

IBM Endpoint Manager
Version 9.1

*Patch Management for Solaris
User's Guide*



IBM Endpoint Manager
Version 9.1

*Patch Management for Solaris
User's Guide*



Note

Before using this information and the product it supports, read the information in "Notices" on page 49.

This edition applies to version 9, release 1, modification level 0 of IBM Endpoint Manager (product number 5725-C45) and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2003, 2014.**

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

Contents

Chapter 1. Overview	1
What's new in this release	1
Supported platforms and updates	2
Chapter 2. Setup	3
Site subscription	3
Download plug-ins	3
Manage Download Plug-ins dashboard	3
Registering the Solaris download plug-in	5
Unregistering the Solaris download plug-in	7
Configuring the Solaris download plug-in	8
Migrating the Solaris download plug-in	9
Upgrading the Solaris download plug-in	11
Download cacher tool overview	11
Running the Solaris Download Cacher Tool task	12
Solaris Image Packaging System Repository Management dashboard overview	14
Chapter 3. Patching using Fixlets	17
Local repositories	19
Single-user mode patch application	20
Creating a baseline for single-user mode.	20
Deploying Solaris packages	23
Uninstalling patches	25
Superseded Fixlets	27

Enabling superseded Fixlets	28
---------------------------------------	----

Chapter 4. Solaris Live Upgrade support	31
Running the Enable Solaris Live Upgrade task.	32
Manage Solaris Boot Environments dashboard overview	33
Endpoint Manager client installation behavior.	34
Installing the Endpoint Manager client	35
Selecting inactive boot environments for Live Upgrade	35
Activating inactive boot environments	36
Rebooting to an alternate boot environment	37

Appendix A. Support.	39
---------------------------------------	-----------

Appendix B. Frequently asked questions	41
---	-----------

Notices	49
Programming interface information	51
Trademarks	51
Terms and conditions for product documentation.	52

Chapter 1. Overview

IBM® Endpoint Manager Patch Management for Solaris provides unified, real-time visibility and enforcement to deploy and manage patches to all Solaris endpoints from a single console. It keeps your Solaris clients current with the latest Oracle updates.

Important: You must have an Oracle Support account to access the patches from the Oracle Support site at <https://support.oracle.com>. Your Oracle account user name must have a valid support identifier to download patches.

Patch management is available from the following sites:

Patches for Solaris

This site includes legacy Solaris 10 and earlier core OS patch content. It uses the older traditional single-user mode for applying patches.

Patches for Solaris Maintenance

This site includes legacy Solaris 10 and earlier non-core OS patch content.

Patches for Solaris Live Upgrade

This site includes patch content that uses the Solaris Live Upgrade utility to install patches to an alternate boot environment rather than the currently running OS.

Patches for Solaris 11

This site includes Fixlet content for Solaris 11/11, 11.1, and 11.2.

For each new supported update that becomes available, Endpoint Manager releases a Fixlet® that identifies and updates all the computers in your enterprise that need it. For information on the supported updates, see “Supported platforms and updates” on page 2.

With a few keystrokes, the Endpoint Manager console operator can apply the patch to all the relevant computers and visualize its progress as it deploys throughout the network. The Endpoint Manager agent checks the operating system version, processors, and the existing installed packages to determine when and if a patch is necessary.

Using Fixlets, you can manage large numbers of updates and patches with comparative ease, enabling automated, highly targeted deployment on any schedule that you want. Large downloads can be phased to optimize network bandwidth and the entire deployment process can be monitored, graphed, and recorded for inventory or audit control.

What's new in this release

This release of IBM Endpoint Manager for Patch Management for Solaris contains Fixlet content for Solaris 11.2.

Previous updates

You need to subscribe to the Patches for Solaris 11 site to access the following additions to the product:

- Fixlet content for Solaris 11/11 and Solaris 11.1.

- Solaris Image Packaging System Repository Management dashboard for assigning local repositories to Solaris 11 endpoints. For more information, see “Solaris Image Packaging System Repository Management dashboard overview” on page 14.

The Solaris 11/11 and Solaris 11.1 patch updates are released through the Solaris Support Repository Update (SRU). These updates contain a number of fixes and are available from the Oracle Support Repository.

Regularly updating the endpoints in your deployment is crucial to the success of your organization. Network restrictions often prevent you from getting the latest set of changes from the Oracle hosted repositories. Maintain your own local package repositories to try to limit this restriction. By using local repositories, you can control which updates the endpoints have access to.

You can have multiple local repositories in your environment. For example, you might have one local repository that is used to mirror the latest SRU changes from Oracle and another repository that contains only one particular SRU.

For more information about Solaris 11, see the Oracle website at <http://www.oracle.com>.

Supported platforms and updates

Endpoint Manager supports several Solaris platforms and Oracle updates.

Endpoint Manager supports Oracle updates on the following platforms:

Table 1. Supported platforms and patches for the Patch Management for Solaris

Fixlet Site Name	Supported Platform	Type of Update
Patches for Solaris	<ul style="list-style-type: none"> • Solaris 9 (SPARC) • Solaris 10 (SPARC, x86) 	<ul style="list-style-type: none"> • Oracle Security Patches
Patches for Solaris Live Upgrade		<ul style="list-style-type: none"> • Oracle Recommended Patches • Oracle Recommended Patch Clusters • Oracle Critical Patch Updates
Patches for Solaris Maintenance		<ul style="list-style-type: none"> • Oracle Non-Security Patches • Oracle Maintenance Patches • Oracle Device Drivers
Patches for Solaris 11	Solaris 11 (SPARC, x86)	Oracle Support Repository Updates
Linux RPM Patching	Previously listed supported platform versions.	Previously listed updates.

Endpoint Manager provides also support for Solaris Zones.

Note: Endpoint Manager does not support unbundled patches.

Chapter 2. Setup

Setting up your environment for patch management.

Site subscription

Sites are collections of Fixlet messages that are created internally by you, by IBM, or by vendors.

Subscribe to a site to access the Fixlet messages to patch systems in your deployment.

You can add a site subscription by acquiring a Masthead file from a vendor or from IBM or by using the Licensing Dashboard. For more information about subscribing to Fixlet sites, see the *IBM Endpoint Manager Installation Guide*.

For more information about sites, see the *IBM Endpoint Manager Console Operator's Guide*.

Download plug-ins

Download plug-ins are executable programs that download a specified patch from the website of the patch vendor. To ease the process of caching, Fixlets have an incorporated protocol that uses download plug-ins.

For the Fixlet to recognize the protocol, the related download plug-in must be registered. You must use the Manage Download Plug-ins dashboard to register the download plug-in. After you register the plug-in, you can run the Fixlets to download, cache, and deploy patches from the IBM Endpoint Manager console.

If you already registered the plug-in, you can use the Manage Download Plug-ins dashboard to run the update. You must use the dashboard also to unregister and configure the download plug-in. For more information about the dashboard, see the following topics.

Note: Use the official mirror server configuration when you plan to download large amounts of packages. Specify the mirror server URL and credentials during the download plug-in registration or configuration to avoid being locked out of your account.

Note: If you install the download plug-in on relays, it is suggested that you also install it on the server.

Manage Download Plug-ins dashboard

Use the Manage Download Plug-ins dashboard to oversee and manage download plug-ins in your deployment.

You can use the Manage Download Plug-ins dashboard to register, unregister, configure, and upgrade the download plug-ins for different patch vendors. For more information about these features, see the following topics.

You must subscribe to the Patching Support site to gain access to this dashboard. To view the Manage Download Plug-ins dashboard, go to **Patch Management domain > All Patch Management > Dashboards > Manage Download Plug-ins**.

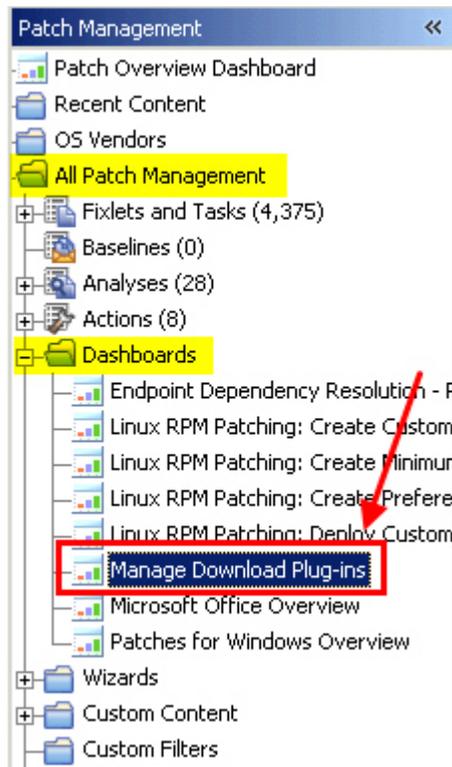


Figure 1. Patch Management navigation tree

The dashboard displays all the servers and windows-only relays in your deployment. Select a server or relay to view all the plug-ins for that computer. The dashboard shows you also the version and status for each plug-in in one consolidated view.

Manage Download Plug-ins

You can use this dashboard to manage download plug-ins for different vendor sites on servers and relays. Select a server or relay to view the applicable download plug-ins.

Servers And Relays

Name	Operating System	Type	Encryption Enabled
ACROBATX-XP-X64	WinXP-2003 5.2.3790	Relay	Yes
TEM-NW-BESSRV	Win2008R2 6.1.7600	Server	Yes

Plug-ins

Register Unregister Configure Upgrade

Plug-in Name	Plug-in Version	Status
AIX Plug-in	1.8.0.0	New Version Available
CentOS Plug-in	N/A	Not Supported
HP-UX Plug-in	2.0.0.0	Up-To-Date
RedHat Plug-in	2.0.0.0	Up-To-Date
Solaris Plug-in	1.7.0.0	New Version Available
SUSE Plug-in	N/A	Not Supported

Figure 2. Manage Download Plug-ins dashboard

A plug-in can be in one of the following states:

- Not Installed
- New Version Available
- Up-To-Date
- Not Supported

Note: CentOS and SUSE Linux download plug-ins are not supported in relays.

The dashboard has a live keyword search capability. You can search based on the naming convention of the servers, relays, and plug-ins.

Registering the Solaris download plug-in

Use the Manage Download Plug-ins dashboard to register the download plug-in for Solaris.

You must complete the following tasks:

- Subscribe to the **Patching Support** site to gain access to the Manage Download Plug-ins dashboard.
- Enable the **Encryption for Clients** Fixlet on servers and relays for which you want to register the download plug-in.
- Activate the **Encryption Analysis for Clients** analysis and **Download Plug-in Versions** analysis.

When you register the download plug-in on a computer without the plug-in, the plug-in is automatically installed and the configuration file is created.

If the download plug-in is already installed on the computer, the configuration file is overwritten.

For Solaris 11, use the Solaris Download plug-in version 2.3 or later.

1. From the Patch Management domain, click **All Patch Management > Dashboards > Manage Download Plug-ins dashboard**.
2. From the Servers and Relays table, select the server or relay on which the download plug-in is to be registered.
3. From the Plug-ins table, select **Solaris Plug-in**.
4. Click **Register**. The Register Solaris Plug-in wizard displays.

Register Solaris Plug-in

This wizard installs and configures the Solaris Plug-in.
Existing configurations are overwritten.

Oracle Credentials

Oracle Username *

Oracle Password *

Confirm Oracle Password *

Proxy Server Settings

Proxy URL

Proxy Username

Proxy Password

Confirm Proxy Password

Figure 3. Register Solaris download plug-in wizard

5. Enter the Oracle credentials that you use to log on to the Oracle Support site.
 - Oracle Username**
Your Oracle account user name to the Oracle Support site. It must have a valid support identifier to download patches.
 - Oracle Password**
Your Oracle account password to the Oracle Support site.
 - Confirm Oracle Password**
Your Oracle account password for confirmation.
6. Optional: Enter the proxy parameters if the downloads must go through a proxy server.

Proxy URL

The URL of your proxy server. It must be a well-formed URL, which contains a protocol and a host name. The URL is usually the IP address or DNS name of your proxy server and its port, which is separated by a colon. For example: http://192.168.100.10:8080.

Proxy Username

Your proxy user name if your proxy server requires authentication. It is usually in the form of domain\username.

Proxy Password

Your proxy password if your proxy server requires authentication.

Confirm Proxy Password

Your proxy password for confirmation.

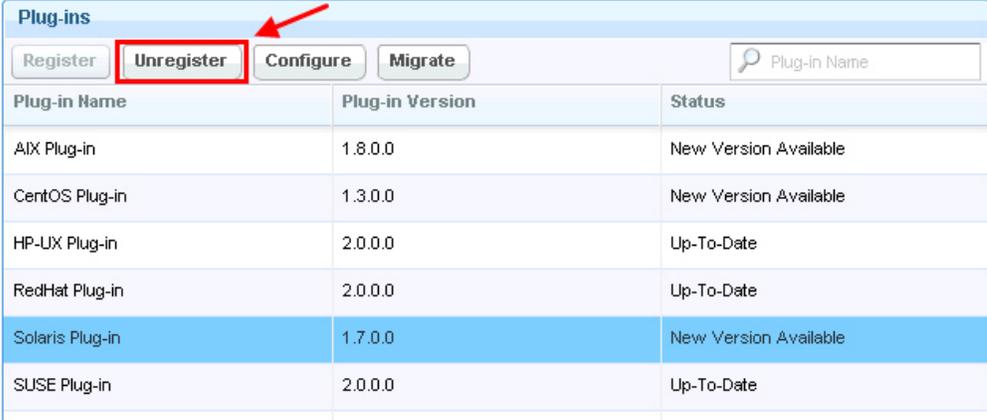
7. Click **OK**. The Take Action dialog displays.
8. Select the target computer.
9. Click **OK**.

You successfully registered the Solaris download plug-in.

Unregistering the Solaris download plug-in

Use the Manage Download Plug-ins dashboard to unregister the download plug-in for Solaris.

1. From the Patch Management domain, click **All Patch Management > Dashboards > Manage Download Plug-ins dashboard**.
2. From the Servers and Relays table, select the server or relay on which the download plug-in is to be unregistered.
3. From the Plug-ins table, select **Solaris Plug-in**.
4. Click **Unregister**.



Plug-ins		
Plug-in Name	Plug-in Version	Status
AIX Plug-in	1.8.0.0	New Version Available
CentOS Plug-in	1.3.0.0	New Version Available
HP-UX Plug-in	2.0.0.0	Up-To-Date
RedHat Plug-in	2.0.0.0	Up-To-Date
Solaris Plug-in	1.7.0.0	New Version Available
SUSE Plug-in	2.0.0.0	Up-To-Date

Figure 4. Unregister the Solaris download plug-in

The Take Action dialog displays.

5. Select the target computer.
6. Click **OK**.

You successfully unregistered the Solaris download plug-in.

Configuring the Solaris download plug-in

Use the Manage Download Plug-ins dashboard to configure the download plug-in for Solaris.

You might want to take note of your existing configuration for the download plug-in because existing configurations are overwritten when you configure the download plug-in.

1. From the Patch Management domain, click **All Patch Management > Dashboards > Manage Download Plug-ins dashboard**.
2. From the Servers and Relays table, select the server or relay on which the download plug-in is to be configured.
3. From the Plug-ins table, select **Solaris Plug-in**.
4. Click **Configure**. The Configure Solaris Plug-in wizard displays.

Configure Solaris Plug-in

This wizard configures the Solaris Plug-in.
Existing configurations are overwritten.

Oracle Credentials

Oracle Username *

Oracle Password *

Confirm Oracle Password *

Proxy Server Settings

Proxy URL

Proxy Username

Proxy Password

Confirm Proxy Password

Figure 5. Configure Solaris download plug-in wizard

5. Enter the Oracle credentials that you use to log on to the Oracle Support site.

Oracle Username

Your Oracle account user name to the Oracle Support site. It must have a valid support identifier to download patches.

Oracle Password

Your Oracle account password to the Oracle Support site.

Confirm Oracle Password

Your Oracle account password for confirmation.

6. Optional: Enter the proxy parameters if the downloads must go through a proxy server.

Proxy URL

The URL of your proxy server. It must be a well-formed URL, which contains a protocol and a host name. The URL is usually the IP address or DNS name of your proxy server and its port, which is separated by a colon. For example: `http://192.168.100.10:8080`.

Proxy Username

Your proxy user name if your proxy server requires authentication. It is usually in the form of `domain\username`.

Proxy Password

Your proxy password if your proxy server requires authentication.

Confirm Proxy Password

Your proxy password for confirmation.

7. Click **OK**. The Take Action dialog displays.
8. Select the target computer.
9. Click **OK**.

You successfully configured the Solaris download plug-in.

Migrating the Solaris download plug-in

You must migrate the download plug-in if the plug-in version is earlier than 2.0.0.0. You only need to do this once. The download plug-in is upgraded to the latest version after migration.

You might want to take note of your existing configuration for the download plug-in because existing configurations are overwritten when you migrate the download plug-in.

1. From the Patch Management domain, click **All Patch Management > Dashboards > Manage Download Plug-ins dashboard**.
2. From the Servers and Relays table, select the server or relay on which the download plug-in is to be migrated.
3. From the Plug-ins table, select **Solaris Plug-in**.
4. Click **Migrate**. The Migrate Solaris Plug-in wizard displays.

Figure 6. Migrate Solaris download plug-in wizard

5. Enter the Oracle credentials that you use to log on to the Oracle Support site.

Oracle Username

Your Oracle account user name to the Oracle Support site. It must have a valid support identifier to download patches.

Oracle Password

Your Oracle account password to the Oracle Support site.

Confirm Oracle Password

Your Oracle account password for confirmation.

6. Optional: Enter the proxy parameters if the downloads must go through a proxy server.

Proxy URL

The URL of your proxy server. It must be a well-formed URL, which contains a protocol and a host name. The URL is usually the IP address or DNS name of your proxy server and its port, which is separated by a colon. For example: `http://192.168.100.10:8080`.

Proxy Username

Your proxy user name if your proxy server requires authentication. It is usually in the form of `domain\username`.

Proxy Password

Your proxy password if your proxy server requires authentication.

Confirm Proxy Password

Your proxy password for confirmation.

7. Click **OK**. The Take Action dialog displays.
8. Select the target computer on which the download plug-in is to be upgraded.
9. Click **OK**.

You successfully migrated and upgraded the Solaris download plug-in.

Upgrading the Solaris download plug-in

Use the Manage Download Plug-ins dashboard to upgrade the download plug-in for Solaris.

1. From the Patch Management domain, click **All Patch Management > Dashboards > Manage Download Plug-ins dashboard**.
2. From the Servers and Relays table, select the server or relay on which the download plug-in is to be upgraded.
3. From the Plug-ins table, select **Solaris Plug-in**.
4. Click **Upgrade**. The Take Action dialog displays.
5. Select the target computer.
6. Click **OK**.

You now have the latest version of the Solaris download plug-in installed.

Download cacher tool overview

The Solaris download cacher tool is an executable program that automatically downloads and caches patch packages on the IBM Endpoint Manager server to facilitate the deployment of Solaris Fixlets.

Important: For Tivoli Endpoint Manager 8.1 and later, which is known as IBM Endpoint Manager, the preferred method for acquiring Solaris patches is to register the Solaris download plug-in. For more information about plug-in registration, see “Registering the Solaris download plug-in” on page 5.

Note: Only use the cacher tool if you are using an air-gapped environment or if you want to cache all the downloads for faster execution of actions. Otherwise, use the download plug-in. For more information about plug-ins, see Download plug-ins.

The tool uses FTP to download large .zip files and, by default, stores them in the sha1 cache folder. You can also choose to store the files in a different existing directory. Your environment must be configured to accept FTP use.

You can access the tool in one of the following ways:

- Running the **Run Solaris Download Cacher Tool - Windows** task from the console.

You must subscribe either to the Solaris or Solaris Maintenance sites to use the **Run Solaris Download Cacher Tool - Windows** task.

This patch caching method is the preferred for earlier versions of the product, which was known as BigFix 8.0.

- Downloading and running the download cacher tool manually.

For more information, see the technote in <http://www-01.ibm.com/support/docview.wss?uid=swg21506020>.

Running the Solaris Download Cacher Tool task

Use the **Run Solaris Download Cacher Tool - Windows** task to download files or packages to the IBM Endpoint Manager server.

Important: For Tivoli Endpoint Manager 8.1 and later, which is known as IBM Endpoint Manager, the preferred method for acquiring Solaris patches is to register the Solaris download plug-in. For more information about plug-in registration, see “Registering the Solaris download plug-in” on page 5.

Note: Only use the cacher tool if you are using an air-gapped environment or if you want to cache all the downloads for faster execution of actions. Otherwise, use the download plug-in. For more information about plug-ins, see Download plug-ins.

In the navigation tree of the Patch Management domain, expand the **OS Vendors** node. Next, expand the **Sun Microsystems Solaris** node and the **Configuration** node, and then select **Task**. In the List Panel, select the task **Run Solaris Download Cacher Tool - Windows**.

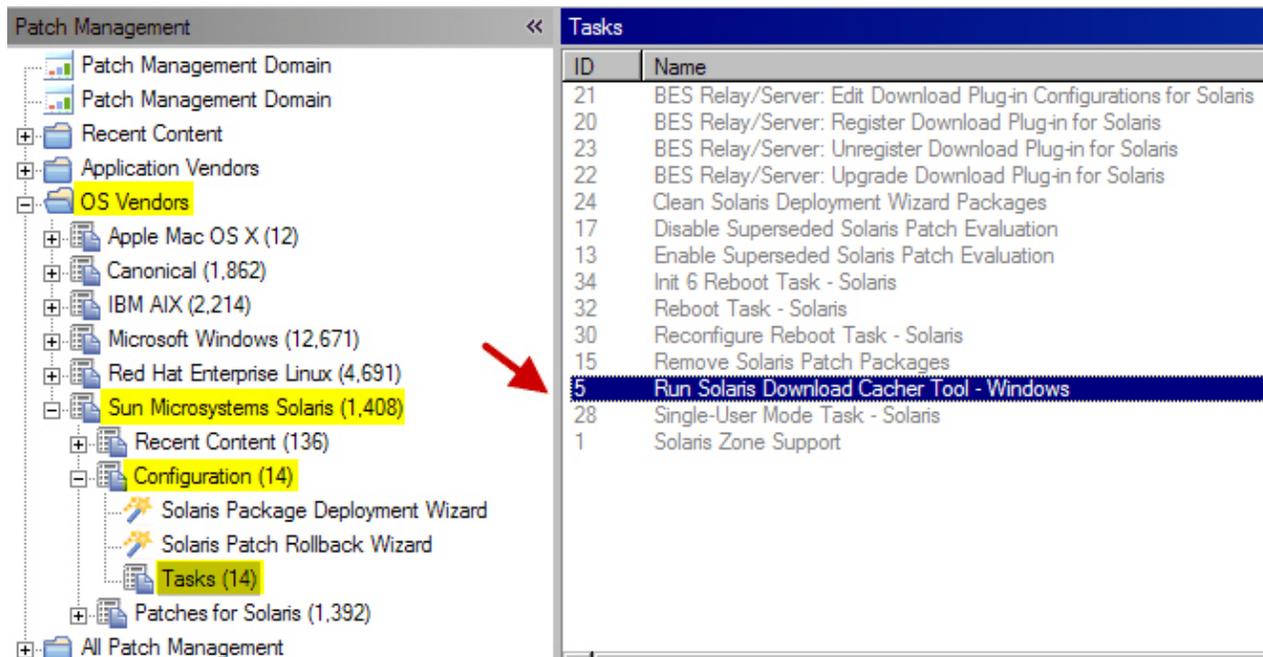


Figure 7. Sun Microsystems Solaris navigation tree - Tasks subnode

When the task window opens, select the appropriate link in the Actions box to start the download. You can choose from the following options:

- Download files directly to the Endpoint Manager Server cache (no proxy).
- Download files to a specified folder (no proxy).
- Download files directly to the Endpoint Manager Server cache (proxy).
- Download files to a specified folder (proxy).
- Download Recommended Patch Clusters to Endpoint Manager Server cache (no proxy).
- Download Recommended Patch Clusters to Endpoint Manager Server cache (proxy).

You are then prompted for the following action parameters:

Required Parameters:

Oracle Username

Your Oracle account user name that is used to log on to <https://support.oracle.com>.

Note: Your Oracle support account must have a valid support identifier to download patches.

Oracle Password

Your Oracle account password that is used to log on to <https://support.oracle.com>.

Optional Parameters:

Server cache limit

If you are downloading files or Recommended Patch Clusters directly to the IBM Endpoint Manager server cache, you can specify whether you want to automatically increase the IBM Endpoint Manager server cache limit. Enter yes to automatically increase the cache limit, otherwise, enter no.

The default value is yes.

Full path name of the folder directory

Specify the full path name of the folder directory where you want to store the files. The directory must already exist. By default, the files are stored in the sha1 cache folder.

This parameter is applicable only if you select to download the files to a specified folder.

Solaris operating system versions

The versions of the Solaris operating system for which you want to cache patches. Use a comma to separate each version. For example: 9, 10, 10x86

Leave the field blank to download all versions.

Patch IDs

The Solaris Patch IDs for the files you want to download. For example: 118833-01,119130-01,121012-01,10_Recommended_CPU_2012-04

Leave this field blank to download all patches.

SMTP server address

The address of your SMTP server to enable notifications.

Leave this field blank if do not want to enable notifications.

Email server Username

The user name of your email server.

Leave this field blank if the user name is not applicable.

Email server Password

The password of your email server.

Leave this field blank if the password is not applicable.

Email address of the sender

The email address to send the report from.

Leave this field blank if the email address is not applicable.

Email address of the recipient

The email address to send the report to. Use a comma to separate each email address.

Leave this field blank if the email address is not applicable.

After you enter all the parameters, the **Take Action** dialog box opens. Deploy the action. For information about deploying actions, see the *IBM Endpoint Manager Console Operator's Guide*.

Solaris Image Packaging System Repository Management dashboard overview

IBM Endpoint Manager provides the Solaris Image Packaging System Repository Management dashboard to help you manage your Solaris 11 endpoints and locally stored repositories.

Local repositories can significantly decrease the time that is taken to download the files that are needed for patching endpoints. Use this dashboard to set a local repository to use for patching. For information about patching, see Chapter 3, "Patching using Fixlets," on page 17.

Note: This dashboard does not support the creation of a physical repository server. You must create the repository separately. For more information about creating repositories, see the Oracle documentation website at <http://docs.oracle.com>.

To access the dashboard, subscribe to the Patches for Solaris 11 site. From the **Patch Management** domain, click **All Patch Management > Dashboards > Solaris Image Packaging System Repository Management**.

To view the endpoints and local repositories in the dashboard, activate the **Solaris Origin Information** analysis.

The dashboard offers filtering options to ease searching. You can filter either by computer name or repository name.



Figure 8. Solaris Image Packaging System Repository Management dashboard

By default, the hosted Oracle Solaris release repository is the configured package repository. You can assign a different repository from the list of repositories in the

dashboard. You can easily add more local repositories into the list. Ensure that the repository settings reflect the real repository server configuration.

Adding repositories

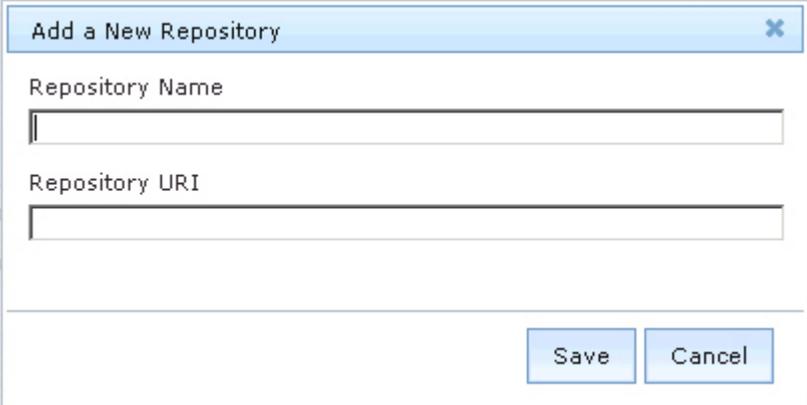
Local repositories must be created separately. Adding a repository to the dashboard does not create a physical repository server.

The dashboard does not check for the status of the local repository. Ensure that the repositories that you add in the dashboard are working.

Complete the following steps to add a local repository to the repository list in the dashboard:

1. From the dashboard, click **Manage Image Packaging System Repositories**.
2. Click **Add**.
3. Enter a repository name and the repository URI. For example, use this repository URI format: *protocol://hostname:port/path/*.

Note: The repository URI is validated only for HTTP and NFS shares.



The image shows a dialog box titled "Add a New Repository" with a close button in the top right corner. Below the title bar, there are two text input fields. The first is labeled "Repository Name" and the second is labeled "Repository URI". At the bottom right of the dialog, there are two buttons: "Save" and "Cancel".

Figure 9. Add a New Repository dialog

4. Click **Save**. The new repository is added to the list, which can be used by the endpoints.

Assigning repositories to endpoints

Complete the following steps to assign a local repository to Solaris 11 endpoints:

1. From the dashboard, click **Manage Endpoints**.
2. Select an endpoint that you want to configure to use a different repository.
3. Click **Assign a new repository**.
4. Select a repository.

	Repository Name	Repository URI
<input checked="" type="radio"/>	Oracle Solaris Support Repository	https://pkg.oracle.com/solaris/support/
<input type="radio"/>	Oracle Solaris Release Repository	http://pkg.oracle.com/solaris/release/
<input type="radio"/>	Local repo1	file:///filetest/
<input type="radio"/>	Local repo2	http://myhostname:22/path/
<input type="radio"/>	test2	http://10.1.234.164/

Repository Key

Repository Certificate

Figure 10. Assign a New Repository dialog

- Specify the repository SSL key and certificate if the selected repository requires those files.

Note: The Solaris Image Packaging System Repository Management dashboard accepts key and certificate files in .pem format only.

Note: The Oracle Solaris 11 Support Repository requires both the certificate and SSL key files to access the repository. Obtain both files from the My Oracle Support site. For more information, see <http://pkg-register.oracle.com>.

- Click **Save**. The Take Action dialog opens.
- Select the endpoint and click **OK**.
- When the action completes, refresh the dashboard to see the changes.

Chapter 3. Patching using Fixlets

You can apply Solaris patches to your deployment by using the Fixlets in the Solaris sites.

To deploy patches from the IBM Endpoint Manager console, register a download plug-in and run the appropriate patch Fixlets. For more information about download plug-ins, see [Download Plug-ins](#).

Notes: For Solaris 11, ensure that you complete the following requirements before patching endpoints:

- Use the Solaris Download plug-in version 2.3 or later.
- Expand the overall cache size for the server and relays to avoid the "Disk Limited" error when downloading SRUs. SRUs can be large, about 2.7 GB per image file. If you do not expand the cache, the gigantic download might flush out the existing files in the cache.
- Use the Solaris Image Packaging System Repository Management dashboard to configure a local repository, if necessary. For more information about the dashboard, see "Solaris Image Packaging System Repository Management dashboard overview" on page 14.

In the All Patch Management Content node of the navigation tree, click **Fixlets and Tasks > By Site**. Next, select the appropriate site:

- **Patches for Solaris** site
- **Patches for Solaris Maintenance** site
- **Patches for Solaris Live Upgrade** site
- **Patches for Solaris 11** site

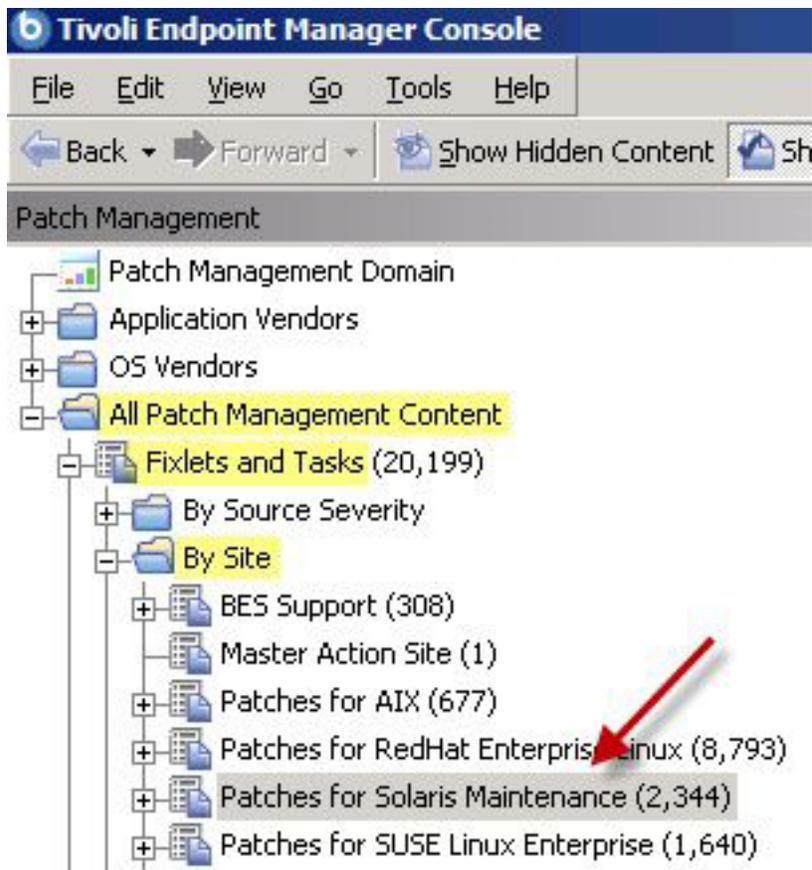


Figure 11. Patches for Solaris Maintenance site navigation tree

View the available content in the list panel on the right and double-click the Fixlet that you want to deploy.

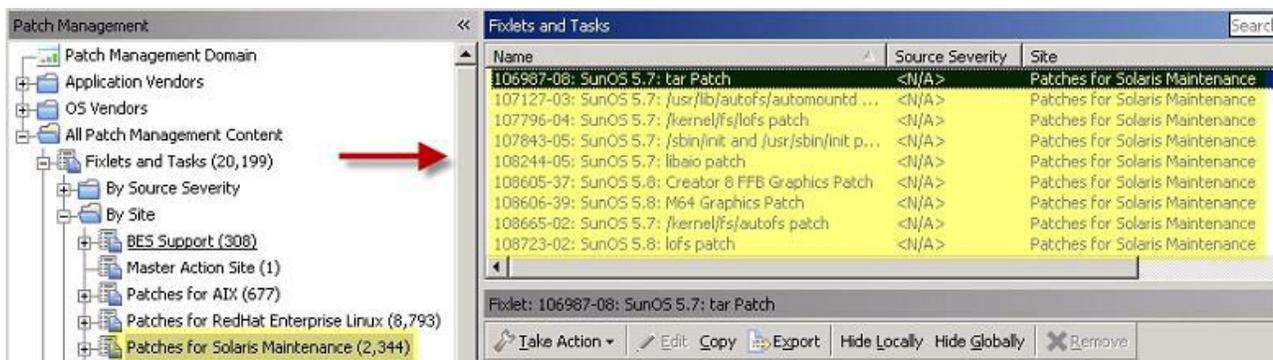


Figure 12. Fixlet and Tasks List panel for the Patches for Solaris Maintenance site

Tip: It is suggested that you deploy the latest Critical Patch Updates (CPU) Fixlets before deploying the Fixlets for the Patch Clusters.

Note: The Oracle Recommended Patch Clusters are updated frequently. The patch vendor updates cause the sha1 value and the size of the patch bundle to change. The frequent patch updates might cause the Fixlets for the Patch Clusters to fail. Updated Fixlets are provided based on the service-level agreement with the patch vendor.

Important: For Solaris 11, ensure that the repository contains the required SRU to patch the endpoints. If the local repository does not contain the latest SRU or the SRU needed for the endpoint, run the tasks to update the repository i.e. Update Repository for Solaris 11 SRU 1 (x86).

Click the tabs at the top of the Fixlet window to review additional details, and then click the appropriate link in the Actions box to start deployment. Click **OK** and enter your Private Key Password, if applicable.

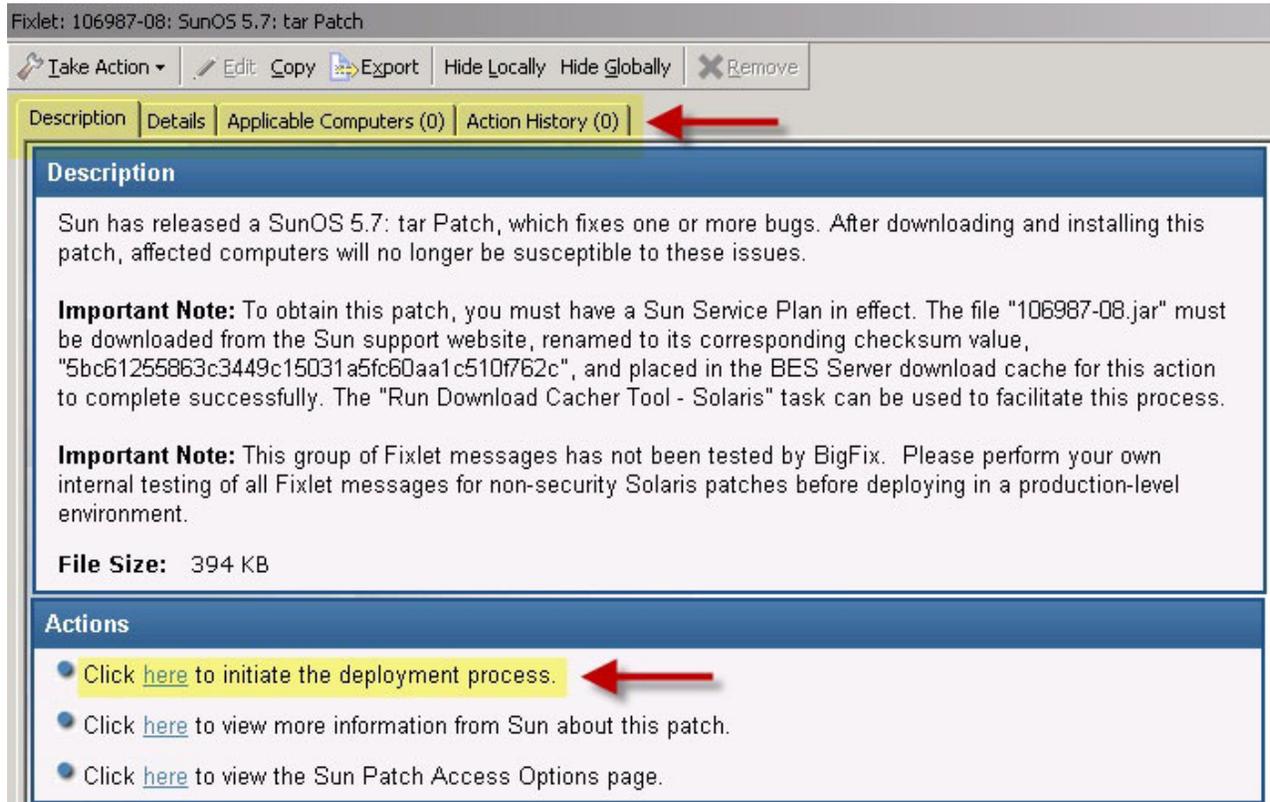


Figure 13. Fixlet window

Local repositories

IBM Endpoint Manager provides a method for using local repositories to store patch updates for Solaris 11.

Solaris 11 uses Image Packaging System, which is a new network-based package management system.

Regularly updating the endpoints in your deployment is crucial to the success of your organization. Network restrictions often prevent you from getting the latest set of changes from the Oracle hosted repositories. Maintain your own local package repositories to try to limit this restriction. By using local repositories, you can control which updates the endpoints have access to.

You can have multiple local repositories in your environment. For example, you might have one local repository that is used to mirror the latest SRU changes from Oracle and another repository that contains only one particular SRU.

For more information about Solaris 11, see the Oracle website at http://docs.oracle.com/cd/E23824_01/html/E21803/repo_intro.html.

Endpoint Manager provides the **Solaris Image Packaging System Repository Management dashboard** to easily configure local repositories to be used for patching Solaris 11 endpoints. For more information about the dashboard, see “Solaris Image Packaging System Repository Management dashboard overview” on page 14.

Note: You need to subscribe to the Patches for Solaris 11 site to access Fixlet content for Solaris 11/11 and Solaris 11.1.

Single-user mode patch application

You must bring computers into single-user mode to prepare them for kernel-level or cluster-level patching.

By default, the Endpoint Manager Solaris Patch solution applies Solaris patches in the current run level of the computer. Typically, Solaris computers use Run Level 3 or Multi-User mode. In some cases, single-user mode is used to successfully apply the Solaris patch.

The Patches for Solaris and Patches for Solaris Maintenance sites provide a task to bring a Solaris system down to single-user mode called **Single-User Mode Task - Solaris** task (ID #28).

Note: Systems in single-user mode have extremely limited functionality and restricted network connectivity. Users who are remotely connected to the computer when the single-user mode action is applied lose their connection. Do not put a system into single-user mode unless you understand the effects of this action.

Creating a baseline for single-user mode

Create a baseline to modify a Solaris patch Fixlet for single-user mode.

Note: Your Endpoint Manager deployment must include a subscription to the **Patches for Solaris** site to complete the following tasks.

Perform the following steps for each Solaris patch Fixlet that you want to apply in single-user mode.

1. Click the **Tools** menu at the top of the IBM Endpoint Manager console and select **Create New Baseline**.

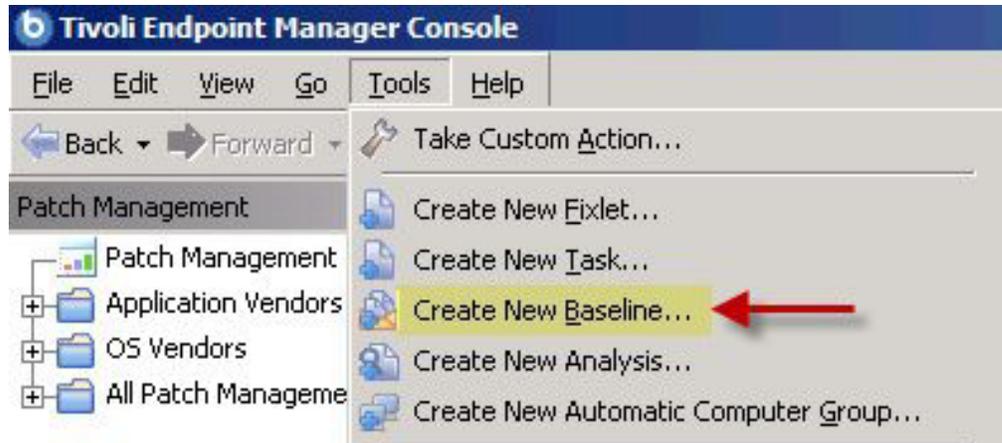


Figure 14. Create a baseline from the Tools menu

The Create Baseline window opens.

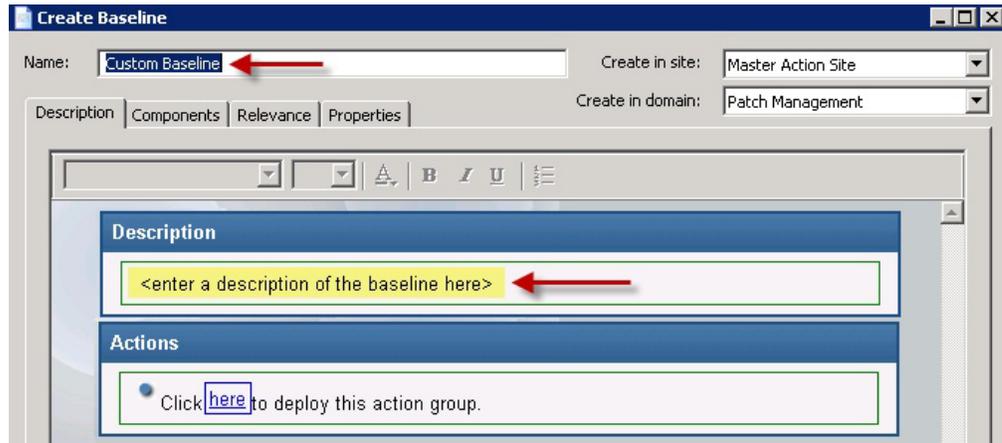


Figure 15. Create Baseline window

2. Enter a Name and Description, such as Recommended Patch Cluster - Solaris 10 (Single User Mode).

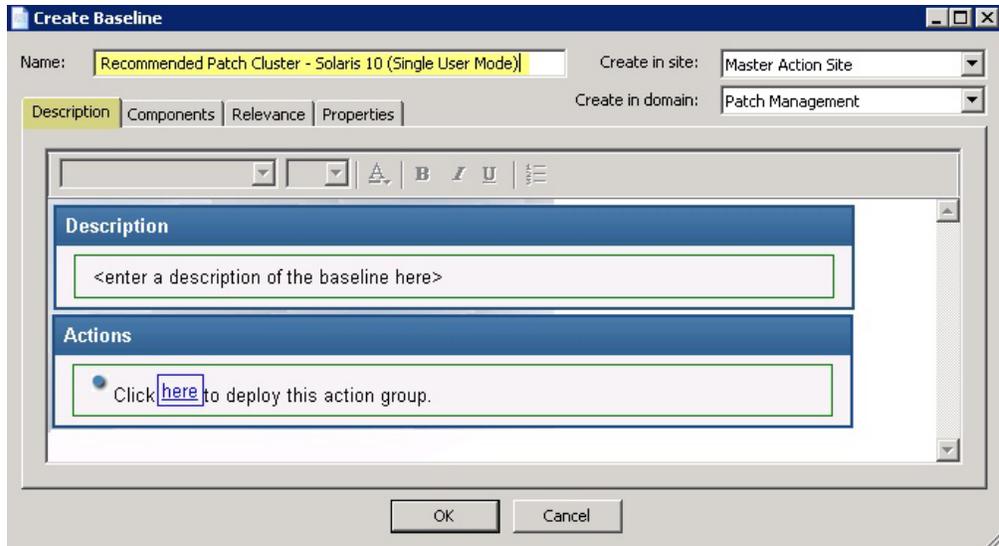


Figure 16. Description tab of the Create Baseline window

3. Click the **Components** tab.

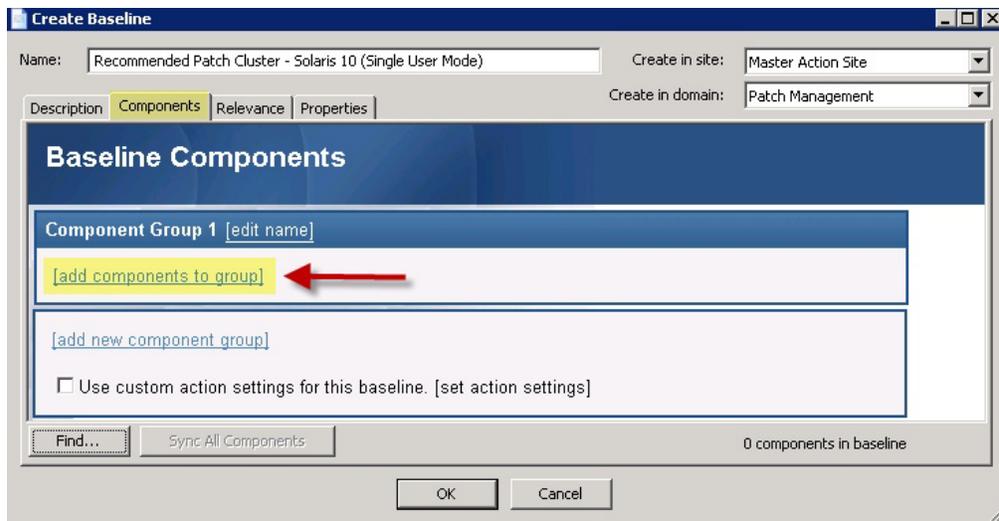


Figure 17. Components tab of the Create Baseline window

4. On the **Components** tab, add the following items to Component Group 1 and ensure that they are ordered as follows:
 - a. The **Single-User Mode Task - Solaris** (ID #28 in the Patches for Solaris site).
 - b. One or more Solaris Patch Fixlets available in the Patches for Solaris site.
 - c. Depending on the requirements of the patch, choose either:
 - **Reboot Task - Solaris** (ID #32 in the Patches for Solaris site)
 - **Reconfigure Reboot Task - Solaris** (ID #30 in the Patches for Solaris site)
5. Click **OK** and enter your Private Key Password. You can now apply the baseline to the Solaris patches that you specified in Single User mode.

Deploying Solaris packages

You can use the Solaris Package Deployment Wizard to deploy Solaris packages on to Solaris computers that have the Endpoint Manager client installed.

After you download a Solaris package, you can use the deployment wizard to facilitate deployment. In the Content Filters section of the navigation tree, click **OS Vendors > Sun Microsystems Solaris > Configuration > Solaris Package Deployment Wizard**.

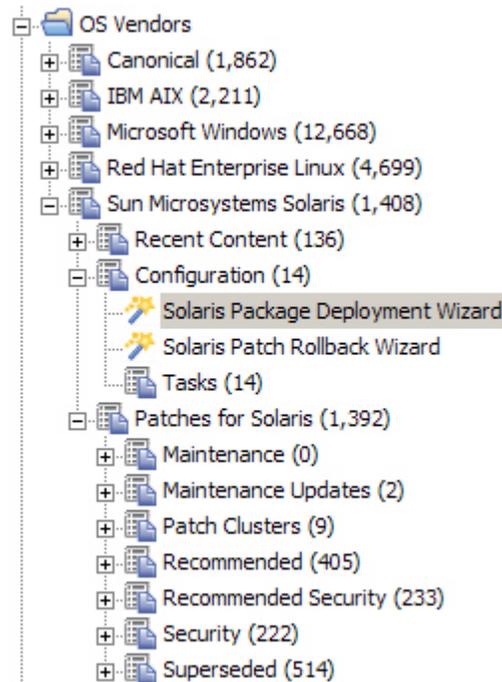


Figure 18. Solaris Package Deployment Wizard navigation tree

When the wizard opens, choose the Solaris package (either patch or cluster) that you want to deploy.

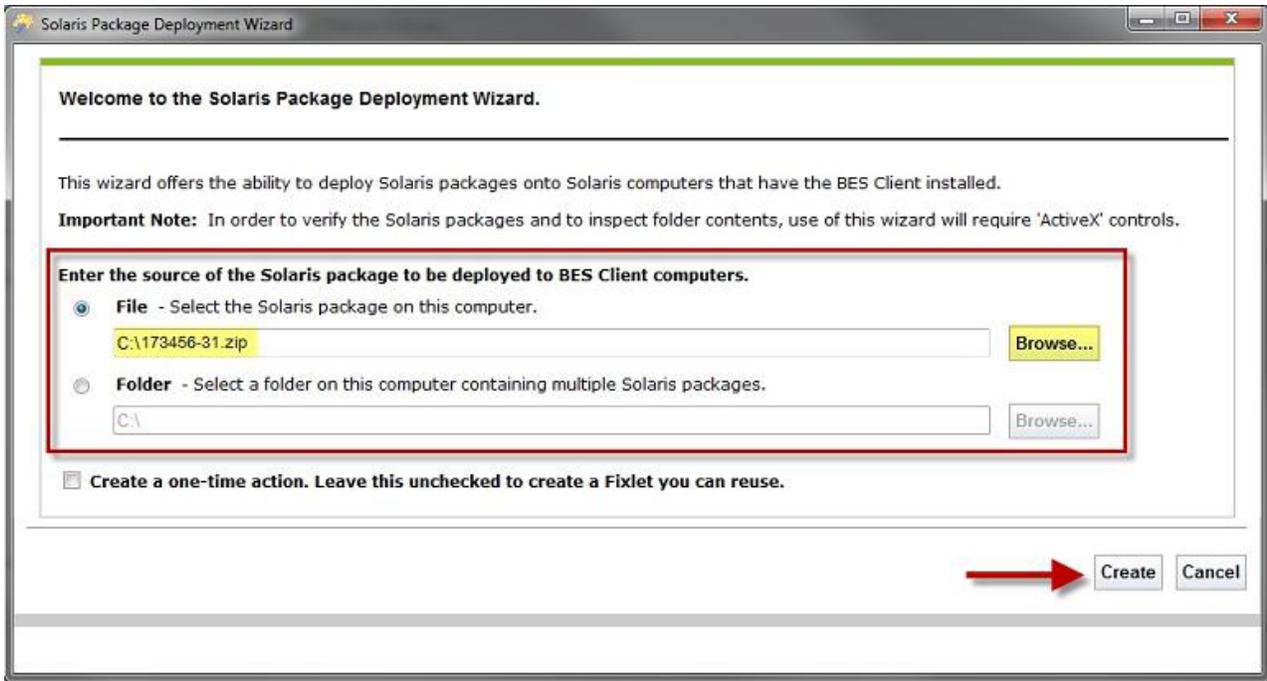


Figure 19. Solaris Package Deployment Wizard

Click the check box to create a one-time action, or leave it blank to create a Fixlet that you can reuse. When complete, click **Create**. You see the following progress screen.

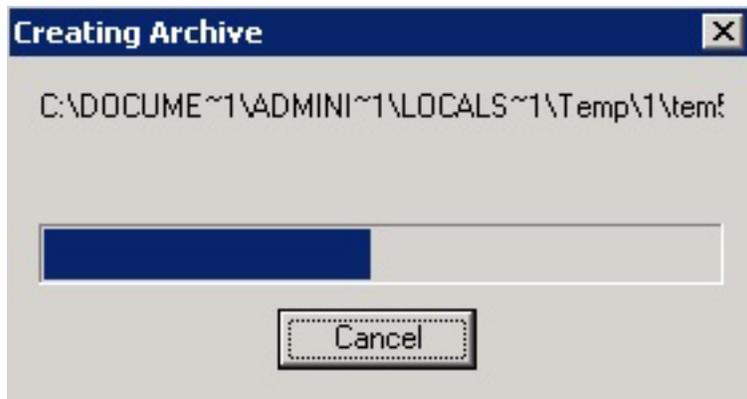


Figure 20. Creating Archive

When the first task window opens, click **OK** and enter your Private Key Password. Then click in the Actions box to start deployment.

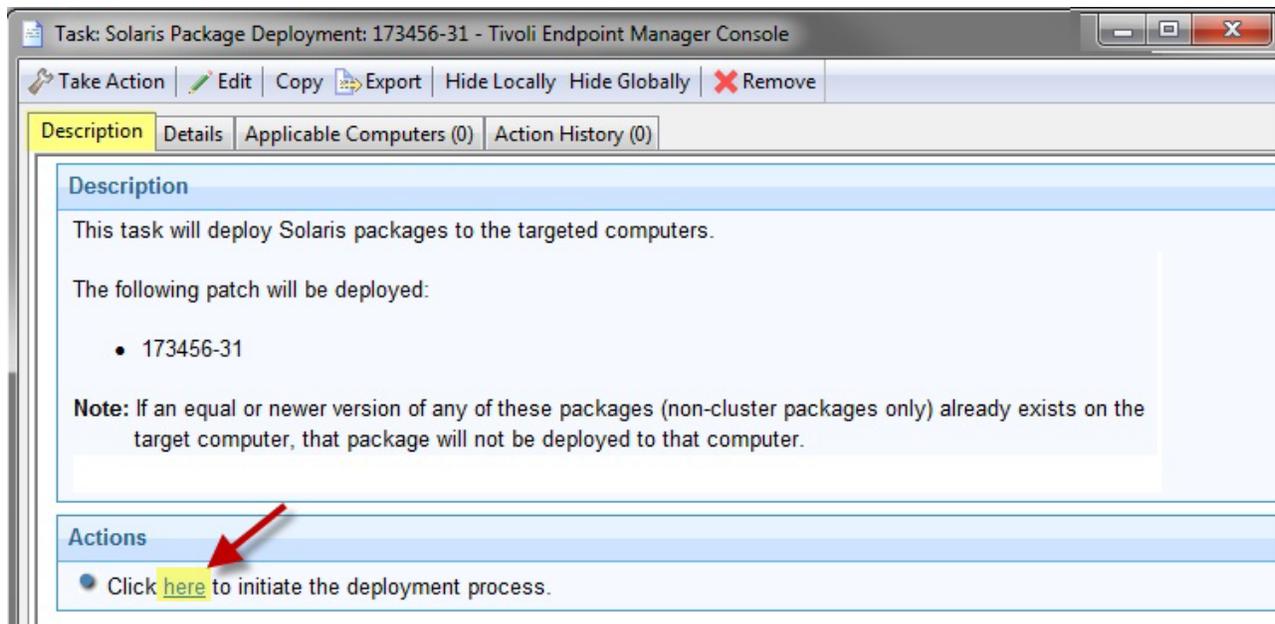


Figure 21. Description tab of the Solaris Package Deployment task

When the Take Action dialog opens, use the tabs across the top of the window to set parameters for this action. Click **OK** and enter your Private Key Password. The wizard deploys this action to your clients.

To avoid problems with disk space, run the **Clean Solaris Deployment Wizard Packages** task (ID #24 in the Patches for Solaris Site) with the options you need.

Uninstalling patches

You can uninstall Solaris patches from Solaris 9 and 10 computers by using the Solaris Patch Rollback Wizard.

Note: The result of the Solaris Patch Rollback Wizard might vary depending on several factors in your environment.

Click **OS Vendors** in the navigation tree, **Sun Microsystems Solaris**, and **Solaris Patch Rollback Wizard**.

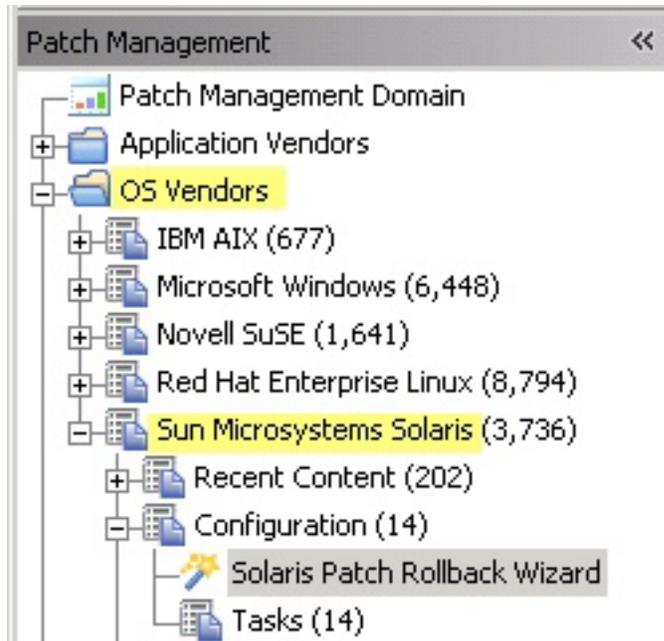


Figure 22. Solaris Patch Rollback Wizard navigation tree

Click the link to activate the *Patchrm Output* property, which you use to view detailed results.



Figure 23. Solaris Patch Rollback Wizard

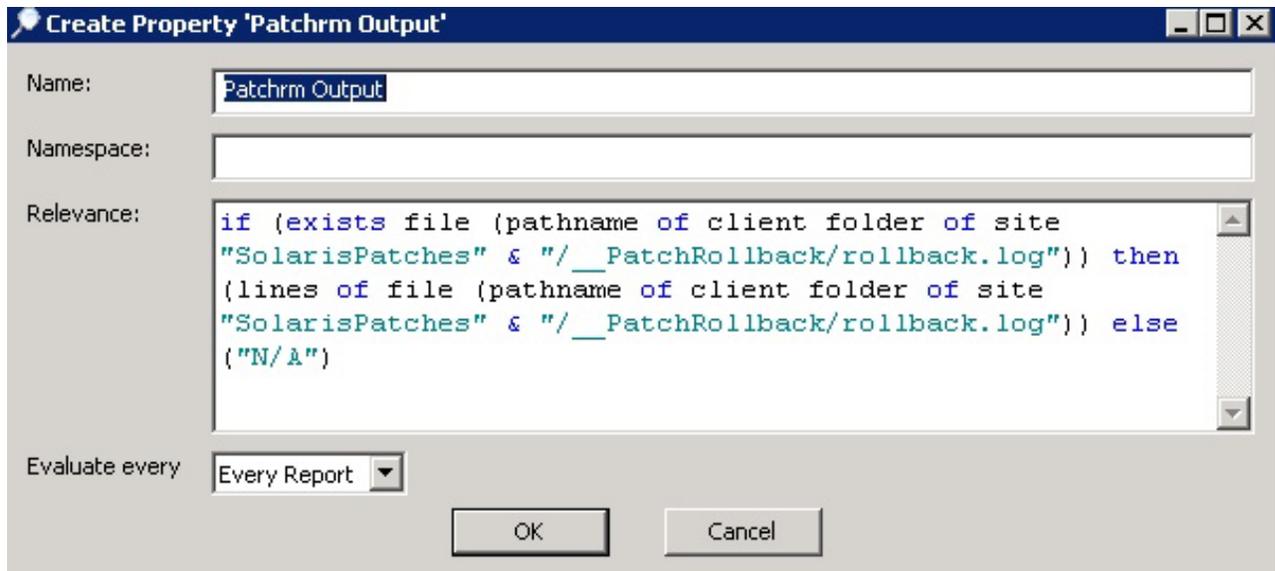


Figure 24. Create Property window

Enter a namespace, and choose the interval for which you want to evaluate output. Click **OK**. When you return to the wizard, you see the message as a note:

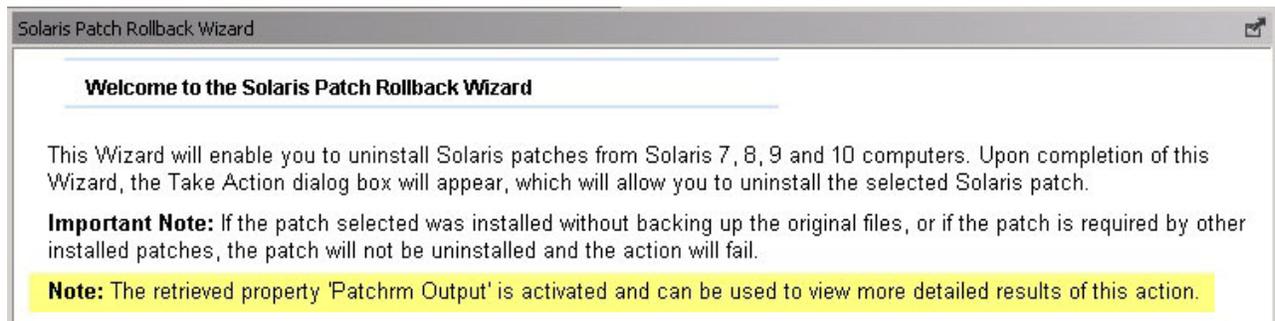


Figure 25. Retrieved property shown in the Solaris Patch Rollback Wizard

Select a Solaris patch from the drop-down menu, or type the Patch ID of the patch that you want to uninstall.

Click **Finish**. The Take Action dialog opens.

Use the tabs across the top of the window to set parameters for this action. Click **OK** and enter your Private Key Password. The wizard deploys this action to your clients.

Superseded Fixlets

Superseded Fixlets are Fixlets that contain outdated patch packages. If a Fixlet is superseded, a newer Fixlet exists with newer versions of the packages.

A superseded Fixlet is identified by (*Superseded*) at the end of its Fixlet name.

Name	Source Sev...	Site
112905-03: SunOS 5.9: acctctl & ippctl patch	<Unspecified>	Patches for Solaris Maintenance
112908-40: SunOS 5.9: krb5, gss patch	<Unspecified>	Patches for Solaris
112912-01: SunOS 5.9: Libinetcfg Patch	<Unspecified>	Patches for Solaris
112913-02: SunOS 5.9: fruadm Patch	<Unspecified>	Patches for Solaris Maintenance
112915-06: SunOS 5.9: snoop Patch	<Unspecified>	Patches for Solaris
112916-01: SunOS 5.9: rtquery Patch	<Unspecified>	Patches for Solaris
112918-01: SunOS 5.9: route Patch	<Unspecified>	Patches for Solaris
112920-03: Obsoleted by: 112920-04 SunOS 5.9: libipp, lp, IKE Patch (Superseded)	<Unspecified>	Patches for Solaris
112921-09: SunOS 5.9: Libkadm5 Patch (Superseded)	<Unspecified>	Patches for Solaris

Figure 26. View of superseded Fixlets from the List panel

You can find the new Fixlet name and ID in the description of the superseded Fixlet.

Name	Source Sev...	Site
112905-03: SunOS 5.9: acctctl & ippctl patch	<Unspecified>	Patches for Solaris Maintenance
112908-40: SunOS 5.9: krb5, gss patch	<Unspecified>	Patches for Solaris
112912-01: SunOS 5.9: Libinetcfg Patch	<Unspecified>	Patches for Solaris
112913-02: SunOS 5.9: fruadm Patch	<Unspecified>	Patches for Solaris Maintenance
112915-06: SunOS 5.9: snoop Patch	<Unspecified>	Patches for Solaris
112916-01: SunOS 5.9: rtquery Patch	<Unspecified>	Patches for Solaris
112918-01: SunOS 5.9: route Patch	<Unspecified>	Patches for Solaris
112920-03: Obsoleted by: 112920-04 SunOS 5.9: libipp, lp, IKE Patch (Superseded)	<Unspecified>	Patches for Solaris
112921-09: SunOS 5.9: Libkadm5 Patch (Superseded)	<Unspecified>	Patches for Solaris

Fixlet: 112920-03: Obsoleted by: 112920-04 SunOS 5.9: libipp, lp, IKE Patch (Superseded)

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

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

Description

Sun has released a **Obsoleted by: 112920-04 SunOS 5.9: libipp, lp, IKE Patch** which fixes several security vulnerabilities. After downloading and installing this patch, affected computers will no longer be susceptible to these vulnerabilities.

Note: Affected computers will report back as 'Pending Restart' once the patch has run successfully, but will not report back their final status until the affected computer is restarted.

Note: Sun recommends that this patch be installed in single-user mode. The "Single-User Mode Task" for Solaris can be used to facilitate this process.

Figure 27. Description of a superseded Fixlet showing the newer Fixlet ID

Enabling superseded Fixlets

You can install an earlier version of a Solaris patch by enabling superseded Fixlets.

Superseded patches are patches that are declared obsolete by Oracle, and have typically been replaced by newer patches.

You can use the **Enable Superseded Solaris Patch Evaluation** task (ID #13 in the Patches for Solaris and Patches for Solaris Maintenance sites) to install an earlier version of a Solaris patch on a client.

1. In the navigation tree of the Patch Management domain, expand the **OS Vendors** node.
2. Expand the **Sun Microsystems Solaris** node, and select **Configuration**.
3. In the List Panel, select the task **Enable Superseded Solaris Patch Evaluation**. The task window opens.
4. Select the link to enable evaluation of superseded Solaris patches in the Actions box. The Take Action dialog box opens.
5. Use the tabs across the top of the window to set parameters for this action.
6. Deploy the action. For information about deploying actions, see the *IBM Endpoint Manager Console Operator's Guide*.

Chapter 4. Solaris Live Upgrade support

Use the Solaris Live Upgrade tool to manage system downtime and risk when installing patches on alternate boot environments on Solaris 9 and 10 computers.

Introduction

An alternate boot environment of a Solaris computer is typically created by copying the entire root file system. With Solaris Live Upgrade, patches are applied in the duplicate boot environment, which is in an inactive state, while the original boot environment is running. After patching is done, you can restart your computer to use the alternate boot environment. For more information about Solaris Live Upgrade, see the Solaris Live Upgrade 2.0 Guide from the Oracle documentation: <http://www.oracle.com/technetwork/indexes/documentation/index.html>.

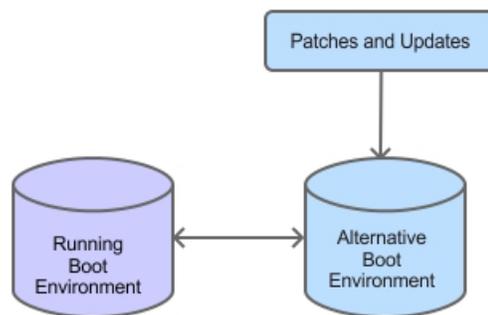


Figure 28. Solaris Live Upgrade overview

Solaris Live Upgrade supports patch management for Security Patches, Recommended Patches, and Critical Patch Updates. You can find the related Fixlets in the Patches for Solaris Live Upgrade site.

Roadmap

To use Solaris Live Upgrade, complete the following steps:

1. Ensure that the download plug-in is enabled. For more information, see Download plug-ins.
2. Run the Enable Solaris Live Upgrade task. See the steps in Running the enable Solaris Live Upgrade task.
3. Ensure that the inactive boot environment that you want to patch has an Endpoint Manager client installed. For more information, see “Installing the Endpoint Manager client” on page 35.
4. The process for patching boot environments depends on the system environment:
 - If there is only one inactive boot environment on the system, proceed with patching. For more information about patching, see Chapter 3, “Patching using Fixlets,” on page 17. Then, proceed to step 5.

- If there are several inactive boot environments, you must select one boot environment for live upgrade from the Manage Solaris Boot Environments dashboard. For more information about this task, see “Selecting inactive boot environments for Live Upgrade” on page 35.

For more information about the dashboard, see “Manage Solaris Boot Environments dashboard overview” on page 33.

5. Activate the newly-patched boot environment. For more information, see “Activating inactive boot environments” on page 36.

Note: You must activate the boot environment that you choose immediately before rebooting the computer.

6. Reboot to the alternate boot environment. For more information, see “Rebooting to an alternate boot environment” on page 37.

Running the Enable Solaris Live Upgrade task

To use Solaris Live Upgrade correctly, you must deploy the Enable Solaris Live Upgrade task on every Solaris computer.

To access the **Enable Solaris Live Upgrade** task (ID #2), you must subscribe to the Patches for Solaris Live Upgrade site.

The **Enable Solaris Live Upgrade** task determines the inactive boot environments and their patch levels on Solaris computers.

1. From the Patch Management domain, click **Patch Management > Fixlets and Tasks**.
2. Click **Enable Solaris Live Upgrade**.

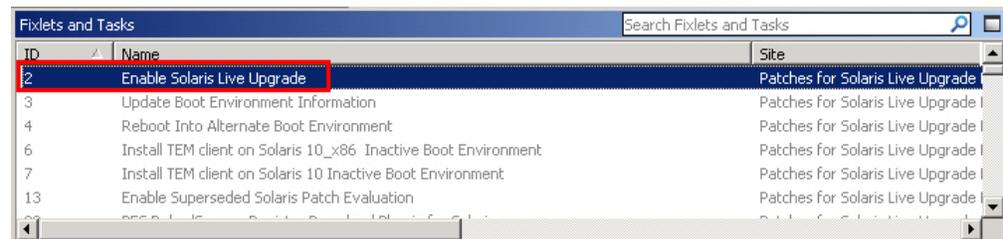


Figure 29. Enable Solaris Live Upgrade task

3. Run the action.

The inactive boot environments for each Solaris computer are now visible in the Manage Solaris Boot Environment dashboard.

For systems with only one inactive boot environment, that inactive boot environment is automatically selected to use Solaris Live Upgrade. All Solaris Live Upgrade Fixlets become relevant.

If you have a system with only one inactive boot environment, you can proceed with patching the boot environment using Fixlets.

If you have more than one inactive boot environment, you must use the Manage Solaris Boot Environments dashboard to identify which inactive boot environment is going to use Solaris Live Upgrade.

Manage Solaris Boot Environments dashboard overview

Patch Management for Solaris provides a dashboard to manage boot environments for Solaris Live Upgrade.

You can use the Manage Solaris Boot Environments dashboard to complete the following tasks:

- Install the Endpoint Manager client in inactive boot environments.
- Select inactive boot environments for Live Upgrade.
- Activate inactive boot environments.
- Reboot systems to boot environments that you have activated.

Before you use the dashboard, you must deploy the following task and analysis:

- **Enable Solaris Live Upgrade** - ID #2 in the Patches for Solaris Live Upgrade site. For more information about the task, see “Running the Enable Solaris Live Upgrade task” on page 32.
- **Boot Environment Information** - ID #5 in the Patches for Solaris Live Upgrade site. This analysis gets boot environment data from Solaris computers.

You can access the dashboard from the navigation pane by clicking **Patch Management > All Patch Management > Dashboards > Manage Solaris Boot Environments**.

The dashboard is divided into two tables: Solaris Computers and Inactive Boot Environments.

<input type="checkbox"/>	Host Name	IP Address	Operating System Ver	Active Boot Environme	Client Version	Number of Boot Environ
<input type="checkbox"/>	unknown	10.1.232.117	SunOS 5.10 (Generic_14	benv1	8.2.1372.0	3
<input type="checkbox"/>	com1	10.1.12.128	SunOS 5.9 (Generic_118	c110d0s0	8.2.1372.0	3
<input type="checkbox"/>	com2	10.1.12.129	SunOS 5.10 (Generic_13	benv1	8.2.1372.0	3
<input type="checkbox"/>	com3	10.1.255.233	SunOS 5.10 (Generic_14	old	8.2.1310.0	3

<input type="checkbox"/>	Boot Environment Name	Computer Name	Client Version	Selected for Live Upgrade	Active on Reboot

Figure 30. Manage Solaris Boot Environments dashboard

The Solaris Computers table displays all Solaris computers in your deployment, and includes the following information:

- Host name
- IP address

- Version of the installed operating system
- Name of the active boot environment
- Version of the client installed on the active boot environment
- Number of boot environments for each computer

You can select multiple Solaris computers to display all the corresponding boot environments in one consolidated view.

The dashboard shows the status of each boot environment. It shows whether the boot environment is selected for Live Upgrade or if it was selected as the running boot environment for when the system restarts.

The dashboard can also determine whether the Endpoint Manager client is installed in a boot environment. If the client is installed, the dashboard displays its corresponding version.

The dashboard has a live keyword search capability for Solaris computers and boot environments. You can search based on the naming convention of the computer or boot environment name.



Figure 31. Search for computer or boot environment name

Endpoint Manager client installation behavior

The version of the client that is installed on an inactive boot environment depends on the client version that is in the running boot environment.

The process of installing the client on an inactive boot environment depends on the state of the inactive boot environment:

Inactive boot environment without the client

The latest available minor version of the client in the active boot environment is installed in the inactive boot environment.

Inactive boot environment that has an earlier version of the client than the active boot environment

The client in the inactive boot environment is upgraded to the latest minor version of the client in the active boot environment.

Inactive boot environment that has a later version of the client than the active boot environment

The client in the inactive boot environment remains unchanged.

For example,

Server Version: 8.2.1175

Running boot environment client version: 8.1.608 (Latest available version is 8.1.634)

Inactive BE_First client version: 8.0.584 (Latest available version is 8.0.627)

Inactive BE_Second client version: 8.2.1078 (Latest available version is 8.2.1372)

Inactive BE_Third client version: 8.1.608

Inactive BE_Fourth client not installed.

Output:

BE_First: Version is upgraded to 8.1.634
 BE_Second: No changes (Version remained at 8.2.1078)
 BE_Third: Version upgraded to 8.1.634
 BE_Fourth: Version 8.1.634 is installed

Installing the Endpoint Manager client

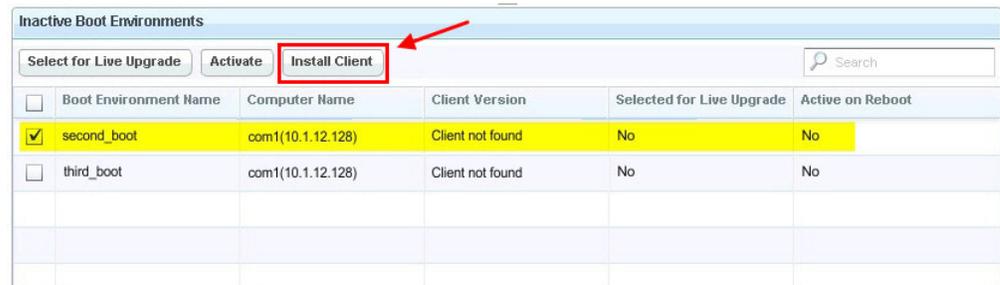
The Endpoint Manager client must be installed on all boot environments to use Solaris Live Upgrade correctly.

You can install the client from the Manage Solaris Boot Environments dashboard. To know more about how the client installation works from the Manage Solaris Boot Environments dashboard, see “Endpoint Manager client installation behavior” on page 34.

You cannot select the boot environment for Live Upgrade from the dashboard if the client is not installed in the boot environment.

Note: Systems with only one inactive boot environment that do not have the client installed are by default selected for Live Upgrade.

1. From the Manage Solaris Boot Environments dashboard, choose the inactive boot environments where you want the client to be installed.
2. Click **Install Client**.



Inactive Boot Environments					
<input type="checkbox"/> Select for Live Upgrade		<input type="button" value="Activate"/>	<input type="button" value="Install Client"/>	<input type="text" value="Search"/>	
<input type="checkbox"/>	Boot Environment Name	Computer Name	Client Version	Selected for Live Upgrade	Active on Reboot
<input checked="" type="checkbox"/>	second_boot	com1(10.1.12.128)	Client not found	No	No
<input type="checkbox"/>	third_boot	com1(10.1.12.128)	Client not found	No	No
<input type="checkbox"/>					
<input type="checkbox"/>					

Figure 32. Installing the Endpoint Manager client in an inactive boot environment

The Take Action dialog opens. For more information about using the Take Action dialog, see the *IBM Endpoint Manager Console Operator's Guide*.

3. Select the computers where the boot environments belong.
4. Click **OK**. It usually takes a few minutes for the targeted computers to report back their Action status.

The client is now installed in the selected boot environments.

Selecting inactive boot environments for Live Upgrade

Use the Manage Solaris Boot Environment dashboard to select the inactive boot environments that you want to patch.

You must install the client in the boot environments that you want to select for Live Upgrade.

You cannot select two boot environments from the same computer to use Live Upgrade. Ensure that the selected boot environments belong to different computers.

1. From the Manage Solaris Boot Environments dashboard, choose the inactive boot environments for Live Upgrade.
2. Click **Select for Live Upgrade**.

<input type="checkbox"/>	Boot Environment Name	Computer Name	Client Version	Selected for Live Upgrade	Active on Reboot
<input checked="" type="checkbox"/>	second_boot	com1(10.1.12.128)	8.2.1372.0	No	No
<input type="checkbox"/>	third_boot	com1(10.1.12.128)	Client not found	No	No

Figure 33. Select Boot Environments for Live Upgrade

The Take Action dialog opens. For more information about using the Take Action dialog, see the *IBM Endpoint Manager Console Operator's Guide*.

3. Select the appropriate settings.
4. Click **OK**. It usually takes a few minutes for the targeted computers to report back their Action status.

The boot environments that you selected are ready for Live Upgrade.

After you select a boot environment for Live Upgrade, you can proceed with patching the environment using Fixlets. For more information, see Chapter 3, "Patching using Fixlets," on page 17.

Activating inactive boot environments

The inactive boot environment that is selected for activation becomes the running boot environment after a restart. Use the Manage Solaris Boot Environment to identify the boot environments that you want to activate.

You cannot activate boot environments that are not selected for Live Upgrade.

You can activate only one inactive boot environment for each computer.

Synchronization between the running boot environment and an inactive boot environment occurs upon activation. The BES configuration file from the running boot environment is copied to the inactive boot environment for a smooth transition.

1. From the Manage Solaris Boot Environments dashboard, choose the inactive boot environments that you want to activate.
2. Click **Activate**.

Inactive Boot Environments					
<input type="checkbox"/> Select for Live Upgrade		<input type="checkbox"/> Activate		<input type="checkbox"/> Install Client	
<input type="checkbox"/>	Boot Environment Name	Computer Name	Client Version	Selected for Live Upgrade	Active on Reboot
<input checked="" type="checkbox"/>	second_boot	com1(10.1.12.128)	8.2.1372.0	Yes	No
<input type="checkbox"/>	third_boot	com1(10.1.12.128)	Client not found	No	No

Figure 34. Activate

The Take Action dialog opens. For more information about using the Take Action dialog, see the *IBM Endpoint Manager Console Operator's Guide*.

3. Select the appropriate settings.
4. Click **OK**. It usually takes a few minutes for the targeted computers to report back their Action status.

The boot environments that you selected are now activated. These boot environments are identified as active after a restart.

Reboot the boot environments immediately after activation.

Rebooting to an alternate boot environment

Use the Manage Solaris Boot Environments dashboard to restart the current running boot environment to the boot environment that you want.

You must select and activate the alternate boot environment before rebooting. If you click **Reboot** without selecting an alternate boot environment for activation, the computer restarts to its existing state.

1. From the Manage Solaris Boot Environments dashboard, choose a computer from the Solaris Computers table.
2. Click **Reboot**.

Solaris Computers						
<input type="checkbox"/> Reboot		<input type="text"/> Search				
<input type="checkbox"/>	Host Name	IP Address	Operating System Ver	Active Boot Environme	Client Version	Number of Boot Environ
<input type="checkbox"/>	unknown	10.1.232.117	SunOS 5.10 (Generic_14	benv1	8.2.1372.0	3
<input checked="" type="checkbox"/>	com1	10.1.12.128	SunOS 5.9 (Generic_118	c110d0s0	8.2.1372.0	3
<input type="checkbox"/>	com2	10.1.12.129	SunOS 5.10 (Generic_13	benv1	8.2.1372.0	3
<input type="checkbox"/>	com3	10.1.255.233	SunOS 5.10 (Generic_14	old	8.2.1310.0	3

Figure 35. Reboot to an inactive boot environment

The Take Action dialog opens. For more information about using the Take Action dialog, see the *IBM Endpoint Manager Console Operator's Guide*.

3. Select the appropriate settings.
4. Click **OK**. It usually takes a few minutes for the targeted computers to report back their Action status.

The Solaris computer restarts to the new active boot environment.

Appendix A. 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

Appendix B. Frequently asked questions

To better understand Patch Management for Solaris, read the following questions and answers.

Why does a patch fail, but complete successfully?

Sometimes under specific circumstances, a patch is successfully applied but the relevance conditions indicate that it is still needed. Check to see if there are any special circumstances that are associated with the patch, or contact IBM Software Support.

If a patch fails to install, what should I do?

If a patch fails to install, check to see if you applied the patch to the correct computers, or run the patch manually by downloading it from the Oracle website.

Why is there no default action?

You must always test on a testbed before applying the Fixlet or patch. There can also be multiple actions that are associated with the Fixlet. Be sure to read the text in the Description tab of the Fixlet before starting the action.

What are superseded patches?

Superseded patches are older versions of patches that no longer need to be applied.

How do I handle missing patches?

IBM Endpoint Manager provides all patches except those patches that are unbundled. Missing patches might be superseded. For recently superseded content, run Task 13 to allow supersedence evaluation. For information about older content, contact IBM Software Support.

I already have an Oracle support account, but the plug-in to download patches still failed. Why is that?

Your Oracle support account must have a valid support identifier to successfully download patches.

How much space do I need to download and install patches of "Recommended Patch Clusters" or "Critical Patch Updates" (CPU)?

You must have at least 5 GB of space for the entire process; approximately 2 GB is used to download the file and approximately 3 GB is used to extract and install the file.

The sha1 value and the size of the Patch Cluster Fixlets are outdated. Why is that?

The sha1 value and the size of the Patch Cluster Fixlet might be outdated due to the frequent Oracle Recommended Patch Clusters updates. Updated Fixlets are provided based on the service-level agreement with the patch vendor.

How do I verify if the download plug-in was registered correctly?

Run a Fixlet with an action task to verify if the download plug-in is registered correctly. Verify that the patch download is successful. Otherwise, you might need to unregister the download plug-in and register it again.

How do I register a download plug-in? Do I use the register download plug-in task or the Manage Download Plug-in dashboard?

To register a download plug-in, you must use the Manage Download Plug-in dashboard in the Patching Support site. Existing register download plug-in tasks are being deprecated. To learn more about plug-in registration, see “Registering the Solaris download plug-in” on page 5.

Note: You must also use the Manage Download Plug-in dashboard to unregister, configure, and upgrade download plug-ins. The existing unregister and edit download plug-in tasks are being deprecated. For more information about the dashboard, see the topic on Manage Download Plug-ins dashboard in the IBM Endpoint Manager Information Center.

I was expecting the password to be obfuscated, but it is still in clear text. Why is that?

Check that your download plug-in version is earlier than 2.0. If so, you are still using an old version of the download plug-in that stores credentials in clear text. To encrypt credentials, upgrade your download plug-in to version 2.0 or later from the Manage Download plug-ins dashboard in the Patching Support site.

I'm having problems with the Solaris download plug-in. What should I do?

Locate the `plugin.ini` file from the `C:\Program Files (x86)\BigFix Enterprise\BES Server\DownloadPlugins\SolarisProtocol` directory. Check and confirm that the configurations are properly set in the `plugin.ini` file.

What happens when I do not select an inactive boot environment for Activation before I reboot a computer?

The computer reboots back to the current active boot environment.

I already have the client in some of the boot environments. What happens to them when I install the client from the Manage Solaris Boot Environment dashboard?

To find out what happens to those boot environments, see “Endpoint Manager client installation behavior” on page 34.

How do I patch boot environments with a baseline?

Use baselines to patch boot environments in the same way that you use baselines to patch computers.

Can I select multiple boot environments for Live Upgrade on a single machine?

Even if you have more than one inactive boot environment on a Solaris machine, you can select only one boot environment for Live Upgrade.

I cannot activate multiple boot environments that are on the same machine. Why is that?

Activating a boot environment makes it bootable on the next reboot of the system. Also, Solaris machines can have only one running boot environment at a time.

I selected multiple boot environments for Live Upgrade. Why are some of the boot environments excluded from the action?

The boot environments that are excluded from an action might not have passed the requirements for that action. Each action has its own set of criteria:

Selecting boot environments for Live Upgrade:

A client must be installed in the boot environment.

Only one boot environment for each computer can be selected for Live Upgrade.

Activating boot environments:

A client must be installed in the boot environment.

The boot environment must first be selected for Live Upgrade before activation.

Only one boot environment for each computer can be activated.

What can I do if an inactive boot environment is selected for Live Upgrade even if it does not have a client installed? Is this scenario even possible?

Yes, this scenario might occur when the "Enable Solaris Live Upgrade" task is deployed on a system with only one inactive boot environment. The task, by default, selects the inactive boot environment for Live Upgrade without checking the existence of a client. If you encounter this scenario, you must install the client from the Manage Solaris Boot Environment dashboard.

Why do I see duplicate computers in the Manage Solaris Boot Environment dashboard?

Computers have different client IDs. When a computer abruptly goes offline and comes back on, a new client ID is assigned to the computer. The console does not recognize the old computer because of its new client ID. It is suggested that you delete the computer with the oldest report time. Complete the following steps:

1. Click **All Content > Computers**.
2. Right-click the computer you want to delete.
3. Click **Remove from Database**.

What does the Enable Solaris Live Upgrade task do?

When Live Upgrade is enabled, a back-end utility script fetches information from all the boot environments. The information is saved in a plain text format, which can be found in `/var/opt/BESClient/__BESData/__Global/LUdata`.

Where can I find the log files for Live upgrade?

The Live Upgrade log files are in `/var/opt/BESClient/__BESData/__Global/LUdata`. The following log files can be used for troubleshooting:

SLU.log

To verify that the boot environment was successfully enabled for Live Upgrade.

restart.log

To verify that the boot environment was successfully activated.

new_package.txt

To verify that the client is already installed in a boot environment. If the client version is not listed in the file, the client is not installed.

What do I do if the active boot environment displays a Null value in the dashboard?

Run the **Enable Solaris Live Upgrade** task or **Update Boot Environment Information** task, whichever is relevant.

I just switched boot environments, however the new running boot environment is not reporting to the server. What do I do?

1. Check that the client is installed.

Tip: Run `pkginfo |grep BES` from the command-line interface to check whether the client exists in the boot environment.

2. Check that the `actionsite.afxm` file is in `/etc/opt/BESClient/`.
3. Check that you can ping the server host name. If you cannot ping the server host name, edit `/etc/hosts` and add the IP address and host name in the file.

Why is it taking so long for the Manage Solaris Boot Environment dashboard to refresh after an action was taken?

The time delay might be caused by the multiple processes that are running at the back end. When an action is taken, the utility script gets the changes from the boot environments and stores the information in a text format.

The client then sends the data to the server. The server gathers the data by using the analysis, which is read by the dashboard. It usually takes a few minutes for the targeted computers to report back their Action status to the dashboard.

How do I create a local Image Packaging System (IPS) package repository?

For information about how to create an Image Packaging System (IPS) package repository, see the Oracle documentation website at <http://docs.oracle.com>.

Where can I get the key and certificate files?

You can obtain both files from the My Oracle Support site. For more information, see <http://pkg-register.oracle.com>.

Are the key and certificate files always in .pem format?

Yes, both files are in .pem format when you download them from the Oracle Support site. Note: The Solaris Image Packaging System Repository Management dashboard accepts key and certificate files in .pem format only.

Should patching Solaris 11 endpoints be done in single-user mode?

Since Live Upgrade is handled by Image Packaging System (IPS), it is not necessary to go to single-user mode. For more information, see <http://www.oracle.com/technetwork/server-storage/solaris11/overview/solaris-matrix-1549264.html>.

How much space do I need to download and install patches of SRUs?

The space that is needed depends on exactly what is installed on the system. With the SRU patching, the system finds out the missing packages on the system and downloads only the relevant files. Important: Expand the overall cache size for server and relays to downloaded large SRUs to avoid the "Disk Limited" error. SRUs can be huge, about 2.7 GB per image file. If you do not expand the cache, the gigantic download might flush out the existing files in the cache.

Does the existing Live Upgrade offer also work for Solaris 11?

No, unfortunately not. The existing Live Upgrade solution works only for Solaris 10.

I am trying to patch my machine, but I have very limited temp space, should I be concerned?

With Image Packaging System (IPS) in Solaris 11, SRUs are not downloaded entirely. The system finds out the missing packages on the system and downloads only the relevant files.

I have a local repository, how do I set it to be used for patching Solaris 11 endpoints?

Use the Solaris Image Packaging System Repository Management dashboard to set a local repository to be used for patching.

I want to patch a Solaris 11 system with the latest SRU, however, I do not have any internet connection. What do I do?

You need to have a local repository where you can bring in the latest SRU image. The endpoint can use that repository instead of connecting internet.

Do I need to run all the tasks to ensure that my local repo is up to date? Or can I run the task with the latest Support Repository Update (SRU)?

You do not need to install all the SRUs. If you want to keep the endpoints up-to-date, install the latest SRU. But if a specific SRU is required on an endpoint, then the repository must host the base repository content and the SRU that you want the endpoint to upgrade to. For example, if you have both Solaris 11/11 and 11.1 endpoints, and you want to keep them up-to-date, then your repository must host the following content:

- Solaris 11 11/11 repo base image + SRU 13.4 (latest SRU)
- Solaris 11 11.1 repo base image + SRU 14.5 (latest SRU)

What is the suggested method to patch SRUs? Is it through a local repo or through the support site?

Having a local repository helps with the download speed and network load.

Where can I find the logs for Solaris 11?

The Solaris 11 logs are in /var/opt/BESClient/IPSDData/. You can use the following log files for troubleshooting patches in Solaris 11.

Note: The logs show the latest result of an action from a Fixlet or task.

•

pkg_set_publisher.log

To verify that the new repository was assigned to an endpoint in the Solaris Image Packaging System Repository Management dashboard.

This log file contains the output from the following command:

```
pkg set-publisher -G '*' -M '*' -g 'THE_NEW_REPOSITORY_URI' solaris
```

Example of a successful message in the pkg_set_publisher.log file:

```
Startup: Refreshing catalog 'solaris' ... Done
Startup: Caching catalogs ... Done
```

Example of a failed message in the pkg_set_publisher.log file due to invalid repo URI:

```
pkg set-publisher: The origin URIs for 'solaris' do not appear to point to a va
Please verify the repository's location and the client's network configuration.
Additional details:
```

```
Unable to contact valid package repository
Encountered the following error(s):
```

Unable to contact any configured publishers.
This is likely a network configuration problem.
Framework error: code: 6 reason: Couldn't resolve host '10.1.240.299'
URL: 'http://10.1.240.299' (happened 4 times)

update_repo_sru.log

To verify that the repository update task was successful. The log file contains information about the various actions: extracting compressed files, mounting images, copying content to the repository, and rebuilding repository indexes.

Note: The log does not contain any information if the repository verification fails. The error only displays in the console. You can check "Show action information..." on the failed computer.

Example of a successful message in the update_repo_sru.log file:

```
Archive: __Download/p17865983_1100_Solaris86-64.zip
  inflating: /var/p17865983_1100_Solaris86-64/readme_11_1_14_5_0.html
  inflating: /var/p17865983_1100_Solaris86-64/readme_11_1_14_5_0.txt
  inflating: /var/p17865983_1100_Solaris86-64/sol-11_1_14_5_0-incr-repo.iso
sending incremental file list

<STATUS DURING COPYING REPOSITORY CONTENT>

sent 3004537729 bytes  received 1989315 bytes  3418450.31 bytes/sec
total size is 2994859457  speedup is 1.00
Initiating repository rebuild.
```

pkg_update_entire.log

To verify that the endpoint was updated with the specified SRU. This log file contains the output from the following command:

```
pkg update entire@PACKAGE_VERSION_FOR_THAT_SRU
```

Example of a successful message in the pkg_update_entire.log file:

```
Startup: Refreshing catalog 'solaris' ... Done
Startup: Caching catalogs ... Done
Planning: Solver setup ... Done
Planning: Running solver ... Done
Planning: Finding local manifests ... Done
Planning: Fetching manifests: 0/178 0% complete
Planning: Fetching manifests: 100/178 56% complete
Planning: Fetching manifests: 178/178 100% complete
Planning: Package planning ... Done
Planning: Merging actions ... Done
Planning: Checking for conflicting actions ... Done
Planning: Consolidating action changes ... Done
Planning: Evaluating mediators ... Done
Planning: Planning completed in 41.85 seconds
      Packages to remove: 1
      Packages to install: 3
      Packages to update: 175
      Mediators to change: 1
      Create boot environment: Yes
      Create backup boot environment: No

Download: 0/10018 items 0.0/328.8MB 0% complete
Download: 253/10018 items 15.3/328.8MB 4% complete (3.4M/s)
Download: 650/10018 items 31.4/328.8MB 9% complete (3.2M/s)
Download: 1302/10018 items 48.3/328.8MB 14% complete (3.2M/s)
```

```
Download: 1661/10018 items 117.2/328.8MB 35% complete (8.6M/s)
Download: 2426/10018 items 162.2/328.8MB 49% complete (11.4M/s)
Download: 3796/10018 items 178.1/328.8MB 54% complete (6.1M/s)
Download: 4630/10018 items 216.7/328.8MB 65% complete (5.4M/s)
Download: 6154/10018 items 243.6/328.8MB 74% complete (6.5M/s)
Download: 7938/10018 items 257.2/328.8MB 78% complete (4.1M/s)
Download: 9311/10018 items 310.0/328.8MB 94% complete (6.6M/s)
Download: Completed 328.80 MB in 54.30 seconds (6.0M/s)
```

Example of a failed message in the `pkg_update_entire.log` file that is due to unavailable SRU content in the repository:

```
Startup: Refreshing catalog 'solaris' ... Done
pkg update: 'entire@0.5.11-0.175.1.1.0.4.0' matches no installed packages
```

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.

Licenses 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.



Product Number: 5725-C45

Printed in USA