいません。ある
いは、正確なネットワーク・インベントリー情報を維持するために、頻度を低くすること
もできます。

Nmap スキャン設定は変更できますか。

はい。デフォルトの Nmap スキャン設定は、高速で完全なスキャンを可能にします。この
設定は、必要に応じて Nmap 設定ウィザードで変更することができます。これにより、す
べての可能な Nmap 設定に対応できます。

**Importer が Nmap ユーティリティーの XML 出力から読み取ることができるデータはどれ
ですか。**

BigFix Asset Discovery Importer は、Nmap の結果から次のデータ (XML 属性) を読み取り
ます。

```
host: starttime=  
host:status: state= reason=  
host:hostnames:hostname: name=  
host:address: addr= addrtype= vendor=  
host:os:osmatch: name= accuracy=  
host:os:osmatch:osclass: accuracy= vendor= osfamily= osgen= type=  
host:ports:port: protocol= portid=  
host:ports:port:state: state=  
host:ports:port:service: name= product= version= extrainfo=  
runstats:finished: time=
```


付録 B. 用語集

この用語集は、BigFix の最新のクライアント管理ソフトウェアおよび製品の用語と定義を記載しています。

この用語集では次の相互参照が使用されています。

- 「を参照」は、非優先用語の場合は優先用語を、省略語の場合は省略していない形式を示すものです。
- 「も参照」は、関連する用語または対比される用語を示します。

[A \(\(ページ\) 33\)](#) [B \(\(ページ\) 34\)](#) [C \(\(ページ\) 35\)](#) [D \(\(ページ\) 37\)](#)
[E \(\(ページ\) 39\)](#) [F \(\(ページ\) 39\)](#) [G \(\(ページ\) 40\)](#) [L \(\(ページ\) 40\)](#)
[M \(\(ページ\) 40\)](#) [N \(\(ページ\) 42\)](#) [O \(\(ページ\) 42\)](#) [P \(\(ページ\) 42\)](#)
[R \(\(ページ\) 43\)](#) [S \(\(ページ\) 43\)](#) [T \(\(ページ\) 46\)](#) [U \(\(ページ\) 46\)](#) [V \(\(ページ\) 46\)](#) [W \(\(ページ\) 47\)](#)

A

アクション (action)

1. 「[Fixlet \(\(ページ\) 39\)](#)」を参照。
2. 操作タスクや管理用タスク (パッチのインストール、デバイスのリブートなど) を実行するアクション・スクリプト・コマンドのセット。

アクション・スクリプト (Action Script)

エンドポイントでアクションを実行するために使用する言語。

エージェント (agent)

「[BigFix エージェント \(BigFix agent\) \(\(ページ\) 34\)](#)」を参照。

あいまいなソフトウェア (ambiguous software)

別の実行可能ファイルとよく似た実行可能ファイルがあるソフトウェア、またはカタログ内の複数の場所に存在するソフトウェア (スタンドアロン製品と

しての Microsoft Word と Microsoft Office にバンドルされた Microsoft Word が存在する場合など)。

監査パッチ (audit patch)

修正不能であり管理者の確認を要する状態を検出するために使用されるパッチ。監査パッチにはアクションが含まれず、監査パッチをデプロイすることはできない。

自動コンピューター・グループ (automatic computer group)

指定されたデバイスのプロパティをグループ・メンバーシップに設定された基準と比較することにより、実行時にメンバーシップが決まるコンピューター・グループ。自動グループ内のデバイスのセットは動的である。これは、そのグループが変化する可能性があること、また実際に変化することを意味する。「[コンピューター・グループ \(\(ページ\) 35\)](#)」も参照。

B

ベースライン (baseline)

一緒にデプロイされるアクションの集合。ベースラインは、通常、デプロイメントを単純化するため、またはアクションのセットが適用される順序を制御するために使用される。「[デプロイメント・グループ \(deployment group\) \(\(ページ\) 37\)](#)」も参照。

BigFix エージェント (BigFix agent)

BigFix による管理とモニタリングを可能にするエンドポイント上の BigFix コード。

BigFix クライアント (BigFix client)

「[BigFix エージェント \(BigFix agent\) \(\(ページ\) 34\)](#)」を参照。

BigFix コンソール (BigFix console)

プライマリー BigFix 管理インターフェース。このコンソールは、完全な機能セットを BigFix 管理者に提供する。

BYOD

独自のデバイスを持ち込む (BYOD) とは、従業員が個人所有のデバイスを使用して組織ネットワークに接続し、業務関連システムや潜在的に重要または機密データにアクセスすることを指します。

C

クライアント (client)

サーバーからのサービスを要求するソフトウェア・プログラムまたはコンピューター。 [サーバー \(server\) \(\(ページ\) 44\)](#) も参照。

クライアント時間 (client time)

BigFix クライアント・デバイス上のローカル時間。

クラウド

コンテナまたは仮想マシンで実行されるコンピューターおよびストレージ・インスタンスまたはサービスのセット。

Common Vulnerabilities and Exposures 識別番号 (CVE ID) (Common Vulnerabilities and Exposures Identification Number (CVE ID))

National Vulnerability Database の特定のエントリーを識別する番号。ベンダーのパッチ文書には、通常、CVE ID が含まれる (CVE ID が使用可能な場合)。「[National Vulnerability Database \(\(ページ\) 42\)](#)」も参照。

Common Vulnerabilities and Exposures (CVE) システム (Common Vulnerabilities and Exposures system (CVE))

米国連邦情報・技術局 (NIST) が保守する National Vulnerabilities Database (NVD) の一部である公式に知られたネットワーク脆弱性の参照。

コンポーネント (component)

複数のアクションを含むデプロイメント内の個々のアクション。「[デプロイメント・グループ \(deployment group\) \(\(ページ\) 37\)](#)」も参照。

コンピューター・グループ (computer group)

関連するコンピューターのグループ。管理者はコンピューター・グループを作成して、システムを意味のあるカテゴリーに編成し、複数のコンピューター

ターへのコンテンツのデプロイメントを容易にできる。「[自動コンピューター・グループ \(\(ページ\) 34\)](#)」、「[手動コンピューター・グループ \(\(ページ\) 41\)](#)」も参照。

console (コンソール)

「[BigFix コンソール \(\(ページ\) 34\)](#)」を参照。

コンテンツ (content)

データ、ルール、クエリー、基準、その他の指示を含むデジタル署名されたファイル。ネットワーク全体でのデプロイメント用にパッケージ化されている。BigFix エージェントはコンテンツ内の検出基準 (Relevance ステートメント) およびアクション指示 (アクション・スクリプト・ステートメント) を使用して、脆弱性を検出したりネットワーク・ポリシーを施行したりする。

コンテンツの関連度 (content relevance)

パッチまたはソフトウェアが 1 つ以上のデバイスへのデプロイメントに適しているかどうかの判定。「[デバイスの関連度 \(\(ページ\) 39\)](#)」も参照。

協定世界時 (UTC) (Coordinated Universal Time (UTC))

世界中で原子時計によって保持される国際標準時。

問題のあるパッチ (corrupt patch)

前のパッチで行われた修正が変更または危殆化された場合にオペレーターに警告するパッチ。この状況は、前のサービス・パックまたはアプリケーションがより新しいファイルを上書きし、パッチが適用されたファイルが現行ファイルではなくなった場合に発生する可能性がある。問題のあるパッチによって、この状態にフラグが立てられる。これを使用して、より新しいパッチを再適用することができる。

カスタム・コンテンツ (custom content)

ユーザーが独自のネットワークで使用するために作成した BigFix コード (カスタム・パッチやカスタム・ベースラインなど)。

CVE

「[Common Vulnerabilities and Exposures システム \(\(ページ\) 35\)](#)」を参照。

CVE ID

「[Common Vulnerabilities and Exposures 識別番号 \(\(ページ\) 35\)](#)」を参照。

D

データ・ストリーム (data stream)

パッケージ・データのソースとして機能する情報のストリング。

デフォルト・アクション (default action)

Fixlet のデプロイ時に実行されるように指定されたアクション。デフォルト・アクションが定義されていない場合、オペレーターには、いくつかのアクションから選択するか、単一アクションに関する情報に基づく意思決定を行うように求めるプロンプトが出されます。

確定パッケージ (definitive package)

コンピューター上のソフトウェアの存在を識別するための主な方法となるデータのストリング。

適用 (deploy)

ソフトウェアのインストールやパッチの更新などの目的で、実行により操作やタスクを完了するために 1 つ以上のエンドポイントにコンテンツをディスパッチすること。

デプロイメント (deployment)

1 つ以上のエンドポイントにディスパッチされたコンテンツに関する情報 (ディスパッチされたコンテンツの特定のインスタンス)。

デプロイメント・グループ (deployment group)

オペレーターがデプロイメント用に複数のアクションを選択した場合、またはベースラインがデプロイされた場合に作成されたアクションの集合。「[ベースライン \(\(ページ\) 34\)](#)」、「[コンポーネント \(\(ページ\)](#)

35)」、[「デプロイメント・ウィンドウ \(\(ページ\) 38\)」](#)、[「複数のアクション・グループ \(\(ページ\) 41\)」](#) も参照。

デプロイメント状態 (deployment state)

エンドポイント上で実行するデプロイメントの適格性。状態には、オペレーターによって設定されたパラメーター (「Start at 1AM, end at 3AM」 など) が含まれる。

デプロイメント状況 (deployment status)

すべての対象デバイスの累積の結果。デプロイメントの成功のパーセンテージとして表示される。

デプロイメント・タイプ (deployment type)

デプロイメントに含まれるアクションが 1 つか複数かを示すもの。

デプロイメント期間 (deployment window)

デプロイメントのアクションが実行に適格である期間。例えば、Fixlet に 3 日間のデプロイメント期間があり、オフラインの適格デバイスがこの 3 日の期間内に BigFix に通信した場合、そのデバイスは Fixlet を取得します。この 3 日間の期限が切れた後にデバイスがオンラインに戻った場合、そのデバイスは Fixlet を取得しません。[「デプロイメント・グループ \(deployment group\) \(\(ページ\) 37\)」](#) も参照。

デバイス (device)

BigFix が管理しているラップトップ、デスクトップ、サーバー、仮想マシンなどのエンドポイント。BigFix エージェントを実行しているエンドポイント。

デバイスの所有者 (device holder)

BigFix 管理対象コンピューターを使用する個人。

デバイス・プロパティ (device property)

BigFix によって収集されたデバイスに関する情報 (デバイスのハードウェア、オペレーティング・システム、ネットワーク状況、設定、BigFix クライアン

トに関する詳細を含む)。カスタム・プロパティをデバイスに割り当てることもできる。

デバイスの関連度 (device relevance)

BigFix コンテンツの一部をデバイスに適用するか (パッチを適用する、ソフトウェアをインストールする、ベースラインを実行するなど) の判定。「[コンテンツの関連度 \(\(ページ\) 36\)](#)」も参照。

デバイスの結果 (device result)

特定のエンドポイントのデプロイメントの状態 (結果を含む)。

災害対策サーバー・アーキテクチャー (Disaster Server Architecture、DSA)

障害が発生した場合に備えて完全な冗長性を実現するために複数のサーバーをリンクするアーキテクチャー。

DSA

「[災害対策サーバー・アーキテクチャー \(DSA\) \(\(ページ\) 39\)](#)」を参照。

動的に対象指定 (dynamically targeted)

コンピューター・グループを使用してデプロイメントを対象にすることに関連する。

E

エンドポイント (endpoint)

BigFix エージェントを実行するネットワーク・デバイス。

F

フィルター (filter)

項目のリストを、特定の属性の項目に絞ること。

Fixlet

操作またはタスクを実行するために一緒にバンドルされた Relevance ステートメントおよびアクション・スクリプト・ステートメントを含む BigFix コン

テンツの一部。Fixlet は BigFix コンテンツの基本的なビルディング・ブロックである。Fixlet は、ネットワーク管理アクションやレポート・アクションを実行するために BigFix エージェントに指示を提供する。

フル・ディスク暗号化

項目のリストを、特定の属性の項目に絞ること。

G

グループ・デプロイメント (group deployment)

複数のアクションが 1 つ以上のデバイスにデプロイされたデプロイメントのタイプ。

H

ハイブリッド・クラウド

クラウド・サービスの異なるセット (通常はパブリック・クラウドとプライベート・クラウド) を最適に組み合わせて使用すること。

L

ロック済み (locked)

デバイスのロックが解除されるまで BigFix のアクションの大部分が実行できないエンドポイントの状態。

M

MAG

「[複数アクション・グループ \(\(ページ\) 41\)](#)」を参照。

管理権限 (management rights)

指定されたコンピューターのグループへのコンソール・オペレーターの制限。サイト管理者またはマスター・オペレーターのみが管理権限を割り当てることができる。

マニュアル・コンピューター・グループ (manual computer group)

オペレーターによる選択によってメンバーシップが決まるコンピューター・グループ。マニュアル・グループ内のデバイスの組み合わせは静的で、従って変化しない。「[コンピューター・グループ \(\(ページ\) 35\)](#)」も参照。

マスター・オペレーター (master operator)

管理権限を持つコンソール・オペレーター。マスター・オペレーターは、サイト管理者とほぼ同等のことを実行できるが、オペレーターを作成することはできない。

マストヘッド (masthead)

BigFix プロセス (Fixlet コンテンツへの URL など) のパラメーターを含むファイルの集合。BigFix エージェントは、サブスクライブされているマストヘッドに基づいてコンテンツを企業内に取り込む。

MCM と BigFix Mobile

ラップトップ (Windows、macOS) を管理する Modern Client Management と、モバイルデバイス (Android、iOS、iPadOS) を管理する BigFix Mobile の両方に共通する BigFix の機能を指す。

ミラー・サーバー (mirror server)

企業で直接の Web アクセスは許可していないが、代わりにパスワード・レベルの認証を必要とするプロキシ・サーバーを使用する場合に必要な BigFix サーバー。

マルチクラウド (Multicloud)

別個のクラウド・サービス・セットを使用すること。通常、複数ベンダーから提供され、特定のアプリケーション群は単一のクラウド・インスタンスに限定される。

複数アクション・グループ (MAG) (multiple action group (MAG))

ベースラインなどで複数のアクションが一緒にデプロイされたときに作成される BigFix オブジェクト。1 つの MAG には複数の Fixlet またはタスクが含まれる。「[デプロイメント・グループ \(deployment group\) \(\(ページ\) 37\)](#)」も参照。

N

National Vulnerability Database (NVD)

米国連邦情報・技術局 (NIST) が保持する公式に知られた情報セキュリティの脆弱性およびエクスポージャーのカatalog。「[Common Vulnerabilities and Exposures 識別番号 \(\(ページ\) 35\)](#)」も参照。

NVD

「[National Vulnerability Database \(\(ページ\) 42\)](#)」を参照。

O

オファー (offer)

デバイスの所有者が、BigFix アクションに同意するか同意しないこと、および実行時に何らかの制御を行うことを可能にするデプロイメントのオプション。例えば、デバイス所有者が、ソフトウェア・アプリケーションをインストールするかインストールしないか、インストールを夜間に実行するか昼間に実行するかを決定できる。

無期限のデプロイメント (open-ended deployment)

終了日も有効期限もないデプロイメント。継続的に実行され、ネットワーク上のコンピューターが準拠しているかを検査するものなど。

オペレーター (operator)

BigFix WebUI または BigFix コンソールの一部を使用する個人。

P

パッチ (patch)

問題を修正するために、2 つのリリースの間にユーザーに提供される当面のソリューションとしてベンダー・ソフトウェアに追加されるコードの断片。

パッチ・カテゴリー (patch category)

バグ修正やサービス・パックなど、パッチのタイプおよび操作の一般領域の説明。

パッチの重大度 (patch severity)

ネットワークの脅威または脆弱性によってもたらされるリスクのレベル、およびそれに関連してそのパッチを適用する重要度。

R

リレー (relay)

特殊なサーバー・ソフトウェアを実行しているクライアント。リレーは、サーバーとクライアントの間の直接ダウンロードを最小限に抑え、アップストリーム・データを圧縮することにより、サーバーとネットワークの負荷を軽減する。

関連度 (Relevance)

指定のエンドポイントへのコンテンツの適用可能性を判別するために使用される BigFix クエリー言語。関連度では「はい」または「いいえ」の質問が行われ、その結果が評価される。関連度のクエリーの結果により、アクションを適用できるか、またはアクションを適用する必要があるかが決定される。関連度は Fixlet のアクション・スクリプトと対になっている。

S

SCAP

「[Security Content Automation Protocol \(\(ページ\) 44\)](#)」を参照。

SCAP チェック (SCAP check)

Security Content Automation Protocol (SCAP) チェックリスト内の特定の構成チェック。チェック項目は XCCDF で記述されており、SCAP テンプレートに従って SCAP 列挙と SCAP マッピングを組み込む必要がある。

SCAP チェックリスト (SCAP checklist)

機械可読言語 (XCCDF) で記述された構成チェックリスト。Security Content Automation Protocol (SCAP) チェックリストは、NIST National Checklist Program に提出され、承認されている。これらは、SCAP 製品およびサービスとの互換性を確保するため、SCAP テンプレートにも準拠している。

SCAP コンテンツ (SCAP Content)

自動化 XML 形式で表されたセキュリティー・チェックリスト・データ、脆弱性および製品名関連の列挙、および列挙間のマッピングで構成されたりポジトリー。

SCAP 列挙 (SCAP enumeration)

すべて既知のセキュリティー関連ソフトウェア欠陥 (CVE)、既知のソフトウェア構成問題 (CCE)、および標準ベンダー名および製品名 (CPE) のリスト。

SCAP マッピング (SCAP mapping)

ソフトウェア欠陥および構成問題に対して標準ベースの影響の測定を提供する列挙の相互関係。

Security Content Automation Protocol (SCAP)

米国連邦情報・技術局 (NIST) による脆弱性およびコンプライアンスの自動化、測定、管理に使用される標準のセット。

サーバー (server)

他のソフトウェア・プログラムまたはコンピューターにサービスを提供するソフトウェア・プログラムまたはコンピューター。「[クライアント \(ページ 35\)](#)」も参照。

署名パスワード (signing password)

デプロイメント用のアクションに署名するためにコンソール・オペレーターが使用するパスワード。

単一デプロイメント (single deployment)

単一のアクションが 1 つ以上のデバイスにデプロイされたデプロイメントのタイプ。

サイト (site)

BigFix コンテンツの集合。サイトは、同様のコンテンツを一緒にまとめる。

サイト管理者 (site administrator)

BigFix のインストール、新規コンソール・オペレーターの承認と作成に関する責任者。

ソフトウェア・パッケージ (software package)

デバイスにソフトウェア製品をインストールする Fixlet の集合。ソフトウェア・パッケージは、配布のためにオペレーターによって BigFix にアップロードされる。BigFix ソフトウェア・パッケージには、インストール・ファイル、ファイルをインストールするための Fixlet、およびパッケージに関する情報 (メタデータ) が含まれる。

SQL Server

Microsoft が提供する完全なデータベース・エンジン。取得して BigFix システムにインストールすると、基本的なレポート作成とデータ・ストレージを超えるニーズを実現できる。

標準デプロイメント (standard deployment)

単一の管理ドメインを持つワークグループおよび企業に適用される BigFix のデプロイメント。すべてのクライアント・コンピューターが単一の社内サーバーに直接アクセスできる設定を目的としている。

静的に対象指定 (statistically targeted)

デバイスまたはコンテンツの一部に対してデプロイメントを対象指定するために使用する方式に関連する。静的に対象指定されたデバイスは、オペレーターによって手動で選択されている。

置き換えられたパッチ (superseded patch)

以前のバージョンのパッチがより新しいバージョンによって置き換えられている場合にオペレーターに通知するパッチのタイプ。新しいパッチが以前のパッチと同じファイルを更新した場合に発生する。置き換えられたパッチは、より新しいパッチで修正可能な脆弱性にフラグを立てる。置き換えられたパッチはデプロイできない。

システムの電源状態 (system power state)

システムの全体的な電力使用量の定義。BigFix 電源管理がトラッキングする主な電源状態は、「アクティブ」、「アイドル」、「スタンバイ」または「休止状態」、「電源オフ」の 4 つです。

T

対象 (target)

デプロイメント用のコンテンツを選択するか、コンテンツを受け取るデバイスを選択することにより、コンテンツをデプロイメント内のデバイスとマッチングすること。

対象指定 (targeting)

デプロイメント内のエンドポイントを指定するために使用する方式。

タスク (task)

継続中の保守タスクを実行するためなど、再使用のために設計された Fixlet のタイプ。

U

UTC

「[協定世界時 \(Coordinated Universal Time\)](#) ([ページ 36](#))」を参照。

V

仮想プライベート・ネットワーク (VPN) (virtual private network (VPN))

パブリック・ネットワークまたはプライベート・ネットワークの既存フレームワーク上で企業のイントラネットを拡張したもの。VPN を使用すると、接続の 2 つのエンドポイント間で送信されるデータを保護できる。

VPN

「[仮想プライベート・ネットワーク \(virtual private network\)](#) ([ページ 46](#))」を参照。

脆弱性 (vulnerability)

オペレーティング・システム、システム・ソフトウェア、またはアプリケーション・ソフトウェア・コンポーネントでの機密漏れ。

W

Wake-from-Standby

アプリケーションが、Wake on LAN を必要とせずに、事前定義された時間にコンピューターを待機モードから起動できるようにするモード。

Wake on LAN

時間外の保守のためにユーザーがシステムをリモートで起動できるテクノロジー。Intel と IBM の Advanced Manageability Alliance の成果であり、Wired for Management Baseline Specification の一部である。このテクノロジーのユーザーは、リモートでサーバーを起動したりネットワーク経由でサーバーを制御したりできるため、ソフトウェアのインストール、アップグレード、ディスク・バックアップ、およびウィルス・スキャンを自動化して時間を節約できる。

WAN

「[広域ネットワーク \(wide area network\)](#) ([ページ 47](#))」を参照。

広域ネットワーク (WAN) (wide area network (WAN))

ローカル・エリア・ネットワーク (LAN) や大都市圏ネットワーク (MAN) で提供されるよりも大きい地理上の領域で、デバイス間の通信サービスを提供するネットワーク。

付録 C. サポート

この製品について詳しくは、以下のリソースを参照してください。

- [BigFix サポート・ポータル](#)
- [BigFix Developer](#)
- [YouTube の BigFix プレイリスト](#)
- [YouTube の BigFix Tech Advisors チャンネル](#)
- [BigFix フォーラム](#)

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.