AIX Version 6.1

IBM PowerVM Workload Partitions Manager for AIX V1.2

IBM
AIX Version 6.1

IBM PowerVM Workload Partitions Manager for AIX V1.2

IBM
Note
Before using this information and the product it supports, read the information in "Notices" on page 59.
## Contents

**About this document** ............................................. v
Highlighting ....................................................... v
Case-sensitivity in AIX ........................................... v
ISO 9000. ......................................................... v

**IBM PowerVM Workload Partitions**

**Manager for AIX V1.2** ....................................... 1
What's new in IBM PowerVM Workload Partitions ............................. 1
Manager for AIX V1.2 ................................................. 1
Accessibility features for WPAR Manager ...................................... 2
WPAR Manager agent .................................................. 3
System profiles ....................................................... 5
Supported operating environments for WPAR Manager ......................... 5
Memory and disk space requirements ......................................... 6
WPAR management in a logically partitioned environment .................... 6
Application mobility ................................................... 7
System compatibility .................................................. 7
WPAR states .......................................................... 9
Relocation domains and system profiles ...................................... 10
Manual relocation ..................................................... 11
Policy-based relocation ............................................... 12
Policy tuning ........................................................ 14
Planning for application mobility ........................................ 16
Planning for Role Based Access Control .................................... 16
Installing WPAR Manager ............................................... 16
Installing WPAR Manager on the management server ....................... 17
Installing the WPAR Manager agent on the managed system ................ 17
Upgrading the WPAR Manager ........................................ 18
Migrating the WPAR Manager database .................................... 19
Migrating from Apache Derby to DB2 .................................... 19
Migrating from DB2 to Apache Derby .................................... 19
Configuring WPAR Manager ........................................... 19
Configuring WPAR Manager in different modes ................................ 20
Configuring WPAR Manager in silent mode .................................. 20
Configuring the WPAR Manager agent .................................... 20
Configuring the environment for application mobility ...................... 23
Configure WPAR Manager with LDAP authentication ....................... 26
Configuring the WPAR Manager agent to use a different agent manager ... 28
Setting up the console in a WPAR environment .............................. 29
Removing WPAR Manager ............................................. 30
Removing the WPAR Manager DB2 database ................................ 30
Removing the WPAR Manager agent ..................................... 30
Managing workload partitions with WPAR Manager .......................... 31
Managed systems ..................................................... 31
Managing WPARs ..................................................... 33
Managing WPAR storage devices .......................................... 39
Administering WPAR Manager .......................................... 41
Administrative scripts ................................................. 41
Changing the passwords for database IDs .................................. 42
Backing up the WPAR Manager database .................................. 42
Restoring the WPAR Manager DB2 database ................................ 43
Security for WPAR Manager .......................................... 43
User authentication ................................................... 43
Configuring authorization roles ........................................... 44
Configuring SSL support ............................................. 45
Managing certificates with ikeyman ......................................... 46
WPAR Manager agent secure certificates .................................... 47
Troubleshooting WPAR Manager .......................................... 47
Log file locations ..................................................... 47
Verifying the agent manager is online ..................................... 48
WPAR Manager problem determination ...................................... 48
Checkpoint and restart ............................................... 52
Problem determination for checkpoint and restart ........................... 52
Glossary for WPAR Manager .......................................... 54

**Notices** .......................................................... 59
Privacy policy considerations ........................................... 61
Trademarks .......................................................... 61

**Index** .......................................................... 63
About this document

IBM® PowerVM® Workload Partitions Manager™ for AIX® is a platform management solution that provides a centralized point of control for managing workload partitions across a collection of managed systems running AIX.

Highlighting

The following highlighting conventions are used in this book:

**Bold**
Identifies commands, subroutines, keywords, files, structures, directories, and other items whose names are predefined by the system. Also identifies graphical objects such as buttons, labels, and icons that the user selects.

*Italics*
Identifies parameters whose actual names or values are to be supplied by the user.

Monospace
Identifies examples of specific data values, examples of text similar to what you might see displayed, examples of portions of program code similar to what you might write as a programmer, messages from the system, or information you should actually type.

Case-sensitivity in AIX

Everything in the AIX operating system is case-sensitive, which means that it distinguishes between uppercase and lowercase letters. For example, you can use the `ls` command to list files. If you type `LS`, the system responds that the command is not found. Likewise, `FILEA`, `FiLea`, and `filea` are three distinct file names, even if they reside in the same directory. To avoid causing undesirable actions to be performed, always ensure that you use the correct case.

ISO 9000

ISO 9000 registered quality systems were used in the development and manufacturing of this product.
IBM PowerVM Workload Partitions Manager for AIX V1.2

IBM PowerVM Workload Partitions Manager for AIX (WPAR Manager) is a platform management solution that provides a centralized point of control for managing workload partitions (WPARs) across a collection of managed systems running the AIX operating system.

Note: This information applies only to IBM PowerVM Workload Partitions Manager for AIX V1.2.

For information about IBM PowerVM Workload Partitions Manager for AIX V2.0, V2.1, or V2.2, see the IBM Systems Director 6.2 Information Center (http://pic.dhe.ibm.com/infocenter/director/v6r2x/topic/com.ibm.director.wparmgt.helps.doc/wparlpp-kickoff.html).

For information about IBM PowerVM Workload Partitions Manager for AIX V2.3 or later, see the IBM Systems Director 6.3 Information Center (http://pic.dhe.ibm.com/infocenter/director/pubs/topic/com.ibm.director.wparmgt.helps.doc/wparlpp-kickoff.html).

What's new in IBM PowerVM Workload Partitions Manager for AIX V1.2

Read about new or significantly changed information for the IBM PowerVM Workload Partitions Manager for AIX 1.2 topic collection.

November 2012

The following information is a summary of the updates made to this topic collection:

The information for the versions of IBM PowerVM Workload Partitions Manager for AIX later than V1.2 can be found in the IBM Systems Director information centers.

For information about IBM PowerVM Workload Partitions Manager for AIX V2.0, V2.1, or V2.2, see the IBM Systems Director 6.2 Information Center (http://pic.dhe.ibm.com/infocenter/director/v6r2x/topic/com.ibm.director.wparmgt.helps.doc/wparlpp-kickoff.html).

For information about IBM PowerVM Workload Partitions Manager for AIX V2.3 or later, see the IBM Systems Director 6.3 Information Center (http://pic.dhe.ibm.com/infocenter/director/pubs/topic/com.ibm.director.wparmgt.helps.doc/wparlpp-kickoff.html).

How to see what's new or changed

In this PDF file, you might see revision bars (|) in the left margin that identifies new and changed information.

WPAR Manager concepts

The IBM PowerVM Workload Partitions Manager for AIX (WPAR Manager) application provides a centralized, single point of administrative control for managing system and application AIX Workload Partitions.

The WPAR Manager Web application user interface provides complete lifecycle management support for WPARs (Discovery, Create, Modify, Delete, and Remove). Complete task history is available on every action performed on a WPAR, including standard output and error. Graphic reports displaying resource use performance are provided for both managed systems and WPARs.

Any version of WPAR Manager includes the following features:
• Cross-system management of WPARs, including lifecycle management
• Global load balancing with application mobility
• Web-based administration of basic WPAR operations and advanced management tasks
• Monitoring and reporting of WPAR performance metrics

The following is a summary of the features provided by WPAR Manager, which require WPAR Manager agent version 1.2 or later.

**Improved live relocation**
Significant reduction of application downtime during relocation.

**Backup and restore**
Create backup images for an existing WPAR and restore a WPAR from a previously created backup image.

**Static relocation**
Static relocation is defined as a shutdown of the WPAR on the departure node and the clean start of the WPAR on the arrival node while preserving the file system state. For system WPARs, static relocation uses the backup and restore capabilities.

**Support for IP version 6 environments**
Configure, view, and modify workload partitions with IP version 6 addresses.

**Support for WPAR specific routes**
Select WPAR specific routing or share that of the global system. You can also configure, view, and modify a routing table specific to the workload partition. WPAR specific routes can only be configured for interfaces using IP version 4.

**Synchronize WPAR**
Synchronize software between a global system and a workload partition.

The following new features are limited to systems with WPAR Manager agent 1.2.1.

**Storage devices support**
Support to allocate and export storage devices to workload partitions.

**Clone WPAR**
Support to create a WPAR using an existing one as a template.

**Accessibility features for WPAR Manager**
Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

**Accessibility features**
The following list includes the accessibility features in WPAR Manager:
• Keyboard-only operation
• Interfaces that are commonly used by screen readers when used from a Web browser on a remote Microsoft Windows system using assistive technology software

The IBM Systems Information Center and its related publications are accessibility-enabled. For additional information on the accessibility features of the information center, select Viewing information in the information center > Accessibility and keyboard shortcuts in the information center.

**Keyboard navigation**
This product uses standard Windows navigation keys when used from a Web browser on a system running the Windows operating system.
When you are using keyboard navigation to select an action from the Select Action combo box, direct focus to the combo box, then use Alt+Down Arrow keys to open the drop-down list, then use the Up Arrow or Down Arrow keys to highlight a menu option, and then press Enter to select the highlighted option.

When you are using keyboard navigation to select an action from an Actions menu in Internet Explorer, use the Tab key to highlight the Actions menu, press Enter to expand the menu, then continue to click the Tab key until the action is selected. For Firefox, the arrow keys can be used to reach the action after the menu has been expanded.

**Interface information**

Some features of the WPAR Manager use Asynchronous JavaScript and XML (AJAX) to dynamically update content in the user interface. JAWS screen readers earlier than version 8 do not support AJAX.

Several user interface components used by WPAR Manager must be configured to work properly with screen readers. These components can be configured by selecting the Accessibility option from the Configure WPAR Manager > User Preferences navigation link. Users not requiring support of accessibility screen readers should leave this setting unchecked.

When a Content page is reloaded, all messages are voiced by reading from the top of the frame.

**IBM and accessibility**

For more information about the commitment that IBM has to accessibility, see the IBM Human Ability and Accessibility Center.

**WPAR Manager agent**

The WPAR Manager agent is a management component that provides a secure interface for the WPAR Manager to perform operations on a managed system.

The WPAR Manager agent must be installed on all managed systems. It enables support for the following functions:

- Performing remote operations on WPARs (for example, create, start, stop, or remove)
- Collecting performance metrics on a managed system for automated relocation and reporting system status
- Determining the compatibility profile of the managed system and providing this information to the WPAR Manager for relocation

**Heterogeneous WPAR Manager agent environments**

The WPAR Manager application has been designed to manage a heterogeneous environment of managed systems at different AIX technology levels and different versions of WPAR Manager agent.

There are limits to the environments that can be supported, and the capabilities of a mixed environment should be considered if you have a heterogeneous environment. There are limits to the environments that can be supported, and the capabilities of a mixed environment should be considered if you have a heterogeneous environment. For the fullest set of features and capabilities, all agents installed on managed systems in the management pool must be installed at, or migrated to the latest, WPAR Manager agent versions and corresponding AIX technology levels. Migrating the WPAR Manager components to the latest AIX technology level requires a specific migration order. The WPAR Manager must be migrated first. WPAR Manager agents are not required to be updated at once and their migration can be staged out.

There are four software components that work together to provide the features and capabilities of the WPAR Manager application. These environments include the following:
• WPAR Manager management console and server
• AIX Version 6.1
• Metacluster Checkpoint and Restart (MCR) kernel extension
• WPAR Manager agent

The MCR kernel extension fileset is part of the WPAR Manager agent image and provides for the checkpoint capabilities, restart capabilities, and live relocation capabilities. Because MCR is an AIX kernel extension, it is closely tied to the AIX technology level deployed on a managed system. Installing the latest version of WPAR Manager agent on the managed system with the correspondingly updated AIX technology level and MCR levels allows for management of all newly supported WPAR properties and operations delivered in the latest WPAR Manager version.

Previous versions of AIX and WPAR Manager agents:

Operating at a previous AIX technology level and WPAR Manager agent software version installed on the managed system precludes you from using the new WPAR properties and WPAR capabilities available in the latest version of WPAR Manager, such as static relocation, WPAR specific routing, IP version 6 network interfaces, and extended WPAR resource controls.

The table below outlines supported configurations available using WPAR Manager with the different AIX technology levels, MCR fileset, and WPAR Manager agent versions.

<table>
<thead>
<tr>
<th>AIX release</th>
<th>MCR level</th>
<th>WPAR Manager agent version</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX Version 6.1</td>
<td>4.1.8</td>
<td>1.1</td>
</tr>
<tr>
<td>AIX Version 6.1 with the 6100-01 Technology Level</td>
<td>4.1.10</td>
<td>1.1</td>
</tr>
<tr>
<td>AIX Version 6.1 with the 6100-02 Technology Level</td>
<td>4.2.0</td>
<td>1.1 or 1.2</td>
</tr>
<tr>
<td>AIX Version 6.1 with the 6100-03 Technology Level</td>
<td>4.2.1</td>
<td>1.1, 1.2, or 1.2.1</td>
</tr>
</tbody>
</table>

While the configuration of using a down-level agent on an updated technology level of AIX is supported, there is no value gained by running in this configuration. You should upgrade the WPAR Manager agent to the latest supported version if the Technology Level of the managed system has been upgraded.

Mixed agents environments:

The extent to which capabilities and functionality are reduced in a mixed agent environment is driven by the extent to which the managed system agent environment diverges from the ideal WPAR Manager agent 1.2.1 configuration (AIX 6.1 with 6100-03, MCR 4.2.1, WPAR Manager agent 1.2.1) or the extensiveness of the heterogeneity in the management pool.

For example, relocation of a WPAR in a heterogeneous agent environment limits the recommended relocation targets to managed systems with similar configurations. It is not possible to relocate a WPAR from a managed system that is running WPAR Manager agent 1.2 to another managed system that is running WPAR Manager agent 1.1. Maintaining a more homogeneous agent population by having all WPAR Manager agents at the same level results in an increase in possible targets for relocation.

In order to support heterogeneous environments and assist in characterizing the capabilities of managed systems and WPARs, the following concepts have been introduced since WPAR Manager 1.2:

**Agent version**

A managed systems property that describes the level of agent software installed on the managed system.
Minimum agent version
A WPAR property that describes the minimum agent version configuration required to support all the properties defined for the given WPAR.

For example, a WPAR that is created without any extended WPAR Manager agent 1.2 properties (IP version 6 network interfaces, WPAR specific routing information, or extended resource control definitions) has a minimum required agent version of 1.1.1.0. A WPAR having a version of 1.1.1.0 allows the WPAR to be deployed on either a WPAR Manager agent 1.1 or a WPAR Manager agent 1.2 configuration. If you create a WPAR using WPAR Manager 1.2 but do not use properties that are specific to WPAR Manager agent 1.2, the WPAR can be deployed and will operate on either WPAR Manager agent 1.1 or 1.2 configuration. Conversely, a WPAR that has extended WPAR Manager agent 1.2 properties defined can only be deployed to managed systems running a WPAR Manager agent 1.2 configuration.

Understanding the Agent version attribute of a managed system and the Minimum agent version attribute of a given WPAR will assist in understanding where a WPAR can be deployed to or relocated to within the management pool, as well as highlight the behavior differences seen in the WPAR Manager 1.2 console between WPARs created on different WPAR Manager agent version levels.

System profiles
System profiles do not represent the actual managed systems, but rather a particular configuration. At any time, one or more managed systems can share the same system profile.

If an existing profile from previous registrations already has the same characteristics as the system being registered, then the existing profile will be assigned to the system. If the system being registered has a unique set of hardware attributes, then a new profile will be created and assigned to the system.

The WPAR Manager takes into consideration cross system compatibility in order to relocate WPARs from one managed system to another. When a new system is registered, the WPAR Manager triggers a background process that compares a predefined set of hardware and software properties for each system that has previously been registered. After this process is completed, the results are stored in the WPAR Manager database and are later used to determine if systems are compatible based on the need of the WPAR being relocated. Because this process occurs in the background, the WPAR Manager may take time to display the compatibility state between different systems. You can determine whether or not the process to analyze compatibility has been completed for a particular managed system by looking at the system properties through the WPAR Manager.

If there are WPARs already created in the managed system at the time of the registration, the WPAR Manager will discover those WPARs and load their configuration into the application database. After the WPARs are discovered, you can perform operations on these WPARs as if you had created them through the WPAR Manager.

Supported operating environments for WPAR Manager
WPAR Manager and application mobility are supported on IBM System p® systems based on the POWER4 processor architecture or later.

WPAR Manager server requirements
The WPAR Manager server supports the following environments:
• AIX Version 6.1 or later
• DB2® 9.5 for Linux, UNIX, and Windows or Apache Derby, for database function
**WPAR Manager agent requirements**

The WPAR Manager agent can be installed on AIX Version 6.1, AIX Version 6.1 with the 6100-01 Technology Level, AIX Version 6.1 with the 6100-02 Technology Level, or AIX Version 6.1 with the 6100-03 Technology Level systems running on a physical server or in a logical partition on a POWER4 or later system. To use all of the new features in WPAR Manager version 1.2.1, you must be running AIX Version 6.1 with the 6100-03 Technology Level.

**WPAR Manager client requirements**

The following table shows the browsers supported by the WPAR Manager client on each operating system:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Supported browser version</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX Version 6.1</td>
<td>Firefox 1.5 or later</td>
</tr>
<tr>
<td>Windows XP</td>
<td>Internet Explorer 6 or later, Firefox 1.5 or later</td>
</tr>
</tbody>
</table>

*Note:* Internet Explorer requires the SVG graphics plugin from Adobe. You can obtain this plugin from the following Web site: [http://www.adobe.com/svg/viewer/install/](http://www.adobe.com/svg/viewer/install/)

**Memory and disk space requirements**

There are memory and disk space requirements for the components of WPAR Manager.

The following table shows the typical memory requirements for WPAR Manager when it is idle. These requirements do not include any additional memory requirements for other software that is running on your system.

<table>
<thead>
<tr>
<th>Application</th>
<th>Memory requirement</th>
<th>Disk space requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPAR Manager</td>
<td>125 MB</td>
<td>• /, 5 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• /var, requires at minimum 180 MB. This includes manager (66 MB), agentmgr (61 MB) and runtime logs (45 MB).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• /opt, requires 61 MB.</td>
</tr>
<tr>
<td>DB2 server</td>
<td>256 MB</td>
<td>/home, (this may be any directory that holds the user home directory) 200 MB, /opt, 500 MB</td>
</tr>
<tr>
<td><strong>Note:</strong> DB2 is optional, and using the embedded database, Apache Derby, will use less space.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent manager</td>
<td>60 MB when idle</td>
<td>/var, 65 MB</td>
</tr>
<tr>
<td>WPAR Agent</td>
<td>45 MB when idle</td>
<td>/var, 110 MB</td>
</tr>
</tbody>
</table>

**WPAR management in a logically partitioned environment**

The managed systems available in WPAR Manager are real or virtual systems running AIX and the WPAR Manager agent that have registered to the WPAR Manager.

WPAR Manager does not recognize HMC or Integrated Virtualization Manager (IVM) configurations. If you are using the HMC or IVM to manage your environment, and you have created a WPAR within the logical partitions on your systems, you will not be able to view the entire environment from WPAR Manager. Logical partitions might not be viewable for the following reasons:
They are running operating systems other than AIX.
They do not have the WPAR Manager agent software installed.
They are not registered to your WPAR Manager server.

**Application mobility**

Application mobility is the process of relocating a WPAR between two different physical servers or LPARs running AIX Version 6.1, or later.

Two types of relocation are possible, live and static, between servers with WPAR Manager agent 1.2 or later. Live relocation is the only relocation option with WPAR Manager agent 1.1 installed.

**Live application mobility**

Live application mobility is the process of relocating a WPAR while preserving the state of the application stack. During live application mobility, WPARs are relocated from the departure server to the arrival server with minimum application downtime and without losing active transactions.

**Static application mobility**

Static application mobility is defined as a shutdown of the WPAR on the departure node and the clean start of the WPAR on the arrival node while preserving the file system state. For system WPARs, static relocation uses the backup and restore capabilities.

**System compatibility**

System compatibility is strictly related to the relocation type.

Live application mobility is the process of relocating a WPAR while preserving the state of the application stack. Static application mobility is defined as a shutdown of the WPAR on the departure node and the clean start of the WPAR on the arrival node while preserving the file system state. Live relocation requires a more extensive compatibility testing than static relocation. Therefore, it is possible that two systems could be incompatible for live relocation, but compatible for static relocation.

Compatibility is evaluated on the following criteria:
- Hardware levels (the two systems must have identical processor types)
- Installed hardware features
- Installed devices
- Operating system levels and patch levels
- Other software or file systems installed with the operating system
- Additional user-selected tests

**Compatibility testing for application mobility**

Compatibility testing includes critical tests and optional tests. Each time a system is registered, the WPAR Manager starts a background process that compares the properties of the new system to the system properties of all previously registered systems.

These compatibility tests help to determine if a WPAR can be relocated from one managed system to another. For each relocation type, live or static, there is a set of critical tests that must pass for one managed system to be considered compatible with another. The critical tests for static relocation are a subset of the tests for live relocation.

For live relocation, the critical compatibility tests check the following compatibility criteria:
- The operating system type must be the same on the arrival system and the departure system.
- The operating system version and level must be the same on the arrival system and the departure system.
• The processor class on the arrival system must be at least as high as the processor class of the departure system.
• The version, release, modification, and fix level of the \texttt{bos.rte} fileset must be the same on the arrival system and the departure system.
• The version, release, modification, and fix level of the \texttt{bos.wpars} fileset must be the same on the arrival system and the departure system.
• The version, release, modification, and fix level of the \texttt{mcr.rte} fileset must be the same on the arrival system and the departure system.
• The \texttt{bos.rte.libc} file must be the same on the arrival system and the departure system.
• There must be at least as many storage keys on the arrival system as on the departure system.

\textbf{Note:} The only critical test for static relocation is that the \texttt{bos.rte.libc} file must be the same on the arrival system and the departure system.

In addition to these critical tests, you can choose to add additional optional tests for determining compatibility. These optional tests are selected as part of the WPAR group policy for the WPAR you are planning to relocate, and are taken into account for both types of relocation. Two managed systems might be compatible for one WPAR and not for another, depending on which WPAR group the WPAR belongs to and which optional tests were selected as part of the WPAR group policy. Critical tests are always applied in determining compatibility regardless of the WPAR group to which the WPAR belongs.

You can choose from optional tests to check the following compatibility criteria:
• NTP must be enabled on the arrival system and the departure system.
• The amount of physical memory on the arrival system must be at least as high as the amount on the departure system.
• The processor speed for the arrival system must be at least as high as the processor speed for the departure system.
• The version, release, modification, and fix level of the \texttt{x1C.rte} file set must be the same on the arrival system and the departure system.

\textbf{Compatibility states}
Depending on the results of compatibility testing, the compatibility states might be compatible, compatible with warnings, or not compatible. The critical tests are different for static relocation and live relocation. Two systems might not be compatible for live relocation but compatible for static relocation.

The compatibility states are as follows:

\textbf{Compatible}
For a given relocation type, all critical and user-selected tests comparing the system properties of the departure system to the system properties of the arrival system pass. A WPAR can be relocated from the departure system to the arrival system and can also be relocated from the arrival system back to the departure system.

\textbf{Compatible with warnings}
For a given relocation type, at least one of the critical or user-selected tests was skipped because the required system property was not collected on either the departure system or the arrival system. No failures are recorded on any of the remaining critical and user-selected tests. Since not all test cases were executed there is a risk that the WPAR cannot be relocated from the departure system to the arrival system or from the arrival system back to the departure system.

\textbf{Not compatible}
For a given relocation type, compatibility testing shows that a WPAR cannot be safely relocated from the departure system to the arrival system and back.

Since some of the testcase rules are based on inequalities, arrival system must have processor class at least as high as departure system. A failure may happen in one direction only. However,
since it will not be possible to safely relocate the WPAR in both directions, the compatibility state between the managed systems will be marked as **Not compatible**.

Notice that when the compatibility state between two managed systems is reported as **Not compatible**, a failure will probably occur if you try to move the WPAR to the incompatible system, but it is possible, in some cases, that the relocation might succeed.

**Unknown**
Indicates that the compatibility analysis was not performed because either the departure server just changed its state to unknown, or the arrival server either appears to be offline.

**Canceled**
Compatibility testing was unable to be completed as a result of an error or a server profile mismatch condition. Possible conditions are:

**Update profile is required**
Indicates that compatibility testing was canceled for the managed system because registration failed for the arrival server.

**Delete complete**
Indicates compatibility testing was canceled because the managed system was deleted.

**Runtime error**
Indicates compatibility testing was canceled for the managed system as the result of an unexpected runtime error.

**WPAR states**
The lifecycle of a WPAR is characterized by the current state of the WPAR.

During its lifecycle, a WPAR can be found in any of the following states:

**Defined**
The WPAR exists on a managed system, but is not currently active. Starting the WPAR moves it to the active state. The defined state is indicated by a **D** when you run the `lswpar` command.

**Active**
The WPAR is deployed on a managed system and is running normally. The active state is indicated by an **A** when you run the `lswpar` command.

**Paused**
The WPAR is in a checkpoint-suspend state. It is not currently running but can be resumed or unpaused. The paused state is indicated by a **P** when you run the `lswpar` command.

**Frozen**
The WPAR has had a checkpoint initiated, and the processes are quiesced, but process states are not saved. The WPAR can be resumed or checkpointed. The frozen state is indicated by an **F** when you run the `lswpar` command.

**Loaded**
The WPAR has been deployed on a server, and is loaded in the kernel, but no processes are active. A Loaded WPAR can be started.

**Transitional**
An administrative operation is in progress. The workload partition is in the process of being created, started, stopped, or configured.

**Broken**
An administrative operation failed, leaving this workload partition in an unusable state.

**Deleted**
The workload partition and its definition in the WPAR Manager database are deleted.
Undeployed
The workload partition is defined in the WPAR Manager database, but is not deployed on a managed system.

Moving
The WPAR is transferring its memory contents to another machine. When the memory transfer is complete, the WPAR will be stopped and removed from the system.

Relocation domains and system profiles
A relocation domain is a grouping of managed systems that you create. The relocation domain identifies a group of systems that serve the same purpose and is used to generate system profiles.

Each relocation domain includes a separate system profile for the different hardware configurations of the managed systems in the relocation domain. If you have multiple managed systems that are used for different purposes, you can tag each system with a relocation domain that matches its function, and tag similar systems with the same relocation domain. A managed system can belong to one relocation domain, and all managed systems are added to the default relocation domain when they are created.

When you create a WPAR group and specify the group to have policy-based relocation, system profiles are used to rank the systems that the WPARs can relocate to. The following rules apply to system profiles:

- System profiles are generated based on the relocation domain tag and the managed system hardware characteristics.
- A system profile can have more than one managed system assigned to it.
- Managed systems in different relocation domains cannot belong to the same profile.
- Managed systems with different hardware configurations cannot belong to the same profile.

The following graphic demonstrates how profiles are generated by applying relocation domain tags to managed systems in the following scenario:

- You have nine managed systems in the default relocation domain.
- The managed systems support human resources, banking, and backup functions.
- The managed systems have two different hardware configurations.
- The managed systems have different operating systems and resources.
- You create a separate relocation domain for each functional area (human resources, banking, and backup).
- You create system profiles within each relocation domain for different hardware configurations.
Manual relocation

WPAR Manager version 1.2 supports static and live relocation methods for manual relocation. Manual relocation to a manually selected server can be done on WPARs that are members of a WPAR group.
enabled for policy-based relocation. WPAR Manager can intervene and attempt to re-relocate to another
system unexpectedly, based on the details of the policy governing the WPAR group.

Before you relocate a WPAR, you must complete the following tasks:
• Ensure your environment meets the requirements to support relocation.
• Configure your environment appropriately so that mobile WPARs can be created.
• Create a WPAR that can be relocated.

After you meet these prerequisites, you can decide which WPAR to relocate and which managed system
to relocate it to. Use WPAR Manager to help you select the best possible system where the workload
partition should be moved based on use and system compatibility. There are two ways you can decide
which system to relocate to:

Automatic selection
Automatic selection is based on the policy specified in the WPAR group to which the WPAR
belongs, the current use of the systems that match the system profiles specified by the policy, and
the current resource use of the WPAR. The system selection is also based on the compatibility
status between the current system and the candidate. Only fully compatible systems are
considered as candidates for hosting the WPAR.

Managed systems that belong to the same relocation domain specified in the policy are analyzed
and a system is selected as the best available fit for the WPAR being considered for relocation. If
WPAR Manager cannot identify an appropriate candidate system, the WPAR Relocation dialog
still will allow the user to select a system manually.

Note: When manually relocating a WPAR belonging to a WPAR group that has been enabled for
policy-based relocation, as a manual relocation of this WPAR may be in conflict with what the
WPAR Manager policy subsystem has determined to be the most appropriate location for the
WPAR and may attempt to re-relocate the WPAR after the manual relocation.

Manual selection
Manual system selection allows you to select the specific system to which a WPAR will be
relocated instead of letting WPAR Manager select one for you. Systems are classified by their
compatibility status, which is determined by a set of hardware and software tests performed
when a managed system is registered. While selecting a fully compatible system is the preferred
option, you can select any system regardless of compatibility.

Compatibility status of possible system targets can be viewed by selecting the Browse button in
the WPAR Relocation dialog. System compatibility status is determined by the type of relocation,
status, either static or live, being performed.

To start the relocation process, first select the WPAR that you want to relocate. Then choose Relocate
from the actions menu. The Relocate WPAR dialog then prompts you to choose a destination system and
the type of relocation to perform.

Related concepts:
"Configuring the environment for application mobility" on page 23
There are restrictions on the setup of the environment to support application mobility. Different
restrictions exist for live and static relocations.

"Setting up the console in a WPAR environment” on page 29
IBM Systems Director Console for AIX is not installed on each WPAR by default. In order to enable
system management for AIX instances within a WPAR, you must use the wparConsole.sh utility.

Policy-based relocation
Policy-based relocation is available only for WPARs that are checkpointable.
The relocation policy also specifies how each metric in the set is weighted and averaged with the other metric values to derive a single performance state value for a WPAR. Individual WPAR performance states are then combined to derive a performance state for the WPAR group. When the group performance state falls outside of specified thresholds, a mobility event is generated, causing one of the WPARs in the group to be relocated. The WPAR Manager generates and processes mobility events within a WPAR group, one at a time. The overall state of the WPAR group is re-analyzed after each event, which helps ensure that excessive or repeated WPAR relocation does not occur.

Based on the overall WPAR group performance state, the performance state of the individual WPARs, and the performance state of the managed systems associated with the WPAR Group, the WPAR Manager policy can perform one of the following corrective actions:

**Scale Up**  
A WPAR is relocated to a more powerful machine.

**Scale Down**  
A WPAR is relocated to a less powerful machine.

**Scale Out**  
A WPAR is relocated to a dedicated machine.

**Scale In**  
A WPAR is consolidated with other WPARs into a shared machine.

The first step in defining a relocation policy is to select from a variety of performance metrics gathered by standard metric providers. All metrics are stored in the WPAR Manager database for subsequent report generation. The relocation policy also includes metric properties and group properties.

**Related concepts:**

*Managing WPAR groups* on page 33
A WPAR group is a defined group of WPARs that are governed by common relocation policy settings.

**Metric policy settings**
To determine the performance state of a server, WPAR Manager performs a weighted average of all policy metrics. Since metrics can be classified in two distinct families, utilization metrics and rate metrics, the concept of limit is needed to be able to express all policy metrics as percentages.

The utilization metric is a percentage of utilization of some resource, such as processor or memory. The rate metric is a measurement of some state value with no clearly-defined upper limit, such as process count, application response time, or disk throughput.

The metric policy settings are as follows:

**Limit**  
Is the normalization factor used to express metrics as percentages which for each type of metrics represents one of the following:

**Utilization metric**  
Because the utilization metric is already define as percentage of utilization, the value of the limit property cannot be changed from the default value of

**Rate metric**  
Maximum expected value so it is possible to convert a rate or count metric into a percentage of the expected maximum value.

**Weight**  
Defines the relative strength of a metric compared to the other metrics in a relocation policy. The minimum value for this setting is zero, but at least one metric must have a weight greater than zero to calculate a performance state value. The WPAR Manager calculates the weighted average of metrics in a relocation policy and uses the result to indicate the performance state. If all metric weight properties are set to zero, then the weighted average calculation always returns a zero value.
Maximum

Specifies a value above which the value of an individual metric will override the weighted average performance state for the WPAR group. If any metric for any WPAR in a group rises above its maximum value, and if the average performance state for the group is lower than this value, then the group performance state is raised to the current value of the metric that is exceeding its maximum. This result makes it more likely that a WPAR relocation will occur.

Minimum

Specifies a value below which the value of an individual metric will override the weighted average performance state for the WPAR group. If any metric for any WPAR in a group goes below its minimum value, and if the average performance state for the group is higher than this value, then the group performance state is lowered to the current value of the metric that is exceeding its maximum. This result makes it more likely that a WPAR relocation will occur.

Group policy settings

Group policy settings define how the WPAR Manager interprets the performance states of all WPAR instances in a WPAR group. These settings define the high level policy that is used to trigger relocations in response to variance in the demand for applications deployed within a collection of WPARs.

The following group policy settings are required:

Maximum threshold

Defines the value above which the performance state of a WPAR instance will throw a hot trigger, indicating that the allocation of system resources is insufficient for the current demand. The maximum setting is also used during a group state analysis to indicate that the average performance state of a WPAR group is too busy and that a WPAR relocation might be warranted.

Minimum threshold

Defines the value below which the performance state of a WPAR instance will throw a cold trigger, indicating that the demand for system resources is well below what the current system can deliver. The minimum policy setting is also used during a group state analysis to indicate that the average performance state of a WPAR group is not busy and that a WPAR relocation might be warranted.

Averaging period

The window of time, in minutes, that is used for the averaging of metrics when you are analyzing the performance state of a WPAR group. When a WPAR instance violates the trigger count, the WPAR Manager analyzes the WPAR group. The current performance state of all WPARs is determined by averaging the metrics collected during the averaging period. These metrics are then normalized and aggregated for each WPAR using the relocation policy settings for its WPAR group. The performance state values derived from this operation are then averaged and compared to the group maximum and minimum values. If the result of this calculation is above or below the maximum or minimum, then a WPAR relocation is ordered.

Adjusting the averaging period allows the user to tune how responsive the WPAR Manager is to load spikes. A short averaging period results in averaging fewer metric values and increased sensitivity to load spikes. A longer averaging period allows more metric samplings to be included in the performance state calculation, which decreases sensitivity to transient load.

Policy tuning

The relocation policy for WPAR Manager is based on the premise that the application’s performance state is strongly correlated with the values of key performance metrics.

When analyzed in the context of the total resources available in the hosting logical partition, these metrics can accurately indicate high or low resource demand by processes running in the WPAR. For example, analysis of a WPAR that is currently consuming 20% of the total processor of the hosting logical partition (LPAR) might appear to indicate that there is not a high demand for services deployed within that WPAR. However, if other processes on that LPAR are consuming 80% of the processor, then there is no
more processor available for the WPAR. WPAR Manager takes into account the resource use by processes outside of the WPAR, and reports the effective use of the processor for the WPAR at 100%. The calculation used by the WPAR Manager to determine effective use of any metric can be described as follows:

\[
\frac{\text{WPAR Utilization}}{1-(\text{LPAR Utilization}\ - \text{WPAR Utilization})}
\]

In this example, this equation will resolve to 20% only when no other processes are consuming any processor cycles on the LPAR. This allows the WPAR Manager to accurately determine when resources are constrained for a particular WPAR without instrumentation of the deployed application or the hosting LPAR. The primary consideration when selecting the metrics that should be monitored in the WPAR group’s policy settings is the magnitude of the linear correlation between the value of a specific performance metric and some key measurement of application performance.

The most common measurement of application performance is application response time (ART). The WPAR Manager is designed to manage similar applications deployed within a WPAR group. Consequently, ART measurements for a WPAR group should come from source transactions that do not traverse multiple WPAR groups. This means that if a test transaction involves dynamic content generated by an application server cluster deployed within a WPAR group, the generated content should not be dependant upon data retrieved from a database deployed within a different WPAR group. Instead, the test transaction for the application server WPAR group should be set up so that the generated content is retrieved from the local file system, and a separate test transaction should be used to determine the ART for the database WPAR group. Separate WPAR relocation policies should be created for the two WPAR groups so that they can be managed independently, eliminating the need for instrumentation of the application stack.

Group averaging

WPAR Manager manages each group of an enterprise application independently as a separate WPAR group. WPAR Manager uses the average performance of these groups to determine whether a WPAR should be relocated.

Common enterprise applications are typically deployed across multiple application instances, typically referred to as tiers. Additionally, high-demand applications can cluster application instances within each tier. The following table shows an example of how groups and policies work in a tiered application environment.

<table>
<thead>
<tr>
<th>Application tiers</th>
<th>Relocation policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction servers</td>
<td>Group 1 policy</td>
</tr>
<tr>
<td>Application servers</td>
<td>Group 2 policy</td>
</tr>
<tr>
<td>Database servers</td>
<td>Group 3 policy</td>
</tr>
</tbody>
</table>

The WPAR group relocation policy for the application tier defines how the performance state of the applications deployed within the WPAR instances is interpreted, as well as how the performance state of the group itself is interpreted. The WPAR Manager analyzes the performance state of all WPAR groups at regular intervals. If the result of this analysis indicates that the average performance state of all WPAR instances in a specific group is above the group policy maximum, or below the minimum, a mobility event is generated if resources are available. Group averaging ensures that mobility events are only generated when the state of all associated WPAR instances indicates that the application performance is out of the expected range.
Planning for application mobility

When planning for application mobility, you should consider the compatibility of the managed systems in your environment, and your goal in relocating the WPARs.

Consider the following information on WPAR compatibility:

- The more compatible your managed systems are with each other, the more potential relocation targets you will have.
- Start with hardware compatibility. If your managed systems have identical or similar hardware, it will be easier to relocate WPARs between them.
- Try to update all of your managed systems to the same technology level and version of AIX.
- Update all WPAR Manager agent software to the same version.

In addition to compatibility, consider the current workload on both the departure system and the arrival system. If the goal of relocation is to improve application performance, find a server with more processor and memory resources available than the current system. Conversely, if your goal is to consolidate workloads to fewer servers because of reduced demand, then finding a server with lower resource usage might not be as important. WPAR Manager tracks performance metrics for managed systems, and considers current resource use when ranking potential arrival systems.

Planning for Role Based Access Control

Use Role Based Access Control (RBAC) to provide greater granularity in controlling access to AIX services based on roles and privileges granted to users.

RBAC is a framework that allows you to delegate administration tasks through roles. Each user is assigned one or more roles, allowing that user to perform several administration tasks without being the super root user. RBAC relies heavily on system privileges to allow regular users to perform privileged tasks. A privilege is a mechanism used to grant a process augmented functionality in system calls.

A system WPAR can be restricted to deny all of the privileged operations that are allowed in a global partition. Privileges assigned to a WPAR can be controlled through the WPAR privilege set (WPS). The WPS determines the hard set of privileges for any process running inside of the system WPAR. Processes in the WPAR are restricted to the WPS at any point in time. The WPAR Manager provides the capability to review and modify the default WPS assigned when a WPAR is created. You can grant additional privileges that are available in the global partition or remove privileges that have been granted as part of the default WPS.

Note: Use caution when removing privileges specified in the default WPS or the processes in the WPAR might not have enough privileges to function properly.

Because privileges can vary between managed systems, WPAR Manager keeps a record of all of the privileges available in each managed system and the default WPS that should be used when a WPAR is created. The default WPS is obtained from the /etc/wpars/secattrs configuration file. The content of this file is loaded into WPAR Manager when the managed system is registered. If this file is modified after registration, the user must trigger a system profile update so the changes are reflected in the WPAR Manager. This can be done by going to the Managed System resource view and using the Update system profile task.

Installing WPAR Manager

The installation process for WPAR Manager includes installing WPAR Manager on the system used as the management server and installing the WPAR Manager agent on each managed system.
Installing WPAR Manager on the management server

You should install the WPAR Manager on any IBM System p system that is running AIX Version 6.1 or later, and have a minimum of 1.5 GB of RAM.

Note: If you are installing over an existing WPAR Manager agent 1.1 you can follow the steps below, however, all filesets and requisite configuration files are migrated to the WPAR Manager agent 1.2 as returned by the `lslpp -h wparmgt.mgr` command. The `lslpp` command displays information about installed filesets or fileset updates.

1. Log in to the system as the root user.
2. If you are installing from media, insert the media containing WPAR Manager into the media drive.
3. Mount the media drive using the following command (where `/mnt` is the mount point for your media drive):
   ```bash
   /usr/sbin/mount -v cdrfs -p -r /dev/cd0 /mnt
   ```
4. Run the `installp` command as follows to install WPAR Manager:
   ```bash
   # installp -acXYgd <MOUNT_POINT>/installp/ppc wparmgt.mgr
   ```

Installing the WPAR Manager database

The WPAR Manager can be configured to use a DB2 V9.5 or Apache Derby database. Apache Derby is an embedded database and requires no additional configuration steps. Additional configuration is required to use a DB2 database.

To install the DB2 database, perform the following steps:

1. Log in to the management server as the root user.
2. If you are installing from media, insert the media containing WPAR Manager into the media drive.
3. Mount the media drive using the following command (where `/mnt` is the mount point for the media drive):
   ```bash
   /usr/sbin/mount -v cdrfs -p -r /dev/cd0 /mnt
   ```
4. To install the WPAR Manager DB2 database fileset, run the following command:
   ```bash
   installp -acqgd <MOUNT_POINT>/installp/ppc wparmgt.db
   ```
5. To install and configure the WPAR Manager database, run the following `DB2Install.sh` script:
   ```bash
   # /opt/IBM/WPAR/manager/db/bin/DB2Install.sh  
   -dbinstallerfile <MOUNT_POINT>/db2-v9.5fp1_aix64_limited_use.tar.gz  
   -dbpassword <db2wmgt_user_password>
   ```
6. Run the installation script using the following command:
   ```bash
   ./DB2Install.sh -dbpassword your_password  
   -dbinstallerdir /mnt/db2
   ```

   Note: The following default values are used: the DB2 user is `db2wmgt`, the DB2 home directory is `/home/db2wmgt`, and the DB2 port 50000.

Related tasks:

- [“Migrating from Apache Derby to DB2” on page 19](#)

Use the `DBMigrate` script to migrate the WPAR Manager Apache Derby database to a DB2 database.

Installing the WPAR Manager agent on the managed system

The WPAR Manager agent runs on the managed system and provides a secure interface for running WPAR commands for managing WPARs, collecting performance metrics, and collecting information for compatibility testing.

The following files are prerequisites for installing the WPAR Manager agent 1.2.1:

- Java5.sdk version 1.5.0.0
- bos.wpars version 6.1.3.0
The WPAR Manager agent is packaged as a set of AIX `installp` filesets. The WPAR Manager CD includes the following WPAR Manager agent filesets:

- `wparmgt.agent.rte`
- `cas.agent`
- `tivoli.tivguid`
- `mcr.rte`

All filesets are required for installation.

To install the WPAR Manager agent with the `installp` command, run the following command from the managed system as the root user:

```
# installp -acqYXd <MOUNT_POINT>/installp/ppc wparmgt.agent
```

Substitute `<MOUNT_POINT>` with the location of the WPAR Manager `installp` filesets. The location should either be the media drive or a local directory on the managed system.

## Upgrading the WPAR Manager

You can upgrade WPAR Manager 1.1 or 1.2 to 1.2.1. These instructions upgrade both the WPAR Manager management server as well as the WPAR Manager agent.

**Prerequisites:**

- WPAR Manager agent 1.2.1 can be installed on AIX Version 6.1 with the 6100-03 Technology Level, or later systems. On AIX 6.1 with 6100-02, WPAR Manager agent 1.2 is the recommended agent.
  - On earlier versions of AIX 6.1, WPAR Manager agent 1.1 is the recommended agent.

**Considerations:**

- You are not required to re-run the `WPMConfig.sh` script as part of the upgrade from WPAR Manager 1.1 or 1.2 to WPAR Manager 1.2.1. All previously configured settings are preserved during the upgrade.
- You are not required to re-run the `DBInstall.sh` script as part of the upgrade from WPAR Manager 1.1 or 1.2 to 1.2.1. WPAR Manager 1.2.1 can continue to use the existing DB2 database.
- When migrating from WPAR Manager agent 1.1 to WPAR Manager agent 1.2.1, the port used to communicate with the WPAR Manager agent will change from the default WPAR Manager agent 1.1 port (8211) to the default WPAR Manager agent 1.2.1 port (9510). When the agent port changes, the managed system will go offline in the WPAR Manager console. To restore connectivity with the WPAR Manager agent in the WPAR Manager console, click **Discover** from the Managed Systems view.

To upgrade to WPAR Manager 1.2.1, complete the following steps:

1. Upgrade the WPAR Manager and agent manager filesets by running the following command:
   ```
   # installp -acXYgd <MOUNT_POINT>/installp/ppc tivoli.tivguid wparmgt.cas.agentmgr wparmgt.mgr
   ```
2. Verify that WPAR Manager is accessible by logging into the console from a Web browser using the following address:
   ```
   http://<wpar-manager-hostname>:<public_port>/ibm/console
   ```
3. To upgrade to WPAR Manager agent 1.2.1, run the following command on each managed system:
   ```
   # installp -acXYgd <MOUNT_POINT>/installp/ppc mcr.rte tivoli.tivguid wparmgt.agent
   ```
4. To complete the upgrade, restart the system where the WPAR Manager agent is installed by running the following command:
   ```
   # shutdown -Fr
   ```

**Post requisite:** After the upgrade is complete, you must clear the browser cache before using the WPAR Manager interface.
Migrating the WPAR Manager database

WPAR Manager 1.2.1 provides support for the Apache Derby database and DB2 database. In order to simplify the process of migrating data from each database, a utility is provided to migrate all of the data from one database type to another.

To migrate a database, the usage of the DBMigrate script is the following:

```
DBMigrate -dbtype {derby|db2} [...]
```

- `dbtype` Database Type (Required)
- `dbhost` Database Hostname (DB2 only)
- `dbport` Database Port (DB2 only)
- `dbuser` Database Username (DB2 only)
- `dbpass` Database Password (DB2 only)
- `dbname` Database Name (DB2 only)

### Migrating from Apache Derby to DB2

Use the DBMigrate script to migrate the WPAR Manager Apache Derby database to a DB2 database.

To migrate data from an Apache Derby database to a DB2 database, complete the following steps:

1. Install and configure the WPAR Manager DB2 database.
2. Stop WPAR Manager by running the following command:
   ```
   # wparmgr stop
   ```
3. Run the following DBMigrate command with the settings for the DB2 database:
   ```
   # /opt/IBM/WPAR/manager/bin/DBMigrate \
   -dbtype db2 \ 
   -dbhost <hostname> \ 
   -dbport <port (default: 50000)> \ 
   -dbuser <username (default: db2wmgt)> \ 
   -dbpass <password> \ 
   -dbname <database name (default: WPARMGT)>
   ```
4. Start WPAR Manager by running the following command:
   ```
   # wparmgr start
   ```

**Related tasks:**

“Installing the WPAR Manager database” on page 17

The WPAR Manager can be configured to use a DB2 V9.5 or Apache Derby database. Apache Derby is an embedded database and requires no additional configuration steps. Additional configuration is required to use a DB2 database.

### Migrating from DB2 to Apache Derby

Use the DBMigrate script to migrate the WPAR Manager DB2 database to an Apache Derby database.

To migrate data from a DB2 database to an Apache Derby database, complete the following steps:

1. Stop WPAR Manager by running the following command:
   ```
   # wparmgr stop
   ```
2. Run the following DBMigrate command:
   ```
   # /opt/IBM/WPAR/manager/bin/DBMigrate -dbtype derby
   ```
3. Start WPAR Manager by running the following command:
   ```
   # wparmgr start
   ```

### Configuring WPAR Manager

You can configure the environment for WPAR application mobility and perform additional post-install customizations.
Configuring WPAR Manager in different modes

WPAR Manager can be configured in either graphical or console mode with the `WPMConfig.sh` command.

The `WPMConfig.sh` command automatically starts in either graphic or console mode. It will run in graphical mode provided there is a X11R6 environment on both AIX and the accessing system. The X11 `DISPLAY` environment variable on the AIX system must be set to the IP address of the accessing system or the host name of the accessing system. If there is not an X11 environment, then the configuration wizard starts in console mode.

**Graphical Mode**

To configure the WPAR Manager using the graphical mode, complete the following steps:

1. Run the following command with the X11 `DISPLAY` environment variable:
   ```bash
   # /opt/IBM/WPAR/manager/bin/WPMConfig.sh
   ```
2. Enter information in the fields as you are prompted for it. The fields contain default values. If you use these default values, you will need to only provide a password for the WPAR Manager agent registration.

**Console Mode**

To configure the WPAR Manager using the console mode, complete the following steps:

1. Run the following command:
   ```bash
   # /opt/IBM/WPAR/manager/bin/WPMConfig.sh -i console
   ```
2. Enter information in the fields as you are prompted for it. The fields contain default values. If you use these default values, you will need to only provide a password for the WPAR Manager agent registration.

Configuring WPAR Manager in silent mode

You can configure WPAR Manager in silent mode if you do not want to be prompted for any input. All required information is extracted from a configuration file.

To configure WPAR Manager in silent mode, complete the following steps.

1. Save the original response file by running the following command:
   ```bash
   # cp /opt/IBM/WPAR/manager/config/wpmInstall.properties /
   /opt/IBM/WPAR/manager/config/wpmInstall.properties.orig
   ```
2. Edit the `/opt/IBM/WPAR/manager/config/wpmInstall.properties` to match your environment. If you use the default installation, the following settings are required:
   - `AM_REG_PASSWD=<the password to be used for agent registration>`
   - `AM_REG_PASSWDV=<verification of the password to be used for agent registration>`
3. To complete the configuration, run the following command:
   ```bash
   # /opt/IBM/WPAR/manager/bin/WPMConfig.sh -i silent 
   -f /opt/IBM/WPAR/manager/config/wpmInstall.properties
   ```

Configuring the WPAR Manager agent

After you install the WPAR Manager agent, you must configure it for use by the WPAR Manager. You can use the `/opt/IBM/WPAR/agent/bin/configure-agent` script to configure the WPAR Manager agent.

If the WPAR Manager ports were not modified from the default values during the installation, run the following `configure-agent` script as root with the hostname of the WPAR Manager and the agent registration password provided in the WPAR Manager configuration:

```bash
# /opt/IBM/WPAR/agent/bin/configure-agent -amhost <wpar-manager.yourdomain.com> \ 
-passwd <agent_registration_password>
```

-`-help` Displays the command usage information
-options <file_name>
  Provide input to the command with a configuration file.

-prompt
  Prompt for agent manager registration password

-force
  Reconfigure a previously configured agent

-name
  Name of the common agent (Default: localhost)

-port <port_number>
  Common agent port number (Default: 9510)

-jport <port_number>
  JVM port number for nonstop service (Default: 9514)

-nport <port_number>
  Native port for the nonstop service (Default: 9515)

-wport <port_number>
  HTTP transport port (Default: disabled)

-wsport <port_number>
  HTTPS transport port (Default: disabled)

-unmanaged
  Common agent not managed by the agent manager

-amhost <host_name>
  Host name of agent manager (Default: AgentManagerServer)

-amport <port_number>
  Public port of agent manager (Default: 9513)

-ctxroot
  Agent manager context root (Default: /AgentMgr)

-password <password>
  Agent registration password

-noinstall
  Do not create a service to auto-start and do not start the common agent

-nostart
  Do not start the common agent after configuration

-hostname amhost
  Agent manager host name (Required)

-pubport port

-Agent Manager Public Port
  (Default: 9513)

-contextroot url
  Agent manager Context Root (Default: /AgentMgr)

-agentport port
  Agent Port (Default: 9510)

-force
  Reconfigure a previously configured agent

At a minimum, specify the -amhost flag to specify the WPAR Manager agent host name and one of either the -passwd flag or -prompt flag to specify the agent registration password. If the agent has previously been configured to another agent manager, specify the -force flag to reconfigure the agent.
The configuration script interactively prompts for the agent registration password. This password is specified when you configure the agent manager.

Configuring the WPAR Manager agent will fail if the following conditions are encountered:

- The configuration process is not able to reach the agent manager at the specified host, port, or context root. This can occur if the agent manager is offline or unreachable, or the host name, public port, or context root parameters have been specified incorrectly.
- The agent manager registration password is incorrect.
- The WPAR Manager agent is already configured to use a WPAR Manager agent. You can use the -force flag to reconfigure the WPAR Manager agent.
- All ports of the specified for use by the WPAR Manager agent (-port, -jport, -nport, -wport, -wspan) are distinct and not in use.

**Starting and stopping the WPAR Manager agent**

You can use the /opt/IBM/WPAR/agent/bin/wparagent command to start, stop, restart, and query the current status of the WPAR Manager agent.

When you start the WPAR Manager agent, it will attempt to retrieve secure certificates from the agent manager if it has not yet received certificates, or if the certificates are close to expiring. After validating that the secure certificates are up to date, the WPAR Manager agent sends a status report to the agent manager indicating that the agent has started successfully. If an error occurs during startup, error messages will be logged to the /var/opt/tivoli/ep/logs/error-log-0.xml file on the system.

Complete the following commands to start, stop, or restart the WPAR Manager agent:

- To start the WPAR Manager agent, run the wparagent start command.
- To stop the WPAR Manager agent, run the wparagent stop command.
- To restart the WPAR Manager agent, run wparagent restart command.

**Configuring WPAR Manager agent logging**

The WPAR Manager agent logs important troubleshooting information to log files in the /var/opt/IBM/WPAR/agent/logs/ directory. You can configure logging in the wparagent_logging.properties file.

The default configuration settings that are shipped with the WPAR agent are in the wparagent_logging.properties file, as follows:

```
# WPAR Agent Logging Properties
# Enable or disable WPAR Agent logging.
log.enabled = true
# Whether to append to existing logs or create new log files.
log.append = false
# Number of log files to keep.
log.count = 5
# Logging level - one of ERROR|WARNING|INFO|VERBOSE|FINE|FINER|FINEST
log.level = INFO
# File size limit of each log file in bytes.
log.limit = 1000000
```

To change the default settings for WPAR Manager agent logging, complete the following steps:

1. Open the /etc/opt/IBM/WPAR/agent/wparagent_logging.properties file in a text editor.
2. Modify the properties you want to change.
3. Restart the WPAR Manager agent using the wparagent restart command.
Configuring the environment for application mobility

There are restrictions on the setup of the environment to support application mobility. Different restrictions exist for live and static relocations.

The following restrictions apply to the environment configuration to support both types of application mobility:

- Managed systems to be used as departure and arrival systems for mobility must be within the same subnet.
- Source and destination servers must be running on compatible hardware and have compatible software installed.
- For IP version 6 networks, NFSv4 is required. To support NFSv4, all systems, such as the WPAR manager, WPAR agent, NFS server, etc, must also be in the same local NFS domain.

There are additional restrictions specific to system WPARs and application WPARs that differ depending on the relocation type.

Related concepts:
- “Managing workload partitions with WPAR Manager” on page 31
  You can use WPAR Manager to manage systems, WPARs, and WPAR groups.
- “Manual relocation” on page 11
  WPAR Manager version 1.2 supports static and live relocation methods for manual relocation. Manual relocation to a manually selected server can be done on WPARs that are members of a WPAR group enabled for policy-based relocation. WPAR Manager can intervene and attempt to re-relocate to another system unexpectedly, based on the details of the policy governing the WPAR group.

Related tasks:
- “Creating a WPAR that supports live relocation” on page 35
  Live relocation is the capability to relocate a WPAR to another system without losing the state of the application stack running within the WPAR.

Configuring application mobility for system WPARs

WPAR Manager 1.2 supports static relocation and an live relocation of WPARs. Static relocation is defined as a shutdown of the WPAR on the departure node and the clean start of the WPAR on the arrival node while preserving the file system state. Live relocation preserves the state of the application stack on the arrival system.

Review the following information to configure the specified type of application mobility.

Related tasks:
- “Viewing or modifying managed system properties” on page 32
  WPAR Manager allows you to view and change configuration details and physical properties for managed systems that have been registered with the application. Using WPAR Manager, you can change the description and the relocation domains assigned to managed systems.

Configuring live application mobility for system WPARs:

To enable live application mobility for system WPARs, you must specify a remote directory that will be the root mount point for the /, /var, /home, and the /tmp directories.

No restrictions exist on the WPAR's filesystems for static relocation mobility. However, a shared file system accessible from both the departure and arrival server needs to be created and configured to store the temporary backup image generated during the static relocation of a WPAR. Because the remote /usr directory and the remote /opt directory are accessed over the network, you might experience slower performance than with local disk access. You should use these remote directories only if you need a private /usr directory and a private /opt directory.
The steps below for configuring application mobility for your system WPAR assume the following network topology:

**wparagent1.yourdomain.com**
A WPAR Manager agent that is installed and configured for use with WPAR Manager.

**wparagent2.yourdomain.com**
Another WPAR Manager agent installed and configured for use with WPAR Manager.

**wparhostname.yourdomain.com**
The host name of a system WPAR that you created as a relocatable WPAR.

**nfssrv1.yourdomain.com**
An NFS server that stores the shared file system hosting the WPAR remote file systems.

To configure your environment for system WPAR relocation, complete the following steps:

1. Create a file system on the nfssrv1.yourdomain.com NFS server to host the system WPAR remote file systems. For example:
   ```
   crfs -v jfs2 -m /wparsfs -A yes -a size=1G -g rootvg
   ```
   **Note:** If you want to use an existing file system, you can skip this step.

2. Mount the file system you created (or the existing file system you plan to use) by running the following command:
   ```
   mount /wparsfs
   ```

3. Create a directory called `wparhostname` on nfssrv1.yourdomain.com by running the following command:
   ```
   mkdir /wparsfs/wpars/wparhostname
   ```

4. Export the directory so that all WPAR Manager agents and WPAR host names have root access to write to the new file system by running the following command:
   ```
   # mknfsexp -d /wparsfs/wpars/wparhostname -r wparagent1,wparagent2,wparhostname -B
   ```
   **Note:** WPAR configured with an IP version 6 address must use NFSv4. Use the `-v` flag to specify the NFS version.

5. Create a WPAR with the NFS server and root directory you specified using either the advanced interface or the Create WPAR wizard.

**Configuring static application mobility for system WPARs:**

No restrictions exist on the WPAR's file systems for static relocation mobility. However, a shared file system accessible from both the departure and arrival server needs to be created and configured to store the temporary backup image generated during the static relocation of a WPAR. You must grant root permissions for the shared file system to the global WPAR Manager agent.

The following steps assume that you are using an NFS file system, and also assume that your system has the following network topology:

**wparagent1.yourdomain.com**
A WPAR Manager agent that is installed and configured for use with WPAR Manager.

**wparagent2.yourdomain.com**
Another WPAR Manager agent installed and configured for use with WPAR Manager.

**nfssrv1.yourdomain.com**
An NFS server that stores the shared file system hosting the WPAR remote file systems.

To configure your environment for system WPAR static relocation, complete the following steps:

1. Create a file system, named `/sfs` in this example, on the nfssrv1.yourdomain.com NFS server where temporary WPAR's backup images will be stored during static relocation. For example:
# crfs -v jfs2 -m /sfs -A yes -a size=1G -g rootvg

**Note:** If you want to use an existing file system, you can skip this step.

2. Mount the file system you created or the existing file system by running the following command:
   ```bash
   # mount /sfs
   ```

3. Export the directory so that all of the WPAR Manager agents have root access to write to the new file system by running the following command:
   ```bash
   # mknfsexp -d /sfs -r wparagent1,wparagent2 -B
   ```

4. Mount the file system on all of the WPAR Manager agent systems (wparagent1 and wparagent2 in Step 3) by running the following command:
   ```bash
   # mknfsmnt -f /var/adm/WPAR -d /sfs -h nfssrv1 -B
   ```

**Note:** The `/var/adm/WPAR` directory is the default mount point. If you would like to use a different mount point, you must configure the WPAR Manager to use that mount point as the new shared file system location. To set this variable, select **WPAR Manager Settings > Application Configuration** and specify the path to the shared file system on all of the WPAR Manager agent systems in the shared directory field.

### Configuring application mobility for application WPARs

WPAR Manager agent 1.2 or later does not impose restrictions on live relocation. However, if you have WPAR Manager agent 1.1 installed, you must create and configure a shared file system for WPAR Manager.

You must grant root permissions for the shared file system to the WPAR Manager agent and the WPAR host name. There are no restrictions for static relocation.

The steps below for configuring live application mobility for application WPARs assume the following network topology:

- **wparagent1.yourdomain.com**
  - A WPAR Manager agent that is installed and configured for use with WPAR Manager

- **wparagent2.yourdomain.com**
  - Another WPAR Manager agent installed and configured for use with WPAR Manager

- **wparhostname.yourdomain.com**
  - The host name of an application WPAR that you created as a relocatable WPAR

- **nfssrv1.yourdomain.com**
  - An NFS server that stores the shared file system hosting the WPAR remote file systems.

To configure your environment for live application WPAR relocation, complete the following steps:

**Note:** , which is basically redeploying the WPAR on the arrival system.

1. Create a file system, named `/sfs` in this example, on the `nfssrv1.yourdomain.com` NFS server where application WPARs states will be stored during checkpoint and restart operations. This file system does not have to be the same file system hosting the remote file systems for your system WPARs. For example:
   ```bash
   crfs -v jfs2 -m /sfs -A yes -a size=1G -g rootvg
   ```

2. Mount the file system you created (or the existing file system you plan to use) by running the following command:
   ```bash
   mount /sfs
   ```

3. Export the directory so that all of the WPAR Manager agents and the WPAR host names have root access to write to the new file system by running the following command:
   ```bash
   # mknfsexp -d /sfs -r wparagent1,wparagent2,wparhostname -B
   ```
Note: WPARs configured with an IP version 6 address must use NFSv4. Use the -v flag to specify the NFS version.

4. Mount the file system on all of the WPAR Manager agent systems (wparagent1 and wparagent2 in Step 3) by running the following command:
   
   ```
   # mknfsmnt -f /var/adm/WPAR -d /sfs -h nfssrv1 -B
   ```

   Note: The /var/adm/WPAR directory is the default mount point. If you would like to use a different mount point, you must configure the WPAR Manager to use that mount point as the new shared file system location. To set this variable, select WPAR Manager Settings > Application Configuration and specify the path to the shared file system on all WPAR Manager agent systems in the State file root directory field.

**Configure WPAR Manager with LDAP authentication**

An LDAP server provides more flexibility for user authentication than using the local users of the WPAR Manager host system. For example, users could set up a single LDAP server for multiple instances of WPAR Manager to use for authentication.

Another reason to use LDAP is that a user may not want the administrator user of WPAR Manager to know the root password (or another non-root user password) on the host system due to security issues.

To configure WPAR Manager with LDAP authentication, complete the following steps:

2. Enter the following settings in the new properties files:

   ```
   com.ibm.lwi.security.jaas.jaasindex = Jaas2.Ldap
   com.ibm.lwi.rolemanagerfragment = com.ibm.lwi.security.rolemanagers.ldap.RoleManagerLdap
   ```

   The following table includes property settings that are configured during the installation of the LDAP server and should be supplied by the LDAP server administrator.

   **Table 5. Settings for the LDAP properties file**
   
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.ibm.lwi.LDAPHost</td>
<td>Specifies the host name of the LDAP server.</td>
</tr>
<tr>
<td>com.ibm.lwi.LDAPPor</td>
<td>Specifies a port defined for the LDAP server. The LDAP default port is 389. If SSL is enabled on the LDAP server, the default port is 636.</td>
</tr>
<tr>
<td>com.ibm.lwi.LDAPAdminUser</td>
<td>Specifies an administrator DN defined for the LDAP server. The default for the IBM Tivoli® Directory Server is cn=admin.</td>
</tr>
<tr>
<td>com.ibm.lwi.LDAPAdminPassword</td>
<td>Specifies an encrypted password of the administrator user defined for the LDAP server. Note: You must encrypt the plain text password using the lwiencoder.sh command found in the <code>/opt/IBM/WPAR/manager/lwi/bin: lwiencoder.sh -filename /opt/IBM/WPAR/manager/lwi/conf/overrides/security.properties -keylist com.ibm.lwi.LDAPAdminPassword</code> path variable. You can enter <code>lwiencoder.sh -help</code> for more options.</td>
</tr>
<tr>
<td>com.ibm.lwi.LDAPBase</td>
<td>Specifies Base (root) DN defined for LDAP server.</td>
</tr>
<tr>
<td>com.ibm.lwi.searchfilter</td>
<td>Specifies user search filter to use for search queries on LDAP server. The following are examples of search filters for user search queries for LDAP servers: Microsoft Active Directory: <code>(&amp;(sAMAccountName=sv)(objectcategory=user))</code> IBM Tivoli Directory Server: <code>(&amp;(uid=sv)(objectclass=account))</code></td>
</tr>
</tbody>
</table>

AIX Version 6.1: IBM PowerVM Workload Partitions Manager for AIX V1.2
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| com.ibm.lwi.rolemanager.ldap.filters.usergroup | Specifies a search filter used for search queries on LDAP server for group objects. The following are examples of search filters for groups on LDAP servers: **Microsoft Active Directory:** 
\{(objectCategory=group)\} 
**IBM Tivoli Directory Server:** 
\{(objectclass=groupOfNames)\} |
| com.ibm.lwi.rolemanager.ldap.filters.users | Specifies search-filter used for search queries on LDAP server for user objects. The following are examples of search filters for users on LDAP servers: **Microsoft Active Directory:** 
\{(objectCategory=person)(objectCategory=user)\} 
**IBM Tivoli Directory Server:** 
\{objectclass=person\} |
| com.ibm.lwi.rolemanager.ldap.names.memberAttribute | Specifies the name of member attribute of group object in directory. If there are more then one property value, values must be separated by a comma. The following are examples of search filters for users on LDAP servers: **Microsoft Active Directory:** member 
**IBM Tivoli Directory Server:** member |
| com.ibm.lwi.rolemanager.ldap.names.loginName | Specifies the name of login ID attribute of user in directory. The following are examples of login id attribute of user on LDAP servers: **Microsoft Active Directory:** sAMAccountName 
**IBM Tivoli Directory Server:** :uid |
| com.ibm.lwi.rolemanager.ldap.attributes.user.fullName | Specifies a full name attribute ID of user object in directory. The following are examples of full name attribute ID of user on LDAP servers: **Microsoft Active Directory:** displayName 
**IBM Tivoli Directory Server:** displayname |
| com.ibm.lwi.rolemanager.ldap.attributes.user.email | Specifies an e-mail attribute name of user object in directory. The following are examples of e-mail attribute name of user on LDAP servers: **Microsoft Active Directory:** mail 
**IBM Tivoli Directory Server:** mail |
| com.ibm.lwi.rolemanager.ldap.attributes.user.description | Specifies a description attribute name of user object in directory. The following are examples of description attribute name of user on LDAP servers: **Microsoft Active Directory:** description 
**IBM Tivoli Directory Server:** description |
| com.ibm.lwi.rolemanager.ldap.attributes.group.description | Specifies a description attribute name of group object in directory. The following are examples of description attribute name of group on LDAP servers: **Microsoft Active Directory:** description 
**IBM Tivoli Directory Server:** description |
Table 5. Settings for the LDAP properties file (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.ibm.lwi.rolemanager.ldap.attributes.user.icon</td>
<td>Specifies an icon attribute name of user object in directory.</td>
</tr>
<tr>
<td></td>
<td>The following are examples of icon attribute name of user on LDAP servers:</td>
</tr>
<tr>
<td></td>
<td>Microsoft Active Directory: thumbnailPhoto</td>
</tr>
<tr>
<td></td>
<td>IBM Tivoli Directory Server: photo</td>
</tr>
</tbody>
</table>

lwiMapRole.sh

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lwiMapRole.sh</td>
<td>Map the desired LDAP user to the administrator role. By default, the root user ID is mapped to the administrator role for WPAR Manager.</td>
</tr>
<tr>
<td></td>
<td>The following example maps the administrator role to another user id on the LDAP server:</td>
</tr>
<tr>
<td></td>
<td>lwiMapRole.sh -add -role administrator -user &lt;user id&gt;</td>
</tr>
<tr>
<td></td>
<td>lwiMapRole.sh -add -role WPARAdministrator -user &lt;user id&gt;</td>
</tr>
<tr>
<td></td>
<td>The following example removes the root user mapping for the administrator role if desired:</td>
</tr>
<tr>
<td></td>
<td>lwiMapRole.sh -remove -role administrator -user root</td>
</tr>
<tr>
<td></td>
<td>lwiMapRole.sh -remove -role WPARAdministrator -user root</td>
</tr>
</tbody>
</table>

The following table includes property settings for that are only required if you are enabling a secure SSL connection to the LDAP server from WPAR manager:

Table 6. SSL property settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.ibm.lwi.ldap.ssl.enable=true</td>
<td>Specifies that you want to use SSL.</td>
</tr>
<tr>
<td>com.ibm.lwi.ldap.ssl.keyStore</td>
<td>Specifies the generated client keystore file path. The path should be relative to the /opt/WPAR/manager/lwi/runtime/core WPAR manager core directory. For example: /../../security/keystore/clientKeyStore.jks</td>
</tr>
<tr>
<td>com.ibm.lwi.ldap.ssl.keyStorePassword</td>
<td>Specifies the encrypted password of keystore.</td>
</tr>
<tr>
<td>com.ibm.lwi.ldap.ssl.trustStore</td>
<td>Specifies the generated client truststore file path. The path should be relative to the WPAR manager core directory (/opt/IBM/WPAR/manager/lwi/runtime/core). For example /../../security/keystore/clientTrustStore.jks.</td>
</tr>
<tr>
<td>com.ibm.lwi.ldap.ssl.trustStorePassword</td>
<td>Specifies the encrypted password of truststor. Use the following command to encrypt the clear-text passwords:</td>
</tr>
<tr>
<td></td>
<td>/opt/IBM/WPAR/manager/lwi/bin/lwiencoder.sh -filename security.properties -keylist com.ibm.lwi.ldap.ssl.keyStorePassword, com.ibm.lwi.ldap.ssl.trustStorePassword</td>
</tr>
</tbody>
</table>

Note: For troubleshooting, use the lwilog.sh command to enable logging for the Light Weight InfraStructure (LWI) component.

lwilog.sh -addlogger com.ibm.lwi.security FINEST

Configuring the WPAR Manager agent to use a different agent manager

After you configure the WPAR Manager agent to use a specific agent manager, further attempts at configuring the WPAR Manager agent to use a different specific agent manager will be unsuccessful. You must specify the -force flag to override the original agent manager configuration.
Using this flag will unregister the WPAR Manager agent from the current agent manager, and configure the WPAR Manager agent to connect to the new agent manager.

To configure the WPAR Manager agent to use a different agent manager, run the configuration script, as follows:

```
configure-agent -hostname agent_manager_hostname -force
```

**Related information:**

“Managed server discovery fails” on page 51

The WPAR Manager fails to discover an agent.

### Setting up the console in a WPAR environment

IBM Systems Director Console for AIX is not installed on each WPAR by default. In order to enable system management for AIX instances within a WPAR, you must use the `wparConsole.sh` utility.

The IBM Systems Director Console for AIX will be installed on all newly created system WPARs if you run the following:

```
#/opt/pconsole/bin/wparConsole.sh -e
```

To disable the installation of the console within system WPARs, run the following:

```
#/opt/pconsole/bin/wparConsole.sh -d
```

The default size of the root file system within a WPAR is not large enough for the console. To increase the file system size when creating a WPAR, pass the following parameters to the `mkwpar` command:

```
#mkwpar -M directory=/ size=128M
```

If the system WPAR has already been created, you can manually increase the size of the root file system using the `chfs` command. You might need to reinstall the `sysmgtpconsole.*` filesets in the WPAR if the console has been accessed prior to the size increase. Enabling and disabling the console on WPAR only affects WPAR created in the future. For more information about the `syncwpar` command see Synchronize a WPAR topic.

### ProxyServer

In order to reduce the start-up resources of the console in a WPAR environment, the console is not started until a connection attempt is made. All HTTP requests to the console are routed to a proxy which will start the console (if needed) before forwarding the request to the console. To see if the proxyServer is configured on your system enter the following command:

```
#lssrc -g pconsole
```

For systems with the proxyServer, you will see two lines: one line for the `pconsoleProxy` subsystem and another line for the `pconsole` subsystem. In addition, the `/etc/inittab` file will have an entry to start `pconsoleProxy` subsystem instead of `pconsole`. To manually enable the `pconsoleProxy` on a system that already has IBM Systems Director Console for AIX installed, run the command:

```
#/opt/pconsole/bin/pconsole_config -enable
```

To disable the proxy so that the console is started at system boot, run the following command:

```
#/opt/pconsole/bin/pconsole_config -disable
```

When the proxy is configured, the console is configured to use ports 5337 and 5338, while the proxy uses 5333 and 5336. These values can be changed by editing the `/pconsole/lwi/conf/overrides/port.wpar.properties` file, the `/pconsole/lwi/conf/webcontainer.properties` file, and the `/opt/pconsole/bin/pconsole_config` file.
Note: The response to the first connection to the proxy will be significantly delayed until the console is started. Subsequent requests should not be delayed.

Related concepts:

"Manual relocation" on page 11
WPAR Manager version 1.2 supports static and live relocation methods for manual relocation. Manual relocation to a manually selected server can be done on WPARs that are members of a WPAR group enabled for policy-based relocation. WPAR Manager can intervene and attempt to re-relocate to another system unexpectedly, based on the details of the policy governing the WPAR group.

Related tasks:

"Synchronizing a WPAR" on page 39
The installed software in a system WPAR can be synchronized with the software in the global AIX system. You should synchronize your WPAR if updates have been applied to the managed system, or if the WPAR has been relocated.

Removing WPAR Manager

You can remove WPAR Manager from your system with the installp command.

To remove WPAR Manager, complete the following steps:
1. Log in as the root user to the system where WPAR Manager is installed.
2. Run the installp command as follows to remove WPAR Manager and the agent manager:

   installp -ug wparmgt.mgr wparmgt.cas.agentmgr

Removing the WPAR Manager DB2 database

You can remove the WPAR Manager DB2 database from your system with the DBUninstall.sh script.

To remove the WPAR Manager DB2 database, complete the following steps:

Note: If you are using Apache Derby as the database for WPAR Manager, no additional steps are required to remove the database. The database is removed when the wparmgt.mgr.rte fileset is removed.
1. Log in as the root user to the system where the WPAR Manager database is installed.
2. Change directories to the /opt/IBM/WPAR/manager/db/bin directory by running the following command:

   cd /opt/IBM/WPAR/manager/db/bin

3. Run the DBUninstall.sh script using the following command:

   ./DBUninstall.sh -a

4. Run the installp command as follows to complete the removal of the database:

   installp -ug wparmgt.db

Removing the WPAR Manager agent

You can remove the WPAR Manager agent from your system with the installp command.

The following filesets must be removed:
- wparmgt.agent.rte
- mcr.rte

To remove all of the WPAR Manager agent filesets, run the installp command, as follows:
installp -u wparmgt.agent.rte mcr.rte
Note: The cas.agent fileset and the tivoli.tivguid fileset are shared components which may be in use by other products on the system and are installed with the WPAR Manager agent. If no other products on the system are using these filesets, then they can also be uninstalled from the system. Running the installp -u cas.agent tivoli.tivguid command will fail if other products are dependent on these filesets. Specify the -g flag with the installp command to remove these filesets and any other dependencies.

Related tasks:
“Remove a managed system” on page 33

When you remove a managed system, the WPAR Manager provides options for handling WPARs that are deployed on the system.

Managing workload partitions with WPAR Manager

You can use WPAR Manager to manage systems, WPARs, and WPAR groups.

Before you can use the WPAR Manager, JavaScript must be enabled in your browser. After you install and configure the WPAR Manager, you can access by entering the following into your web browser, http://<wpar-manager.yourdomain.com>:<public_port>/ibm/console. The default WPAR Manager public port is 14080. When you are prompted to log in, use the root user name and password for the WPAR Manager system.

If you are using Internet Explorer to access the WPAR Manager interface, you must have the SVG graphics plug-in from Adobe installed. You can download the plug-in from the following Adobe web site: http://www.adobe.com/svg/viewer/install/

Related concepts:
“Configuring the environment for application mobility” on page 23

There are restrictions on the setup of the environment to support application mobility. Different restrictions exist for live and static relocations.

Managed systems

A managed system is an AIX logical partition (LPAR) with the WPAR Manager agent installed and configured.

A managed system can be either of the following types of systems:

Physical system
A POWER4 or later system running AIX with WPAR support. Even if a server is not being managed by a Hardware Management Console (HMC) or the Integrated Virtualization Manager, the firmware defines a full system partition or manufacturing default configuration, so that the system appears as one logical partition that is using all of the system resources.

Virtual system
An LPAR on a POWER4 or later system where AIX is installed and running.

Defining a managed system
When a managed system is registered into the WPAR Manager, a system profile is automatically assigned to it based on the hardware and software characteristics of the system that have been retrieved from the agent.

To bring an AIX server or LPAR into the management environment of the WPAR Manager as a managed system, perform the following steps:

1. Ensure that the system is running a version of AIX that supports WPARs. If your system supports WPARs, when you run the ls1pp -lq bos.wpars command, it returns basic information about the fileset. If your system does not support WPARs, a message indicating that the fileset is not installed is displayed.
2. Ensure that you have installed and configured an instance of the WPAR Manager software.
3. Install the WPAR Manager agent on the system.
4. Register the agent with the WPAR Manager server software and start the agent.

When an WPAR Manager agent is installed on a managed system, it must be discovered by WPAR Manager in order to communicate with the system. To discover the new managed system in WPAR Manager, select the Discover button on the Managed Systems resource view. When a managed system is successfully discovered and registered, it is displayed in the WPAR Manager and is in the Online state.

**Viewing or modifying managed system properties**

WPAR Manager allows you to view and change configuration details and physical properties for managed systems that have been registered with the application. Using WPAR Manager, you can change the description and the relocation domains assigned to managed systems.

Complete the following steps to modify or view the properties for the system:

1. Go to the Resource Views section of the navigation area.
2. Select Managed Systems.
3. In the table of managed systems, click the name of the system.

**Related concepts:**

“Configuring application mobility for system WPARs” on page 23

WPAR Manager 1.2 supports static relocation and an live relocation of WPARs. Static relocation is defined as a shutdown of the WPAR on the departure node and the clean start of the WPAR on the arrival node while preserving the file system state. Live relocation preserves the state of the application stack on the arrival system.

**Updating the profile for a managed system**

When a system is first registered, the WPAR Manager stores hardware and software configuration parameters specific to the managed system. Any time a system undergoes configuration changes, including the WPAR privilege set (WPS) specified in the /etc/wpars/secattrs, the system profile assigned to the managed system is longer valid and must be updated.

Updating the system profile triggers the Compatibility analysis that is used to recommend relocation targets and refreshes the WPAR privilege set for the managed system.

**Note:** Managed systems are assigned to WPAR groups through their system profiles; therefore the managed system could be removed as a target for automatic relocation if the configuration changes result in the assignment of the managed system to a different profile.

1. Go to the Resource Views section of the navigation area.
2. Select Managed Systems.
3. In the table of managed systems, select a managed system by selecting the corresponding check box in the Select column.
4. Select Update system profile.

**Viewing performance metrics for a managed system**

You can view current and historical data for selected performance metrics for both managed systems and WPARs.

Viewing performance metrics helps you determine whether systems are over-used or under-used. This information can help you make decisions as to how you should manage your WPARs. For example, it might help you decide whether adding a new WPAR would impact performance, or whether it would improve performance to relocate a WPAR to another managed system.

To view performance metrics for managed systems and WPAR complete the following steps:

1. Go to the Managed Systems view in the WPAR Manager.
2. Select a system.

From the Performance Metrics page, you can view the following information:
- Recent performance trends for selected metrics
- Longer-term historical performance data

**Remove a managed system**
When you remove a managed system, the WPAR Manager provides options for handling WPARs that are deployed on the system.

It is possible to delete or preserve the database definitions for the WPARs in the WPAR Manager database, and also to undeploy the WPARs from the system when the managed system is removed.

When a managed system is removed from the WPAR Manager, the initial registration is revoked and the agent installed on the managed system can no longer communicate with the application. When a managed system is removed from the WPAR Manager, it is no longer monitored or shown in the WPAR Manager user interface. However, the WPAR Manager agent software continues to run on the system.

**Related tasks:**
[“Removing the WPAR Manager agent” on page 30](#)

You can remove the WPAR Manager agent from your system with the `installp` command.

**Managing WPARs**
WPAR Manager allows you to perform basic management tasks, such as creating, starting, and stopping WPARs.

**Managing WPAR groups**
A WPAR group is a defined group of WPARs that are governed by common relocation policy settings.

In order to take advantage of policy-based WPAR relocation, create a WPAR group and assign WPARs on the basis of application affinity. For example, a hotel reservation application might consist of three WPAR groups:
- Web server group, containing all WPARs hosting the Web server
- Application server group, containing all WPARs hosting the application server
- Database server group, containing all WPARs hosting the database

Each WPAR group works as a tier in the hotel application stack where the set of WPARs in the group host clustered applications.

The definition of a WPAR group contains not only the list of the WPARs that belong to the group, but also the definition of the policy that governs the automated relocation of WPARs in response to various workload-related metrics. To create a WPAR group, select **Guided Activities > Create WPAR Group**. The following figure depicts the general composition of a WPAR group.
Creating WPARs

The WPAR Manager allows you to create and manage WPARs across multiple systems.

When a WPAR is created through the WPAR Manager, you can choose from a set of options that allow you to deploy the WPAR into a particular system. If the WPAR is not deployed, then its configuration is stored into the WPAR Manager database and saved for later use. A WPAR that is not deployed in a system is in the undeployed state, which means that no resources are allocated for that WPAR in any of the managed systems controlled by the application. WPARs in the undeployed state can be deployed later if they are needed.

Note: Although the WPAR Manager does not restrict the use of multiple WPARs with the same network configuration, use caution. If the new WPAR is deployed into a managed system that is already using that network configuration for another WPAR, the deployment task will fail. Alternatively, if the WPAR is deployed into a system different to that hosting the WPAR with the same network configuration, no error are raised and two WPARs share the same network address.

To create a WPAR, you can use either the Create Workload Partition wizard or the Advanced interface. It is recommended that you use the Create Workload Partition wizard the first time you create a workload partition in WPAR Manager.

To create a WPAR using the Create Workload Partition wizard, complete the following steps:

1. Log in as the root user to the system where WPAR Manager is installed.
2. Select **Select Guided Activities > Create Workload Partition**.
3. Select **Next** to start the wizard.
4. Follow the instructions on each page to complete the wizard.

To create a WPAR using the Advanced interface, complete the following steps:

**Note**: You should only use the Advanced interface if you are familiar with the process of creating workload partitions in WPAR Manager.

1. Log in as the root user to the system where WPAR Manager is installed.
2. Select **Select Guided Activities > Create Workload Partition**.
3. In the Create Workload Partition page, select **Use advanced interface**.
4. Complete all of the required fields marked with an asterisk (*) for each page.

**Creating a WPAR that supports live relocation**:

Live relocation is the capability to relocate a WPAR to another system without losing the state of the application stack running within the WPAR.

In order to create a WPAR that supports live relocation, you must configure your WPAR as follows:

- To support live relocation a WPAR must enable the checkpoint option. This setting can be specified when the WPAR is created through the **Enable checkpoint** option. A WPAR with the checkpoint option enabled allows the application to save the internal state of applications running within the WPAR to be restored on another similarly configured system.
- Specify a valid network configuration. WPARs without network connectivity cannot be relocated. If the name of your WPAR resolves to a valid network host name, the WPAR connects to the network automatically. If the name of your WPAR does not resolve to a valid network host name, you must provide connection information.

**Note**: WPAR Manager does not check to see if the name of a WPAR resolves to a valid network host name.

- All file systems for a checkpoint-enabled WPAR must be specified as NFS mounts, except for the /usr file system and the /opt file system, which can be mounted as read-only namefs file systems from the managed system. NFS file systems must be exported with read-write access and root access to the WPAR host name, the departure system host name, and the arrival system host name.

**Related concepts**:  
"Configuring the environment for application mobility" on page 23

There are restrictions on the setup of the environment to support application mobility. Different restrictions exist for live and static relocations.

"Mounting the /, /tmp, /var, and /home file systems" on page 36

For mobile WPARs, you must mount the / file system, the /tmp file system, the /var file system, and the /home file system remotely as read-write file systems using NFS.

Mounting the /opt file system and the /usr file system:

Mobile WPARs can either mount the /usr file system and the /opt file system over the network using NFS or mount it as a read-only file system using namefs.

Because creating a WPAR with a remote /usr file system and a remote /opt file system is a extensive operation, it is recommended that you mount them locally as read-only file systems. Mounting the file systems locally reduces the file system size requirements on the NFS server that will host the file systems of the WPAR. For example, a WPAR that is created using a local /usr file system and a local /opt file system requires a minimum of approximately 450 MB on the NFS server that will host the remaining file systems. When the /usr file system and the /opt file system are configured remotely, the minimum space...
required increases to approximately 2 GB. Although there are advantages to mounting these file systems locally, if the WPAR is to have its own set of programs installed and requires a private /usr file system and a private /opt file system, then using local read-only file systems is not possible. In this case, the /usr file system and the /opt file system need to be mounted remotely as read-write file systems using NFS.

Mounting the /, /tmp, /var, and /home file systems:

For mobile WPARs, you must mount the / file system, the /tmp file system, the /var file system, and the /home file system remotely as read-write file systems using NFS.

Each of these file systems must be empty unless the Preserve file system option is used.

A typical directory structure on the NFS server might look like the following example:

```
/parent-dir
    /wpardirname
        /home
        /tmp
        /var
```

Related tasks:

“Creating a WPAR that supports live relocation” on page 35

Live relocation is the capability to relocate a WPAR to another system without losing the state of the application stack running within the WPAR.

Working with WPARs created from the command line:

WPARs created from the command line will be discovered by the WPAR Manager.

The configuration for the discovered WPARs is stored in the WPAR Manager database of the application. After the WPARs are discovered, you can perform operations on these WPARs as if you had created them through the WPAR Manager.

Related information:

Configuring system WPARs in IBM Workload Partitions for AIX
Configuring application WPARs in IBM Workload Partitions for AIX

Viewing or modifying WPAR properties

The WPAR Manager provides the ability to view or modify the configuration for WPARs managed by the application.

When a WPAR is not deployed in a managed system, the WPAR Manager allows you to modify all of the properties of the WPAR. If the WPAR is currently deployed on a managed system, only selected properties of the WPAR's configuration can be modified, depending on the state of the WPAR.

To view the Properties page for a WPAR, go to the Resource Views section of the navigation area, and select Workload Partitions. In the table of managed systems, click the name of the WPAR, which is a link to the Properties page. Alternatively, you can select a WPAR by selecting the check box in the Select column, and then selecting View/Modify Properties.

Working with WPARs modified with AIX commands:

Although the WPAR Manager provides a user interface to modify the configuration of WPARs, you can also use the command line to make modifications. When a change is completed through the command line, the WPAR Manager discovers the changes after a short delay and the WPAR Manager database is updated to reflect the new configuration.
Deploying a WPAR
Use the definition of a WPAR in the database to create the WPAR on a managed system.

Deploying a WPAR works differently depending on the type of the WPAR. When a system WPAR is deployed, resources are allocated on the target managed system and, unless otherwise specified as part of the deployment options, the WPAR will not be started. A system WPAR will not go back to the Undeployed state unless it is removed from the system by the user. Application WPARs, however, are started as soon as the WPAR is deployed on the system. After the application running within the WPAR is completed, the lifespan of the WPAR is also completed. Because the WPAR no longer exists on the server, the WPAR Manager changes the state of the WPAR back to Undeployed.

To deploy a WPAR on a managed system, complete the following steps:
1. Locate the WPAR that you want to deploy. In the Navigation area, expand Resource Views, then select Workload Partitions. A tabular view of all defined workload partitions, both deployed and undeployed is displayed.
2. Select a WPAR that is not deployed, then select Deploy. The Deploy Workload Partition page is displayed.
3. From the Deploy Workload Partition page, enter the target system for deployment and click OK to deploy the selected WPAR.

Backing up WPARs
The back up operation in WPAR Manager will back up the selected file to a backup image file.

This function is equivalent to using the mkwpardata command followed by the savewpar command. The resulting backup image can be used to recreate a WPAR using the restwpars command or the WPAR Manager user interface.

The following are restrictions for this operation:
- Only system WPARs in the defined state or the active state can be backed up. For other WPARs, the Back up menu option will be disabled.
- You can only back up to an AIX file. To back up to a CD-ROM, DVD, or tape, you must log on to the managed system and use the mkwpardata and savewpar commands with the desired options.

To backup a workload partition to an image file on a managed system, complete the following steps:
1. Locate the WPAR that you want to deploy. In the Navigation area, expand Resource Views, then select Workload Partitions. This displays a tabular view of all defined workload partitions, both deployed and undeployed.
2. Select the WPAR that you want to back up, then click the Action button and select Back up.
3. From the Backup WPAR page, specify the backup directory location and any other backup options.
4. Click OK to complete the backup.

Restoring WPARs
You can restore a WPAR from a backed-up image file that was created using either WPAR Manager or the savewpar command.

A workload partition backup image contains an image.data file and a workload partition specification file that are used to establish the characteristics of a WPAR name.

To restore a workload partition from a backup image, complete the following steps:
1. Locate the WPAR that you want to deploy. In the Navigation area, expand Resource Views, then select Workload Partitions. This displays a tabular view of all defined workload partitions, both deployed and undeployed.
2. Click the Action button and select Restore.
3. From the Restore WPAR page, specify the full host name of the managed system on which the backup image was created and the path to the backup image. You can specify other options by selecting the Synchronization tab or the Other Options tab.

4. Click OK to complete the task.

**Starting a system WPAR**

After the WPAR is created, only the infrastructure for the WPAR is in place. You must start the WPAR.

Before the partition is started, the file systems are not mounted, network configuration is not active, and processes are not running. Unless you specified to start the WPAR after it was created, the WPAR will go to the Defined state and cannot be used until it is started. Only system WPARs that are in the Defined state can be started. You can only perform this action for system WPARs because application WPARs are started as soon as they are deployed into a system and never go through the Defined state.

To start a system WPAR, complete the following steps:
1. From the Navigation area, open a view of the WPARs by selecting Resource Views > Workload Partitions.
2. Select one or more WPAR in the Defined state that you want to start. From the drop-down menu, select Start.

**Stopping a WPAR**

System WPARs and application WPARs can be stopped while they are active in a managed system.

Depending on the type of the WPAR, the stop operation behaves differently. For both system WPARs and application WPARs, the stop operation deactivates the running WPAR. System WPARs remain on the system but the state of the WPAR changes to Defined. When an application WPAR is stopped, the configuration of the WPAR is removed from the system and the state changes to Undeployed.

To stop a WPAR, complete the following steps:
1. Select an Active WPAR. You can do this by selecting Resource Views > Workload Partitions.
2. Select one or more WPARs that you want to stop. From the drop-down menu, select Stop.

**Pausing a WPAR**

The WPAR Manager allows you to pause WPARs that are deployed on a managed system.

A WPAR can only be paused if the checkpoint option is enabled. When a WPAR is paused, all of its processes are frozen, a snapshot of the state of the processes is taken on disk, network traffic is halted, and the state of the WPAR is changed to Paused. You can later use this saved state to resume operations on the WPAR from the point where it was paused. If a WPAR has active network connections when it is paused, the connections will time out if the WPAR remains paused for a long period of time.

To pause a WPAR, use the following steps:
1. Select an Active WPAR. You can do this by selecting Resource Views > Workload Partitions.
2. Select one or more WPARs that you want to pause. From the drop-down actions menu, select Pause.

**Resuming a WPAR**

A WPAR that is in the Paused or Frozen state can be resumed through the WPAR Manager.

When a WPAR is resumed, all of the processes for the WPAR continue to run. Network connections are also resumed for the WPAR, unless they have expired.

To resume a WPAR, use the following steps:
1. Select an Active WPAR. You can do this by selecting Resource Views > Workload Partitions.
2. Select one or more WPARs in the Paused or Frozen state. From the drop-down menu, select Resume.
Synchronizing a WPAR
The installed software in a system WPAR can be synchronized with the software in the global AIX system. You should synchronize your WPAR if updates have been applied to the managed system, or if the WPAR has been relocated.

The synchronize page allows you to choose options for synchronizing installp filesets, RPM filesets, or all of the installed software. Synchronization is also available when you are restoring a WPAR from a backup image. The synchronize page is not available for undeployed WPAR or application WPARs.

To synchronize a WPAR, complete the following steps:
1. Select a system WPAR that is deployed on a managed system. You can do this by selecting Resource Views > Workload Partitions.
2. Select one or more WPARs from the table that you want to synchronize.
3. From the drop-down menu, select Synchronize.

Related concepts:
“Setting up the console in a WPAR environment” on page 29
IBM Systems Director Console for AIX is not installed on each WPAR by default. In order to enable system management for AIX instances within a WPAR, you must use the wparConsole.sh utility.

Ending WPAR processes
WPARs that are in the Paused state cannot be stopped from a managed system using the conventional stop mechanism, you have to use the ending processes.

If a WPAR in the paused state needs to be stopped, you must use the End Processes action. Ending the process on a WPAR is similar to stopping a WPAR, but it only works for WPARs in the Paused state. Depending on the type of the WPAR, the End Processes action will behave differently. For both WPAR types, the End Processes action forces the deactivation of the paused WPAR, however, system WPARs remain in the system but their state changes to Defined. When processes on an application WPAR are ended, the WPAR is removed from the system and its state changes to Undeployed.

To end the processes on a paused WPAR, complete the following steps:
1. Select a Paused WPAR. You can do this by selecting Resource Views > Workload Partitions.
2. Select one or more Paused WPARs, and select End Processes from the drop-down menu.

Removing a WPAR
When you remove a WPAR, you must decide whether to remove the WPAR from a particular managed system or to completely remove the WPAR from the managed environment.

When a WPAR is removed from a system, its configuration remains in the WPAR Manager database and its state is changed to Undeployed. If you try to remove a WPAR that is in the Undeployed state or if you choose to remove the definition of the WPAR it will be removed from the WPAR Manager database.

A WPAR that is currently deployed into a managed system can be removed. Any resources allocated for the WPAR are then released to the managed system that is hosting the WPAR. If the WPAR is active when the delete action is requested, the WPAR will be stopped first.

For system WPARs, an additional option is provided if file systems used by the WPAR must be preserved. This option is useful if the WPAR will be deployed again and the same file systems are used again instead of creating new ones.

Managing WPAR storage devices
WPAR Manager allows you to allocate and export storage devices to workload partitions. A storage device is allocated to a WPAR when you assign the device to the WPAR. The storage device is exported
to the WPAR when the WPAR is started or automatically if you allocate the storage device to a WPAR that is started. The WPAR cannot use the storage devices until they are successfully exported.

Before exporting a storage device to a WPAR, note the following prerequisites and restrictions:

- The storage device must be connected to the managed server through a Storage Area Network.
- You can only allocate a storage device to WPARs that are managed systems.
- You cannot allocate a storage device to a Checkpoint Enabled WPAR.
- You cannot export a storage device to a WPAR if it is in use in the Global environment.
- You cannot export a storage device to multiple WPARs.

Use the Create Workload Partition wizard to export storage devices to a new WPAR. Otherwise, use Modify WPAR to export a storage device to an existing WPAR.

**Exporting a storage device to an existing WPAR**

Use Modify WPAR in WPAR Manager to allocate storage to an existing workload partition (WPAR).

To export a storage device to an existing WPAR, use the Modify WPAR action. To do this, complete the following steps:

1. Log in as the root user to the system where WPAR Manager is installed.
2. Select Managing workload partitions with WPAR manager > Managing WPARs > Viewing or modifying WPAR properties.
3. Select Modify WPAR.
4. On the Devices tab, click Add. The Add Devices for Export page displays. This page shows the available storage devices on the managed system. On this page, you can view the device type, device name, device ID, whether the device is currently exported to a WPAR, and the number of WPARs that the device is allocated to.
5. Select the checkbox next to each device you want to export to the WPAR.
6. Click OK to allocate the selected storage devices to the WPAR and to close the Add Devices for Export page.

If the Modify WPAR action is performed on a WPAR in the Defined state, the devices are allocated to it. Performing a Start action on the WPAR will attempt to export the allocated storage devices from the managed system to the WPAR. If the devices are not being used in the Global environment or by another WPAR, the devices will be available for use within the WPAR. If the devices are otherwise in use, then the WPAR will successfully start but an error message will display.

If the Modify WPAR action is performed on a WPAR that is started the devices will automatically export, if otherwise not in use. For devices exported to a WPAR that is started, you must run the cfgmgr command inside the WPAR before the devices are available for use. The cfgmgr command is automatically run when a WPAR is started.

**Exporting a storage device to a new WPAR**

Use the Create Workload Partition wizard in WPAR Manager to export a storage device to a new workload partitions (WPAR).

To export a storage device to a new WPAR, complete the following steps:

1. Log in as the root user to the system where WPAR Manager is installed.
2. Select Guided Activities > Create Workload Partition.
3. Click Next to start the wizard.
4. Follow the instructions on each page as indicated.
5. On the Devices tab, click Add. The Add Devices for Export page displays. This page shows the available storage devices on the managed system. On this page, you can view the device type, device name, device ID, whether the device is currently exported to a WPAR, and the number of WPARs that the device is allocated to.

6. Select the checkbox next to each device you want to export to the WPAR.

7. Click OK to allocate the selected storage devices to the WPAR and to close the Add Devices for Export page.

8. Complete the remaining pages of the wizard as desired.

9. When you are finished working in the wizard, click Finish to close the wizard.

A new WPAR in the Defined state with the selected devices allocated to the WPAR is created. Performing a Start action on the WPAR will attempt to export the allocated storage devices from the managed system to the WPAR. If the devices are not being used in the Global environment or by another WPAR, the devices will be available for use within the WPAR. If the devices are otherwise in use, then the WPAR will successfully start but an error message will be displayed.

**Viewing storage devices for WPARs**

WPAR Manager provides you with an overall view of the storage devices available on a managed system.

Complete the following steps to display a full inventory of storage devices for a managed system:

1. Log in as the root user to the system where WPAR Manager is installed.
2. Go to the Resource Views section of the navigation area.
3. Select Managed Systems.
4. In the table of managed systems, click the name of the system.
5. Click the Devices tab. The following information about the devices allocated to the managed system are displayed:
   - Type – Specifies the device type such as disk, tape, or CD-ROM.
   - Device – Specifies the name of the device as configured in the Global environment.
   - Device ID – Specifies the unique ID of the disk. This does not apply to devices of the type tape or CD-ROM.
   - Exported – Specifies the name of the WPAR that the device is currently exported to, if any.
   - Allocated – Specifies the number of WPARs that the device is currently allocated to, if any.

**Administering WPAR Manager**

You can administer the WPAR Manager environment using scripts to backup the database, change passwords, stop and start the WPAR Manager, and enable diagnostic tracing.

**Administrative scripts**

You can run the scripts to perform useful administrative tasks such as, dynamically enabling or disabling the trace utility in the running application, maps users or groups to J2EE roles defined by the WPAR Manager, or perform an offline backup of the WPAR Manager database.

**Note:** The actual locations of these scripts might differ if the default installation location was overridden during installation.
Table 7. Administrative script information

<table>
<thead>
<tr>
<th>Script</th>
<th>Description</th>
<th>Default Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>lwilog.sh</td>
<td>Dynamically enables or disables the trace utility in the running application.</td>
<td>/opt/IBM/WPAR/manager/lwi/bin/lwilog.sh</td>
</tr>
<tr>
<td></td>
<td>- To enable the trace utility, run:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>lwilog -addLogger -name package_name -level \</td>
<td></td>
</tr>
<tr>
<td></td>
<td>package_level</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- To disable the trace utility, run:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>lwilog -removeLogger -name package_name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information is logged into the /opt/IBM/WPAR/manager/lwi/logs/trace-log-#.html file and the /opt/IBM/WPAR/manager/lwi/logs/error-log-#.html file, where # is replaced by numerals, with zero (0) representing the most recent trace log file written into.</td>
<td></td>
</tr>
<tr>
<td>lwiMapRole.sh</td>
<td>Maps users or groups to J2EE roles defined by the WPAR Manager. This script can be used to modify the users or groups that are authorized to log in to the WPAR Manager and the roles of each user or group.</td>
<td>/opt/IBM/WPAR/lwi/bin/lwiMapRole.sh</td>
</tr>
<tr>
<td></td>
<td>Run this script with no parameters for usage information.</td>
<td></td>
</tr>
<tr>
<td>wparmgr start</td>
<td>Starts, stops, restarts, or provides status for WPAR Manager.</td>
<td>/opt/IBM/WPAR/manager/bin/wparmgr</td>
</tr>
<tr>
<td>wparmgr stop</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wparmgr restart</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wparmgr status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>db-offline-backup.sh</td>
<td>Performs an offline backup of the WPAR Manager database. An offline backup means that no applications can be using the database that is being backed up.</td>
<td>/opt/IBM/WPAR/manager/db/bin/db-offline-backup.sh</td>
</tr>
<tr>
<td>db-offline-restore.sh</td>
<td>Restores a copy of the WPAR Manager database that was previously backed up.</td>
<td>/opt/IBM/WPAR/manager/db/bin/db-offline-restore.sh</td>
</tr>
</tbody>
</table>

**Changing the passwords for database IDs**

You can change the user ID and password used for connecting to the WPAR Manager database.

To change the password for database IDs, complete the following steps:

1. Stop the WPAR Manager using the **wparmgr stop** command.
3. To change the user ID, find the **dswparmgt.dbuser** property in the /opt/IBM/WPAR/manager/lwi/conf/overrides/wpmcfg.properties file and change the value to the new user ID.
4. To change the password associated with the new user ID, complete the following steps:
   a. Find the **dswparmgt.dbpassword** property in the /opt/IBM/WPAR/manager/lwi/conf/overrides/wpmcfg.properties file.
   b. Replace the value for the password with the new plain-text password to access the database.
   c. Use the **lwiencoder.sh** script to generate an encrypted password in the file by running the following command:

   ```bash
   /opt/IBM/WPAR/manager/lwi/bin/lwiencoder.sh \\
   -f /opt/IBM/WPAR/manager/lwi/conf/overrides/wpmcfg.properties \\
   -keylist dswparmgt.dbpassword
   ```
5. Restart the WPAR Manager using the **wparmgr start** command.

**Backing up the WPAR Manager database**

WPAR Manager uses IBM DB2 Database for Linux, UNIX, and Windows Version 9 (DB2 Version 9) as its database engine.
Backups are configured to be stored in the $INSTHOME/sqllib/backup directory (where the $INSTHOME environment variable is set to the /home/username directory). The filename looks similar to the following:

* WPARMGT.0.DB2.NODE0000.CATN0000.2007022792703.001

Each full backup can occupy between 80 MB to 110 MB of disk space.

**Back up the WPAR Manager DB2 database**

You can back up the WPAR Manager database using the `db-offline-backup.sh` script.

To back up the WPAR Manager database, complete the following steps:

1. Log in as the DB2 instance user using the `su` command. For example, if your user name is `db2wmgt`, you would run the following command:
   
   ```
   su - db2wmgt
   ```

2. Verify that the $INSTHOME directory is exported.

3. Change the directory to the WPAR Manager home by running the following command:
   
   ```
   cd /opt/IBM/WPAR/manager/db/bin
   ```

4. Run the `db-offline-backup.sh` script to perform a full backup.

**Restoring the WPAR Manager DB2 database**

The `db-restore-backup.sh` script uses a combination of the last full backup and the incremental backups to restore the WPAR Manager DB2 database.

**Attention:** Restoring a backed up database replaces the existing database completely.

To restore the WPAR Manager database, complete the following steps:

1. Change the directory to the WPAR Manager home by running the following command:
   
   ```
   cd /opt/IBM/WPAR/manager/db/bin
   ```

2. Run the `db-restore-backup.sh` script.

**Security for WPAR Manager**

WPAR Manager provides several security features, including local operating system user authentication, role-based control of access to various application constructs and actions, and SSL support for Web browser-to-server communications.

**Related tasks:**

"Configuring authorization roles" on page 44

You can configure authorization roles for WPAR Manager using the Console User Authority window or the `lwiMapRole.sh` script.

**User authentication**

User access to application windows and management actions for WPAR Manager is controlled by user ID and role mappings.

WPAR Manager supports the following four application roles:

**administrator**

Determines whether a given user ID can create user ID-to-application role mappings using the `lwiMapRole.sh` script found in the `/opt/IBM/WPAR/manager/lwi/bin` directory, or you can use the user interface and select **Settings > Console User Authority**. This role also has access to other administrative windows that are a part of the Integrated Solutions Console but that are not used by WPAR Manager, such as the Global Refresh window and the Credential Store window.
**WPARAdministrator**

Provides access to all WPAR Manager windows and management actions.

**WPARUser**

Provides access to all basic WPAR actions, such as creating, modifying, starting, stopping, and deploying. This role does not provide access to any of the following higher-level administrative tasks:

- Discovering managed systems
- Modifying or deleting managed systems
- Creating or modifying relocation policies
- Modifying general WPAR settings

**WPARMonitor**

Provides read-only access to all application constructs (such as managed systems, WPARs, and WPAR groups), but does not allow you to make any changes to the environment.

During WPAR Manager installation, the administrator and WPARAdministrator roles are mapped to the root user. There are no other role mappings configured during installation. To map additional roles to existing AIX user IDs at a later time, run the `lwiMapRole.sh` script or use the Console User Authority window.

WPAR Manager uses the local AIX user repository for user authentication to WPAR Manager. Any user with a user ID and password on the local AIX system hosting the WPAR Manager application can authenticate to WPAR Manager, but the actions available in the interface differ depending on the role assigned to the user. If a user ID is not mapped to any of the four application roles, then the user will be able to authenticate to the management console but unable to view any specific information or perform any application actions.

### Configuring authorization roles

You can configure authorization roles for WPAR Manager using the Console User Authority window or the `lwiMapRole.sh` script.

Before you can configure the authorization roles for user IDs, you must log in as the root user and create any necessary IDs on the system where the WPAR Manager is installed.

After you create the user IDs, you can create access-appropriate role mappings for them. If the root user wants to delegate user ID and role mapping authority to another user ID, that user ID must be mapped to the administrator role. You can do this using the Console User Authority page or using the `lwiMapRole.sh` script.

To access the Console User Authority page, go to the Navigation area and select **Settings > Console User Authority**.

The `lwiMapRole.sh` script provides mechanisms for mapping AIX groups to application roles, querying the role-mapping infrastructure, or deleting role access. This script is installed by default in the `/opt/IBM/WPAR/manager/lwi/bin` directory. You must have administrator access to run this script.

You can see the usage statement of the `lwiMapRole.sh` script by invoking the `lwiMapRole.sh` script without any additional parameters, as shown in the following example:

```bash
# lwiMapRole.sh
lwiMapRole -add -role roleName [-user user1,user2,...] [-group group1,group2,...]
lwiMapRole -remove -role roleName [-user user1,user2,...] [-group group1,group2,...]
lwiMapRole -purge -role roleName lwiMapRole -query criteria
```

Where criteria is one of:

- `getRoles`
- `getRolesByUser userName`

44 AIX Version 6.1: IBM PowerVM Workload Partitions Manager for AIX V1.2
You must restart the WPAR Manager server after running the lwimapRole.sh script in order for the user ID role mappings to be available to the management console. Changes made with the Console User Authority window take effect immediately.

Related concepts:
“Security for WPAR Manager” on page 43

WPAR Manager provides several security features, including local operating system user authentication, role-based control of access to various application constructs and actions, and SSL support for Web browser-to-server communications.

Configuring SSL support
The SSL protocol support provides for WPAR Manager server authentication, data privacy, and data integrity using a default self-signed certificate and private key to support HTTPS protocol connections during installation and configuration.

You can configure the SSL subsystem by installing a certificate signed by a trusted certificate authority (CA) and generating a different private key. You can do this using the standard Java™ keytool command-line interface, or the ikeyman graphical user interface. These tools are located in the /usr/java5/jre/bin directory on most AIX systems.

The certificate configured by default during installation enables communication between the client and the server to be encrypted over SSL, but it does not make it possible to authenticate the server name. To enable server authentication, you must specify the host name, as a fully qualified domain, of the server in the Common Name field of the certificate, or in the CA-signed certificate installed at a later time. The first time the client browser attempts an HTTPS connection, it returns messages indicating that the signer is not recognized, because it is a self-signed certificate, and that the server cannot be authenticated because the Common Name in the certificate does not match the host name entered in the URL.

You can choose to accept the certificate, but this certificate does not provide an adequate level of security in a production environment. You should use ikeyman to replace the default certificate with your own self-signed or CA-signed certificate. You should also change the default keystore password to a value other than the default (ibmpassword). You can also use ikeyman to periodically renew expired certificates.

Related information:
Secure Sockets Layer Introduction and iKeyman User’s Guide

Editing the webcontainer.properties file
You can deploy a new certificate to replace the default certificate in the default keystore using ikeyman without affecting any other SSL configuration settings. However, if you want to change the keystore password or deploy a new keystore file, you must change the settings in the webcontainer.properties file.

The webcontainer.properties file is located in the /opt/IBM/WPAR/manager/lwi/conf directory. The following lines show the default properties included in the webcontainer.properties file:
com.ibm.ssl.keyStorePassword.14443=xor 9MW08GTL+uut1b0=
com.ibm.ssl.clientAuthentication.14443=false
com.ibm.ssl.trustStorePassword.14443=xor 9MW08GTL+uut1b0=
com.ibm.ssl.trustStore.14443=../security/keystore/ibmjsse2.jts
com.ibm.ssl.keyStore.14443=../security/keystore/ibmjsse2.jks sslEnabled=true

The keyStorePassword property value and the trustStorePassword property value are encrypted and are not readable in this file.
To change the keystore password or deploy a new keystore file, complete the following steps:

1. Make a backup of the existing webcontainer.properties file, the trust file, and the keystore files.
2. Create a file in the /opt/IBM/WPAR/manager/lwi/conf directory called sslconfig by copying the contents of the webcontainer.properties file into the sslconfig file.
3. Specify the new settings in the sslconfig file.
4. Remove the webcontainer.properties file.
5. Remove the sslEnabled=true line from the sslconfig file.
6. Restart WPAR Manager. When you restart, a new webcontainer.properties file is created using the settings in the sslconfig file and the sslconfig file is removed.

An example conf/sslconfig file contains the following lines:

```properties
com.ibm.ssl.keyStorePassword.14443=mynewpassword
com.ibm.ssl.keyStore.14443=/../../security/keystore/mynewkeystore.jks
com.ibm.ssl.clientAuthentication.14443=false
com.ibm.ssl.trustStorePassword.14443=mynewpassword
com.ibm.ssl.trustStore.14433=/../../security/keystore/mynewkeystore.jts
```

In this example, the keyStore property and the trustStore property point to the same file. Client authentication is not enabled by default, so the trustStore property, which could contain the signer certificates that the Web container trusts, is not actually used. However, the WPAR Manager Web container requires that the trustStore property be set to a legitimate value. The default keyStore password is ibmpassword.

**Managing certificates with ikeyman**

You can use ikeyman to create a request for a certificate authority (CA) signed certificate to use in the WPAR Manager. You can also use ikeyman to import a CA signed certificate into the keystore.

The preferred setup for a production environment is for the server to be configured with a certificate in which the Common Name field contains the host name of the server (to enable server authentication), and the certificate is signed by a trusted third party CA. To generate a CA-signed certificate for production use, you must create a certificate request, submit the certificate request to a CA for signing, and receive the signed certificate into the keystore.

To manage certificate with ikeyman, complete the following steps:

1. Start ikeyman. The ikeyman command is found in the /usr/java5/jre/bin directory.
2. Open the keystore with the following steps:
   a. On the menu bar, select Key Database File > Open.
   b. Use the Browse button to locate the keystore under the /opt/IBM/WPAR/manager/lwi/security directory.
   c. Click OK. You will be prompted for the keystore password.
3. Create a certificate request with the following steps:
   b. Enter a descriptive string for the Key Label.
   c. Enter the fully qualified host name for the Common Name.
   d. Enter appropriate values in the other fields.
   e. Enter the name of a file in which to store the certificate request. You will submit this file to a CA.
4. Send the certificate request file to a CA for signing.
5. Receive the signed certificate and complete the following steps:
   a. In the Key database content area, click Personal Certificates.
   b. Select the Receive button. You are prompted for the location of the signed certificate.
c. Enter the location of the signed certificate.
d. Click OK. The signed certificate is added to the keystore.

6. Add the CA’s public key to the client browser’s truststore. Most browsers already have the CA public keys of well-known CAs in their truststore, so this step is usually not necessary. If you find that it is necessary, your CA should provide you with instructions.

**WPAR Manager agent secure certificates**

The WPAR Manager agent maintains secure certificates and additional security files in the 
/var/opt/IBM/WPAR/cas/agent/runtime/agent/cert_to/var/opt/tivoli/ep/runtime/agent/cert directory.

The following files are included in the directory:

`amRevocationList.crl`
This file contains the list of revoked certificates that is distributed to all agents by the agent manager.

`agentKeys.jks`
This file is the public and private keystore issued to the agent by the agent manager.

`agentTrust.jks`
This file is the truststore downloaded from the agent manager.

`pwd`
This file contains a randomly generated password used to lock the agent certificates.

**Troubleshooting WPAR Manager**

You can use log files and problem determination procedures to troubleshoot WPAR Manager.

**Log file locations**

You can use the various WPAR Manager log files to troubleshoot problems.

**WPAR Manager logs**

The following table displays the location and descriptions for WPAR Manager logs.

<table>
<thead>
<tr>
<th>Log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/var/opt/IBM/WPAR/manager/lwi/logs/error-log-*</code></td>
<td>WPAR Manager log files</td>
</tr>
<tr>
<td><code>/var/opt/IBM/WPAR/manager/lwi/logs/trace-log-*</code></td>
<td>WPAR Manager trace log files</td>
</tr>
<tr>
<td><code>var/opt/IBM/WPAR/manager/logs/policy.log</code></td>
<td>WPAR Manager policy log</td>
</tr>
<tr>
<td><code>/var/opt/IBM/WPAR/manager/logs/install/*.log</code></td>
<td>WPAR Manager</td>
</tr>
</tbody>
</table>

**Agent manager logs**

The following table displays the location and descriptions for agent manager logs.

<table>
<thead>
<tr>
<th>Log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/var/opt/IBM/WPAR/cas/agentmgr/logs/error-log-*</code></td>
<td>Agent manager log files</td>
</tr>
<tr>
<td><code>/var/opt/IBM/WPAR/cas/agentmgr/logs/trace-log-*</code></td>
<td>Agent manager trace log files</td>
</tr>
</tbody>
</table>

**WPAR Manager agent logs**

The following table displays the location and descriptions for WPAR Manager agent logs.
Live relocation log files

During live relocation, the WPAR Manager agent creates log files on the departure and arrival systems that can be used to troubleshoot live relocation failures. The log file location has changed in WPAR Manager agent 1.2.

In the log file locations listed in the table, substitute wparname with the WPAR’s name, state_path with the configured location of the WPAR’s state file root directory, and departure_hostname with the host name of the departure system.

Table 11. Live Relocation Logs

<table>
<thead>
<tr>
<th>Log File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/var/opt/IBM/WPAR/agent/logs/mcr/wparname.log</td>
<td>WPAR Manager agent 1.2 log file</td>
</tr>
<tr>
<td>/wpars/wparname/state_path/wparname/departure_hostname/mcr.log</td>
<td>WPAR Manager agent 1.1 system WPAR log file</td>
</tr>
<tr>
<td>/state_path/wparname/departure_hostname/mcr.log</td>
<td>WPAR Manager agent 1.1 application WPAR log file</td>
</tr>
</tbody>
</table>

Verifying the agent manager is online

The agent manager provides configuration information to clients over an unsecured HTTP port. It can be useful in problem determination to verify the agent manager is online and operational.

To view the agent manager configuration, go to the following Web page:

http://agent_manager_hostname.yourdomain.com:agent_manager_public_port/context_root/Info

The context_root variable should be the context root for the agent manager. The default context root is the /AgentMgr directory. For example, if the agent manager is installed at am.austin.ibm.com with the default configuration, you would access the agent manager configuration at the following Web page:

http://am.austin.ibm.com:9513/AgentMgr/Info

WPAR Manager problem determination

You can find known problems and solutions for WPAR Manager. Look for the symptom that matches the problems you are experiencing and perform the recommended corrective actions.

Live and static relocation failures

The various troubleshooting methods for live and static relocation failures can depend on the WPAR Manager agent version.

Live relocation failures with WPAR Manager agent 1.2 or later

When you are using WPAR Manager agent 1.2 or later on the departure and arrival systems, live relocation uses an advanced method where the state of the WPAR is transferred directly between the two systems without the need of an intermediate state file stored to disk.

When you are performing live relocation with WPAR Manager agent 1.2 or later, the following relocation problems can occur:
• The arrival system does not have connectivity to the departure system. The arrival system must be able to connect to a port on the departure system to initiate the state transfer.

• Departure and arrival systems must be on the same network subnet as the WPAR.

• If the checksum of a binary or shared library used by the WPAR on the departure system does not match the checksum on the arrival system, the relocation could fail. To resolve these issues, look at the `/opt/IBM/WPAR/agent/logs/mcr/wparname.log` log file specified for relocation for detailed information on which files failed the checksum test. The `lslpp -w /path/to/filename` command can be used to search for the fileset that ships a specific file. Ensure that the fileset is installed on both the departure system and the arrival system, and that the versions match.

• Other failures can occur during live relocation, including device incompatibilities and clocks between the departure and arrival systems being out of sync. View the MCR `/opt/IBM/WPAR/agent/logs/mcr/wparname.log` log file on both the departure managed system and arrival managed system to determine the reason for relocation failure.

**Live relocation failures with WPAR Manager agent 1.1**

WPAR Manager agent 1.1 saves the state of the WPAR to a shared file system location on the departure system, and uses the shared file system on the arrival system to restore the WPAR.

When you are performing live relocation with WPAR Manager agent 1.1, the following relocation problems can occur:

• Ensure that the shared file system specified for relocation is mounted on the departure and arrival systems at the same location, with root privileges granted to the departure system host name, the arrival system host name, and the host name of the WPAR being relocated.

• Incompatible software versions between the departure and arrival systems. If the checksum of a binary or shared library used by the WPAR on the departure system does not match the checksum on the arrival system, the relocation could fail. To resolve these issues, look at the log file for specifics on which files failed the checksum test. The log files can be found in the following locations:
  - Use the `/wpars/wparname/state_path/wparname/source_hostname/mcr.log` for system WPARs.
  - Use the `/state_path/wparname/source_hostname/mcr.log` log file for application WPARs.

The `lslpp -w /path/to/filename` command can be used to look up the fileset that ships a specific file. Ensure that the fileset is installed on both the departure system and the arrival system, and that the versions match.

• Other failures can occur during live relocation, including device incompatibilities and clocks between the departure system and the arrival system being out of sync. View the MCR log file on the managed system to determine the reason for relocation failure.

**Static relocation failures**

Static relocation consists of a backup and restore operation for system WPARs, or a stop and deploy operation for application WPARs.

When performing static relocation, the following relocation problems can occur:

• Static relocation for system WPARs requires a shared file system location to store the backup file for the WPAR. If the shared file system is not mounted at the same location on the departure system and the arrival system with adequate privileges, then static relocation will fail to restore the WPAR on the arrival system.

• If the WPAR has a network interface defined, ensure that the departure and arrival systems are on the same subnet as the WPAR's network. Otherwise, the WPAR may fail to deploy on the arrival system.

**Managed system missing**

The managed system does not appear in the list of servers.
Probable cause

The WPAR Manager agent software is not running or is not properly configured on the managed system.

Action

1. Log in to the managed system as the root user.
2. Verify that the agent manager is online. If the agent is not running, restart the agent.
3. Examine the log files in the /opt/IBM/WPAR/manager/logs directory for any error messages from registration.
4. In the WPAR Manager, click Discover on the Managed Systems page.

Related tasks:

"Installing the WPAR Manager agent on the managed system“ on page 17

The WPAR Manager agent runs on the managed system and provides a secure interface for running WPAR commands for managing WPARs, collecting performance metrics, and collecting information for compatibility testing.

Deploy operation of a WPAR fails because of permissions

The deploy operation on a relocatable WPAR fails with this message: AKMWA0002E. The command failed to run on the target system.

The Error tab in the Operations Details page shows the following output:

mkwpar: Creating filesystems...

mount: access denied for <NFS server="">:<filesystem>
mount: giving up on:
<NFS server="">:<filesystem>
Permission denied
Failed to mount the '/wpars/<wpar name="">' filesystem.

Probable cause

The NFS file system was not exported with root permissions to the managed system and the WPAR host name.

Action

1. Export the NFS file system with root permissions to the managed system and the WPAR host name.
2. Retry the deploy task from the WPAR Manager.

Managed system marked offline

The managed system is marked offline when the agent is running.

Probable cause

The WPAR Manager is not able to communicate with the WPAR Manager agent installed on the managed server.

Action

Note: Perform the following steps in order. Only perform the next step in this procedure if this previous step did not produce the desired result.

1. Ensure that the WPAR Manager can communicate with the agent HTTP port (the default is 9510) and is not blocked by a firewall.
2. Go to the Managed Systems view, select the managed system, and click Update.
3. Set the log.level value to FINEST in the /opt/IBM/WPAR/agent/conf/wparagent_logging.properties file and restart the agent. Tracing and debugging information is added to the agent log files in the /opt/IBM/WPAR/agent/logs directory.

4. Verify that the DB2 instance home directory file system is not full with the following command:
   df -m /home/db2wmgt

5. Uninstall and reinstall the agent.

**Task fails in the Task Details page**
A task fails in the Task Details page and no operations are created for this task.

**Probable Cause**
The WPAR Manager failed to establish a secure connection to the managed system.

**Action**
Verify that a firewall is not blocking communication from the WPAR Manager to the managed system.

**Managed server discovery fails**
The WPAR Manager fails to discover an agent.

**Probable cause**
The WPAR Manager agent was configured with an incorrect WPAR Manager host name or invalid registration password.

**Action**
1. Verify that the agent is started on the managed system by running the /opt/IBM/WPAR/agent/bin/wparagent status command.
2. Examine the /opt/IBM/WPAR/agent/cas/logs/trace-log-0.xml file for any error messages related to registration. For example, if the registration password is invalid, the log will contain the following error message:
   SEVERE: BTC5074E The common agent registration failed. The failure was caused by exception: Agent Manager returned: CTGEM0020E An agent registration request from <ip_address> was rejected because the password is not correct. The password that was specified is *****.
3. Verify that the WPAR Manager agent can resolve the IP address of the host name passed to the configure-cas script.
4. Examine the log files in the /opt/IBM/WPAR/manager/logs directory for any error messages from registration.

**Related tasks:**
"Configuring the WPAR Manager agent to use a different agent manager" on page 28
After you configure the WPAR Manager agent to use a specific agent manager, further attempts at configuring the WPAR Manager agent to use a different specific agent manager will be unsuccessful. You must specify the -force flag to override the original agent manager configuration.

**Deploy operation fails because of incorrect IP address**
The deploy operation of a WPAR fails with this message: AKMWA0002E. The command failed to run on the target system.

The Error tab in the operations details page displays the following error:
Failed to determine the appropriate interface for address <ip address="">.
Probable cause

The IP address assigned to the WPAR is not in the same subnet as the managed server IP address.

Action

1. Go to the Workload Partitions view.
2. Select the WPAR, view its properties, and select the Network tab.
3. Select the network interface with the invalid IP address, and select Modify.
4. Enter an IP address in the same subnet as the managed server where the WPAR will be deployed.
5. Click Finish.
6. Retry the deploy task from the WPAR Manager.

Checkpoint and restart

The checkpoint and restart function is used to implement live application mobility in the WPAR Manager, but you can also run checkpoint and restart commands from the command line to pause and resume WPAR operations without relocating the WPAR.

Checkpoint and restart enables you to optimize and protect 32-bit and 64-bit applications running in system WPARs or application WPARs across multiple physical systems. You can checkpoint and restart WPARs to protect them against failures or to balance loads across systems at a production site.

Checkpoint and restart can be used with the following types of applications:
- Multi-processed and multi-threaded 32-bit applications
- Multi-processed and multi-threaded 64-bit applications
- Statically linked applications
- Dynamically linked applications
- Off-the-shelf applications and custom applications

Checkpoint and restart operates transparently at the application level, capturing the full context of the application memory, including the following:
- Resources
- Process hierarchies
- States
- Signals
- Inter-process communication pipes
- Semaphores
- Shared memory
- Open files
- TCP/IP sockets

The checkpoint part of the operation interacts at the binary level only, so no changes are made to the source code, and it is not necessary to recompile the application or link the application. The original running WPAR is then restarted from the saved checkpoint. You can restart the WPAR either on the same physical system or on another compatible system.

Problem determination for checkpoint and restart

You can find known problems and solutions for checkpoint and restart. Look for the symptom that matches the problems you are experiencing and perform the recommended corrective actions.

Restart of a system WPAR fails

Restarting a system WPAR fails with this error: Invalid wpar name. No mcr.log file is created.
**Probable cause**

Restart must always be processed from the global environment, not from within the WPAR.

**Action**

1. Verify that you are not running the restart while being logged in to the WPAR.
2. If Step 1 did not solve the problem, verify that the WPAR you want to restart is configured on your server. Verify that the WPAR exists and is in the Defined (D) state.
3. If the WPAR is not in the Defined state, store the specifications, such as name, network, and mount settings used to create the checkpointed WPAR, and recreate a system WPAR with those specifications.

**Restart of a system WPAR ends**
The restart of a system WPAR begins, but ends with the following error: Restart command failed.

**Probable cause**
The checkpoint directory that you supplied does not exist.

**Action**

1. Look in the traces displayed on the standard output for the following message: - mcr: could not restart WPAR mywpar from /mydirectory: invalid statefile -
2. Supply a checkpoint directory that does exist.

**Checkpointing a system WPAR fails**
Checkpointing a system WPAR fails with the following error: Invalid wpar name. No mcr.log file is created.

**Probable cause**
Checkpoints must always be processed from the global environment, not from within the WPAR.

**Action**

1. Verify that you are running the checkpoint while you are logged in to the WPAR. Checkpoints must always be processed from the global environment, not from within the WPAR.
2. If Step one did not solve the problem, then check if the WPAR you are checkpointing exists on your server. It must exist and be active.

**Checkpointing a system WPAR fails because of the checkpoint directory**
Checkpointing a system WPAR fails with the following error: Invalid statefile.

Check the mcr.log file for the following message: - Pathname of statefile must be visible inside and outside the WPAR -

**Probable cause**
The checkpoint directory you specified is not accessible from the WPAR you want to checkpoint.

**Action**

Make sure that the checkpoint directory can be reached from the global environment and from within the WPAR, otherwise the checkpoint will fail.
**Glossary for WPAR Manager**

Certain terms are specific to the WPAR Manager environment.

**A**

**active state**
A WPAR that is deployed on a managed system and running normally.

**agent**
Software running on a managed system that communicates with the WPAR Manager agent manager component of WPAR Manager and performs actions on the managed system.

**agent manager**
The component of the WPAR Manager that communicates with the agent software on managed systems, and communicates their status to WPAR Manager server.

**agent version**
The software version of the WPAR Manager agent installed on a managed system. The agent version corresponds to the version and release level of the WPAR Manager with which it was shipped (1.1.0.0, 1.2.0.0, etc.). If the agent software installed on a managed system is at an earlier level than the current WPAR Manager server, then the new actions and properties may not be available for WPARs on that managed system.

**Application WPAR**
One of the two basic types of WPAR on AIX. Application WPARs do not provide the highly virtualized system environment offered by system WPARs. Rather, they provide an environment for segregation of applications and their resources. These environments can be dynamically relocated using checkpoint and restart for appropriately configured WPARs, or statically relocated using via stop and redeploy between compatible managed systems. Application WPARs have less overhead on system resources and are lighter weight compared to system WPARs. Application WPARs do not require their own instance of system services.

**arrival system**
The managed system specified as the target or destination for a WPAR to be relocated.

**B**

**back up WPAR**
To copy critical WPAR data to a backup file

**broken state**
A WPAR on which an administrative operation failed, leaving this WPAR in an unusable state.

**C**

**checkpoint**
To save the state, including process state, of an active WPAR and later restart that WPAR on the same or different system. When creating a WPAR, it is necessary to specify checkpoint support if checkpointing the WPAR will be necessary.

**compatibility**
The similarity of two managed systems that allows a WPAR to be relocated from one to the other without problems. The two systems must have identical values for a number of required properties, and also for any user-specified optional properties.

**compatibility policy**
The set of test cases used to determine compatibility between managed systems. This set includes all critical test cases and any optional test cases selected by the user.
Critical metric
A critical metric is one which, if its value falls outside the specified maximum or minimum values, indicates that a managed system should be immediately relocated to other systems if policy-based relocation is used.

D
Defined state
A WPAR that exists on a managed system, but is not currently active. Starting the WPAR moves it to the active state. This only applies to system WPARs.

Departure system
The managed system on which a WPAR is deployed prior to relocation.

Deploy
To create a WPAR on a managed system from the definition or specification stored in the WPAR Manager database. Application WPARs are started when they are deployed, but a system WPAR can be deployed without being started.

Discovery
Refers to the WPAR Manager discovering and registering new managed systems in the environment. Discovery can be initiated by selecting the ‘Discover’ button on the Managed Systems view.

E
Evacuate
Relocate all WPARs deployed on a managed system to other systems (automatic evacuation is not currently supported).

L
Limit
With regard to performance metrics, limits are used to enable disparate measurements of resource consumption to be normalized.

Live relocation (live application mobility)
The method of relocation that attempts to preserve the state of running processes, so that an application or system WPAR appears to keep running during relocation, with minimal interruption of service.

Loaded state
A WPAR that is deployed on a server and is loaded in the kernel, but is not running any active processes. No operations can be performed on a WPAR in this state. Only WPARs that have been created supporting the checkpoint property can be relocated using this relocation method.

M
Managed system
A server or logical partition running AIX and the WPAR Manager agent software that has registered with the WPAR Manager server. Managed systems appear in the Managed Systems view. WPARs can be created on managed systems, and relocated from one managed system to another, using the WPAR Manager.

Managed system profile
A set of system properties collected from a managed system by the agent.

Minimum required agent version (minimum agent version, minimum version)
A WPAR related property which specifies the oldest level of agent software that can support the defined properties of the specific WPAR. This value (determined by programmatically examining the defined properties for a given WPAR) determines which managed systems are possible.
targets for deployment. For a given WPAR, a managed system must be running at least the minimum required agent version to deploy the WPAR on that system.

**mobility**

The ability to relocate WPARs from one managed system to another. Non-checkpointable WPARs can be relocated in WPAR Manager 1.2 if they are deployed on a managed system running the WPAR Manager agent at the 1.2 level.

**multiplier**

The multiplier to be applied to the limit value as the hardware profile rank for the WPAR increases. This allows for transaction rate use metrics to be proportional to available hardware resources, if required.

**O**

**operation**

An action taken by the WPAR Manager as part of the completion of a task. A task might result in several operations.

**P**

**pause (action)**

An action causing the WPAR Manager to take a checkpoint, then lock the processes within a WPAR.

**paused state**

A WPAR in a checkpoint-suspend state; it is not currently running but can be resumed (started) or unpaused (stopped).

**performance metric**

A measure of WPAR or managed system performance. Processor use and memory use are two metrics used by WPAR Manager.

**R**

**rate metric**

A performance metric that is expressed as a count or rate (contrast with a use metric, such as a percentage processor or memory use). Examples of rate metrics might include the number of processes, the number of threads, or page faults.

**recovery**

A manager invoked when an error is detected while performing operations on managed systems or WPARs. The default goal of recovery is to synchronize the information in the WPAR Manager database with the real state of the managed systems and WPARs. When a relocation operation fails, WPAR Manager analyzes the departure and arrival systems to do whatever is possible to bring the WPARs back to a useful state after a failure. The most likely action is to restart the WPAR on the departure system and remove all traces of the WPAR on the arrival system, in an attempt to restore the environment to its state before the relocation was initiated.

**relocate**

To move a WPAR from one managed system to another (sometimes referred to as migration). Relocation requires that all processes running in the WPAR be checkpointed, paused, copied from the departure system to the arrival system, then restarted.

**relocation domain**

When server profiles are assigned to a WPAR group a dynamic relocation domain is created. All servers with matching profiles will be automatically part of the WPAR group dynamic relocation domain. If a more static relocation domain is desired, for each server that should be part of the relocation domain the relocation domain server property tag should be set, then add all the
profiles with a given relocation domain tag to the WPAR group. Note that the best available server for relocation will always be selected from the relocation domain of the WPAR group which a WPAR belongs to.

**relocation policy**
The set of metrics and rules that determine when a WPAR should be relocated. With WPAR Manager 1.2 there is support for both static and an improved live relocation of WPARs. During static relocation WPARs are stopped and then restarted on the arrival system while preserving the file system state. Live mobility preserves the state of the application stack on the arrival system.

**remove WPAR**
To delete a WPAR from a managed system. Optionally, the definition of the WPAR in the WPAR Manager database can also be deleted.

**resource controls**
Settings to either limit the amount of managed system resources that can be used by a WPAR, or to guarantee a minimum share of system resources to the WPAR. WPAR resource controls are based on AIX workload manager concepts.

**restart**
To resume operation of a WPAR after it has been checkpointed.

**restore WPAR**
To recreate a WPAR from critical information saved in a backup file on a managed system.

**resume**
To unlock the processes of a paused WPAR, and resume operation from the point at which the WPAR was paused.

**Role Based Access Control (RBAC)**
A framework for restricting system access to authorized users. WPAR Manager queries a deployment system to retrieve the overall set of privileges for a system, as well as the default privileges. When you deploy a WPAR, you can choose to assign either the default set of privileges or a customized set of privileges to the WPAR.

**S**

**static Relocation**
Static application mobility is defined as a shutdown of the WPAR on the departure node and the clean start of the WPAR on the arrival node while preserving the file system state. For system WPARs, static relocation uses the backup and restore capabilities.

**synchronize WPAR**
To bring software installed on a system WPAR to the same level as the software installed in the global AIX system on which it is deployed.

**system WPAR**
One of the two basic types of WPARs on AIX. System WPARs are autonomous virtual system environments with their own private root file systems, users and groups, login, network space, and administrative domain. The majority of traditional system services is virtualized at the WPAR level and can be independently used and managed within each WPAR. While the system WPAR environment is largely partitioned and isolated, read-only file systems can be shared between WPARs to facilitate the sharing of application data and text.

**T**

**task (event)**
A significant WPAR management task initiated either by the WPAR Manager user or by the WPAR Manager in response to policy-driven trigger events. A task can initiate additional tasks, or lower-level workload management operations, as part of its processing.
transitional state
A WPAR on which an administrative operation is in progress. The WPAR is in the process of
being created, started, stopped, or configured.

U
undeployed state
A WPAR that is defined in the WPAR Manager database, but is not currently deployed on a
managed system. Deploying a WPAR creates, and optionally starts, the WPAR on a managed
system.

use metric
A performance metric that is expressed as a percentage or proportion of total use. Processor and
memory use are use metrics. Contrast with rate metrics.

W
WPAP Manager agent
See the definition for agent.

Workload partition (WPAP)
WPAPs are virtualized operating system environments within a single instance of the operating
system. WPAPs complement other virtualization tools such as logical partitions (LPAR). They
differ from LPAR in that WPAPs have less overhead and are based in the operating system rather
than the system firmware. There are two types of WPAPs: system WPAPs and application
WPAPs.

WPAP group
A group of WPAPs, defined by the administrator, that are governed by common relocation policy
settings. By default, WPAPs that you create are assigned to a default WPAP group unless you
reassign them to a different group.
Notices

This information was developed for products and services offered in the U.S.A.

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 give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

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
Dept. LRAS/Bldg. 903
11501 Burnet Road
Austin, TX 78758-3400
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:
Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as the customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.


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 Copyright and trademark information at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

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

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

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

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

A
accessibility 2
agent
  configuring 20
  installing 17
agent manager 48
  configuring 29
application mobility
  configuring 23
  planning 16

B
backing up
  database 43

C
checkpoint and restart 52
  states 9
compatibility
  testing 7
configuring
  agent 20
  agent manager 29
  application mobility 23
  logging 22
  SSL 45
  WPAR agent 22, 29
  WPAR Manager server 20

D
database
  backing up 43
  restoring 43

I
ikeyman 46
  installing 17
  agent 17

L
logical partitions 6

M
managed system
  defining 31
  problem determination 50, 51, 53
  properties 32
managing
  certificates 46
  manual relocation 12
  mobility
    compatibility 7, 8

P
planning
  application mobility 16
  WPAR Manager agent 3
policy
  tuning 14
policy-based relocation 13
  group averaging 15
  group policy settings 14
  metric policy settings 13
  tuning 14
problem determination
  checkpointing 53
  deploy 51
  deploy operation 50
  managed system 50, 51, 53
  discovery 51
  missing managed system 50
  offline 50
  restart 53
  secure connection 51
properties
  managed system 32

R
relocation
  manual 12
  removing 30
    WPAR Manager agent 30
restoring
  database 43

S
SSL 45
starting 38
  WPAR agent 22
stopping 38
  WPAR agent 22

W
webcontainer.properties file 45
WPAR
  states 9
  WPAR agent 3
    configuring 22, 29
    secure certificates 47
    starting 22
    stopping 22
  WPAR groups 33
  WPAR Manager 17
  WPAR Manager agent
    planning 3
    removing 30

© Copyright IBM Corp. 2007, 2014