

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 48).

Edition notice

This edition applies to BigFix version 10 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。

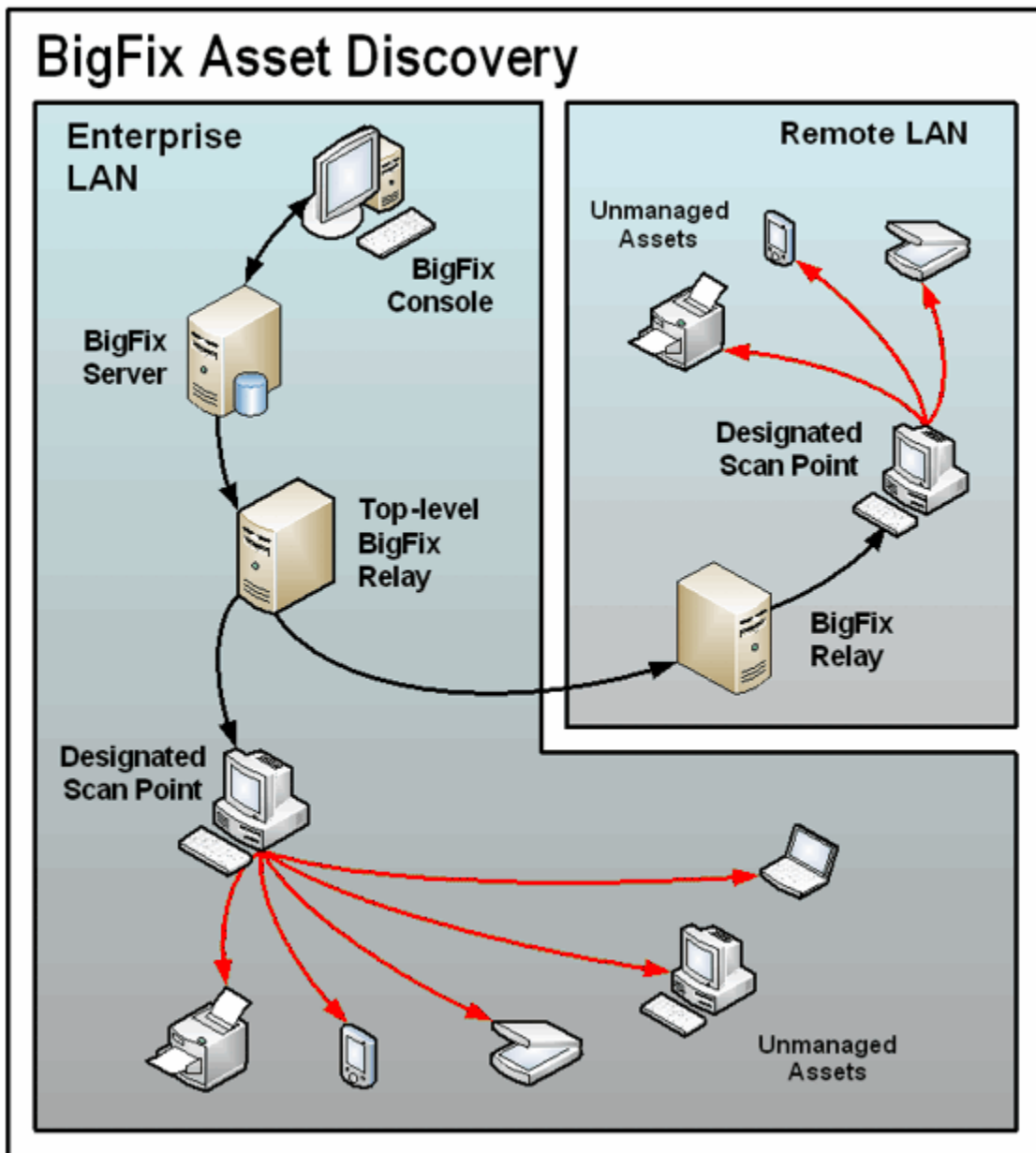


注: Linux プラットフォームでAsset Discovery Fixlet を使用するには、BES サーバー・プラグイン・サービスをインストールする必要があります。このプラグインは、BigFix サポート・サイトで入手して、インストールできます。

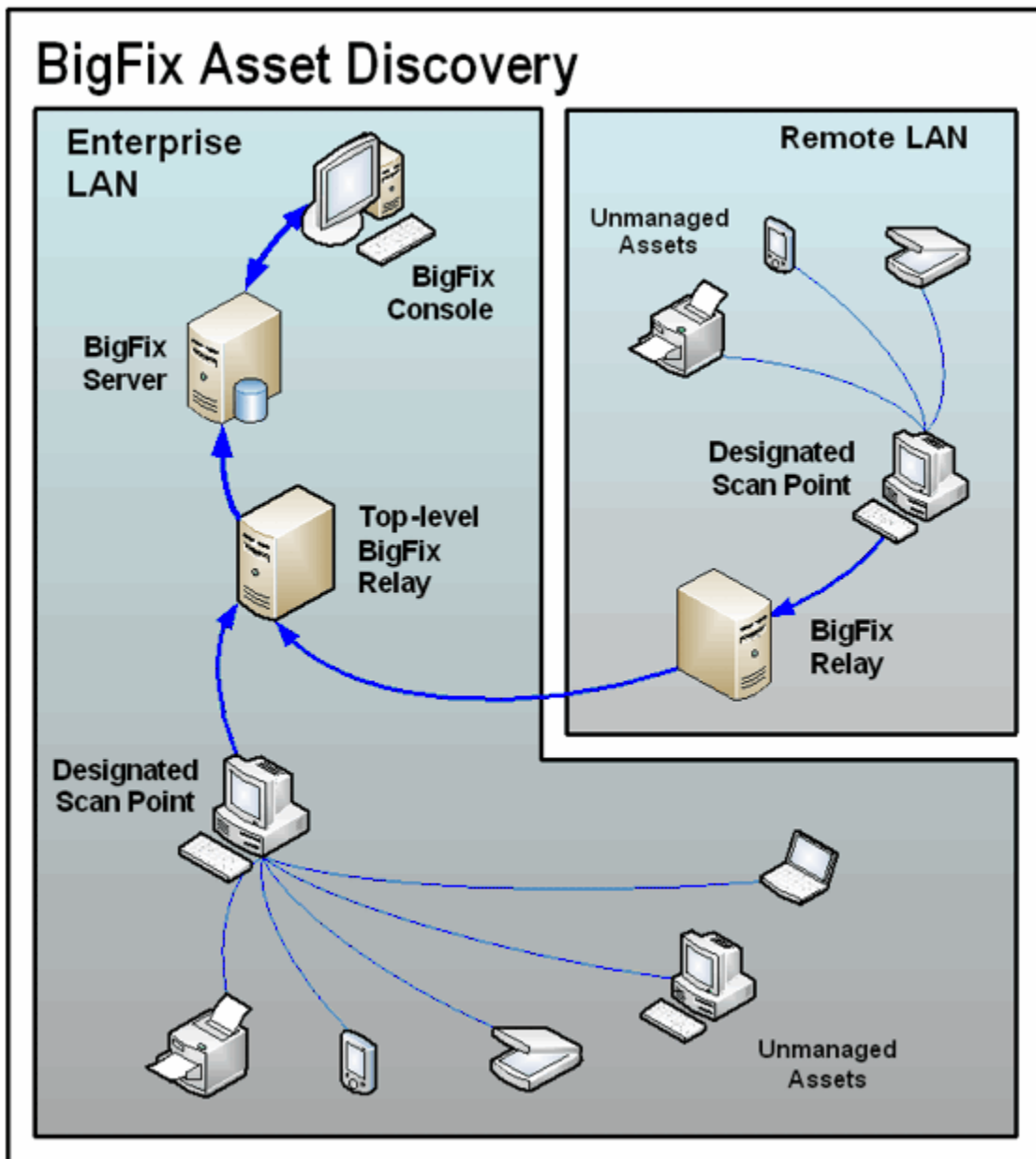
第 2 章. 概要

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。



システム要件

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 Asset Discovery では、Windows 7、Windows Vista、Windows 2008、Windows 2012、Windows 2016、Windows 2019、Windows 8、Windows 10 または Red Hat

Enterprise Linux 6、Red Hat Enterprise Linux 7、および Red Hat Enterprise Linux 8、x86-64 アーキテクチャーがサポートされます。

Red Hat Enterprise Linux 8、x86-64 アーキテクチャーでスキャン・ポイントを使用する前提条件として、`compat-openssl10.x86-64` パッケージをインストールする必要があります。

さらに、Nmap の旧バージョンでは、BigFix Asset Discovery は Red Hat Linux 5、CentOS 5、および Linux Tiny Core 8.2. もサポートします。

BigFix Asset Discovery では Amazon Linux 2 はサポートされません。

nmap.org Web サイトによると、Nmap では、Windows 7 以降、および Windows Server 2008 以降がサポートされます。また、Nmap は Linux オペレーティング・システムもサポートします。

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。



注: インポーター・サービスが正しく作動するには、Windows システムでデータ実行防止 (DEP) を無効にしておく必要があります。

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。

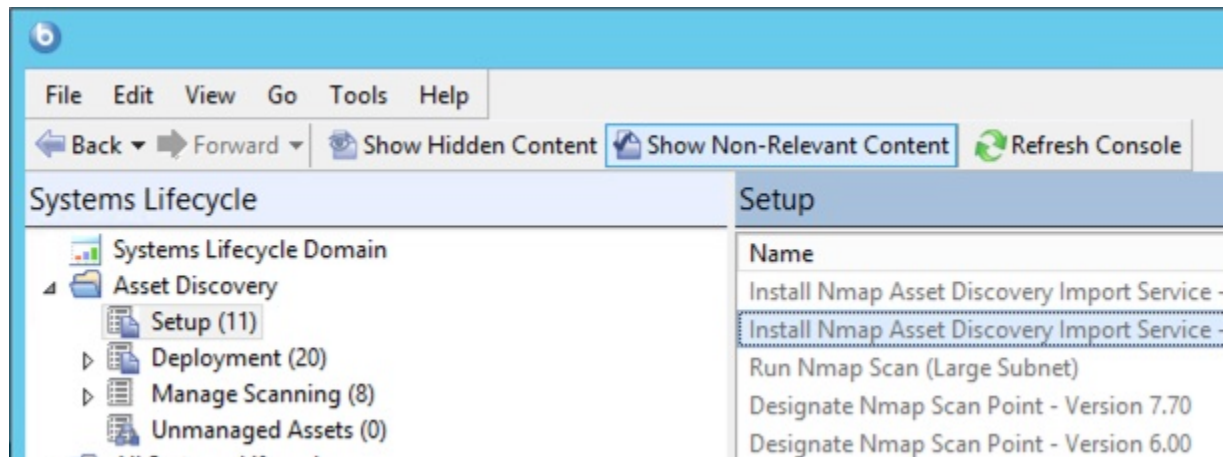
インポート・サービス・タスクのインストール

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。

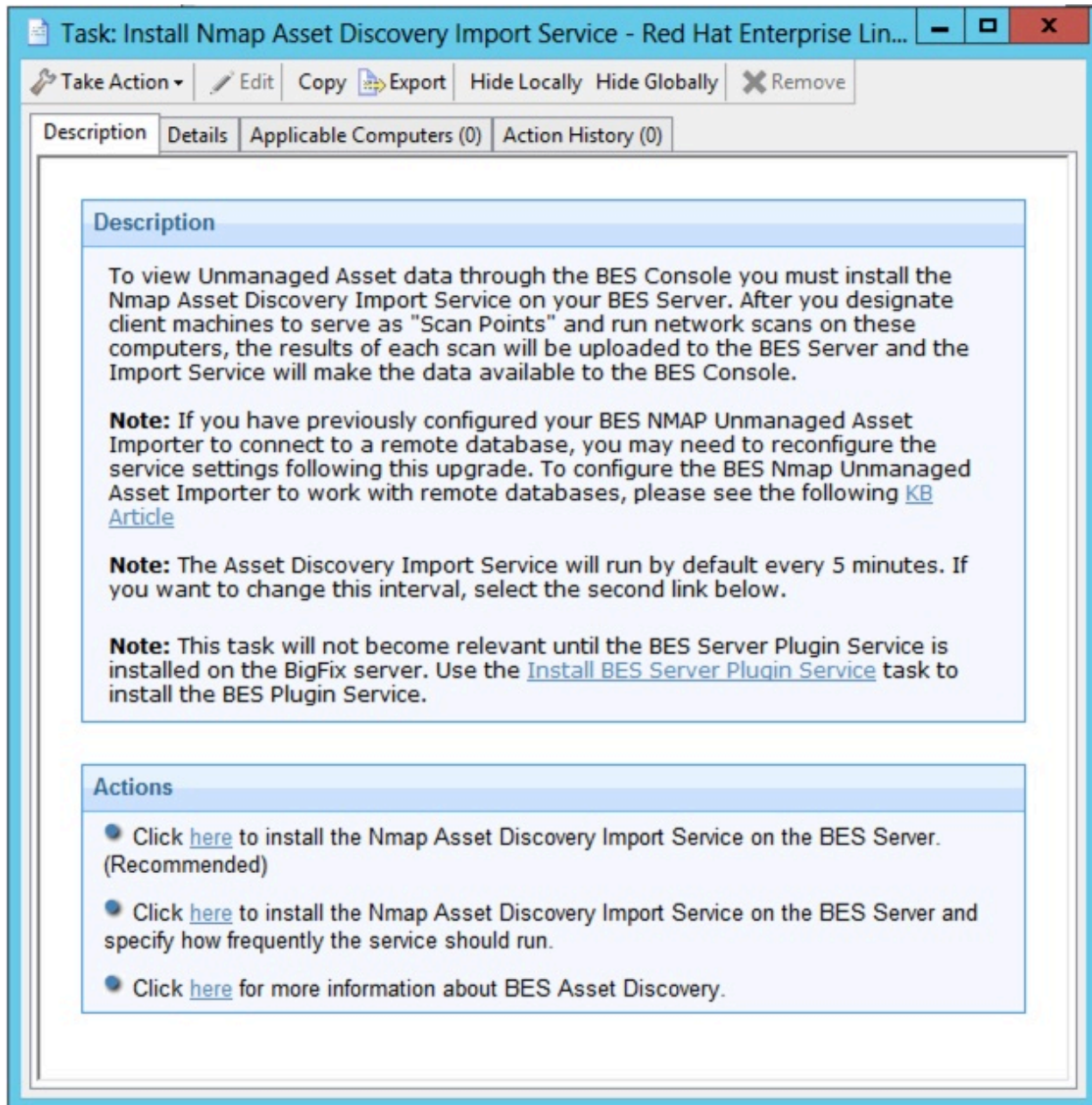


注: リモート・データベースにアクセスする場合は、NMAP インポート・サービスをドメイン・ユーザーとして実行する必要があります。これは、SQL データベースへのアクセスには標準ローカル・システムを使用することができないからです。このサービスは、リモート・データベース環境内の他の BigFix サービスと同様に構成する必要があります。

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。



The screenshot shows a web interface window titled "Task: Install Nmap Asset Discovery Import Service - Red Hat Enterprise Lin...". The window has a toolbar with buttons for "Take Action", "Edit", "Copy", "Export", "Hide Locally", "Hide Globally", and "Remove". Below the toolbar are tabs for "Description", "Details", "Applicable Computers (0)", and "Action History (0)". The "Description" tab is active, showing a text area with the following content:

Description

To view Unmanaged Asset data through the BES Console you must install the Nmap Asset Discovery Import Service on your BES Server. After you designate client machines to serve as "Scan Points" and run network scans on these computers, the results of each scan will be uploaded to the BES Server and the Import Service will make the data available to the BES Console.

Note: If you have previously configured your BES NMAP Unmanaged Asset Importer to connect to a remote database, you may need to reconfigure the service settings following this upgrade. To configure the BES Nmap Unmanaged Asset Importer to work with remote databases, please see the following [KB Article](#)

Note: The Asset Discovery Import Service will run by default every 5 minutes. If you want to change this interval, select the second link below.

Note: This task will not become relevant until the BES Server Plugin Service is installed on the BigFix server. Use the [Install BES Server Plugin Service](#) task to install the BES Plugin Service.

Actions

- Click [here](#) to install the Nmap Asset Discovery Import Service on the BES Server. (Recommended)
- Click [here](#) to install the Nmap Asset Discovery Import Service on the BES Server and specify how frequently the service should run.
- Click [here](#) for more information about BES Asset Discovery.

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。

The screenshot shows the BigFix Console interface. The left sidebar displays the 'Systems Lifecycle' tree with 'Asset Discovery' > 'Setup (11)' selected. The main area shows a table of tasks:

Name	Source Severity	Site	A
Install Nmap Asset Discovery Import Service - BES <= 6.0	<Unspecified>	BES Asset Discov...	0
Designate Nmap Scan Point - Version 6.00	<Unspecified>	BES Asset Discov...	0
Run Nmap Scan	<Unspecified>	BES Asset Discov...	0
Run Nmap Scan (Large Subnet)	<Unspecified>	BES Asset Discov...	0
Run Nmap Scan - Red Hat Enterprise Linux CentOS TinyCo...	<Unspecified>	BES Asset Discov...	0
Designate Nmap Scan Point - Red Hat Enterprise Linux Cent...	<Unspecified>	BES Asset Discov...	0
Run Nmap Scan (Large Subnet) - Red Hat Enterprise Linux ...	<Unspecified>	BES Asset Discov...	0
Designate Nmap Scan Point - Version 7.70	<Unspecified>	BES Asset Discov...	0
Designate Nmap Scan Point - Red Hat Enterprise Linux Cent...	<Unspecified>	BES Asset Discov...	0
Install Nmap Asset Discovery Import Service - Red Hat Enter...	<Unspecified>	BES Asset Discov...	0
Install Nmap Asset Discovery Import Service - BES >= 7.0	<Unspecified>	BES Asset Discov...	0

The 'Task: Designate Nmap Scan Point - Version 6.00' is selected. Below the table, the task's description is shown:

Description

This Task will deploy Nmap and WinPcap to targeted machines and designate them as "Scan Points". After this Task completes, you will be able to initiate network scans to search for unmanaged computers and network devices from each selected "Scan Point". The results of each scan will be uploaded to the BES Server and the Import Service will make the data available to the BES Console.

Note: Nmap is an open-source utility for network scanning. You must accept

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 を実行していなければなりません。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。

Info-zip の使用許諾契約を確認することもできます。

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。

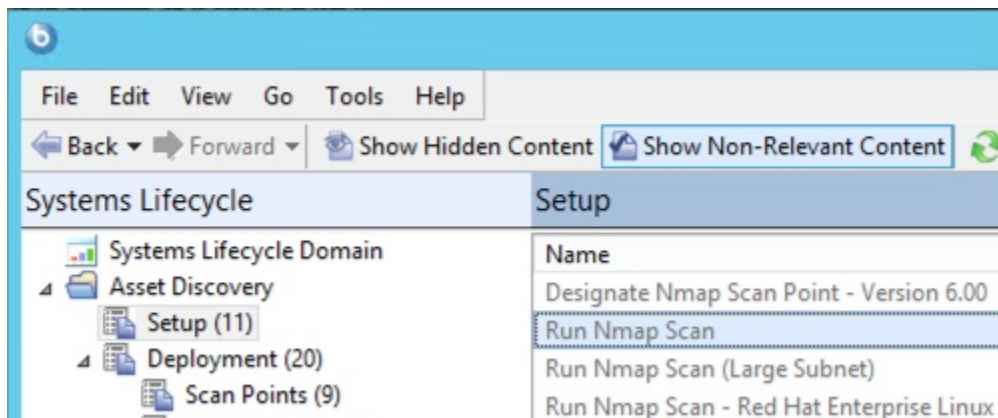
Linux の場合、「Nmap スキャン・ポイントの指定 - Red Hat Enterprise Linux」タスクをクリックします。

「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

操作

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 shows the BigFix Console interface. The main window is titled 'Scan Point Statistics' and contains a table with the following data:

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

Below the table, there is a section titled 'Analysis: Nmap Scan Point Statistics - Windows'. It includes a 'Description' tab and a 'Details' tab. The 'Description' tab is active, showing the following text:

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

The interface also shows a sidebar with 'Systems Lifecycle' and 'All Systems Lifecycle' sections, and a bottom status bar indicating '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」ノードの下の「スキャン・ポイント」をクリックします。

Deployment		Search Deployment	
Name	Source Severity	Site	Applica
Designate Nmap Scan Point - Version 7.70	<Unspecified>	BES Asset Discov...	0 / 0
Remove Nmap Scan Point - Version >= 7.70	<Unspecified>	BES Asset Discov...	0 / 0
Designate Nmap Scan Point - Red Hat Enterprise Linux CentOS - Version 7.70	<Unspecified>	BES Asset Discov...	0 / 0
Upgrade Nmap - Version 6.00		BES Asset Discov...	0 / 0
Change UAImporter Delete Mode		BES Asset Discov...	0 / 0

< III

Task: Remove Nmap Scan Point - Version >= 7.70

Take Action ▾ Edit Copy Export Hide Locally Hide Globally Remove

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

Description

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.

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

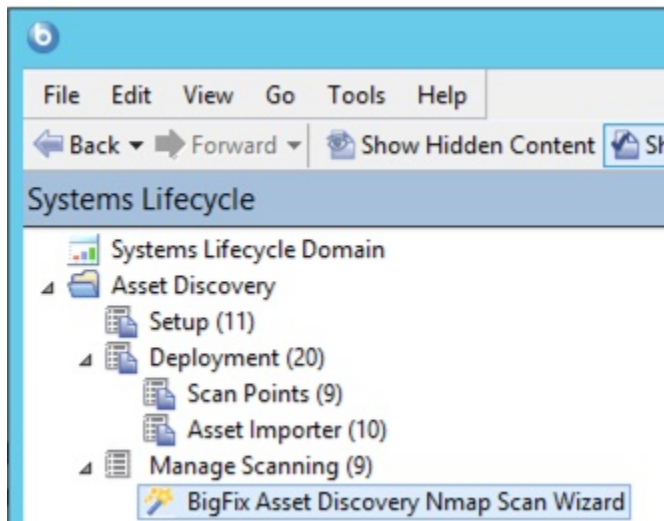
Nmap スキャナーを要件に合わせてカスタマイズする方法について説明します。

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。

 **注:** Linux システムで SELINUX が適用されている場合、Nmap スキャンは実行できません。


ナビゲーション・ツリーの「スキャンを管理」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.

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)

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.


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

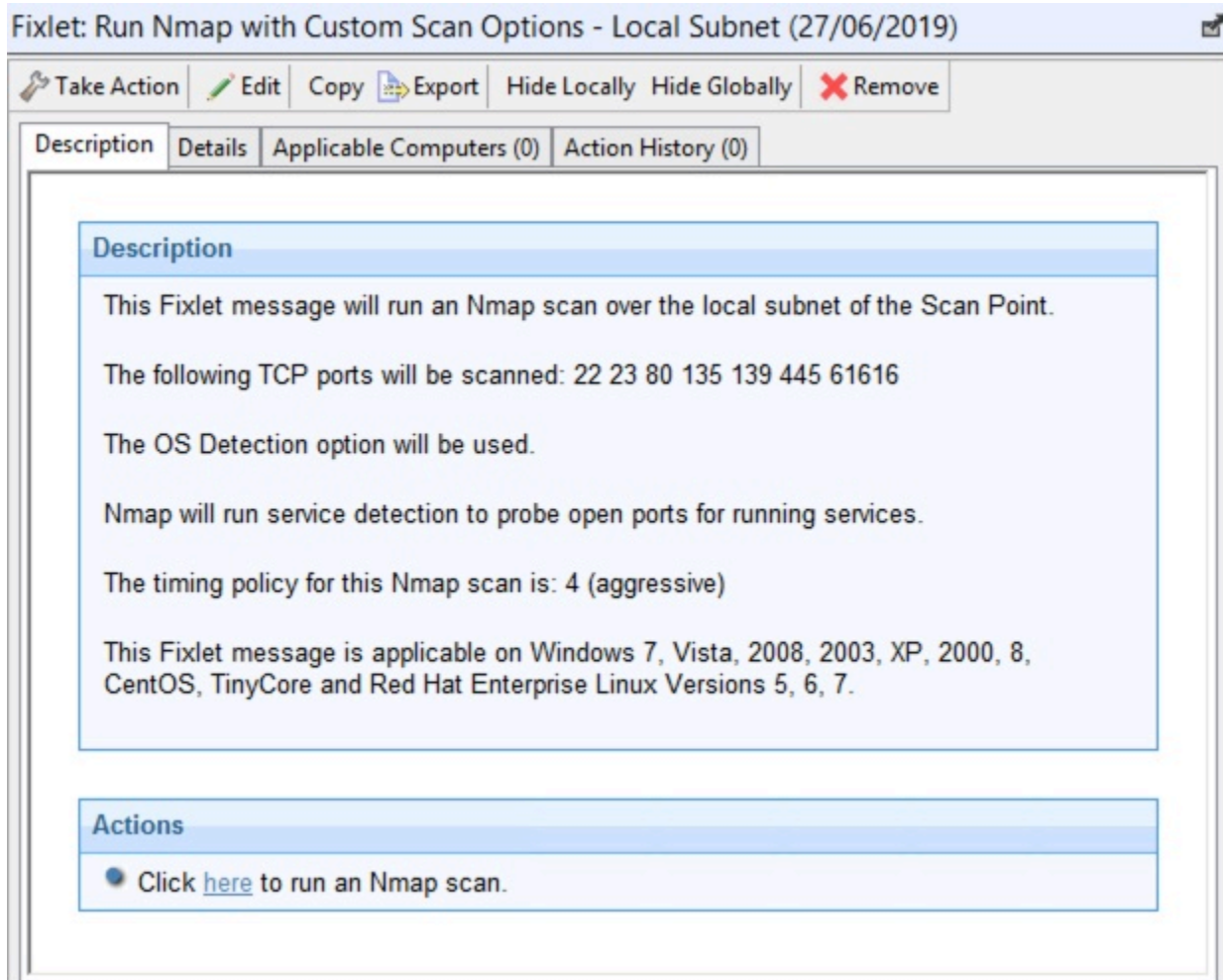
The OS Detection option will be used.

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

- 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)。

- Nmap は .zip ファイルとして配布されます。このファイルを解凍するために、BigFix は一時的に Info-Zip の解凍ツールをダウンロードして使用します。Info-Zip は、オープン・ソース解凍ユーティリティです。Info-Zip について詳しくは、<http://www.info-zip.org/> を参照してください。

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、「UAImporater-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ー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
どないため、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=
```


Appendix B. Glossary

This glossary provides terms and definitions for the Modern Client Management for BigFix software and products.

The following cross-references are used in this glossary:

- *See* refers you from a non-preferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

[A \(on page 33\)](#) [B \(on page 34\)](#) [C \(on page 35\)](#) [D \(on page 37\)](#) [E \(on page 39\)](#) [F \(on page 39\)](#) [G \(on page 39\)](#) [L \(on page 39\)](#) [M \(on page 40\)](#) [N \(on page 41\)](#) [O \(on page 41\)](#) [P \(on page 42\)](#) [R \(on page 42\)](#) [S \(on page 42\)](#) [T \(on page 45\)](#) [U \(on page 45\)](#) [V \(on page 45\)](#) [W \(on page 46\)](#)

A

action

1. See [Fixlet \(on page 39\)](#).
2. A set of Action Script commands that perform an operation or administrative task, such as installing a patch or rebooting a device.

Action Script

Language used to perform an action on an endpoint.

agent

See [BigFix agent \(on page 34\)](#).

ambiguous software

Software that has an executable file that looks like another executable file, or that exists in more than one place in a catalog (Microsoft Word as a standalone product or bundled with Microsoft Office).

audit patch

A patch used to detect conditions that cannot be remediated and require the attention of an administrator. Audit patches contain no actions and cannot be deployed.

automatic computer group

A computer group for which membership is determined at run time by comparing the properties of a given device against the criteria set for group membership. The set of devices in an automatic group is dynamic, meaning that the group can and does change. See also [computer group \(on page 35\)](#).

B

baseline

A collection of actions that are deployed together. A baseline is typically used to simplify a deployment or to control the order in which a set of actions are applied. See also [deployment group \(on page 37\)](#).

BigFix agent

The BigFix code on an endpoint that enables management and monitoring by BigFix.

BigFix client

See [BigFix agent \(on page 34\)](#).

BigFix console

The primary BigFix administrative interface. The console provides a full set of capabilities to BigFix administrators.

BYOD

Bring Your Own Device (BYOD) refers to employees using personal devices to connect to their organizational networks and access work-related systems and potentially sensitive or confidential data.

C

client

A software program or computer that requests services from a server. See also [server \(on page 43\)](#).

client time

The local time on a BigFix client device.

Cloud

A set of compute and storage instances or services that are running in containers or on virtual machines.

Common Vulnerabilities and Exposures Identification Number (CVE ID)

A number that identifies a specific entry in the National Vulnerability Database. A vendor's patch document often includes the CVE ID, when it is available. See also [National Vulnerability Database \(on page 41\)](#).

Common Vulnerabilities and Exposures system (CVE)

A reference of officially known network vulnerabilities, which is part of the National Vulnerabilities Database (NVD), maintained by the US National Institute of Standards and Technology (NIST).

component

An individual action within a deployment that has more than one action. See also [deployment group \(on page 37\)](#).

computer group

A group of related computers. An administrator can create computer groups to organize systems into meaningful categories, and to facilitate deployment of content to multiple computers. See also [automatic computer group \(on page 34\)](#) and [manual computer group \(on page 40\)](#).

console

See [BigFix console \(on page 34\)](#).

content

Digitally-signed files that contain data, rules, queries, criteria, and other instructions, packaged for deployment across a network. BigFix agents use the detection criteria (Relevance statements) and action instructions (Action Script statements) in content to detect vulnerabilities and enforce network policies.

content relevance

A determination of whether a patch or piece of software is eligible for deployment to one or more devices. See also [device relevance \(on page 38\)](#).

Coordinated Universal Time (UTC)

The international standard of time that is kept by atomic clocks around the world.

corrupt patch

A patch that flags an operator when corrections made by an earlier patch have been changed or compromised. This situation can occur when an earlier service pack or application overwrites later files, which results in patched files that are not current. The corrupt patch flags the situation and can be used to re-apply the later patch.

custom content

BigFix code that is created by a customer for use on their own network, for example, a custom patch or baseline.

CVE

See [Common Vulnerabilities and Exposures system \(on page 35\)](#).

CVE ID

See [Common Vulnerabilities and Exposures Identification Number \(on page 35\)](#).

D

data stream

A string of information that serves as a source of package data.

default action

The action designated to run when a Fixlet is deployed. When no default action is defined, the operator is prompted to choose between several actions or to make an informed decision about a single action.

definitive package

A string of data that serves as the primary method for identifying the presence of software on a computer.

deploy

To dispatch content to one or more endpoints for execution to accomplish an operation or task, for example, to install software or update a patch.

deployment

Information about content that is dispatched to one or more endpoints, a specific instance of dispatched content.

deployment group

The collection of actions created when an operator selects more than one action for a deployment, or a baseline is deployed. See also [baseline \(on page 34\)](#), [component \(on page 35\)](#), [deployment window \(on page 38\)](#), and [multiple action group \(on page 41\)](#).

deployment state

The eligibility of a deployment to run on endpoints. The state includes parameters that the operator sets, such as 'Start at 1AM, end at 3AM.'

deployment status

Cumulative results of all targeted devices, expressed as a percentage of deployment success.

deployment type

An indication of whether a deployment involved one action or multiple actions.

deployment window

The period during which a deployment's actions are eligible to run. For example, if a Fixlet has a deployment window of 3 days and an eligible device that has been offline reports in to BigFix within the 3-day window, it gets the Fixlet. If the device comes back online after the 3-day window expires, it does not get the Fixlet. See also [deployment group \(on page 37\)](#).

device

An endpoint, for example, a laptop, desktop, server, or virtual machine that BigFix manages; an endpoint running the BigFix Agent.

device holder

The person using a BigFix-managed computer.

device property

Information about a device collected by BigFix, including details about its hardware, operating system, network status, settings, and BigFix client. Custom properties can also be assigned to a device.

device relevance

A determination of whether a piece of BigFix content applies to applies to a device, for example, where a patch should be applied, software installed, or a baseline run. See also [content relevance \(on page 36\)](#).

device result

The state of a deployment, including the result, on a particular endpoint.

Disaster Server Architecture (DSA)

An architecture that links multiple servers to provide full redundancy in case of failure.

DSA

See [Disaster Server Architecture \(on page 38\)](#).

dynamically targeted

Pertaining to using a computer group to target a deployment.

E**endpoint**

A networked device running the BigFix agent.

F**filter**

To reduce a list of items to those that share specific attributes.

Fixlet

A piece of BigFix content that contains Relevance and Action Script statements bundled together to perform an operation or task. Fixlets are the basic building blocks of BigFix content. A Fixlet provides instructions to the BigFix agent to perform a network management or reporting action.

Full Disk Encryption

To reduce a list of items to those that share specific attributes.

G**group deployment**

A type of deployment in which multiple actions were deployed to one or more devices.

L**locked**

An endpoint state that prevents most of the BigFix actions from running until the device is unlocked.

M

MAG

See [multiple action group \(on page 41\)](#).

management rights

The limitation of console operators to a specified group of computers. Only a site administrator or a master operator can assign management rights.

manual computer group

A computer group for which membership is determined through selection by an operator. The set of devices in a manual group is static, meaning they do not change. See also [computer group \(on page 35\)](#).

master operator

A console operator with administrative rights. A master operator can do everything that a site administrator can do, except creating operators.

masthead

A collection of files that contain the parameters of the BigFix process, including URLs to Fixlet content. The BigFix agent brings content into the enterprise based on subscribed mastheads.

MCM and BigFix Mobile

Refers to the offering by Bigfix that is common for both Modern Client Management to manage laptops (Windows and macOS) and BigFix Mobile to manage mobile devices (Android, iOS, and iPadOS).

mirror server

A BigFix server required if the enterprise does not allow direct web access but instead uses a proxy server that requires password-level authentication.

Multicloud

The utilization of distinct sets of cloud services, typically from multiple vendors, where specific applications are confined to a single cloud instance.

multiple action group (MAG)

A BigFix object that is created when multiple actions are deployed together, as in a baseline. A MAG contains multiple Fixlets or tasks. See also [deployment group \(on page 37\)](#).

N

National Vulnerability Database (NVD)

A catalog of officially known information security vulnerabilities and exposures, which is maintained by the National Institute of Standards and Technology (NIST). See also [Common Vulnerabilities and Exposures Identification Number \(on page 35\)](#).

NVD

See [National Vulnerability Database \(on page 41\)](#).

O

offer

A deployment option that allows a device holder to accept or decline a BigFix action and to exercise some control over when it runs. For example, a device holder can decide whether to install a software application, and whether to run the installation at night or during the day.

open-ended deployment

A deployment with no end or expiration date; one that runs continuously, checking whether the computers on a network comply.

operator

A person who uses the BigFix WebUI, or portions of the BigFix console.

P

patch

A piece of code added to vendor software to fix a problem, as an immediate solution that is provided to users between two releases.

patch category

A description of a patch's type and general area of operation, for example, a bug fix or a service pack.

patch severity

The level of risk imposed by a network threat or vulnerability and, by extension, the importance of applying its patch.

R

relay

A client that is running special server software. Relays spare the server and the network by minimizing direct server-client downloads and by compressing upstream data.

Relevance

BigFix query language that is used to determine the applicability of a piece of content to a specified endpoint. Relevance asks yes or no questions and evaluates the results. The result of a Relevance query determines whether an action can or should be applied. Relevance is paired with Action Script in Fixlets.

S

SCAP

See [Security Content Automation Protocol \(on page 43\)](#).

SCAP check

A specific configuration check within a Security Content Automation Protocol (SCAP) checklist. Checks are written in XCCDF and are required to include SCAP enumerations and mappings per the SCAP template.

SCAP checklist

A configuration checklist that is written in a machine-readable language (XCCDF). Security Content Automation Protocol (SCAP) checklists have been submitted to and accepted by the NIST National Checklist Program. They also conform to a SCAP template to ensure compatibility with SCAP products and services.

SCAP content

A repository that consists of security checklist data represented in automated XML formats, vulnerability and product name related enumerations, and mappings between the enumerations.

SCAP enumeration

A list of all known security related software flaws (CVEs), known software configuration issues (CCEs), and standard vendor and product names (CPEs).

SCAP mapping

The interrelationship of enumerations that provides standards-based impact measurements for software flaws and configuration issues.

Security Content Automation Protocol (SCAP)

A set of standards that is used to automate, measure, and manage vulnerability and compliance by the National Institute of Standards and Technology (NIST).

server

A software program or a computer that provides services to other software programs or other computers. See also [client](#) (*on page 35*).

signing password

A password that is used by a console operator to sign an action for deployment.

single deployment

A type of deployment where a single action was deployed to one or more devices.

site

A collection of BigFix content. A site organizes similar content together.

site administrator

The person who is in charge of installing BigFix and authorizing and creating new console operators.

software package

A collection of Fixlets that install a software product on a device. Software packages are uploaded to BigFix by an operator for distribution. A BigFix software package includes the installation files, Fixlets to install the files, and information about the package (metadata).

SQL Server

A full-scale database engine from Microsoft that can be acquired and installed into the BigFix system to satisfy more than the basic reporting and data storage needs.

standard deployment

A deployment of BigFix that applies to workgroups and to enterprises with a single administrative domain. It is intended for a setting in which all Client computers have direct access to a single internal server.

statistically targeted

Pertaining to the method used to target a deployment to a device or piece of content. Statically targeted devices are selected manually by an operator.

superseded patch

A type of patch that notifies an operator when an earlier version of a patch has been replaced by a later version. This occurs when a later patch updates the same files as an earlier one. Superseded patches flag vulnerabilities that can be remediated by a later patch. A superseded patch cannot be deployed.

system power state

A definition of the overall power consumption of a system. BigFix Power Management tracks four main power states Active, Idle, Standby or Hibernation, and Power Off.

T

target

To match content with devices in a deployment, either by selecting the content for deployment, or selecting the devices to receive content.

targeting

The method used to specify the endpoints in a deployment.

task

A type of Fixlet designed for re-use, for example, to perform an ongoing maintenance task.

U

UTC

See [Coordinated Universal Time \(on page 36\)](#).

V

virtual private network (VPN)

An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure.

VPN

See [virtual private network \(on page 45\)](#).

vulnerability

A security exposure in an operating system, system software, or application software component.

W

Wake-from-Standby

A mode that allows an application to turn a computer on from standby mode during predefined times, without the need for Wake on LAN.

Wake on LAN

A technology that enables a user to remotely turn on systems for off-hours maintenance. A result of the Intel-IBM Advanced Manageability Alliance and part of the Wired for Management Baseline Specification, users of this technology can remotely turn on a server and control it across the network, thus saving time on automated software installations, upgrades, disk backups, and virus scans.

WAN

See [wide area network \(on page 46\)](#).

wide area network (WAN)

A network that provides communication services among devices in a geographic area larger than that served by a local area network (LAN) or a metropolitan area network (MAN).

Appendix C. Support

For more information about this product, see the following resources:

- [BigFix Support Portal](#)
- [BigFix Developer](#)
- [BigFix Playlist on YouTube](#)
- [BigFix Tech Advisors channel on YouTube](#)
- [BigFix Forum](#)

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.