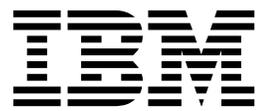


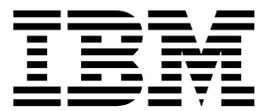
IBM Endpoint Manager
Version 9.1

Asset Discovery User's Guide



IBM Endpoint Manager
Version 9.1

Asset Discovery User's Guide



Note

Before using this information and the product it supports, read the information in "Notices" on page 25.

This edition applies to version 9, release 1, modification level 0 of IBM Endpoint Manager and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2013, 2014.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1. Setting up your environment	1	Considerations	18
Chapter 2. Overview	3	Appendix A. Frequently asked questions	21
System requirements.	4	Appendix B. Support.	23
Installation	4	Notices	25
Installing the site	5	Programming interface information	27
Installing the Import Service task	5	Trademarks	27
Installing Scan Points	6	Terms and conditions for product documentation.	28
Running a scan	9		
Chapter 3. Using Asset Discovery	13		
Operation	13		
Using the Nmap Scan Wizard	14		

Chapter 1. Setting up your environment

IBM Endpoint Manager Asset Discovery has some key uses in enterprise environments:

- Identification of network assets – including devices such as routers, printers, switches, wireless access points, or anything with an IP address.
- Identification of unmanaged and rogue computers including computers that have had the IBM Endpoint Manager agent disabled or rogue computers that are not managed by the company.

With this information, important license inventory questions can be answered regarding what kind of device it is, when it was installed and where it is located. Additionally, security questions and concerns can be answered regarding unauthorized employee computers, wireless units or rogue devices on the network.

The IBM Endpoint Manager Asset Discovery solution is unique because the scanning is done by other agents of nearby computers. This is known as distributed scanning. This approach has several key benefits:

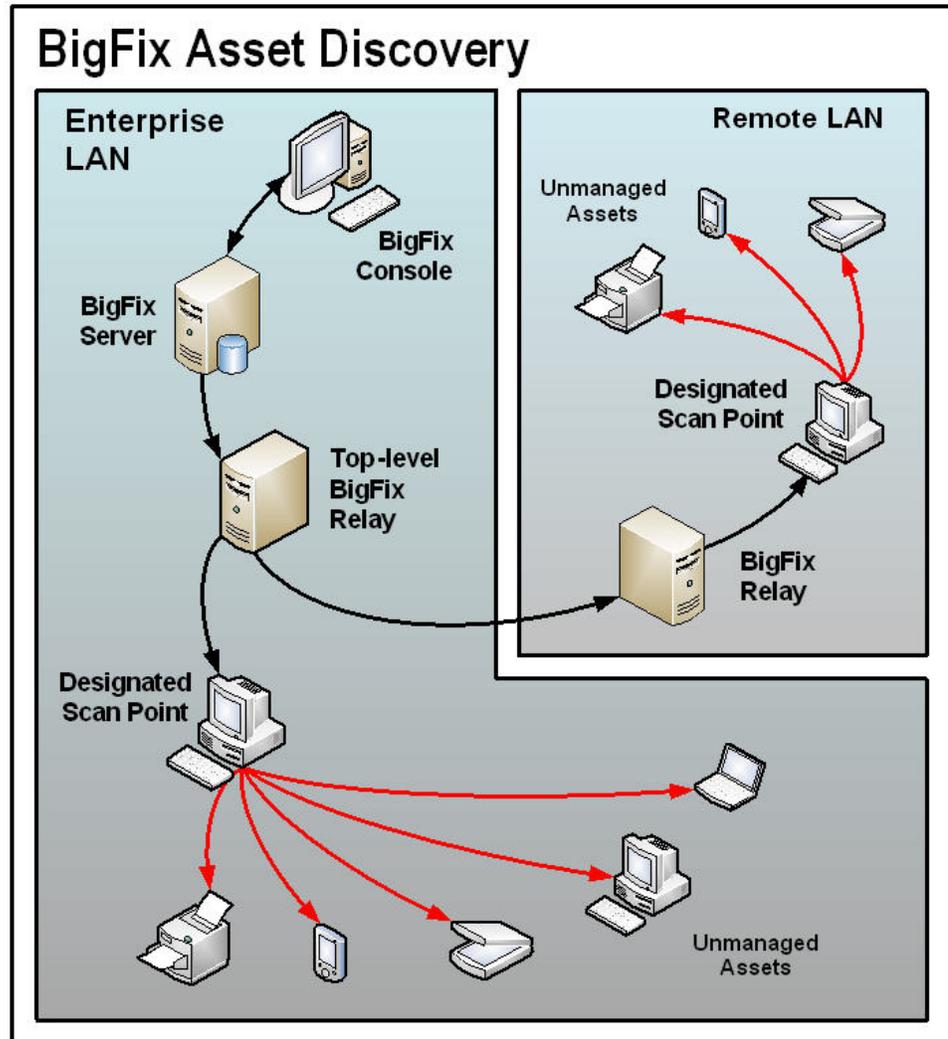
- Conserves WAN bandwidth
- Scanning can be done in parallel for much faster results, in minutes instead of weeks
- Can be easily customized to work in complex network configurations, including isolated subnets
- Individual subnets can run customized scan types

IBM Endpoint Manager Asset Discovery works by using Fixlets and Tasks to deploy Scan Points to specified agents in your network. You can then use other Fixlets and Tasks to run Nmap scans at intervals of your choosing. Scan results are automatically sent to the IBM Endpoint Manager server, which imports the data into the IBM Endpoint Manager database. The scan information can then be viewed in the IBM Endpoint Manager console using the *Unmanaged Assets* tab.

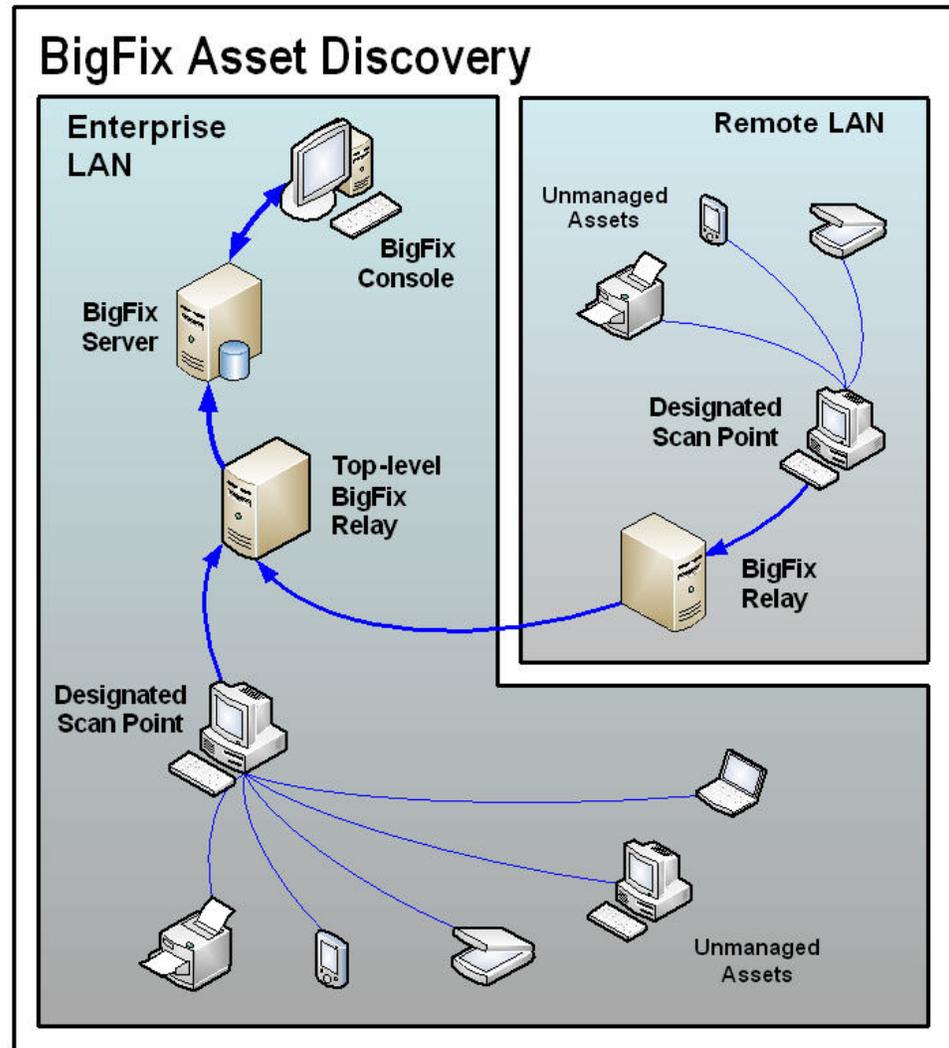
Note: You must install the BES server plug-in service to work with Asset Discovery Fixlets. This plug-in is available for installation in the BES Support site.

Chapter 2. Overview

IBM Endpoint Manager Asset Discovery works by designating certain computers as *Scan Points*. Any agent can be designated as a Scan Point if it is running a supported operating system. These Scan Points query the unmanaged assets in your network. The following image illustrates this process.



Information is retrieved from these unmanaged assets by the Scan Points and sent back through relays to the database on the IBM Endpoint Manager server. From there, you can examine the results on the IBM Endpoint Manager console:



System requirements

The nmap.org website indicates that Nmap supports all versions of Windows since NT, including Windows 2000, Windows XP, Windows Vista, Windows 7, and Server 2003/2008. Nmap supports also Linux operating systems.

Installation

You perform the following installation tasks in the Asset Discovery site:

- Enable the Unmanaged Asset Importer Service on your IBM Endpoint Manager server
- Designate specific agents as scan points
- Run the scan

Note: To view Unmanaged Assets, you must have the proper permissions set through the BES Administration Tool. To access the tool, click **Start > All Programs**

> **IBM Endpoint Manager Enterprise > BES Administration Tool**). A user can be granted permission to view all unmanaged assets or only those connected to the Scan Points that they administer.

Installing the site

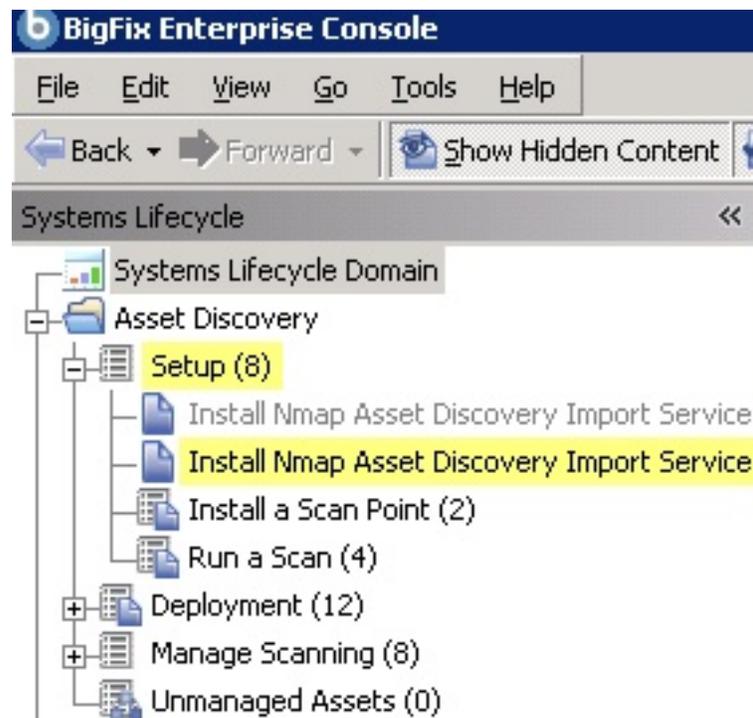
To enable and subscribe all the computers to the external site using the IBM Endpoint Manager Console, perform the following steps:

1. Open the BigFix Management domain and scroll to the top to view the associated dashboards.
2. In the Licensing dashboard, click the external site and enable it, if not already enabled, by clicking the name of the site in the list of sites.
3. In the properties panel of the external site, select the **Computer subscriptions** tab and click **All computers** to subscribe all the computers in the IBM Endpoint Manager environment to the external site.
4. Click **Save Changes** to save the site subscription settings.

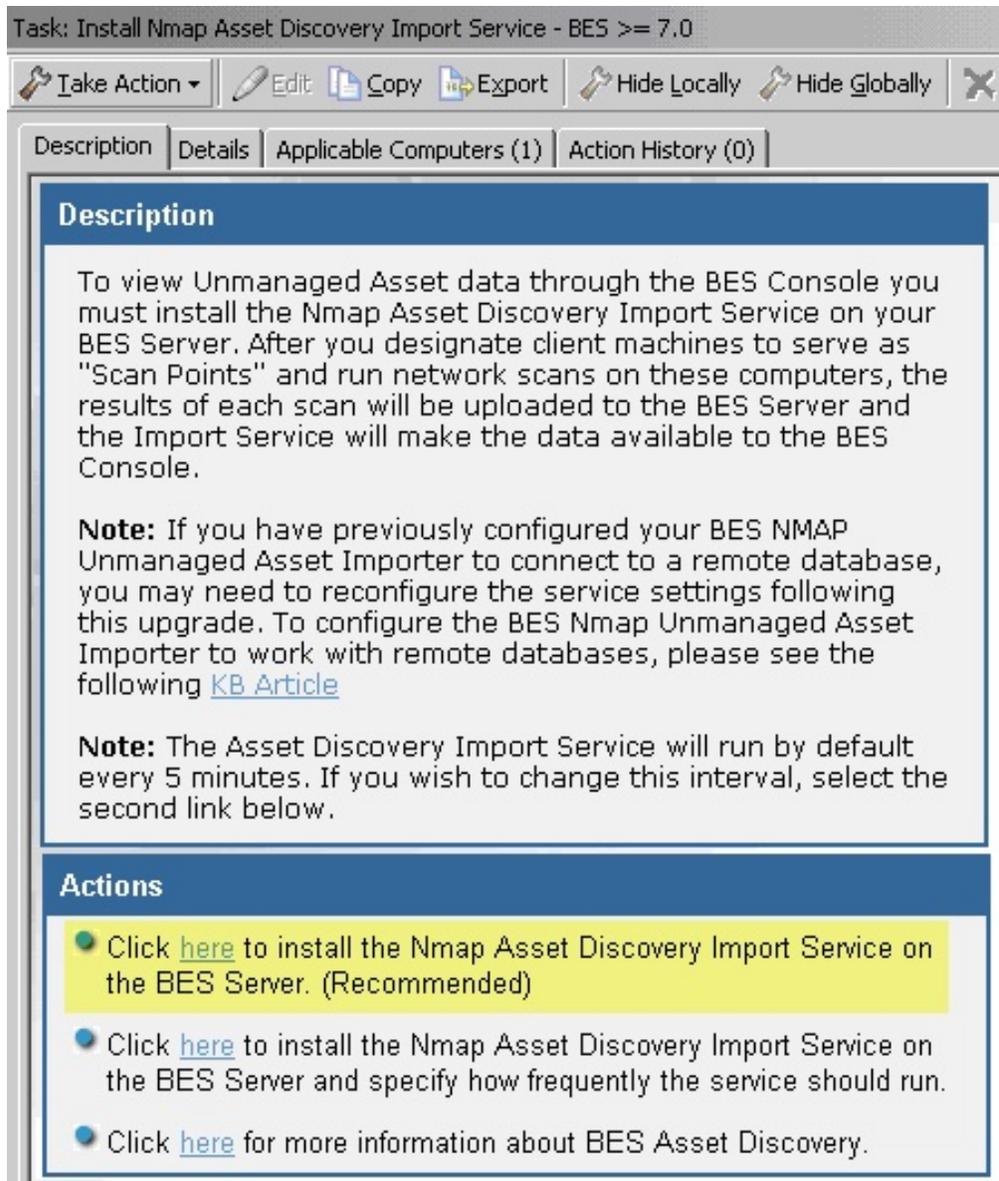
Installing the Import Service task

Note: When accessing a remote database, the NMAP Import Service needs to be run as a domain user, as the standard local system will not allow access to the SQL database. This service should be configured like other IBM Endpoint Manager services in a remote database environment.

Expand the Setup node in the Asset Discovery navigation tree to find the *Install Nmap Asset Discovery Import Service* Task.



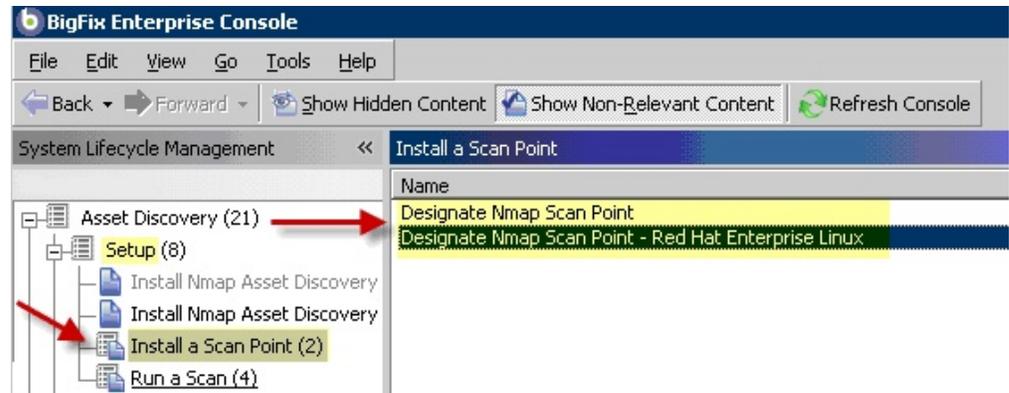
Click the task and view the description in the work area.



To install the Nmap Asset Discovery Import Service on the IBM Endpoint Manager server, click the link in the Actions box. By default, the Import service runs every five minutes and checks for new Nmap scan data that has been delivered to the IBM Endpoint Manager server. If you want to establish a different frequency, select the second Action link.

Installing Scan Points

In the Setup node of the Asset Discovery navigation tree, click *Install a Scan Point*. A list of the scan point designation tasks are displayed in the List Panel on the right.



The computers you designate as Scan Points must be running Windows. These Scan Points are the hubs from which the local subnet is scanned. You can also view the license agreements for Nmap, WinPcap and Info-zip.

Click the *Designate Nmap Scan Point* Task.

Task: Designate Nmap Scan Point

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

Description | Details | Applicable Computers (1) | Action History (0)

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 the license agreement for Nmap before deploying this application. By applying this Task message, you are implicitly accepting the license agreement. The end user will NOT be prompted to accept the new license. For more information on Nmap, as well as advanced configuration options, visit the link below.

Note: WinPcap is an open-source library that Nmap needs to examine network packets. You must accept the license agreement for WinPcap before deploying this application. By applying this Task message, you are implicitly accepting the license agreement. The end user will NOT be prompted to accept the new license. To view the license agreement for WinPcap, visit the link below.

Note: Nmap is distributed in a .zip file. In order to extract it, this Task will download Info-Zip's decompression tool. Info-Zip is an open-source decompression utility. You must accept the license for Info-Zip before deploying this application. By applying this Task message, you are implicitly accepting the license agreement. The end user will NOT be prompted to accept the new license. To view the license agreement for Info-Zip, visit the link below.

File Size: 6.9 MB

Actions

- Click [here](#) to designate computers as Nmap scan points.
- Click [here](#) for more information about Nmap and to view the license.
- Click [here](#) to view the WinPcap license.
- Click [here](#) to view the Info-Zip license.
- Click [here](#) for more information about BES Asset Discovery.

Click the first Actions box link to access the Take Action dialog. From the Target tab, select the computers that you want to designate as Scan Points.

Click the *Designate Nmap Scan Point – Red Hat Enterprise Linux* Task. Click the first Actions box link to designate Nmap Scan Points.1

Task: Designate Nmap Scan Point - Red Hat Enterprise Linux

Take Action Edit Copy Export Hide Locally Hide Globally Remove

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

Description

This Task will deploy Nmap 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 the license agreement for Nmap before deploying this application. By applying this Task message, you are implicitly accepting the license agreement (the end user will NOT be prompted to accept the new license). For more information on Nmap, as well as advanced configuration options, visit the link below.

Note: In order to avoid conflicts, this task will uninstall older nmap, and nmap-frontend before installing nmap-5.00-1.

File Size: 2.33 MB

Actions

- Click [here](#) to designate computers as Nmap Scan Points.
- Click [here](#) for more information about Nmap and to view the license.
- Click [here](#) for more information about BES Asset Discovery.

Running a scan

In the Setup node of the Asset Discovery navigation tree, click *Run a Scan*. You see that there are available tasks associated with this action. Click one of the available scans.

BigFix Enterprise Console

File Edit View Go Tools Help

Back Forward Show Hidden Content Show Non-Relevant Content Refresh

System Lifecycle Management << Run a Scan

Name
Run Nmap Scan
Run Nmap Scan (Large Subnet)
Run Nmap Scan - Red Hat Enterprise Linux
Run Nmap Scan (Large Subnet) - Red Hat Enterprise Linux

Task: Run Nmap Scan

Asset Discovery (21)

- Setup (8)
 - Install Nmap Asset Disco
 - Install Nmap Asset Disco
 - Install a Scan Point (2)
 - Run a Scan (4)



When the task opens in the work area, select one of the available links in the Actions box to initiate the Nmap scan. You can specify a local or large subnet.

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/agressiveness 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.

Note: Nmap is an open-source utility for network scanning. For more information on Nmap, as well as advanced configuration options, 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.

A scan on a class C network (255 IP addresses) usually takes anywhere from 10-30 minutes, depending on your network. You can also create your own custom Tasks to schedule and configure Nmap scans using the *Asset Discovery Nmap Configuration Wizard*.

When a Scan Point completes its local scan, the results are uploaded to the IBM Endpoint Manager server and imported into the database by the Importer service. The scan results are then visible on the Unmanaged Asset tab in the IBM Endpoint Manager console.

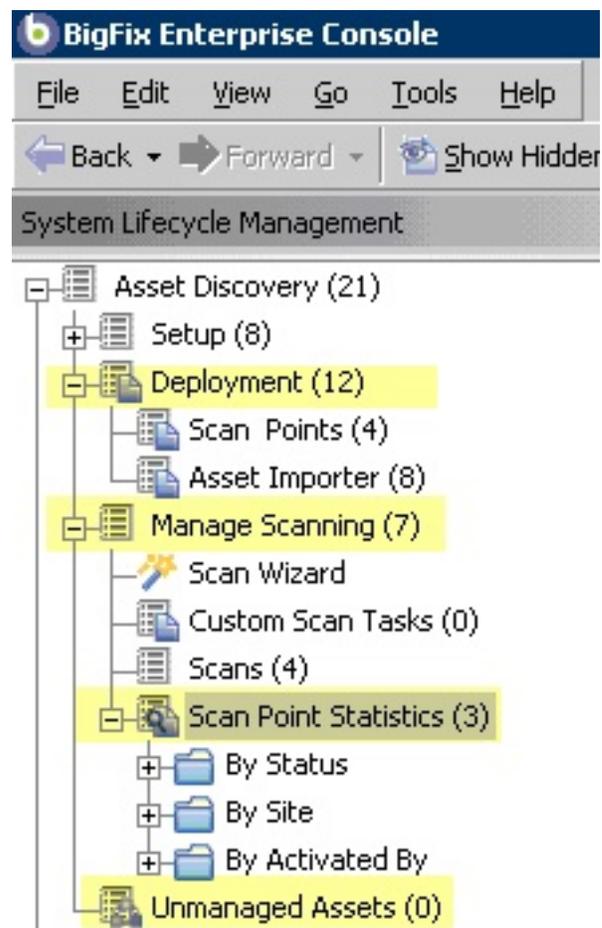
This completes the installation of the Asset Discovery service.

Chapter 3. Using Asset Discovery

Operation

Once installed, you can view all unmanaged asset information that has been retrieved by your various Scan Point computers.

At any point, you can activate the *Scan Point Statistics* to view information about designated Nmap Scan Points. Click *Scan Point Statistics* under the *Manage Scanning* node of the navigation tree. You can view statistics *By Status*, *By Site* or *By Activation*.





To decommission a Scan Point computer, use the *Remove Nmap Scan Point* task in the Deployment node. To access the Remove Nmap Scan Point tasks, click *Scan Points* under the Deployment node.

Name	Source Severity	Site	Applicable Com...	Open Action
Remove Nmap Scan Point	<Unspecified>	BES Asset Discov...	0 / 1	0
Remove Nmap Scan Point - Red Hat Enterprise Linux	<Unspecified>	BES Asset Discov...	0 / 1	0
Designate Nmap Scan Point	<Unspecified>	BES Asset Discov...	1 / 1	0
Designate Nmap Scan Point - Red Hat Enterprise Linux	<Unspecified>	BES Asset Discov...	0 / 1	0

Task: Remove Nmap Scan Point

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 WinPcap.
- Click [here](#) for more information about Nmap.
- Click [here](#) for more information about BES Asset Discovery.

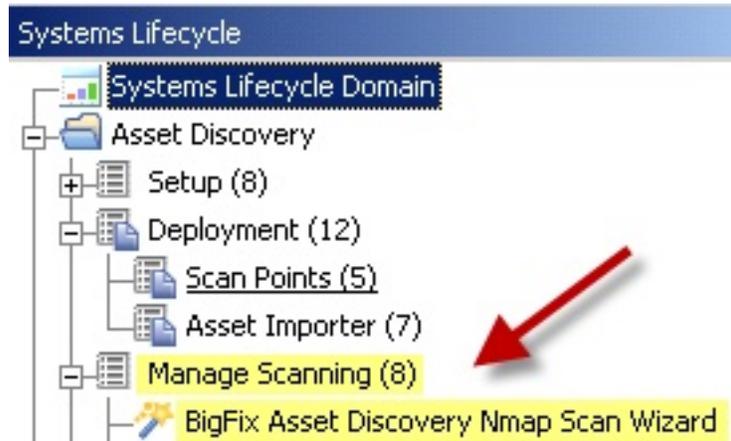
This removes Nmap from the specified Scan Point and can also remove WinPcap. Click in the Actions box to access the Take Action dialog and select the Scan Point computers you wish to decommission. To delete an unmanaged asset, click *Unmanaged Assets* at the bottom of the navigation tree.

Using the Nmap Scan Wizard

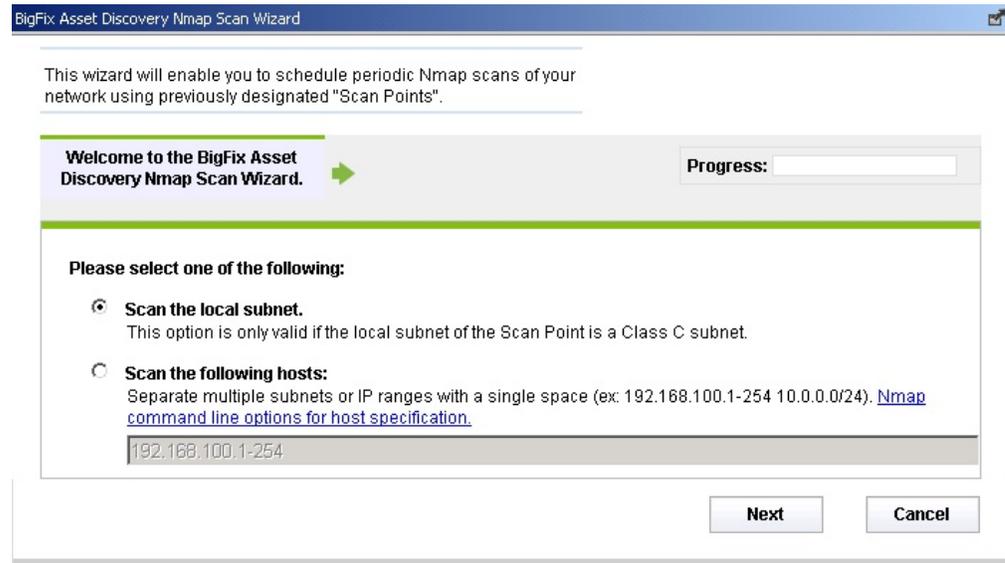
You can change various aspects of the Nmap scanner by using the *Asset Discovery Nmap Scan Wizard*. You can schedule periodic Nmap scans of your network using previously designated Scan Points.

Note: The Nmap scanner requires that the **UnmanagedAssetImporter -NMAP** service is running on the server.

Click *Scan Wizard* under the *Manage Scanning* node in the navigation tree.

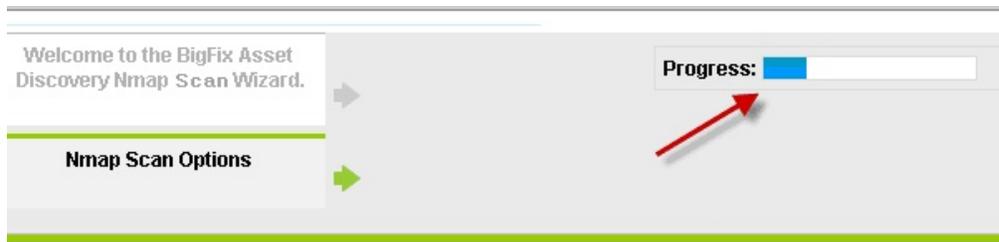


The wizard is displayed on the right.



Begin by selecting a type of scan. You can scan the local subnet or scan a particular host. Click *Next*.

If you select *Scan the local subnet*, you set specific parameters of the scan in the next screen. Check the Progress bar at the top of the window.



Nmap Scan Options

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

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

22 23 80 135 139 235 445 61616

Select the desired timing policy. 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 wish 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

On this screen, you scan ports, run operating system detection, enable version detection, and list hosts to exclude. Make your selections and click *Next*.

On the next screen, you can enable Advanced Nmap configuration options, select Ping Options, and additional Nmap scan options. Make your selections and click *Next*.

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

Nmap Scan Options → **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.

- PO: 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.

80

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.](#)

Back Next Cancel

In the next screen, you can customize the text fields for the Fixlet. You can edit the title and the description of the Fixlet. When you have customized all text fields, click *Finish* and enter your Private Key Password.

BigFix Asset Discovery Nmap Scan Wizard

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

Enable Advanced Nmap Configuration Options. → Nmap Scan Options → Scheduling Options → **Customize the textfields 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 (4/24/2010)

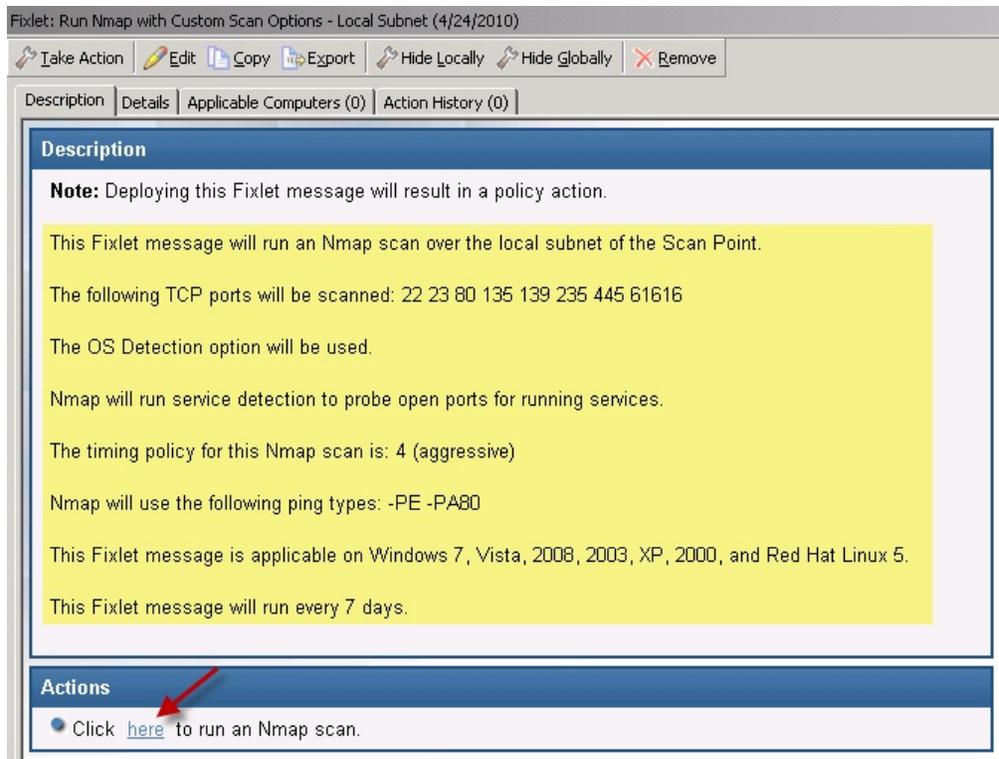
Edit the description:

Note: Deploying this Fixlet message will result in a policy action.
 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 80 135 139 235 445 61616
 The OS Detection option will be used.

Show Custom Fixlet Dialog before creating this Fixlet message.

Back Finish Cancel

You now see the Fixlet that includes the specific parameters and customizations you entered in the wizard. Review the text in the Description field, and click in the Actions box to run an Nmap scan.



Considerations

Licensing

- When you designate Scan Points, you are installing the Nmap scanner application available from <http://www.insecure.org/nmap>.
- When you designate Scan Points, you are installing the packet capture library, WinPcap 3.1 from <http://winpcap.polito.it/install/default.htm>.
- Nmap is distributed as a .zip file. To extract it, IBM Endpoint Manager temporarily downloads and uses Info-Zip's decompression tool. *Info-Zip* is an open-source decompression utility. For more information about Info-Zip, see <http://www.info-zip.org/>.

Potential scanning issues

- Network scans might trigger Intrusion Detection Systems. To minimize this possibility, set the Nmap scanning mode to 0 ("Paranoid"), or modify your IDS to allow Nmap scans. This might cause scans to take longer.
- Network scans might cause certain legacy network devices, such as old network printer devices, to fail if scanned.
- Network scans might cause personal firewalls to advise you that a computer is scanning the local computer. Modify your firewall to allow Nmap scans.
- Nmap is sometimes flagged by virus scanners as a potentially harmful tool. Ensure that your virus scanner is not set to block Nmap from running.
- If you set Nmap to scan a very large network, it might take several hours and consume significant bandwidth during the scan. The default scan is the local Class C network, which is usually a fast LAN. It is not recommended that you scan large networks across the WAN with this tool.

- Using Nmap to scan is typically a very safe operation, but there may be issues specific to your organization that must be addressed. Obtain the appropriate authorization from your network team before proceeding.

Appendix A. Frequently asked questions

I started a scan – where are the results?

When first installed, Asset Discovery might take several minutes to initially scan the system and report on your unmanaged assets. If you still do not see anything in the IBM Endpoint Manager console after 20 minutes, press F5 on your keyboard to force a full refresh.

Where is the Unmanaged Assets tab?

The Unmanaged Assets tab is only visible after you install the Nmap Asset Discovery Import Service. It might take a few minutes to display in the interface. When it is displayed, you can open the tab and click the individual assets to learn more about them.

How long does a typical scan take?

Scanning a Class C subnet typically takes 10-30 minutes, but this can vary based on your specific network. On bigger networks, the scans may take several hours to run.

What are the bandwidth requirements?

The Nmap scanner sends small packets that are unlikely to cause any bandwidth concerns, especially because it is designed to scan nearby computers on fast networks. Once the scan is finished, the scan results are uploaded to the IBM Endpoint Manager server. Normally this is a relatively small file - generally 10-200 KB - depending on the number of endpoints scanned. Scanning large networks with a single Scan Point can result in bigger files, but these scans are only run periodically.

How often can I run a scan?

When Asset Discovery is set up correctly, there is very little network impact and it can be run fairly often without issues. Scans can be run as often as several times a day to find unauthorized network devices, or less often to maintain accurate network inventory information.

Can the Nmap scan settings be changed?

Yes. The default Nmap scan settings enable fast and thorough scanning. The settings can be changed as necessary using the Nmap Configuration Wizard and support any possible Nmap configuration.

Appendix B. Support

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

- http://pic.dhe.ibm.com/infocenter/tivihelp/v26r1/topic/com.ibm.tem.doc_9.1/welcome/welcome.html
- IBM Endpoint Manager Support site
- IBM Endpoint Manager wiki
- Knowledge Base
- Forums and Communities

Notices

This information was developed for products and services that are offered in the USA.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM 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:

*IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America*

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

*Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan*

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION 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 states 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. IBM 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-IBM 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 IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply 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:

*IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.*

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 IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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 the names and addresses used by an actual business enterprise 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 IBM, 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. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM 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:

Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. _enter the year or years_. All rights reserved.

Programming interface information

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM® Corp. and Quantum in the U.S. and other countries.

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 IBM 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 IBM.

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 IBM.

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.

IBM 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 IBM, 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.

IBM 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.



Printed in USA