Before using this information and the product it supports, read the information in “Notices” on page 51.

Fifth Edition (September 2010)

This edition applies to AIX Version 7.1 and to all subsequent releases and modifications until otherwise indicated in new editions.

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

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

**IBM PowerVM Workload Partitions Manager for AIX V2.2.1** .......................... 1
WPAR Manager overview ........................... 1
WPAR Manager 2.2.1 Release Notes ............. 3
What's new in WPAR Manager 2.2.1 ............. 4
Supported operating environments for WPAR Manager ........................................... 7
Memory and disk space requirements ........... 8
WPAR Manager agent ............................... 8
WPAR management in a logically partitioned environment ........................................ 9
Accessibility features for WPAR Manager .... 10
Installing WPAR Manager ......................... 10
Installing WPAR Manager as an IBM Systems Director advanced manager .............. 10
Upgrading the WPAR Manager .................... 11
Installing the WPAR Manager subagent on the managed system ............................. 11
Removing the WPAR Manager Advanced Manager .................................................. 13
Removing the WPAR Manager agent .......... 13
WPAR Manager license enablement ............... 13
Configuring WPAR Manager ..................... 13
Configuring the WPAR Manager agent ........ 14
Configuring the environment for application mobility .......................................... 15
Managing workload partitions with WPAR Manager .............................................. 19
Managed systems .................................... 19
Managing WPARs ................................. 22
Managing WPAR storage devices ............... 30
Role Based Access Control support .......... 32
Application mobility .............................. 33
Planning for application mobility ............... 33
System compatibility .............................. 34
WPAR states ....................................... 36
WPAR relocation domains ....................... 37
Manual relocation ............................... 38
Policy-based relocation ......................... 38
Security for WPAR Manager ..................... 39
Troubleshooting WPAR Manager ................. 39
Log file locations .............................. 39
Verifying the agent manager is online ....... 40
WPAR Manager problem determination ......... 41
Command-line Interface ......................... 44
Glossary for WPAR Manager ..................... 45

**Notices** ........................................... 51
Trademarks ......................................... 53

**Index** ............................................ 55
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 V2.2.1

IBM PowerVM Workload Partitions Manager for AIX (WPAR Manager) is an advanced manager for IBM Systems Director. WPAR Manager that provides a centralized point of control for managing workload partitions (WPARs) across a collection of managed systems running AIX.

To view or download the PDF version of this topic, click IBM PowerVM Workload Partitions Manager for AIX.

Downloading Adobe Reader: You need Adobe Reader installed on your system to view or print this PDF. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html).

Related information
- AIX 6.1: Workload partitions for AIX
- AIX 7.1: Workload partitions for AIX

WPAR Manager overview

The IBM PowerVM Workload Partitions Manager for AIX (WPAR Manager) is an advanced manager for IBM Systems Director. WPAR Manager and provides a centralized, single point of administrative control for managing system and application AIX workload partitions.

The WPAR Manager web application provides complete life cycle management support for WPARs (Discover, Create, Modify, Delete, and Remove). A complete task history is available on every action performed on a WPAR, including standard output and error. Graphic reports display resource usage and performance that are provided for both managed systems and WPARs.

WPAR Manager can manage heterogeneous environments of managed systems at different AIX technology levels. However, to use full management capabilities, the WPAR Manager agent is updated to the latest version.

The following features are supported on all AIX technology levels:
- Cross-system management of WPARs, including life cycle 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
- WPAR Manager command line

The following is a summary of the features provided by WPAR Manager that requires AIX Version 6.1 with the 6100-02 Technology Level, or later:

Improved live relocation
- Reduce application downtime during relocation.

Back up and restore
- Create backup images for an existing WPAR and restore a WPAR from a previously created backup image.
Static relocation
Shut down the WPAR on the departure node and start 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 IPv6 addresses.

Support for WPAR-specific routes
Select WPAR-specific routing or share that routing of the global system. You can also configure, view, and modify a routing table specific to the WPAR. WPAR-specific routes can only be configured for interfaces using IPv4.

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

The following is a summary of the features provided by WPAR Manager that requires AIX Version 6.1 with the 6100-03 Technology Level, or later:

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

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

The following is a summary of the features provided by WPAR Manager that requires AIX Version 6.1 with the 6100-04 Technology Level, or later:

Support for WPAR-owned rootvg
Support to designate disks as the holders of the WPAR rootvg file systems, live relocation, and static relocation of WPARs that own their rootvg.

Kerberos support
Support to use Kerberos encryption for the communication between the departure and arrival servers during live relocation.

Back up
Support for WPAR backups where WPAR files are accessed with read-write namefs mounts.

The following is a summary of the features provided by WPAR Manager that requires AIX Version 6.1 with the 6100-06 Technology Level, or later:

Support for virtual I/O SCSI Disk Support for WPARs
Support to assign virtual I/O SCSI disk to WPARs.

The following is a summary of the features provided by WPAR Manager that requires AIX Version 7.1, or later:

Support for AIX 5.2 versioned WPARs
Support to create versioned WPARs from an AIX 5.2 mksysb image.

For more information about versioned WPARs, see "Versioned Workload Partitions" on page 24.

Support for Controlled Kernel Extension Enablement for WPARs
Support to assign Kernel Extension to WPARs so that they can be loaded and unloaded within a WPAR.
**WPAL Manager 2.2.1 Release Notes**

The WPAR Manager 2.2.1 Release Notes contain limitation and restriction information, and information about WPAR Manager documentation.

**Known issues**

After restarting the IBM Systems Director 6.2, the host relationship between managed systems and WPARs get lost. To avoid this, an IBM Systems Director patch must be installed. You can download the patch from IBM PowerVM Workload Partitions Manager for AIX.

The syncwpar command might fail when you create a WPAR on a system that is running AIX Version 6.1 with the 6100-02 Technology Level or AIX Version 6.1 with the 6100-03 Technology Level and has the Director agent installed. To avoid this problem, run the following command before you create the WPAR:

```
# swvpdmgr -p DirectorCommonAgentLive
```

Relocation of a system WPAR might fail if the ctrmc daemon is running inside the WPAR. To avoid running the ctrmc daemon by default inside the WPAR, apply the IZ59217 APAR on AIX Version 6.1 with the 6100-04 Technology Level and previous releases.

**Limitations and restrictions**

This section lists the restrictions and limitations that apply to the WPAR Manager.

- The COMPAT_AUTOMOUNT environment variable that is used to specify a different automount command behavior is not compatible with application WPARs that have an IP address that is different from the Global environment IP address. If the COMPAT_AUTOMOUNT environment variable is set to any value before you run the automount command, the file system access from the application WPAR might hang indefinitely.

- The application WPARs that are created from the command line cannot be relocated with the WPAR Manager. This limitation does not exist for system WPARs.

- The processes that are launched from inside a system WPAR with the clogin command are not relocatable.

- A process that is running in an unlinked working directory cannot be relocated. This limitation was lifted on MCR 4.2.2.0; therefore, it only applies to AIX Version 6.1 with the 6100-03 Technology Level or older.

- A checkpoint fails if processes or threads are stopped in the WPAR.

- The relocation of applications with memory regions that are created by using the mmap (MAP_SHARED) subroutine for an unlinked file is not supported.

- The relocation of applications with deleted POSIX shm maps is not supported.

- During static relocation or backing up a system, WPAR might fail in some instances with the following error message: A file cannot be larger than the value set by ulimit. To correct this problem, use the smitty chuser command to increase the maximum file size for the root user and restart the WPAR Manager agent (wparagent restart). If you are backing up to a remote file system (for static relocation), a similar change on the NFS server must allow larger files to be created.

- Mobility of system WPARs with an NFS file system mounted with Kerberos security is not supported.
• Collecting All Inventory from IBM Systems Director does not start WPAR Extended Inventory. WPAR Extended Inventory must be collected individually.
• Cloning a WPAR with devices with Device Control setting of type storage does not clone the data from the original set of devices to the new set of devices.
• WPAR Manager does not provide complete support for WPARs with files systems of type directory. These WPARs can be created through the command-line and managed by WPAR Manager.
• WPAR Manager does not provide support for WPARs with allocated devices adapters.
• Only JFS2 and NFS file systems are supported by WPARs live mobility.

Documentation and purchase information

Additional information about the IBM PowerVM Workload Partitions Manager for AIX is available in the IBM Systems Director Information Center. To view the WPAR Manager content, see [IBM PowerVM Workload Partitions Manager for AIX V2.2.1](https://www.ibm.com)

Detailed information about Workload partitions is available in the AIX 7.1 Information Center. To view the WPAR content, see [IBM Workload Partitions for AIX](https://www.ibm.com)

Detailed information about IBM AIX 5.2 Workload Partitions for AIX 7 is available in the AIX 7.1 Information Center. To view this WPAR content, see [AIX 5.2 Workload Partitions for AIX 7](https://www.ibm.com)

If you have an evaluation license, you can contact your IBM marketing representative to purchase a permanent license activation for IBM PowerVM Workload Partitions Manager for AIX.

What's new in WPAR Manager 2.2.1

Read about new or significantly changed information for the WPAR Manager topic collection.

WPAL Manager v 2.2.1 provides the following new functionality:
• Enablement to manage WPARs on AIX 6.1 with 6100-06 and AIX 7.1.
• Support for AIX 5.2 Workload Partitions for AIX 7.
• Support for Controlled Kernel Extension Enablement for WPARs on AIX 7.1.
• Support for virtual SCSI devices in a WPAR.
• WPAR Manager command-line interface (CLI)
• Support to persist WPAR definitions

Enablement to manage WPARs on AIX 6.1 with 6100-06 and AIX 7.1

WPAL Manager 2.2.1 is capable of managing WPARs on AIX 6.1 with 6100-06 and AIX 7.1.

Support for AIX 5.2 Workload Partitions for AIX 7

WPAL Manager 2.2.1 provides management support for AIX 5.2 Workload Partitions for AIX 7 systems. These are system WPARs which provide an AIX 5.2 runtime environment on an AIX 7.1 system.
Support for Controlled Kernel Extension Enablement for WPARs on AIX 7.1

WPAR Manager 2.2.1 provides the administrative support to control the loading and configuration of Kernel Extensions in a WPAR.

Support for virtual SCSI devices in a WPAR

In addition to Fiber channel devices, WPAR Manager 2.2.1 enables support for allocating virtual I/O SCSI devices to a WPAR.

WPAR Manager command-line interface (CLI)

WPAR Manager 2.2.1 delivers centralized WPAR Management capabilities from a CLI.

Support to persist WPAR definitions

WPAR Manager 2.2.1 enables support to preserve WPAR definitions after a WPAR is deleted to be reused at a later time.

What's new in WPAR Manager 2.2

Read about new or significantly changed information for the WPAR Manager topic collection.

WPAR Manager v 2.2 provides the following new functionality:
• Added NLS support.
• Enablement to manage WPARs on AIX 6.1 with 6100-05.
• Enablement for IBM Systems Director 6.2.
• Migration support from WPAR Manager 2.1 on IBM Systems Director 6.1 to WPAR Manager 2.2 on IBM Systems Director 6.2.

Added NLS support

National Language Support enablement is provided in WPAR Manager 2.2 for all languages supported by IBM Systems Director.

Enablement to manage WPARs on AIX 6.1 with 6100-05

WPAR Manager 2.2 is capable of managing WPARs on AIX 6.1 with 6100-05.

The AIX 6.1 with 6100-05 WPAR Manager agent configuration is as follows:
• MCR version: 4.2.2.4
• Director common agent version: 6.1.2.0
• WPAR Manager agent version: 2.2.0.0

Enablement for IBM Systems Director 6.2

WPAR Manager 2.2 is the required version to run on IBM Systems Director 6.2.
Migration support from WPAR Manager 2.1 on IBM Systems Director 6.1 to WPAR Manager 2.2 on IBM Systems Director 6.2

Existing instance of WPAR Manager 2.1 on IBM Systems Director 6.1 can be migrated to WPAR Manager 2.2 on IBM Systems Director 6.2 without requiring the rediscovering of the WPAR configuration.

What's new in WPAR Manager 2.1

Read about new or significantly changed information for the WPAR Manager topic collection.

Integrated product with IBM Systems Director

The WPAR Manager Standalone Licensed Program (v1.2.1) is replaced by the WPAR Manager advanced manager that is a plug-in to the IBM Systems Director product. The WPAR Manager function is integrated with the IBM Systems Director. WPAR Manager version 2.1 requires IBM Systems Director 6.2.

In addition to fully integrating with IBM Systems Director, WPAR Manager v 2.1 provides new functionality not previously provided.

• Provides a new setup advisor to configure WPAR Manager.
• Provides distributed agent installation support for SAN-based storage for WPARs.
• Provides support for Kerberos encryption of network traffic during live WPAR relocation.
• Improvements to the policy management compared to previous releases.
• Enhancements to WPAR back up and resource control facilities.

Provides a new setup advisor to configure WPAR Manager

Setup advisor is a new capability that is designed to assist you when configuring WPAR Manager. This capability allows you to:

• Discover WPAR-capable AIX Systems.
• Guide the user through the steps of discovering systems.
• Authenticate and get access to AIX systems through remotely through IBM Systems Director, WPAR Manager.
• Install WPAR Manager agents on managed AIX systems.
• Run inventory collection tasks to inventory all software and WPAR-extended inventory information.
• Discover existing WPARs on newly managed systems.
• View or change WPAR Manager configuration settings.
• Create WPARs.

Provides function to ease installation on agent systems remotely

WPAR Manager leverages IBM Systems Director, WPAR Manager capabilities that allow you to deploy and install subagent bundles on remote machines directly, without using the Setup Advisor. When the WPAR Manager advanced manager is installed, the WPAR Manager subagent is provided and available as a Common Agent subagent package.
Support for the WPAR-owned rootvg volume groups

SAN connected storage devices can be allocated to WPARs for use as private root volume group storage repositories. Creation, back up, restore and relocation of this class of WPARs is now possible.

Enhancements to Live WPAR relocation

Enhancements to Live WPAR relocation allow you to relocate WPARs that own their rootvg. In addition, you can specify, optionally, to use kerberos encryption to encrypt the network traffic during an asynchronous live WPAR relocation. Use of Kerberos-encrypted relocation requires that Kerberos is configured on both the systems involved in the relocation. In addition, NFSv4 must be configured with Kerberos support on both departure and arrival system.

Enhancements to the WPAR policy management interface

The policy algorithm and user interface are simplified and uses the standard IBM Systems Director, WPAR Manager Group and Jobs interface. The policy monitors for CPU and memory utilization. The System Administrator can set maximum utilization thresholds and customized averaging periods.

Provide support to back up writable namefs-mounted file systems

The WPAR Back up now function supports backing up files from writable namefs-mounted file systems.

Provides new total virtual memory limit resource control

WPAR Manager provides a new total virtual memory limit WPAR resource control. This resource control allows a WPAR administrator to specify a total virtual memory limit for both application and system WPARs. You can change this new resource control while the WPAR is active or inactive.

Supported operating environments for WPAR Manager

WPAR Manager and application mobility are supported on IBM Systems Director systems based on the POWER4™ processor architecture or later.

The WPAR Manager server requires that you are using IBM Systems Director on AIX, Windows, or Linux.

WPAR Manager agent requirements

The WPAR Manager agent can be installed on AIX Version 6.1 with the 6100-03 Technology Level, or later. To use the features in WPAR Manager, you must be running the latest available AIX version and the latest available WPAR Manager agent version. Operating at a previous AIX technology level and WPAR Manager agent software version that are installed on the managed system, prevents you from using the WPAR properties and WPAR capabilities that are available in the latest version of WPAR Manager. Using a down-level version of WPAR Manager agent results in degraded functions. You can always upgrade the WPAR Manager agent to the latest supported version, regardless of the Technology Level of the managed system.
Table 1. WPAR Manager supported configurations

<table>
<thead>
<tr>
<th>Operating System</th>
<th>MCR version</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX Version 6.1 with the 6100-03 Technology Level</td>
<td>4.2.1.0</td>
</tr>
<tr>
<td>AIX Version 6.1 with the 6100-04 Technology Level</td>
<td>4.2.2.0</td>
</tr>
<tr>
<td>AIX Version 6.1 with the 6100-05 Technology Level</td>
<td>4.2.2.0</td>
</tr>
<tr>
<td>AIX Version 6.1 with the 6100-06 Technology Level</td>
<td>4.2.4.0</td>
</tr>
<tr>
<td>AIX Version 7.1</td>
<td>4.3.0.0</td>
</tr>
</tbody>
</table>

Note: On all systems before AIX Version 6.1 with the 6100-04 Technology Level, you must update the Director agent to 6.1.0.4 or later.

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 2. WPAR Manager memory and disk space requirements

<table>
<thead>
<tr>
<th>Application</th>
<th>Memory requirement</th>
<th>Disk space requirement</th>
</tr>
</thead>
</table>
| WPAR Manager     | 125 MB             | • /, 5 MB
|                  |                    | • /var, minimum 180 MB.
|                  |                    | This includes manager (66 MB), agentmgr (61 MB)
|                  |                    | and runtime logs (45 MB).
|                  |                    | • /opt, 15 MB. |
| WPAR Agent       | 45 MB when idle    | /var, 1 MB             |

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

Heterogeneous WPAR Manager agent environments

The WPAR Manager application can manage a heterogeneous environment of managed systems at different AIX technology levels. However, to make use of full management capabilities, the WPAR Manager agent must be updated to the latest version.
There are limits to the environments that can be supported, and the capabilities of a mixed environment must be considered if you have a heterogeneous environment. For the full 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. The WPAR Manager must be migrated first. WPAR Manager agents are not required to be updated immediately and their migration can be staged.

The following software components work together to provide the features and capabilities of the WPAR Manager application:

- IBM Systems Director console and server with WPAR Manager extension
- AIX Version 6.1 or later
- Metacluster Checkpoint and Restart (MCR) kernel extension
- WPAR Manager agent
- Director Common Agent

The MCR kernel extension file set 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 corresponding updated AIX technology level and MCR levels allow for management of all newly supported WPAR properties and operations delivered in the latest WPAR Manager version.

Related concepts
“Mixed agents environments”

Mixed agents environments:

To manage WPARs, the WPAR Manager agent is required.

IBM Systems Director can discover systems with older versions of the WPAR Manager agents installed and they are recognized as WPAR capable systems; however, all WPAR operations on those systems are blocked. The system problem status reflects that there is a problem with these systems and that the WPAR Manager agent must be upgraded.

In addition to not being able to perform WPAR related functions, if the WPAR Manager agents are not upgraded to the required level the WPAR inventory and state might be out of sync between the systems and the IBM Systems Director interface.

Related concepts
“Heterogeneous WPAR Manager agent environments” on page 8

WP AR management in a logically partitioned environment

The managed systems accessible through WPAR Manager are real or virtual systems running both AIX and the WPAR Manager agent. They are discovered by IBM Systems Director through the agent Discovery and Inventory processes.

WP AR 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 cannot 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.

**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 IBM Workload Manager plug-in for IBM Systems Director supports the accessibility features that are supported in IBM Systems Director.

When using JAWS screen reader with IBM Workload Manager, follow these tips to improve JAWS usability:

- Access IBM Systems Director Server using a supported Mozilla Firefox browser.
- Enable accessibility features in the IBM Systems Director:
  1. Open **Settings → Navigation Preferences**.
  2. Turn on the following options:
     - Enable tables for accessibility
     - Play sound when data on the page changes
     - Use resource table view as default view for topology perspectives
  3. Click **OK** or **Apply** to save your settings.

For more information, see [Accessibility features for IBM Systems Director](#).

---

**Installing WPAR Manager**

You can install the WPAR Manager plug-in on IBM Systems Director, WPAR Manager management servers running AIX, Linux, or Windows.

View the following topics to learn how to install WPAR Manager on the management server as well as the WPAR Manager agent on agent systems.

**Related tasks**

"Upgrading the WPAR Manager" on page 11

**Related information**

[Installing, upgrading, and migrating IBM Systems Director](#)

---

**Installing WPAR Manager as an IBM Systems Director advanced manager**

You must install the WPAR Manager on the same system on which the IBM Systems Director server is installed.

**Prerequisites**

Ensure that you have the authority to complete the installation.

- For Windows, administrator authority is required.
- For AIX or Linux, root authority is required.
Complete the following steps to install WPAR Manager as an IBM Systems Director advanced manager:

1. Log in to the system with the required authority level.
2. If you are installing from media, insert the media containing WPAR Manager into the media drive. If installing from a download, copy the installer to the target system.

   **Note:** If you are media installing for AIX or Linux you can mount the media drive using the following command (where /mnt is the mount point for your media drive).

   ```
   /usr/sbin/mount -v cdrfs -p -r /dev/cd0 /mnt
   ```

3. Copy the platform-specific product archive into a local directory.
4. Unzip or untar the archive. This action creates a platform-specific subdirectory.
5. Run the cd into the platform subdirectory.
6. Start the installation by running the following command to install WPAR Manager from the directory that contains the installer:
   - For AIX or Linux: WparMgrSetup.bin
   - For Windows: WparMgrSetup.exe

   By default, the installation uses the GUI mode on Windows and console mode on AIX and Linux. Use the -i option to specify the console mode. For example, WparMgrSetup.exe -i console.

### Upgrading the WPAR Manager

Starting with version 2.1, WPAR Manager is an advanced manager for IBM Systems Director. Upgrading from previous releases of the stand-alone WPAR Manager to the new WPAR Manager is not possible.

#### Related concepts

- [“Installing WPAR Manager” on page 10](#)

### Installing the WPAR Manager subagent on the managed system

The WPAR Manager agent is a subagent to the IBM Systems Director Common Agent that is running on the managed system. It enhances the IBM Systems Director agent to provide an interface for creating and managing WPARs, such as collecting metrics and event data on WPARs among other functions.

You must use the IBM Systems Director to install the WPAR Manager agent. In either installation method, IBM Systems Director or manual, the subagent installation procedure installs the following two file sets on the managed system(s):

- wparmgt.agent.rte
- mcr.rte

Both file sets are required for the installation. However, only the version of the file sets that are required for your operating system technology level are installed.
Related tasks
“Defining a managed system” on page 20

Using IBM Systems Director to install the WPAR Manager agent on the managed system
Use IBM Systems Director to install the WPAR Manager agent on a managed system or systems. This method is quick and easy, while allowing you to install on multiple systems simultaneously.

Before installing the WPAR Manager agent on a managed system, ensure that it has at least 200 MB of free space in the /var file system. If it does not, execute the following command as root:

```
chfs -a size=+200MB /var
```

**Note:** To install the WPAR Manager agent from the server, OpenSSH must be installed on the agent. For more information, see [Preparing to install Common Agent on AIX](#).

To install the WPAR Manager agent on one or more managed systems, perform the following steps:

1. From the IBM Systems Director web interface, expand Release management and click Agents. The Agents window is displayed.
2. Select Common Agent Subagent Packages in the table.
3. Select the latest version of the CommonAgentSubagent WPAR Manager Agent package.
4. Click Install Agent. The installation window is displayed.
5. On the Welcome window, click Next.
6. On the Agents window, click Next.
7. On the Systems window, do the following:
   a. Select the name of the system or systems on which you want to install the WPAR Manager Agent.
   b. Click Add → Next → Finish.
8. Click OK to complete the installation.

Using the manual mode to install the WPAR Manager agent on the managed system
You must not use the manual mode to install the WPAR Manager agent on the managed system. However, if you want to use manual mode for your installation review the following information.

The following files are prerequisites for installing the WPAR Manager agent 2.2.1:

- `bos.wpars` version 6.1.2, or later.
- IBM Systems Director agent 6.1.2, or later.

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

```
# installp -acqYXd <IMAGE_DIR> wparmgt.agent
```

Substitute `<IMAGE_DIR>` with the location of the WPAR Manager installp file sets. The location can either be the media drive or a local directory on the managed system.
Removing the WPAR Manager Advanced Manager
You can remove WPAR Manager from your system using IBM Systems Director.

Perform the following steps to remove WPAR Manager from your system using IBM Systems Director by running the uninstaller:
1. Log in as the administrator user to the system where WPAR Manager is installed.
2. Run the following command:
   `<Director_install_location>/WPARManager/uninstall/UninstallWPMP`

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

The following file sets must be removed:
- `wparmgt.agent.rte`
- `mcr.rte`

To remove all of the WPAR Manager agent file sets, run the installp command, as follows:
`installp -u wparmgt.agent.rte mcr.rte`

Note: The cas.agent file set and the tivoli.tivguid file set are shared components which might 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 the file sets, then they can also be uninstalled from the system. Running the installp -u cas.agent tivoli.tivguid command fails if other products are dependent on these file sets. Specify the -g flag with the installp command to remove these file sets and any other dependencies.

WPAR Manager license enablement
WPAR Manager is delivered by default with a temporary license that enables you to explore the WPAR Manager benefits and capabilities free of charge for 60 days.

The IBM Systems Director welcome page displays the status of the WPAR Manager license and how many days remain before the temporary license expires.

You must contact your IBM Customer Representative to request the WPAR Manager permanent license. If you purchase the permanent license, you will receive a WPAR Manager license installer that must be run after the product is installed. This installer promotes the temporary license to a permanent license.

The location of the license installers on the media are:
- AIX: `<media root>/manager/AIX/WparMgrKey.bin`
- Linux: `<media root>/manager/Linux/WparMgrKey.bin`
- Windows: `<media root>/manager/Windows/WparMgrKey.exe`

Configuring WPAR Manager
You can configure the environment for WPAR application mobility and perform additional post-install action customizations.
Configuring the WPAR Manager agent

It is not necessary to perform any manual configuration steps for the system to be discovered by the Director manager. However, if you want to manually register the system to an agent manager, use the `/var/opt/tivoli/ep/runtime/agent/toolkit/bin/configure.sh` script.

If the agent manager ports were not modified from the default values during its installation, log in as root and run the following `configure.sh` script with the host name of the agent manager and its registration password:

```
# /var/opt/tivoli/ep/runtime/agent/toolkit/bin/configure.sh
-amhost <agent-manager.yourdomain.com>
```

- `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` Re-configure 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)
- `passwd <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
- `force` Re-configure a previously configured agent

At a minimum, use the `amhost` flag to specify the agent manager 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 \textbf{-force} flag to re-configure the agent.

Configuring the WPAR Manager agent fails 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 an agent manager. You can use the \textbf{-force} flag to re-configure the WPAR Manager agent.
- All ports specified for use by the WPAR Manager agent (\textbf{-port}, \textbf{-jport}, \textbf{-nport}, \textbf{-wport}, \textbf{-wsport}) are distinct and not in use.

**Starting and stopping the WPAR Manager agent**

Use the endpoint.sh command to start, stop, and restart the WPAR Manager agent.

When you start the WPAR Manager agent, it attempts 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 are logged to the \texttt{/var/opt/tivoli/ep/logs/error-log-0.xml} file on the system.

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

- To start the WPAR Manager agent, use the following command:
  \texttt{/var/opt/tivoli/ep/runtime/agent/bin/endpoint.sh start}.
- To stop the WPAR Manager agent, use the following command:
  \texttt{/var/opt/tivoli/ep/runtime/agent/bin/endpoint.sh stop}.
- To restart the WPAR Manager agent, use the following command:
  \texttt{/var/opt/tivoli/ep/runtime/agent/bin/endpoint.sh restart}.

**Configuring WPAR Manager agent logging**

The WPAR Manager agent logs important troubleshooting information to log files in the \texttt{/var/opt/tivoli/ep/logs/} directory. You can configure logging in the \texttt{/var/opt/tivoli/ep/conf/overrides/logging.properties} file.

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

1. Open the \texttt{/var/opt/tivoli/ep/conf/overrides/logging.properties} file in a text editor.
2. Add the class or package that you want to log more information about, and add the desired detail level. For example:
   \texttt{com.ibm.mc.wparmgt.agent.cmd.impl.action.aix=FINEST}
3. Refresh the logging configuration by executing the \texttt{/var/opt/tivoli/ep/bin/lwilog.sh -refresh} 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 in the same subnet.
- Source and destination servers must be running on compatible hardware and have compatible software installed.
- For IPv6 networks, NFSv4 is required. To support NFSv4, all systems, such as the WPAR manager, WPAR agent, NFS server, 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 19
- “Manual relocation” on page 38
- “Application mobility” on page 33

**Related tasks**

- “Creating a WPAR that supports live relocation” on page 22

### Configuring application mobility for system WPARs

WPAR Manager supports static relocation and 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 managed system properties” on page 20

### Configuring live application mobility for system WPARs:

There are two requirements to enable live application mobility for system WPARs. First, you must specify that the WPAR is checkpointable by selecting **Enable relocation** during WPAR creation. Second, either the WPAR must be configured in a remote directory, or it must own its root volume group.

**Configuring system WPARs in a remote directory:**

This configuration uses a remote directory that is the root mount point for the /, /var, /home, and the /tmp directories. 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 might use these remote directories only if you need a private /usr directory and a private /opt directory.

To configure 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, perform 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 IPv6 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 previously specified using the advanced interface or the Create WPAR wizard.

/configuring system wpars with root volume group devices:

WPAR Manager supports creating a WPAR with file systems contained within a specified storage device.

The specified storage device is referred to as a root volume group (rootvg) device. When creating the WPAR, you must specify at least one rootvg storage device using either the mkwpar command from the command line or the WPAR Manager Create WPAR wizard. Refer to the mkwpar command for the proper syntax. When you use the Create WPAR wizard, the Devices step allows you to specify a storage device to be used by the WPAR. Click **Add** to view and select the desired storage devices to be assigned to the WPAR. After selecting one or more devices, you must use the pull-down selector in the rootvg disk column to specify that the device is intended to be a rootvg device. If the disk previously contained any volume group data, you must select **Overwrite existing volume group on rootvg devices**.

**Related tasks**

"Managing WPAR storage devices" on page 30

Securing live application mobility data with Kerberos encryption:
WPAR Manager supports Kerberos encryption for securing data transferred during live application mobility.

Securing live application mobility data with Kerberos encryption requires NFS with Kerberos enablement. The departure node acts as a temporary NFS server during the relocation of the WPAR. The departure and arrival nodes must be able to read configuration data from a Kerberos server. Required packages for a Kerberos client can be found as part of the IBM Network Authentication Service for AIX package, shipped on the AIX expansion media.

Both the departure and arrival node must have NFSv4 configured with Kerberos support. For AIX, you also must have the CLiC library package (clic.rte) and the Cryptographic Library package (modcrypt.base) installed.

To verify your NFS setup, refer to the following commands:

- The `/usr/sbin/chnfsdom` command displays the NFS domain.
- The `/usr/sbin/nfskey -l` command lists the keytab entry for the NFS server.
- The `/usr/sbin/chnfssrtd` command lists the mapping between the Kerberos realm and the NFS domain.
- The `lsr -g nfs` command displays if the gssd subsystem and nfsrgyd subsystem are active.

**Configuring Kerberos for the mcr service on the departure node**

To configure Kerberos for the mcr service on the departure node, you must create principal for the mcr service on the departure node. To create principal, use the `/usr/krb5/sbin/kadmin.local` command or the `/usr/krb5/sbin/kadmin` command. Use the following format from the Kerberos command prompt when you are creating principal:

```
addprinc mcr/departurenod.domain.com
```

The keytab entry for the mcr service must be defined on the departure node. To define the keytab entry, use the `/usr/krb5/sbin/kadmin` command and the following format from the Kerberos command prompt:

```
ktadd mcr/departurenod.domain.com
```

This configuration must be performed for all nodes which serve as departure nodes during live application mobility.

**Configuring Kerberos credentials on the arrival node**

To configure Kerberos credentials on the arrival node you might not perform any specific configurations. However, for the mobility to complete, the root user must be authenticated with Kerberos credentials using the `/usr/krb5/bin/kinit` command.

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

No restrictions exist on the WPARs file systems for static relocation mobility. However, a shared file system accessible from both the departure and arrival server can 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, perform the following steps:

1. Create a file system, named `/sfs` in this example, on the `nfssrv1.yourdomain.com` NFS server where temporary WPARs backup images are 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:
   ```
   # 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:
   ```
   # 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:
   ```
   # 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 **Application Configuration** from the WPAR Manager Welcome window and specify the path to the shared file system on all of the WPAR Manager agent systems in the **Shared Directory** field.

---

### Managing workload partitions with WPAR Manager

WPAR Manager is an advanced platform management extension for IBM Systems Director used to manage WPARs and enable WPAR relocation across systems.

Functionality provided by IBM Systems Director is augmented with the necessary capabilities to discover WPARs and WPAR-specific properties on managed systems, to perform basic life cycle operations on WPARs and to provide workflows for WPAR static and live mobility.

**Related concepts**

"Configuring the environment for application mobility" on page 15

**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 that is running AIX.

**Defining a managed system**
Configuring a managed system to work with WPAR Manager requires discovering, installing WPAR Manager sub agent, and collecting software and WPAR Extended inventory on the system. After those steps are completed, additional capabilities such as Create workload partition and Restore workload partition are available.

To bring an AIX system or LPAR into the management environment of the WPAR Manager, complete the following steps:

1. Identify the IP address, for each individual system that you want to discover. You can discover all systems within a specified IP address range.
2. Click **System Discovery**.
3. To authenticate to systems that have been discovered so that you can perform administrative tasks on them, complete the following steps:

   **Note:** You only need to complete the following tasks once for each system you want to authenticate to.
   a. From the IBM Systems Director **Welcome** window, select **Systems have no access**.
   b. Find the systems that you discovered. For each system, right-click the **No access** link.
   c. Enter a valid administrator user name and password for the selected system.
4. Install the WPAR Manager subagent on each system.
5. Now that you have discovered new managed systems, you can collect software and WPAR Extended inventory to discover any existing workload partitions on those systems. Systems that are WPAR-capable are also identified.

WPAR Manager provides an integrated step-by-step guide to configuring managed systems and other settings in the application. For more information about managed systems, see the **Setup Advisor** or go the IBM Systems Director **Welcome** page and click **Set up WPAR Manager** from the **Manage** panel.

**Related tasks**
“Installing the WPAR Manager subagent on the managed system” on page 11

**Related information**
Discovery
Accessing a secure system with request access
Collecting inventory

**Viewing managed system properties**
WPAR Manager uses IBM Systems Director facilities to display configuration details, physical system inventory details, system-specific software inventory,
system related events, and activities, in addition to displaying WPAR-related properties associated with the managed system.

To view managed system properties, complete the following steps in IBM Systems Director with the WPAR Manager advanced manager plug-in,

1. From IBM Systems Director, select **Navigate Resources**. This allows you to navigate to the **Navigate Resources** panel.
2. Select **Workload Partitions Groups** in the table.
3. Select **WPAR-capable systems** in the next table displayed. The table in the next page displays all the systems managed by IBM Systems Director that have been identified as WPAR-capable systems.
4. Click the name of any managed system in the table. The **Resource Properties** view displays that includes a list of properties and other detailed information associated with the managed system. Using the **Resource Properties** view, you can access troubleshooting information and other important details about the managed system.

**Related concepts**
- “Configuring application mobility for system WPARs” on page 16

**Related tasks**
- “Exporting a storage device to an existing WPAR” on page 30
- “Exporting a storage device to a new WPAR” on page 31

**Related information**
- Properties view

### Updating managed system attributes required by WPAR Manager

When a system is first discovered and inventory is collected, the WPAR Manager stores hardware and software configuration parameters specific to the managed system. These properties are used to calculate compatibility between systems for WPAR mobility, provide default values for WPAR attributes such as RBAC, and present the list of possible resources to use in the WPARs.

If a system undergoes configuration changes, the properties assigned to the managed system are no longer valid and must be updated. The WPAR Manager sub-agent constantly monitors the properties that the application depends on and if changes are detected an event is sent to update the information.

To manually update the managed system configuration, perform the following steps:

1. In the IBM Systems Director web interface navigation area, expand Inventory and then click **View and Collect Inventory**.
2. From the Target Systems list, select the system for which you want to update the configuration information.
3. From the Manage inventory profiles list, select **Extended WPAR Discovery**.
4. Click **Collect Inventory**.

**Related information**
- Collecting inventory

### Viewing performance metrics for a managed system

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

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

Creating WPARs

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

To create a WPAR, you can use the Create Workload Partition wizard.

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

1. From the IBM Systems Director Welcome Page, select the Manage panel.
2. Select WPAR Manager to open the WPAR Manager Summary page.
3. Select Create workload partition from the Common tasks section to start the wizard.
4. Follow the instructions on each page to complete the wizard.

Note: Although 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 create task fails. Alternatively, if the WPAR is deployed into a system different from that hosting the WPAR with the same network configuration, no error is raised and two WPARs will be sharing the same network address.

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 have the checkpoint option enabled. This setting can be specified when the WPAR is created through the Enable checkpoint option. A WPAR with the checkpoint option enabled allow the application to save the internal state of applications running within the WPAR to be restored on another similarly configured system.
- The WPAR owns the devices where the rootvg is created (WPAR-owned rootvg) or the WPAR must be NFS-based.
- NFS-based WPAR must have a valid network configuration. NFS-based 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 verify whether the name of a WPAR resolves to a valid network host name.
Related concepts

"Configuring the environment for application mobility" on page 15

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

WPAR-owned rootvg:

The root file systems for the WPAR resides in storage area network (SAN) devices or virtual SCSI devices. To relocate the WPAR, both the host system and the destination system have access to the storage disk that is assigned to the WPAR.

Storage devices can be configured in the Devices panel of the Create WPAR wizard. At least one of the disks must have a device control setting as rootvg.

NFS-based WPAR:

The root file systems for an NFS-based WPAR resides on an NFS server and must be configured to be accessed from the WPAR.

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

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

Creating a WPAR with a remote /usr file system and a remote /opt file system is an extensive operation, you must mount them locally as read-only file systems. Mounting the file systems locally reduces the file system size requirements on the NFS server that hosts 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 hosts 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 must be mounted remotely as read-write file systems using NFS.

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

For NFS based WPARs, you must mount /, /tmp, /var and /home remotely as read-write NFS filesystems.

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
  /wparname
    /home
    /tmp
    /var
```
Related tasks

“Creating a WPAR that supports live relocation” on page 22

Working with WPARs created from the command line:

WPARs created from the command line are discovered by the WPAR Manager.

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

**Note:** Live mobility of application WPARs created from the command line will fail if the WPAR is relocated from the WPAR Manager user interface and vice versa.

Related information

- Configuring system WPARs
- Configuring application WPARs

Versioned Workload Partitions:

Versioned Workload Partitions are unshared or detached system WPAR that provide a different version of the AIX runtime environment than the global system. Base AIX version 7.1 versioned workload partition support is provided by separately purchased licensed programs which must be installed on each of global workload partition environments where this support is required.

Currently, the licensed program that provides an AIX version 5.2 WPAR runtime environment is available. For more information about hardware and software prerequisites for the IBM AIX 5.2 Workload Partitions for AIX 7, see IBM AIX 5.2 Workload Partitions for AIX 7 in the AIX V7.1 Information Center.

IBM PowerVM Workload Partitions Manager for AIX plug-in for IBM Systems Director provides support for managing versioned WPARs. If the appropriate licensed program for the alternate runtime environment is installed on the managed systems, all the hardware and software prerequisites identified in the Information Center documentation are met. The current version of the WPAR Manager agent software is installed on the managed systems where versioned workload partition support is needed.

WPAR Manager provides support for basic life cycle management of versioned workload partitions as well as supporting tasks such as backup, restore, clone, and relocation. By definition, the runtime environment of a versioned WPAR is different from the runtime environment of the global environment. So, synchronization of runtime environments is not supported between versioned WPARs and the global environment.

**Note:** Live relocation of AIX 5.2 versioned WPARs requires the installation of additional software within the AIX 5.2 versioned WPAR before live mobility can be attempted. After installing the separately purchased AIX versioned WPARs licensed program, it is necessary to rerun the IBM Systems Director software inventory task on any managed systems recently updated with the new software support for versioned WPARs. This identifies the newly updated managed systems as versioned WPAR capable systems to the WPAR Manager software.
For more information to do live mobility with versioned WPARs, see Creating a versioned WPAR in the AIX 7.1 Information Center.

Creating versioned WPARs:

Versioned workload partitions are detached system WPARs that operate with a runtime environment different from that provided by the global system environment.

Perform the following steps to create a versioned WPAR by using the Create Versioned Workload Partition wizard.

1. From the IBM Systems Director navigation panel, select Navigate Resources.
   This action opens the Navigate Resources table in IBM Systems Director.
2. Select Workload Partitions Groups in the table.
   x– indicates the number of managed systems that WPAR Manager has identified as meeting the prerequisites for hosting versioned workload partitions. If there are no (0) managed systems that have been identified as versioned WPAR-capable systems and you have previously installed the separately purchased AIX Versioned Workload Partitions licensed product, then you must re-run the IBM Systems Director software inventory task on the appropriate managed systems. This can appropriately inventory the newly installed licensed product and identify the managed system or systems as version WPAR-capable managed systems.
   The managed systems that are capable of hosting versioned workload partitions are listed.
4. Select the check box next to the name of the required system and then click Actions in the table toolbar to view the Actions menu.
5. From the Actions menu, click Workload Partitions Management → Create versioned workload partition.
   This action launches the Create Versioned Workload Partitions wizard. This wizard is similar to the Create Workload Partitions wizard.
6. Follow the instructions to complete the wizard and create the versioned workload partition on the selected managed system.

Creating a versioned 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 that is running within the WPAR.

To create a WPAR that supports live relocation, you must configure your WPAR as follows:

- To support live relocation, a WPAR must have the checkpoint option enabled. This setting can be specified when the WPAR is created through the Enable checkpoint option. A WPAR with the checkpoint option enabled allow the application to save the internal state of applications that are running within the WPAR to be restored on another similarly configured system.
- The WPAR owns the devices where the rootvg is created (WPAR-owned rootvg) or the WPAR is NFS-based.
- NFS-based WPAR must have a valid network configuration. NFS-based 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:** Live relocation of AIX 5.2 versioned WPARs requires the installation of additional software within the AIX 5.2 versioned WPAR before live mobility can be attempted. For more information about versioned WPARs, see Creating a versioned WPAR in AIX 7.1 Information Center.

**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, you can modify the properties of the WPAR. However, only selected properties of the WPAR's configuration can be modified depending on the state of the WPAR.

To view or modify WPAR properties, complete the following steps:

1. From the console navigation area, select **Navigate Resources**.
2. In the table, click **Workload Partitions Groups**.
3. In the table, click **All Workload Partitions**.
4. Select the WPAR you want to view or modify from the list.
5. Click **Actions**, and select **Properties**.

**Working with WPARs modified with AIX commands:**

Although the WPAR Manager provides an user interface to modify the configuration of WPARs, you can also use the command line to modify. When a change is performed through the command line, the WPAR Manager discovers the changes after a short delay, and the IBM Systems Director database is updated to reflect the new configuration.

**Backing up WPARs**

The backup operation in WPAR Manager will back up the selected WPAR 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 can be backed up. For application WPARs, the back up menu option is not shown.
- 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 command and the savewpar command with the desired options.

To back up a workload partition to an image file on a managed system, complete the following steps:

1. From the IBM Systems Director web interface navigation area, click **Navigate Resources**.
2. In the table, click **Workload Partitions Groups**.
3. In the table, click All Systems Workload Partitions to list all of the system workload partitions currently identified by the application.
4. Select the workload partition that you want to back up.
5. Click Actions, and select Back up.
6. From the Back up page, specify the backup directory location and any other backup options.
7. 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 the WPAR to be restored.

To restore a workload partition from a backup image, complete the following steps:

1. From the IBM Systems Director web interface navigation area, click Navigate Resources.
2. In the table, click Workload Partitions Groups.
3. In the table, click WPAR-capable systems.
4. Select the system you want to restore.
5. Click Actions, and select Workload Partition Management → Restore.
6. 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.
7. Click OK to complete the task.

**Starting a system WPAR**

After the system 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 goes 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 created on a managed system and never go through the Defined state.

To start a system WPAR, perform the following steps:

1. From the IBM Systems Director web interface navigation area, click Navigate Resources.
2. In the table, click Workload Partitions Groups.
3. In the table, click All Systems Workload Partitions to list all of the system workload partitions currently identified by the application.
4. Select one or more WPARs in the Defined state that you want to start.
5. Click Actions, and select Start.
6. A dialog box is displayed confirming your request. Click OK to continue. You can monitor the progress of the task by selecting the Display Properties button in the message box at the top of the window, after the task request has been submitted.

**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, 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 WPAR is removed from the system and depending on whether preserving the workload partitions is desired or not a workload partition definition could be preserved. This definition is represented by the undeployed state.

To stop a WPAR, perform the following steps:

1. From the IBM Systems Director web interface navigation area, click **Navigate Resources**.
2. In the table, click **Workload Partitions Groups**.
3. In the table, click **All Workload Partitions**
4. In the table, select one or more WPARs that you want to stop.
5. Click **Actions**, and select **Stop**.
6. Select the type of stop you want to perform. You must select one of the following options:
   - **Normal** - Select this option to slowly stop the workload partition.
   - **Hard** - Select this option to have the workload partition stop in 60 seconds.
   - **Force** - Select this option to stop running processes more aggressively and force an unmount of file systems. If any processes remain, the workload partition is placed in the Broken state, and cannot be restarted.
7. If the selected targets are application WPARs the Preserve workload partition definition option is rendered. The value is preset with the corresponding application configuration setting. You can override the application configuration setting by toggling this value.

**Synchronizing a system WPAR**

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

The type of WPAR determines the type of synchronization available.

If the WPAR shares the /usr and /opt file system with the global AIX system, which is typically called a Shared WPAR, the synchronize page allows you to choose options for synchronizing install file sets, RPM file sets, or all of the installed software.

If the WPAR has its own private /usr and /opt file system, which is typically called a Detached WPAR, the Synchronize page allows you to specify the installation directory or device.
Synchronization is also available when you are restoring a WPAR from a backup image. The synchronize task is unavailable for application WPARs or versioned WPARs.

To synchronize a system WPAR, perform the following steps:
1. From the IBM Systems Director navigation area, click Navigate Resources.
2. In the table, click Workload Partitions Groups.
3. In the table, click All System Workload Partitions to list all of the system workload partitions currently identified by the application.
4. In the table, select the workload partition that you want to synchronize.
5. Click Actions, and select Synchronize.
6. From the Synchronize page, specify the synchronization options for the WPAR, and click OK.

**Cloning a WPAR**
You can clone an existing system WPAR to create a new copy of that WPAR.

When you clone a WPAR, the data from existing external devices is not copied. However, if one or more external devices contains rootvg information, that information is copied to a new specified external device.

To clone a WPAR, complete the following steps:
1. From the IBM Systems Director Web interface navigation area, click Navigate Resources.
2. In the table, click Workload Partitions Groups.
3. In the table, click All System Workload Partitions to list all the system workload partitions currently identified by the application.
4. Select the workload partition from the table that you want to synchronize.
5. Click Actions, and select Clone.

   **Note:** If the WPAR contains a rootvg device, you can only clone the WPAR if the WPAR is in an active state.
6. From the Clone page, specify the clone options for the WPAR, and click OK.

**Removing and deleting a WPAR**
You can remove a WPAR reference from the IBM Systems Director database, retaining the WPAR and its artifacts intact on the managed system. You can also delete a WPAR reference from the Director database and the WPAR from the managed system that it is running on. WPAR Manager provides an application configuration setting to preserve WPAR definitions after a WPAR is removed or deleted. These WPAR definitions are represented by the undeployed WPAR state. This behavior can toggle from the WPAR Application Configuration window or the Preserve workload partition definitions on the delete panel.

Perform the remove and delete tasks depending on whether the WPAR definition tasks must be preserved. Consider the following scenarios:

- WPAR definitions are not preserved
  The remove task removes the WPAR managed endpoint definition from within the IBM Systems Director environment. The delete task deletes the definition from the IBM Systems Director and also deletes the WPAR and its artifacts from the managed system.
- WPAR definitions are preserved
The remove task on a WPAR that is deployed on a managed system disassociates the WPAR from the managed system and preserves the WPAR-managed endpoint definition in the IBM Systems Director environment as an undeployed WPAR. The delete task deletes the WPAR and its artifacts from the managed system and preserves the WPAR-managed endpoint definition in the IBM Systems Director environment as an undeployed WPAR. The remove task on an undeployed WPAR removes the WPAR-managed endpoint definition from within the IBM Systems Director environment.

**Deploying a WPAR definition**

With WPAR Manager, you can deploy a WPAR definition from a previously deleted WPAR on a managed system.

To deploy a WPAR definition, perform the following steps:

1. Click **Navigate Resources** from the IBM Systems Director.
2. Click **Workload Partitions Groups** from the table.
3. Click **Workload Partition Definitions** to list all the workload partition definitions from previously deleted or removed WPARs.
4. Select the workload partition definition that you want to deploy.
5. Click **Actions → Deploy**.
   
   The corresponding Create WPAR wizard is launched.
6. Select the target system where the workload partition definition is deployed and follow the steps on the wizard. The values from the workload partition definition are shown in the wizard.

The deploy action can also be initiated from any other view where the Workload Partition definitions are displayed, for example, Workload Partitions and Hosts.

**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 already active.

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

- The storage device must be configured on the managed server as either a Fibre Channel or virtual SCSI disk.
- You can only allocate a storage device to system WPARs.
- 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.

**Related concepts**

“Configuring system WPARs with root volume group devices” on page 17

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

Use **Edit** in WPAR Manager to allocate storage to an existing workload partition (WPAR).
To export a storage device to an existing WPAR using the **Edit** action, perform the following steps:

1. Log in as the root user to the system where WPAR Manager is installed.
2. From WPAR Manager, select **View workload partitions**.
3. Right-click the wanted WPAR and select **Edit**.
4. On the **Devices** tab, click **Add**. The **Devices for export** window is displayed. This window shows the available storage devices on the managed system. On this window, you can view the device type, device name, device ID, whether the device is currently exported to a WPAR, the number of WPARs that the device is allocated to, and the device subclass.
5. Select the check box next to each device you want to export to the WPAR.
6. Click **Add** to move the devices to the selected box.
7. Click **OK** to allocate the selected storage devices to the WPAR and to close the **Add Devices for Export** window.

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 attempts 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 are available for use within the WPAR. If the devices are otherwise in use, then the WPAR is successfully started but an error message is displayed.

If the **Modify WPAR** action is performed on a WPAR that is started, the devices automatically export if they are 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.

**Related tasks**

"Viewing managed system properties" on page 20

**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, perform the following steps:

1. Log in as the root user to the system where WPAR Manager is installed.
2. Select **Select WPAR Manager → Create workload partition**.
3. To start the wizard, click **Next**.
4. Follow the instructions on each window as indicated.
5. On the **Devices** tab, click **Add**. The **Devices for export** window is displayed. This window shows the available storage devices on the managed system. On this window, you can view the device type, device name, device ID, whether the device is currently exported to a WPAR, the number of WPARs that the device is allocated to, and the device subclass.
6. To move the devices to the selected box, click **Add**.
7. Select the check box next to each device you want to export to the WPAR.
8. Click **OK** to allocate the selected storage devices to the WPAR and to close the **Add Devices for Export** window. By default, the device is considered a standard storage device. If attaching the device to be part of the root volume group is wanted, select the rootvg option. Only devices of type disk can be part of the root volume group.
9. Complete the remaining wizard as desired.
10. 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 attempts 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 are available for use within the WPAR. If the devices are otherwise in use, then the WPAR successfully starts but an error message is displayed.

**Related tasks**

"Viewing managed system properties" on page 20

**Viewing storage devices for WPARs**

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

Perform 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. Select **WPAR Manager**.
3. Select **View WPAR capable systems**.
4. In the table of managed systems, click the name of the system.
5. Click WPAR related properties.
6. Click the **Devices** tab. The following information about the devices allocated to the managed system are displayed:

   **Device**
   Specifies the name of the device as configured in the Global environment.

   **Type**
   Specifies the device type such as disk, tape, or CD-ROM.

   **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.

   **Subclass**
   Specifies if the device is a Fibre Channel or Virtual SCSI disk

**Role Based Access Control support**

Use **Role Based Access Control (RBAC)** to provide greater granularity in controlling access to AIX services based on the 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 because 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 recognized as a WPAR-capable system and Extended WPAR inventory is collected. If the file is modified after collecting inventory, the content will be automatically uploaded to the WPAR Manager server. To trigger a manual update, you can collect the inventory for the Extended WPAR Discovery profile.

---

**Application mobility**

Application mobility is the process of relocating a WPAR between two hosts or virtual servers running AIX Version 6.1 or later.

There are environment configurations required for WPAR mobility. Two types of relocation are possible, live, and static.

**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.

**Related concepts**

“Configuring the environment for application mobility” on page 15

---

**Planning for application mobility**

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

Consider the following information about WPAR compatibility:

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

System compatibility
System compatibility is the degree of similarity between two servers about relocating a WPAR from one server to another.

Live relocation requires more extensive compatibility testing than static relocation. Therefore, it is possible that two systems can 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 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 bos.rte file set must be the same on the arrival system and the departure system.
• The version, release, modification, and fix level of the bos.wpars file set must be the same on the arrival system and the departure system.
• The version, release, modification, and fix level of the mcr.rte file set must be higher on the arrival system than on the departure system.
• The 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.
• Devices exported to the WPAR must be available and not exported to any other WPAR on the arrival system.
• Devices allocated to the WPAR must be available on the arrival system.
Note: In addition to the devices test cases, the only additional critical test for static relocation is that the 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. You can select these optional tests in IBM Systems Director WPAR Manager advanced manager interface. When creating a WPAR or editing a WPAR through the Create WPAR or the Edit WPAR wizard, select Advanced Settings. From the Advanced Settings, you can select test options that are taken into account when the WPAR is relocated, regardless of which type of relocate is used. Two managed systems might be compatible for one WPAR and not for another, depending on which WPAR optional tests were selected for each WPAR. Critical tests are always applied in determining compatibility regardless of the WPAR optional test cases.

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 of physical memory 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 xlC.rte file set must be the same on the arrival system and the departure system.

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:

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.

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. Because 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.

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.

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

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

**Unknown**
Indicates that the compatibility analysis was not performed because 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 for the server profile are:

**Update profile is required**
Indicates that compatibility testing was canceled for the managed system because collecting the Extended WPAR inventory has either not been performed or it 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**
A WPAR can be in any of a number of operating states during its life cycle.

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 stops and is removed from the system.

**WPAR relocation domains**
A relocation domain is a grouping of managed systems that you create. The relocation domain identifies a group of systems that serve the same managed systems.

The relocation domain represents the set of WPAR capable systems used to restrict the possible destination of a WPAR during automatic relocation.

WPAR relocation domains are a special type of IBM Systems Director group where the type of the group is WPAR Relocation Domain. Only WPAR-capable systems can be members of this type of group.

A managed system can only be a member of one WPAR relocation domain at a time. If the system already belongs to a WPAR relocation domain, the user is not able to add it to a different relocation domain until the system is removed from the other group.

Automatic relocation for a WPAR is restricted by the relocation domain where the WPAR is deployed. If the system where the WPAR is deployed belongs to a relocation domain, the application looks for other systems in the same domain when relocation is necessary. If a suitable system is not found in the relocation domain, the WPAR is not relocated.

Manual relocation allows the user to relocate a WPAR to a different relocation domain. Since the relocation domain is associated with the system where the WPAR is deployed, moving the WPAR to a system with a different relocation domain results in a change of relocation domains for that WPAR.

**Creating a relocation domain**
To create a relocation domain, perform the following steps:
1. From the IBM Systems Director web interface navigation area, click Navigate Resources.
2. Click Create Group on the navigation area toolbar.
Note: If Create Group is not shown, you can click Action and select the Create Group menu item.
3. Enter the name and description of the Relocation Domain and click Next.
4. Select WPAR relocation domain as the group type, enter the group location, and click Next.
5. Select the members of the relocation domain and click Next. Only WPAR-capable systems can be selected.
6. Click Finish.

Note: To add or remove members from the relocation domain, go to a view where the relocation domain is shown and select Edit.

Manual relocation
WPAR Manager 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 complete these prerequisites, you can decide which WPAR to relocate and to which managed system to relocate it. Use WPAR Manager to help you select the best possible system where the workload partition should be moved based system compatibility. System compatibility status is determined by the type of relocation, status, either static or live, being performed. While selecting a fully compatible system is the preferred option, you can override the compatibility recommendation at your own risk and select any system regardless of compatibility.

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 15

Policy-based relocation
The relocation policy specifies the thresholds of the overall system-supported metrics as well as policy window which is the time window to be used for metric history collected by the WPAR Manager agent, and agent polling time which states how long the agent should wake up to analyze policy violations.

Policy-based relocation is available only for WPARs that meet the following requirements:
• The WPARs are checkpointable.
• The WPARs are marked as policy enabled.
• The WPARs hosting systems belong to relocation domains.
• The WPARs do not have target shares set.
When a system performance state falls outside of the policy-specified thresholds, WPAR Manager will try to find the WPAR that, if relocated, will have the biggest impact to remove the policy violation threshold of that system. The candidate system to relocate the WPAR belongs to the same relocation domain of the system in trouble. Notice that multiple policy violation relocations might be required to achieve the goal of removing the threshold violation.

When a policy violation is reported. The WPAR capable system problem status is set to **Warning** to notify the user that a policy violation has occurred. The system will also be listed in the **Director Health Summary** scoreboard.

Details of the analysis performed to resolve the reported policy violation can be seen in list of **Applied Activities** of the managed system where the violation occurred. There is also a corresponding **Job** in the **Active and Scheduled Jobs** view with the same information.

**Metric policy settings**
To determine the performance state of the managed system, WPAR Manager performs an average of the metric values and compares it to the metric threshold defined in the policy. The policy can be configured with two system metrics, processor and memory use, and with their thresholds.

**Relocation domain policy settings**
A relocation domain group can be associated with one policy at a time. If the group is already associated with a policy then the user will not be able to associate it with another group until the policy is removed from the group.

A policy can be associated with a relocation domain group during the group creation or with an already existing group. After the policy is associated with the group, then WPAR Manager extension starts to monitor the systems of the group for policy violations.

---

**Security for WPAR Manager**

WPAR Manager makes use of the security features provided by IBM Systems Director, WPAR Manager.

For detailed information about IBM Systems Director, WPAR Manager security, see the [Security](Security) topic.

---

**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**

WPAR Manager problems are stored in the IBM Systems Director log files. The following table displays the location and descriptions of these logs.
Table 3. WPAR Manager logs

<table>
<thead>
<tr>
<th>Log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;Director_install_location&gt;/lwi/logs/</code></td>
<td>IBM Systems Director log files</td>
</tr>
<tr>
<td><code>&lt;Director_install_location&gt;/lwi/logs/</code></td>
<td>IBM Systems Director trace log files</td>
</tr>
<tr>
<td><code>&lt;Director_install_location&gt;/WPARManager/</code></td>
<td>WPAR Manager Installer</td>
</tr>
<tr>
<td><code>wpmInstall.log</code></td>
<td></td>
</tr>
</tbody>
</table>

Agent manager logs

When using the Agent Manager embedded with IBM Systems Director, the Agent Manager logs to the IBM Systems Director log files.

WP AR Manager agent logs

The WPAR Agent does not have dedicated log files. It logs to the Common Agent log files.

Table 4. WPAR Manager agent logs

<table>
<thead>
<tr>
<th>Log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/opt/ibm/director/agent/logs/error-log-*</code></td>
<td>Common Agent log files</td>
</tr>
<tr>
<td><code>/opt/ibm/director/agent/logs/trace-log-*</code></td>
<td>Common Agent trace log files</td>
</tr>
</tbody>
</table>

Live relocation logs

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.

In the log file locations listed in the following table, substitute `wparname` with the WPARs name.

Table 5. Live Relocation Logs

<table>
<thead>
<tr>
<th>Log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/var/opt/IBM/WPAR/agent/logs/mcr/</code></td>
<td>WPAR Manager agent log file</td>
</tr>
<tr>
<td><code>wparname.log</code></td>
<td></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 that 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.

**WPAR Manager agent fails to install**
If deploying the WPAR Manager agent package on a managed system fails, ensure that it has at least 200 MB of free space in the `/var` file system. If it does not, execute the following command as root: `chfs -a size=+200MB /var`

**Managed system does not appear in WPAR-capable systems group**
The system with WPAR capabilities does not appear in WPAR-capable systems group.

**Probable cause**
Software inventory and Extended WPAR inventory were not collected, or a failure occurred when collecting them.

**Action**

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

1. If the system does not appear in the list of servers, review *The managed system does not appear in All Operating Systems group* topic.
2. If the Director Common Agent software is not running, restart the agent.
3. Verify that the agent manager is online. If the common agent is not registered to the agent manager, reregister it.
4. Login to the IBM Systems Director console and click View and Collect Inventory. Choose the managed system and collect software inventory from it.
5. Examine Director server log files in the `<Director_install_location>/lwi/logs/` directory for any error messages reported by the USMi discovery service.
6. After the Software Inventory is collected successfully, select the managed system again and from the View and Collect Inventory window, collect WPAR Extended inventory.

**Related information**
- [Troubleshooting connectivity issues](#)
- [Troubleshooting Common Agent remote access](#)

**WPAR inventory collection fails**
WPAR extended inventory fails on a system that has the WPAR Manager agent installed.

**Probable cause**
The WPAR Manager extension is not able to communicate with the WPAR Manager subagents installed on the managed server.

**Action**

1. Log in to the managed system as the root user. If the common agent is not running, restart the agent.
2. Verify that the agent manager is online. If the common agent is not registered to the agent manager, re-register it.

3. Verify that the WPAR Manager subagents are correctly installed by running the following command:

   /opt/ibm/director/agent/runtime/agent/bin/agentcli.sh deployer list bundles | grep wpar

4. Set the logger level com.ibm.director.wparmgt to FINEST, collect WPAR inventory once again and refer to the /opt/ibm/director/agent/logs/trace-log-0.xml log file for any errors reported by the WPAR Manager extension.

Related information

Troubleshooting connectivity issues

**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**

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 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 about 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.

**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 WPARs network. Otherwise, the WPAR might fail to deploy on the arrival system.

Create or deploy operation of an NFS-based WPAR fails because of permissions
The deploy operation on a relocatable NFS-based WPAR fails with this message: AKMWA0002E. The command failed to run on the target system.

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

```
mkwpars: Creating filesystems...
mount: access denied for <NFS server="">
mount: giving up on: <NFS server="">
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 IBM Systems Director server is not able to communicate with the Director Common Agent software installed on the managed system.

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. Right-click the Access property of the system and select Verify Connection. Wait to see if the Access state switches to OK.
2. Ensure that IBM Systems Director can communicate with the agent HTTP port (the default is 9510) and is not blocked by a firewall.
3. Set the log level of com.ibm.usmi.kernel.discovery to FINEST and remove the system from the IBM Systems Director database by removing it from the All Operating Systems group, then, rediscover the system once again from System Discovery window of the IBM Systems Director console and inspect the logs file in the <$Director_install_location>/lwi/logs directory for error messages.
4. Uninstall and reinstall the Director Common Agent software.

Job or task activation fails
If a job or task activation fails, check whether the managed system is online and if you have access.
You can get additional diagnostic information by looking at the task activation properties. View the task activation properties from the IBM Systems Director console by selecting **Task Management** → **Active and Scheduled Jobs** and find the job that has failed from the table. Open the properties for that job and navigate to the **Job steps** panel.

**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="" greater-than signs are enclosed in angular brackets>

**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.

**Command-line Interface**

WPAR Manager functionality can be accessed both from the IBM Systems Director console and from the IBM Systems Director command-line interface (CLI). All WPAR Manager CLI commands are grouped in the wparmgr command bundle.

To obtain a list of all the CLI commands available for WPAR Manager, run the following command:

```
smcli wparmgr/help
```

To obtain a short description of a particular command (for example, startwpar), which includes usage and a brief description of the flags, run the following command:

```
smcli wparmgr/startwpar -h
```

To obtain a long description of a particular command (for example, startwpar), which includes usage, a full description of the flags, and execution examples, run the following command:

```
smcli wparmgr/startwpar --help
```

**Note:** Most commands are executed by a user in the administrator role.

For more information about smcli command, see [smcli - Systems Management command-line interface](http://www.ibm.com/support/docview.wss?uid=swg24031031).
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. Because IBM Systems Director also has an agent, the WPAR Manager agent software might also be referred as a subagent.

agent manager
The agent manager is the IBM Systems Director, WPAR Manager component that provides authentication and authorization services for installed common agents and resource managers. It also maintains a registry of configuration information about Common-Agent managed systems.

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 (2.1.0.0, 2.2.0.0, and so on). 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 might 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 stop and redeploy between compatible managed systems. Application WPARs have less 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.

automatic relocation
Relocation of a WPAR as a result of high processor or memory usage on a managed AIX system. Automatic relocation is controlled by a relocation policy.

averaging period
In a relocation policy, the averaging period is the interval of time over which processor or memory utilization is averaged to determine whether workload on a managed system exceeds the policy threshold. Utilization is averaged over the period to avoid relocation of WPARs in response to brief spikes in workload.
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.

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 is 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 exceeds the policy threshold, indicates that a WPAR is immediately relocated to other systems to mitigate the threshold violation if policy-based relocation is used.

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 before 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 IBM Systems Director process of identifying and registering new managed systems in the environment. Discovery can be initiated by selecting the Inventory and then System Discovery links in the navigation area of the IBM Systems Director, WPAR Manager console.

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

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 WPAR-capable Systems view of the IBM Systems Director Resource Navigator. Using WPAR Manager, WPARs can be created on managed systems, and relocated from one managed system to another.

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

mobility
The ability to relocate WPARs from one managed system to another.

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

policy
See relocation policy.

policy analysis
Analysis of workloads in multiple AIX systems, to determine whether a WPAR can be moved from a busy system to a less busy system for improved performance. Policy analysis is initiated by WPAR Manager in response to a policy violation.

policy metric
A measure of performance for a managed AIX system, used in a relocation policy to determine whether automatic relocation of one or more WPARs is initiated. Policy metrics currently supported by WPAR Manager are processor utilization and memory utilization in a global AIX system.

policy violation
An event that occurs when either average processor or memory utilization on an AIX system exceeds a specified threshold over a specified period. Threshold values and averaging period are specified in a relocation policy in effect for the system. A policy violation results in the initiation of a policy analysis, which might in turn cause one or more WPARs to be automatically relocated.

recovery
A manager started 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). With WPAR Manager 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.

**relocation domain**
A group of AIX systems that can be considered as possible destination systems for automatic WPAR relocation. A relocation domain is defined as a Group in IBM Systems Director. This group is associated with a relocation policy, so that when a policy violation occurs due to heavy workload on a managed system, only the members of the group are evaluated as potential destinations for WPAR relocation.

**relocation policy**
The set of metrics and rules that determine when a WPAR is automatically relocated. A relocation policy sets maximum utilization thresholds for either processor or memory on managed systems, and might be associated with a relocation domain which specifies which systems can be considered as potential destination systems for automatic relocation.

**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.

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

**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. Most traditional system services are 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. In IBM Systems Director, WPAR Manager tasks equate to Jobs, which can be tracked in the Active and Scheduled Jobs table, or on the Applied Activities tab of a WPAR-capable system Properties window.

**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.

**V**
**versioned workload partition**
Versioned workload partitions are system WPARs that provide a different version of the AIX runtime environment than the global system.

**W**
**WPAR Manager agent**
See the definition for agent.

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

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

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

The manufacturer may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to the manufacturer.

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: THIS INFORMATION IS PROVIDED “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. The manufacturer 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 Web sites not owned by the manufacturer are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this product and use of those Web sites is at your own risk.

The manufacturer 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 the manufacturer.

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, IBM License Agreement for Machine Code, 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 products not produced by this manufacturer was obtained from the suppliers of those products, their published announcements or other publicly available sources. This manufacturer has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to products not produced by this manufacturer. Questions on the capabilities of products not produced by this manufacturer should be addressed to the suppliers of those products.

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

The manufacturer's prices shown are the manufacturer'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 the manufacturer, 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. The manufacturer, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. The manufacturer shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

52 IBM Systems: IBM PowerVM Workload Partitions Manager for AIX
If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

### 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

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

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

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

Other company, product, or service names may be trademarks or service marks of others.
### Index

**A**
- accessibility 10
- agent
  - configuring 14
  - installing 12
- agent manager 40
- application mobility
  - configuring 16
  - planning 33

**C**
- checkpoint and restart
  - states 36
- compatibility
  - testing 34
- configuring
  - agent 14
  - application mobility 16
  - logging 15
  - WPAR agent 15

**I**
- installing 10
  - agent 12

**L**
- logical partitions 9

**M**
- managed system
  - defining 20
    - problem determination 43, 44
    - properties 21
  - manual relocation 38
  - mobility
    - compatibility 34, 35

**P**
- planning
  - application mobility 33
  - WPAR Manager agent 9
- policy-based relocation 38
  - group policy settings 39
  - metric policy settings 39
- problem determination
  - deploy 44
  - deploy operation 43
  - managed system 43, 44
  - offline 43
  - secure connection 44
  - properties
    - managed system 21
  - WPAR Manager agent

**R**
- relocation
  - manual 38
  - removing 13
    - WPAR Manager agent 13

**S**
- starting 27
  - WPAR agent 15
- stopping 28
  - WPAR agent 15

**W**
- WPAR
  - states 36
  - WPAR agent 8
    - configuring 15
    - starting 15
    - stopping 15
  - WPAR Manager 10
  - WPAR Manager agent
    - planning 9
    - removing 13