Before using this information and the product it supports, read the information in "Notices" (publib.boulder.ibm.com/infocenter/systems/topic/UNKNOWN_PLUGIN/idmap.xml).

This edition applies to IBM PowerVM Workload Partitions Manager for AIX V2.3 (product number 5765-G83) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2010, 2012.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
# Contents

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

## V2.3.1.1
- What's new in 2.3.1.1 1
- WPAR Manager overview 2
  - WPAR Manager 2.3 Release Notes 4
  - Supported operating environments for WPAR Manager 6
  - Accessibility features for WPAR Manager 6
  - WPAR Manager agent 7
  - WPAR management in a logically partitioned environment 8
- Installing WPAR Manager 9
  - Memory and disk space requirements 9
  - Installing WPAR Manager as an IBM Systems Director Advanced Manager 9
  - Upgrading the WPAR Manager 11
  - Installing the WPAR Manager subagent on the managed system 12
  - Removing the WPAR Manager Advanced Manager 13
  - Removing the WPAR Manager agent 13
  - WPAR Manager license enablement 14
- Configuring WPAR Manager 14
  - Configuring Workload Partitions Manager application with the Setup Advisor 14
  - Configuring the WPAR Manager agent 15
- Configuring the environment for application mobility 17
- Managing workload partitions with WPAR Manager 21
  - Navigate to the WPAR Manager resources 22
  - Managed systems 23
  - Managing WPARs 25
  - Managing WPAR storage devices 36
- Viewing performance metrics for a managed system 42
- Viewing performance metrics for managed systems and WPARs 42
- Application mobility 43
  - Planning for application mobility 43
  - System compatibility 43
  - WPAR relocation domains 46
  - Manual relocation 47
  - Policy-based relocation 47
- Security for WPAR Manager 48
  - Command-line interface 48
  - Troubleshooting WPAR Manager 49
  - Log file locations 49
  - Verifying the agent manager is online 50
  - WPAR Manager problem determination 50
- Glossary for WPAR Manager 56

## Notices 63
- Trademarks 65

## Index 67
About this document

is a platform management solution that provides a centralized point of control for managing workload partitions across a collection of managed systems running the AIX® operating system.

Highlighting

The following highlighting conventions are used in this document:

**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.
V2.3.1.1

(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 website (www.adobe.com/products/acrobat/readstep.html).

Note:
The information in this topic collection applies only to V2.3 or later.

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


Related information:

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

What's new in 2.3.1.1

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

March 2013

The following items summarize the updates in this topic collection:

- Added the locations of the different versions of the topic collections:
  - For information about V2.3 or later, see the IBM Systems Director 6.3 Information Center (http://pic.dhe.ibm.com/infocenter/director/pubs/topic/com.ibm.director.wparmgt.helps.doc/wparlpp-kickoff.html).
  - For information about V2.0, V2.1, or V2.2, see the IBM Systems Director 6.2 Information Center (http://pic.dhe.ibm.com/infocenter/director/v6r2x/topic/com.ibm.director.wparmgt.helps.doc/wparlpp-kickoff.html).
- Corrected the reference to the user interface label: Enable checkpoint in the "Configuring live application mobility for system WPARs" on page 18 topic.
February 2012

The following items summarize the updates in this topic collection:

- Added the topic “Installing WPAR Manager in silent mode” on page 10.
- Updated links to the AIX Information Center throughout the topic collection.

December 2011

WPAR Manager 2.3 provides the following new functions:

- **Enablement to manage WPARs on AIX 6 with Technology level 7 and AIX 7 with Technology level 1:** WPAR Manager 2.3 is capable of managing WPARs on AIX 6 with Technology level 7 and AIX 7 with Technology level 1. For more information about managing WPARs, see “Managing WPARs” on page 25.
- **Support to export or allocate fiber channel storage adapters to WPARs:** In addition to fiber channel and virtual I/O SCSI devices, 2.3 provides support for allocating fiber channel storage adapter to a WPAR. Storage devices controlled by the fiber channel storage adapter could either be used for storage or to host the rootvg of the WPAR. For more information about support to export or allocate fiber channel storage adapters to WPARs, see “Managing WPAR storage devices” on page 36.
- **Support for AIX 5.3 workload partitions for AIX 7:** In addition to AIX 5.2 workload partitions, 2.3 provides management support for AIX 5.3 workload partitions for AIX 7 operating systems. These are system WPARs that provide an AIX 5.3 runtime environment on a system running AIX 7 with Technology Level 1. For more information about AIX 5.3 workload partitions for AIX 7, see “Versioned Workload Partitions” on page 27.
- **Enhancements to the command-line interface (CLI):** 2.3 provides a full set of additional CLI commands. For more information about enhancements to the CLI, see “Command-line interface” on page 48.
- **Accessibility path through CLI:** 2.3 provides a complete CLI as an alternate interface to fully manage WPARs. This is considered the accessibility path for the product. For more information about accessibility with the CLI, see “Command-line interface” on page 48.

**WPAR Manager overview**

The WPAR Manager is an advanced manager for IBM Systems Director which 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, Remove, and so on). A complete task history is available on every action performed on a WPAR, including standard output and error. Graphic reports displaying resource usage and performance metrics 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 must be 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 distributed command-line interface

The following is a summary of the features provided by WPAR Manager that require 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 back up 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 the 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 feature 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 for allocating and exporting virtual I/O SCSI disks 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 if the appropriate versioned WPAR support licensed program software has been purchased and installed on the managed systems where these WPARs need to be created.

**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.

**Support for allocating and exporting fiber channel storage adapters to WPARs**
Support to assign fiber channel storage adapters to WPARs. Disk devices controlled by the adapters can either be used as storage or to hold the rootvg of the WPAR. Installation of AIX 7.1 Service Pack 2 is required for complete support of this feature.

The following is a summary of the feature provided by WPAR Manager that requires AIX Version 7.1 with the 7100-01 Technology Level, or later:

**Support for AIX 5.3 versioned WPARs**
Support to create versioned WPARs from an AIX 5.3 mksysb image if the appropriate versioned WPAR support licensed program software has been purchased and installed on the managed systems where these WPARs need to be created.

**WPAR Manager 2.3 Release Notes**
The WPAR Manager 2.3 Release Notes contain limitation and restriction information, as well as information about WPAR Manager documentation.

**Known issues**
- 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.
- During an overwrite installation or while updating WPAR Manager 2.2.1 to 2.3.0 on an AIX system, the WPAR Manager installer might report that the install was not complete. You can ignore this message. All the errors are related to collisions during the registration of IBM PowerVM Workload Partitions Manager for AIX into the Software Vital Product Data (SWVPD) registry. These errors have no functional impact.

**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.
- Static relocation of a system WPAR 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.
- During the discovery and setup of a WPAR-capable system, collecting All Inventory from IBM Systems Director does not collect WPAR Extended Inventory. WPAR Extended Inventory must be collected in a separate step during the setup. Once a system has been recognized as WPAR-capable system, the need to execute extended WPAR inventory individually no longer applies and WPAR Extended Inventory is collected as part of the All Inventory collection task.
- 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 file systems of type directory. These WPARs can be created through the command-line and managed by WPAR Manager.
- Only JFS2 with extended attributes v2 and NFS file systems are supported for live mobility of WPARs.
- For WPARs that own their rootvg, live relocation of applications running with a mmap area created from a file descriptor opened with the `O_NSHARE` or `O_RSHARE` flags set will fail. To prevent DB2® from falling into this scenario, the sync point manager name configuration parameter `SPM_NAME` must be unset by running the following command: `db2 update dbm cfg using SPM_NAME NULL`.
- In order to successfully perform live relocation of an NFS-based WPAR, the NFS server cannot be running on either the departure or the arrival system.

**Documentation and purchase information**

Additional information about the IBM PowerVM Workload Partitions Manager for AIX is available in the IBM Systems Director Information Center.

Detailed information about workload partitions and versioned WPARs is available in the AIX 7.1 Information Center.

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

WPARs and application mobility are supported on AIX 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 with Technology Level 6, 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. To manage an earlier AIX Technology Level, update the WPAR Manager agent software to the version that matches the WPAR Manager version in use. Failing to update the WPAR Manager agent that is installed on the managed system could result in unpredictable behavior and prevents you from using the WPAR properties and capabilities that are available in the latest version of WPAR Manager. 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 with Technology Level 4</td>
<td>4.2.2.0</td>
</tr>
<tr>
<td>AIX Version 6 with Technology Level 5</td>
<td>4.2.2.0</td>
</tr>
<tr>
<td>AIX Version 6 with Technology Level 6</td>
<td>4.2.4.0</td>
</tr>
<tr>
<td>AIX Version 6 with Technology Level 7</td>
<td>6.1.7.0</td>
</tr>
<tr>
<td>AIX Version 7.1</td>
<td>4.3.0.0</td>
</tr>
<tr>
<td>AIX Version 7 with Technology Level 1</td>
<td>7.1.1.0</td>
</tr>
</tbody>
</table>

Note: On all systems before AIX Version 6 with Technology Level 4, you must update the Director agent to 6.1.0.4 or later.

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 full function WPAR Manager command-line interface (CLI) is now the preferred path to full application accessibility. The existing graphical interface technology stack does not provide support for newer accessible mechanisms such as WAI-ARIA attributes prescribed by the latest versions of accessibility standard checklists. A complete mapping of functions has been implemented using the IBM Systems Director smcli command extensions for the WPAR Manager application. For more information on using the CLI, see the WPAR Manager command-line interface section in the InfoCenter, "Command-line interface" on page 48.
The graphical interface for the IBM Workload Manager plug-in for IBM Systems Director continues to support many of the accessibility features that are supported in IBM Systems Director, but the fully accessible path is provided by the WPAR Manager CLI.

When using JAWS screen reader with IBM Workload Manager graphical user interface, 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.

**Related concepts:**
[“Command-line interface” on page 48](#)

**Related information:**
[Accessibility features for IBM System Director](#)
[smcli - Systems Management command-line interface](#)

**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 manage earlier AIX technology levels, you need to update the WPAR Manager agent software to the version that matches the WPAR Manager version in use.

Failing to update the WPAR Manager agents that are installed on the managed systems could result in unforeseen behaviors and prevents you from using the WPAR properties and WPAR capabilities that are available in the latest version of WPAR Manager.

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 provides the checkpoint capabilities, restart capabilities, and live relocation capabilities. Prior to AIX 7 with Technology Level 1, the MCR kernel extension file set was a part of the WPAR Manager agent, and was installed as part of the agent installation. However, starting with AIX 7 with Technology Level 1, the MCR kernel extension file set is installed as part of the AIX operating system and is no longer included with the WPAR Manager agent. Because MCR is an AIX kernel extension, it is closely tied to the AIX technology level that is 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 allows for management of all newly supported WPAR properties and operations delivered in the latest WPAR Manager version.

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.

**WPAR 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.

WPAR Manager does not recognize HMC or Integrated Virtualization Manager (IVM) configurations. If you are using the HMC or IVM to manage your environment, and you have created a WPAR within the logical partitions on your systems, you 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.
Installing WPAR Manager

You must install the WPAR Manager plug-in on the IBM Systems Director management server that is running on any of the following operating systems: 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 concepts:
- “Upgrading the WPAR Manager” on page 11

Related information:
- Installing IBM Systems Director

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 memory requirements for other software that is running on your system or disk space requirements for other software installations.

<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             |

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.

Ensure that you have the authority to complete the installation:

• For the Microsoft Windows operating system, administrator authority is required.
• For the AIX or Linux operating system, root authority is required.

Note: To install WPAR Manager in accessible mode, see “Installing WPAR Manager in silent mode” on page 10.

Complete the following steps to install WPAR Manager as an IBM Systems Director Advanced Manager in silent mode:

1. Log in to the system with the required authority level.
2. If you are installing from media, insert the media containing the WPAR Manager into the media drive. If you are installing from a download, copy the installer to the target system.
Note: If you are installing from media for the AIX or Linux operating system, you can mount the media drive by 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 the installation files in a WPARMgr subdirectory.

5. Start the installation of WPAR Manager by running the following command from the subdirectory that contains the installer:
   
   - For AIX or Linux: `WparMgrSetup.sh`
   - For Windows: `WparMgrSetup.bat`

By default, the installation uses the graphical interface mode in the Windows environment and the console in the AIX and Linux environments. Use the `-i` option to specify the console mode, for example, `WparMgrSetup.bat -i console`.

### Installing WPAR Manager in silent mode

If you install WPAR Manager in silent mode, no status indication is displayed.

Ensure that you have the authority to complete the installation:

- For the Microsoft Windows operating system, administrator authority is required.
- For the AIX or Linux operating system, root authority is required.

Complete the following steps to install WPAR Manager as an IBM Systems Director Advanced Manager in silent mode:

1. Log in to the system with the required authority level.

2. If you are installing from media, insert the media containing the WPAR Manager into the media drive. If you are installing from a download, copy the installer to the target system.

   **Note:** If you are installing from media for the AIX or Linux operating system, you can mount the media drive by 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 installation archive to a local directory.

4. Unzip or untar the archive. This action creates a WPARMgr subdirectory that contains the installation files.

5. Issue the following command to install the WPAR Manager in silent mode:
   
   - AIX or Linux: `WparMgrSetup.sh -i silent -f response_file`
   - Windows: `WparMgrSetup.bat -i silent -f response_file`

   where `response_file` contains the path to the response file. The response file can be generated from a previous installation in console or GUI mode. You can also create a response file by creating a text file that includes the following options:

   ```
   LICENSE_ACCEPTED=true|false
   RESTART_DIRECTOR=true|false
   ```

   **LICENSE_ACCEPTED**

   Set this option to `true` to indicate that you accept all license agreements. The silent installation cannot install WPAR Manager unless this option is set to `true`.  

**RESTART DIRECTOR**
Set this option to `true` if you want IBM Systems Director to be restarted automatically after the installation of WPAR Manager. Set this value to `false` if you do not want to restart IBM Systems Director automatically.

IBM Systems Director must be restarted before using WPAR Manager, but you are not required to restart IBM Systems Director when you perform the installation. You can manually restart IBM Systems Director at a later time.

**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.

**Table 3. The major WPAR Manager releases and the corresponding Director releases**

<table>
<thead>
<tr>
<th>WPM® version</th>
<th>Director version</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>6.1.2</td>
</tr>
<tr>
<td>2.2.1</td>
<td>6.2.1</td>
</tr>
<tr>
<td>2.3</td>
<td>6.3</td>
</tr>
</tbody>
</table>

Upgrading involves moving up from one release to the next while preserving all data and configuration of WPAR Manager and Director. You can only perform an upgrade to the next successive release. Therefore, you cannot upgrade from WPAR Manager 2.1 to 2.3 without first upgrading to 2.2.1. You cannot uninstall an upgrade after it is installed.

**Upgrading from WPAR Manager 2.1 to WPAR Manager 2.2.1**
To upgrade to WPAR Manager 2.2.1, you must first migrate from Director 6.1.2 to 6.2.1. To perform a migration installation, run the Director 6.2.1 installer on the system that has Director 6.1.2 installed. This preserves all data from Director 6.1.2. After you have migrated to Director 6.2.1, WPAR Manager 2.1 is disabled. You must run the WPAR Manager 2.1 uninstaller to remove it. When running the uninstaller, specify that you want existing WPAR Manager data to be preserved. After WPAR Manager 2.1 is uninstalled, run the WPAR Manager 2.2.1 installer. After completion, you have successfully upgraded all of your existing data and configuration to Director 6.2.1 and WPAR Manager 2.2.1.

**Upgrading WPAR Manager 2.2.1 to WPAR Manager 2.3**
To upgrade to WPAR Manager 2.3, you must first migrate from Director 6.2.1 to 6.3. To perform a migration installation, run the Director 6.3 installer on the system that has Director 6.2.1 installed. The migration preserves all data from Director 6.2.1. After you have migrated to Director 6.3, WPAR Manager 2.2.1 is disabled. Run the WPAR Manager 2.3 installer to upgrade the existing WPAR Manager 2.2.1 install. After completion, you have successfully upgraded all of your existing data and configuration to Director 6.3 and WPAR Manager 2.3.

**Note:** The Derby database is no longer supported in Director 6.3; therefore, a Director 6.2.1 instance configured with Derby is migrated to DB2.

Prior to WPAR Manager 2.3 release, WPARs with storage adapter support that were created from the AIX command line could not be managed by the WPAR Manager application.
After migrating from WPAR Manager 2.2.1 to WPAR Manager 2.3, it is necessary to rerun Extended WPAR Inventory on any managed system that is hosting a WPAR of this type. This action will allow for correct management of this certain class of WPARs.

**Related concepts:**

"Installing WPAR Manager" on page 9

### 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, starting with AIX 7 with Technology Level 1, the mcr.rte file set is already installed with the AIX operating system.

**Related information:**

"The managed system does not appear in All Operating Systems group” on page 51

### 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
```

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**

Manual installation of the WPAR Manager agent is not recommended because it prevents the Director Server from automatically detecting when the agent needs an update. It is recommended that you install the WPAR Manager agent through the Director Server. However, if you want to install the WPAR Manager agent manually, review the following information.

The following files are prerequisites for installing the WPAR Manager agent 2.4:
- `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:
   - AIX or Linux: `<Director_install_location>/WPARManager/uninstall/uninstallWPM.sh`
   - Windows: `<Director_install_location>/WPARManager/uninstall/uninstallWPM.bat`

   By default, the uninstaller runs in the same mode as the installer, that is, if the installer ran in console mode the uninstaller will also run in console mode. You can explicitly set the mode with the `-i` flag. For example, to run the uninstall in silent mode execute the following command:
   ```sh`
   <Director_install_location>/WPARManager/uninstall/uninstallWPM.sh
   -i silent -f <response_file>
   ```

**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`

**Note:** The `mcr.rte` file set is only deployed by the WPAR Manager agent in AIX versions prior to AIX 7 with Technology Level 1. Thus, you must manually remove the `mcr.rte` file set in AIX versions prior to AIX 7 with Technology Level 1.
Example

To remove all the WPAR Manager agent file sets on an AIX operating system with a version earlier than AIX 7 with Technology Level 1 run the installp command, as follows:

installp -u wparmgt.agent.rte mcr.rte

Example

To remove the WPAR Manager agent file set on an AIX system running AIX 7 with Technology Level 1 or later, run the installp command as follows:

installp -u wparmgt.agent.rte

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 90 days.

The Plug-in tab on the IBM Systems Director Home page displays the status of the WPAR Manager temporary license and the number of days that remain before the temporary license expires. Once a permanent license for the product is purchased and installed, the notification regarding the temporary license is removed.

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 follow:
- AIX or Linux: <media root>/WPARMgr/WparMgrKey.sh
- Windows: <media root>/manager/Windows/WparMgrKey.bat

Configuring WPAR Manager

The WPAR Manager application environment requires certain postinstallation configuration tasks to be performed prior to the use of the environment. You can perform these initial postinstallation tasks by using the WPAR Manager Setup Advisor.

If you plan to utilize the application mobility functionality in the WPAR Manager, you must also configure the environment for WPAR mobility after the application installation.

Configuring Workload Partitions Manager application with the Setup Advisor

You can use the Workload Partitions Manager Setup Advisor to guide you through the required postinstallation configuration tasks.

There are a number of tasks that must be performed after the WPAR Manager application plug-in has been installed in IBM Systems Director.

The Setup Advisor can be launched from the Plug-ins tab on the IBM Systems Director 6.3 Home page after Workload Partitions Manager 2.3 has been installed. Before the configuration occurs, a message stating that Additional configuration
is required. WPAR capable systems have not been identified will be displayed below the **Home** page entry for the WPAR Manager 2.3 plug-in.

You can also access the Setup Advisor from the WPAR Manager summary page

1. Click **Setup Advisor** to launch the Setup Advisor wizard.
2. Perform the following tasks in the Setup advisor wizard:

   **Discovery**
   Launches the System Discovery task in the IBM Systems Director and assists you in discovering any AIX operating system-based systems on which you may want to manage WPARs.

   **Get access**
   Guides you through the task of requesting access to the systems you have previously discovered so that you can perform administrative tasks on them in IBM Systems Director.

   **Install agents**
   Installs the WPAR Manager subagent software on each system so that you can manage workload partitions on previously discovered and accessed systems.

   **Inventory**
   Provides information on the process of creating an inventory of the software installed on previously discovered systems and identifies these systems as WPAR capable.

   WPAR capable systems are systems that have the requisite levels of the AIX operating system and WPAR Manager subagent software installed.

   **Settings**
   Allows you to launch the WPAR Manager Application Configuration portlet and to override certain application wide configuration settings, if necessary.

After all the necessary configuration steps have been completed, the WPAR Manager application is identified as configured and as capable of managing WPARs on the identified WPAR-capable systems.

**Related tasks:**
[“WPAR Manager summary page” on page 22](#)

### 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 `/opt/ibm/director/agent/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:

```bash
# cd /opt/ibm/director/agent/runtime/agent/toolkit/bin
# ./configure.sh -amhost <agent-manager.yourdomain.com> -passwd <AMRegPassword>
```

The options for the `configure.sh` script are:

- `-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)

-wsweb <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 -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 -force flag to re-configure the WPAR Manager agent.
• All ports specified for use by the WPAR Manager agent (\(-port, -jport, -nport, -wport, -wsport\)) are distinct and not in use.

Starting and stopping the WPAR Manager agent
Use the \texttt{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{/opt/ibm/director/agent/logs/error-log-0.html} 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{/opt/ibm/director/agent/runtime/agent/bin/endpoint.sh start}.
• To stop the WPAR Manager agent, use the following command:
  \texttt{/opt/ibm/director/agent/runtime/agent/bin/endpoint.sh stop}.
• To restart the WPAR Manager agent, use the following command:
  \texttt{/opt/ibm/director/agent/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{/opt/ibm/director/agent/logs/} directory. You can configure logging in the \texttt{/opt/ibm/director/agent/conf/overrides/logging.properties} file.

To change the default settings for WPAR Manager agent logging, perform the following steps:
1. Open the \texttt{/opt/ibm/director/agent/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{/opt/ibm/director/agent/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 21
- "Manual relocation" on page 47
- "Application mobility" on page 43

**Related tasks:**
- "Creating a WPAR that supports live relocation" on page 25

**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.

**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 checkpoint 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.

**Note:** In order to successfully perform live relocation of NFS-based WPARs, the NFS server cannot be running on either the departure or the arrival system.

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:
   ```bash
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:
   ```bash
   mount /wparsfs
   ```

3. Create a directory called wparhostname on nfssrv1.yourdomain.com by running the following command:
   ```bash
   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:
   ```bash
   # 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. It can either be a virtual local adapter-attached disk device or a virtual shared adapter-attached disk device. When creating a WPAR that owns its volume group, you must specify at least one rootvg disk device using either the `wparmgr` or `mkwpar` command from the `smcli` command line or one of the WPAR Manager Create WPAR wizards (Create WPAR Wizard or the Create Versioned WPAR wizard).

When you use one of the Create WPAR wizards to create a rootvg WPAR, the Device Control step allows you to specify one or more disk devices or one or more storage adapters and one or more adapter-attached disk devices to be used by the WPAR for its root volume group. If selecting disk devices individually, click **Add** on the **Devices** tab panel to view and select the desired storage devices to be assigned to the WPAR. If selecting disk storage using storage adapters, click **Add Adapters** on the **Adapters** tab panel to view and select the desired storage adapter for allocation.

After selecting one or more devices (using the Device tab) or one ore more storage adapters (using the Adapters tab), you must use the pull-down selector in the rootvg column to specify that a given disk device is intended to be a rootvg device. Only disk devices can be selected as rootvg devices. If the disk previously contained any volume group data, you must select **Overwrite existing volume group on rootvg devices**.
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 (clirc.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/nfshostkey -l` command lists the keytab entry for the NFS server.
- The `/usr/sbin/chnfsrtd` command lists the mapping between the Kerberos realm and the NFS domain.
- The `lssrc -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/departurenode.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/departurenode.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 must 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 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 17

**Navigate to the WPAR Manager resources**

You can navigate to the WPAR Manager resources in three ways by using the WPAR Manager summary page, the Resource Explorer task in IBM Systems Director or through the Workload Partitions and Hosts view.

**WPAR Manager summary page**

You can use the **WPAR Manager summary** page to monitor and manage WPAR resources, set application configuration settings, run the Setup Advisor, and view licensing and version information.

To launch the WPAR Manager summary page, perform the following steps:

1. In the IBM Systems Director navigation area, click **System Configuration** to expand.
2. Click **WPAR Manager**.

   You can also access **WPAR Manager summary** page from the **Plug-ins** tab on the IBM Systems Director **Home** page by scrolling to the bottom of that page and selecting the **WPAR Manager** link.

**Related concepts:**

“Configuring Workload Partitions Manager application with the Setup Advisor” on page 14

**Resource Explorer task**

You can use the Resource Explorer task in IBM Systems Director to access WPAR Manager resources.

When WPAR Manager is installed, a set of WPAR Manager groups are created containing all discovered resources that WPAR Manager can manage. As new supported resources are discovered, they are added to the appropriate groups.

To access WPAR Manager resources using the IBM Systems Director Resource Explorer task, perform the following steps:

1. In the left-hand navigation area of IBM Systems Director, click **Resource Explorer**.
2. Click **Workload Partitions Groups**.

**Workload Partitions and Hosts view**

When WPAR Manager is installed, a Workload Partitions and Hosts view is created. This view provides a tree view of all WPARs and their hosting systems.

To access WPAR Manager resources using the IBM Systems Director Resource Explorer task, perform the following steps:

1. In the left-hand navigation area of IBM Systems Director, expand Inventory.
2. Expand Views.
3. Click **Workload Partitions and Hosts** view.

This view can also be accessed from the WPAR Manager summary page.
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 also discover all systems within a specified IP address range.
2. Log in to the IBM Systems Director, and select Inventory.
3. Select System Discovery to launch the IBM Systems Director System Discovery portlet where you can discover system resources to be managed by IBM Systems Director.
4. Enter an IP address or a range of IP addresses, as appropriate, and select Discover Now. The system discovery action starts and as the system or systems are discovered, they are listed in the table on the page.
5. 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. For each system discovered in the previous step and listed in the Discovered Manageable Systems table, right-click No access under the Access column in the table and select Request Access. The IBM Systems Director Request Access portlet is launched.
   b. Enter a valid administrator user name and password for the selected system you are requesting access for, and then click Request Access. If you provide the correct credentials, the Request Access portlet closes, you return to the previous page, and the Access state of the discovered system shows OK.
6. Install the WPAR Manager subagent on each system.
   Now that you have discovered and installed 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. For more information about installing the WPAR Manager subagent, see “Using IBM Systems Director to install the WPAR Manager agent on the managed system” on page 12.
WPAR Manager provides an integrated step-by-step procedure to configure managed systems and other settings in the application. For more information about configuring managed systems, see the Configuring Workload Partitions Manager application with the Setup Advisor or go to the Plug-ins tab on the IBM Systems Director Home page and click the link to launch the WPAR Manager Setup Advisor.

**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 installed with the WPAR Manager advanced manager plug-in.

1. From IBM Systems Director, select **Resource Explorer**. This allows you to navigate to the **Resource Explorer** 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 a list of properties and other detailed information associated with the managed system. By using the **Resource Properties** view, you can access information related to troubleshooting and other important details about the managed system.

**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**.
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.

1. From the IBM Systems Director Home page, select the Plug-ins tab.
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 17
“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 must have access to the storage disk that is assigned to the WPAR.

Storage adapters and storage devices can be configured in the device control panel of the Create WPAR wizard. To create a WPAR that owns its own root volume group, at least one of the disks attached to a Fibre Channel storage adapter (a virtual local adapter-attached device) or at least one of the disks associated with a virtual shared adapter must have a device control setting configured as rootvg. It is not possible to modify the WPAR after creation and change the designation of the device control to rootvg. This must be done when the WPAR is created.

Relocation of a WPAR that owns its own root volume group and has a Fibre Channel storage adapter exported to is not possible. Only WPARs that own their own root volume group residing on Fibre Channel or virtual SCSI devices explicitly exported to the WPAR can be relocated.

**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 WPARs with remote /usr and /opt files systems can cause space constraints on the NFS server. Therefore, it is recommended that you mount them locally as read-only file systems. Mounting the file systems locally reduces the file system size requirements on the NFS server that hosts the file systems of the WPAR. For example, a WPAR that is created by 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 and the /opt file systems are configured remotely, the minimum space required increases to approximately 2 GB per WPAR.

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 the 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 files systems by 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
   /wpasename
   /home
   /tmp
   /var
```

**Related tasks:**
- “Creating a WPAR that supports live relocation” on page 25

**Working with WPARs created from the AIX command line:**

WPARs created from the AIX 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 AIX command line fails if the WPAR is relocated from the WPAR Manager user interface and vice versa.

**Related information:**
- [Configuring system WPARs (AIX information center)](Configuration/topic/Configuring-system-WPARs-AIX-information-center.htm)
- [Configuring application WPARs (AIX information center)](Configuration/topic/Configuring-application-WPARs-AIX-information-center.htm)

**Versioned Workload Partitions:**

Versioned workload partitions are unshared or detached system WPARs that provide a different version of the AIX runtime environment than the version running in the global system. Versioned workload partition support for AIX 7.1 is provided by separately purchased licensed programs, which must be installed on each global workload partition environment where this support is required.

Currently, licensed programs that provide AIX version 5.2 and AIX version 5.3 WPAR runtime environments are available. For more information about hardware and software prerequisites for either the IBM AIX 5.2 Workload Partitions for AIX 7 licensed program or the IBM AIX 5.3 Workload Partitions for AIX 7 licensed program, see [Versioned workload partitions in the AIX 7.1 Information Center](Versioned-workload-partitions-in-the-AIX-7.1-Information-Center.htm).

The IBM PowerVM Workload Partitions Manager advanced manager plug-in for IBM Systems Director provides support to manage versioned WPARs only if the following conditions are met:

- The appropriate licensed program for the alternative runtime environment has been purchased and installed on the managed systems where this support is needed.
- All hardware and software prerequisites for the specific purchased versioned workload partition support product identified in the product Information Center documentation are met.
- The current version of the WPAR Manager agent 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 back up, restore, clone, and relocation. The runtime environment of a versioned WPAR is different from the runtime environment of the global environment. Hence, synchronization of software levels between versioned WPARs and the global environment is not supported.

Notes:

- After installing the separately purchased AIX versioned WPARs licensed program, rerun the IBM Systems Director software inventory task on any managed systems recently updated with the new software support for versioned WPARs. This task identifies the newly updated managed systems as versioned WPAR-capable systems to the WPAR Manager software.
- Live relocation of AIX 5.2 versioned WPARs requires the installation of additional software within the AIX 5.2 versioned WPAR before you can perform live mobility.

For more information on performing live mobility with versioned WPARs, including details about the additional software that must be installed within the AIX 5.2 versioned WPAR, see Additional software required for Live Application Mobility of versioned WPARs 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.

The Create Versioned Workload Partition action can also be initiated from any other view where versioned WPAR capable systems are displayed, for example, Workload Partitions and Hosts.

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 Resource Explorer to open the Resource Explorer 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 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 program, then you must rerun the IBM Systems Director software inventory task on the appropriate managed systems. This will appropriately inventory the newly installed licensed program and identify the managed systems as version WPAR capable managed systems.
   The managed systems that are capable of hosting versioned workload partitions are listed. The level or levels of versioned WPARs supported on the managed systems are identified in the versioned column of the table.
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, but it has an additional panel for collecting the information required to create a versioned WPAR.

6. Follow the instructions to complete the wizard and create the versioned workload partition on the selected managed system.

**Note:** When selecting an mksysb image to create the versioned WPAR, ensure that the mksysb image of AIX version matches the version supported by the versioned WPAR licensed program support that is installed 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.

Versioned WPARs are capable of supporting both static and live relocation. Certain levels of versioned WPARs have specific prerequisite requirements that must be met before they can successfully be relocated using live relocation.

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 WPARs must have valid network configurations. 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 and 5.3 versioned WPARs requires the installation of additional software within the versioned WPAR before live mobility can be attempted. For more information about preparing a versioned WPAR for live mobility, see the [Additional software required for Live Application Mobility of versioned WPARs](https://www.ibm.com) in the IBM Workload Partition for AIX Information Center.

**Related information:**

- [Creating a versioned WPAR](https://www.ibm.com)

**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.

**Viewing or modifying WPAR properties**

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

WPAR definitions, also known as undeployed WPARs, can have any of the properties associated with the WPAR definition modified during the process of deployment by using the **Deploy Workload Partition Definition** wizard.

If the WPAR is currently deployed on a managed system, you can modify the properties of the WPAR. However, you can modify only selected properties of the WPAR configuration, depending on the state of the WPAR.

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

1. From the console navigation area, select **Resource Explorer**.
2. In the table, click **Workload Partitions Groups**.
3. In the table, click one of the workload partition groups, such as **All Workload Partitions**.
4. Select the WPAR you want to view or modify from the list.
5. Click **Actions**, and select **Edit**.
   - The WPAR Manager Modify Workload Partition wizard is displayed.
   - Depending on the state of the deployed WPAR, certain attributes of the WPAR can be changed and other cannot.
6. Click **OK** to submit the changes to the WPAR.

The edit action can also be initiated from any other view where the WPARs are displayed, for example, **Workload Partitions and Hosts**.

Viewing or modifying WPAR definition properties is carried out as part of the definition deployment process. To deploy WPAR definition properties, complete the following steps:

1. From the console navigation area, select **Resource Explorer**.
2. Navigate to any of the views displaying WPARs, such as WPAR groups, Workload Partitions and Hosts, and so on.

3. Select the WPAR definition you want to view or modify during deployment from the list.

4. Click **Actions**, and select **Deploy**.
   
   The WPAR Manager **Deploy Workload Partition Definition** wizard is displayed.

5. To view the WPAR definition attributes, navigate through the panels without making any changes. Click **Cancel** when you complete viewing the WPAR definition attributes.

6. To make changes to the WPAR definition attributes and deploy the WPAR created from the changed definition, navigate through the panels and make the required changes. Click **Finish** to create and deploy the WPAR from the definition changes onto the specified managed system.

The deployment action can also be initiated from any other view where WPAR-capable systems are displayed, for example, Workload Partitions and Hosts.

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

Although the WPAR Manager provides a graphical interface and an IBM Systems Director distributed command-line interface extension to modify the configuration of WPARs, you can also use the AIX command line on the managed system that hosts the WPAR to modify a given WPAR.

When a change is performed through the AIX command line hosting system using the base AIX `wpar` commands, the WPAR Manager discovers the changes after a short delay. Later, the IBM Systems Director database is updated to reflect the new configuration.

WPAR definitions can only be viewed or modified by using the WPAR Manager graphical interface or the WPAR Manager extensions to the IBM Systems Director distributed command line subsystem.

**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.

**Maintenance**
The WPAR has been started in maintenance mode and networks that are associated with the workload partition are not configured. The only access to the workload partition is from the global system as long as the WPAR is in maintenance mode.

**Backing up WPARs**
The Back up operation in WPAR Manager creates a backup image of a selected WPAR.

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 restwpar command or the WPAR Manager user interface.

The following are restrictions for the backup 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 required 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 Resource Explorer.
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.

    The backup action can also be initiated from any other view where the WPARs are displayed, for example, **Workload Partitions and Hosts**.

**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 **Resource Explorer**.
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.

    The restore action can also be initiated from any other view where WPAR-capable systems are displayed, for example, **Workload Partitions and Hosts**.

**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 **Resource Explorer**.
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.

   The start action can also be initiated from any other view where WPARs are displayed, for example, Workload Partitions and Hosts.

**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 Resource Explorer.
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.

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

**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 Resource Explorer.
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.

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

**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 the specified external device.

To clone a WPAR, complete the following steps:
1. From the IBM Systems Director web interface navigation area, click Resource Explorer.
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 clone.
5. Click Actions, and select Clone.
6. From the Clone page, specify the clone options for the WPAR, and click OK.

The clone action can also be initiated from any other view where WPARs are displayed, for example, Workload Partitions and Hosts.

**Note:** When the WPAR contains a rootvg device, you can only clone the WPAR that is in an active state.

**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 **Resource Explorer** 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 **Deploy Workload Partition** wizard is launched.
6. Select the target system where the workload partition definition must be deployed and follow the steps on the wizard.
   The values from the workload partition definition are shown in the wizard and can be modified as required before the modified definition is used to create the new WPAR on the selected managed system. As part of the definition deployment process, after the new WPAR is created from the WPAR definition, the WPAR definition is removed from the WPAR Manager database.

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.

Storage devices can be allocated individually to a WPAR by the global administrator, or starting with WPAR Manager 2.3, as a group of devices connected to a fiber-channel storage adapter by allocating the storage adapter to the workload partition. The advantage of allocating devices by using the storage adapter interface is that once allocated and exported to the WPAR, the WPAR administrator can manage the pool of devices as needed in the WPAR.

Storage devices or storage adapters are allocated to a WPAR when you assign the device to the WPAR while the WPAR is being created or when you modify an
inactive WPAR. The storage devices or storage adapters are exported to the WPAR
when the WPAR is started, or automatically exported if you allocate the storage
device to a WPAR that is already active.

Before exporting storage adapters or individual storage devices to a WPAR, note
the following prerequisites and restrictions:

- Fibre channel storage adapters and adapter-attached devices must be configured
  in the managed system global environment before adapters and adapter-attached
  storage devices can be allocated to WPARs. The Adapters tab on the Device
  Control page of the Create and Deploy workload partition wizards and the
  Device Control tab in the Modify workload partition wizard are not displayed
  if storage adapter support is not configured for the managed system that hosts
  or will host the WPAR.
- To assign storage devices individually to a WPAR, the storage devices must first
  be configured on the managed server by the LPAR or system administrator as
  either virtual shared adapter attached Fibre Channel or SCSI devices (disk or
  tape).
- You can only allocate storage devices to system WPARs. Storage support is not
  applicable to application WPARs.
- Support for virtual local storage adapters is not available for versioned WPARs.
  Only virtual shared devices can be allocated or exported to versioned WPARs.
- You cannot export storage adapters or virtual shared storage devices to a WPAR
  if the adapter or devices are in use in the global environment.
- You cannot export a storage adapter (and its attached devices) or a virtual
  shared storage device to multiple WPARs. For more information, see the
  glossary entries for allocate storage and export storage.
- Adapter multipath support provides for an environment where a pool of storage
devices can be controlled by more than one parent adapter. In a configured
multipath environment, it is recommended that all adapters controlling a given
pool of storage devices are allocated or exported to the same WPAR.

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 19

Exporting a virtual shared storage device to an existing WPAR
You can allocate virtual shared storage devices to an existing workload partition
(WPAR).

To export a virtual shared 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 the IBM Systems Director console, select Resource Explorer. Select the
   table link for Workload Partitions Groups, and then select the link in the table
   for All System Workload Partitions to display a list of system WPARs.
3. Right-click the WPAR and select Edit to launch the Modify Workload Partition
   wizard.
   If the managed system that hosts the WPAR is configured with storage support
   (either virtual shared device support or virtual local adapter support), a Device
   Control tab is present in the Modify Workload Partition wizard.
4. The **Device Control** tab, if present, displays one or two subtabs, **Devices** and **Adapters**, depending on the storage support configured in the global environment.

5. On the **Devices** subtab, click **Add**. The **Devices for export** page is displayed. This page shows the available virtual shared storage devices on the managed system. In this page, 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. Select the check box next to each device you want to export to the WPAR.

7. Click **Add** to move the devices to the selected box.

8. Click **OK** to allocate the selected storage devices to the WPAR and to close the **Add Devices for Export** window.

9. Click **OK** in the **Modify Workload Partition** wizard to submit the selected changes to the WPAR. The edit action can also be initiated from any other view where WPARs are displayed, for example, **Workload Partitions and Hosts**.

If the **Modify WPAR** action is performed on a WPAR in the **Defined** state, the virtual shared storage 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, the WPAR is successfully started but an error message is displayed.

If the **Modify WPAR** action is performed on a WPAR that is started and in the **Active** state, the virtual shared storage devices automatically export if they are otherwise not in use. For devices exported to a WPAR that is started and in the **Active** state, you must run the `cfgmgr` command inside the WPAR before the devices are available for use. The `cfgmgr` command is automatically run when a WPAR is started.

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

Use the **Create Workload Partition** wizard or the versioned equivalent in WPAR Manager to export a virtual shared storage device to a new workload partition (WPAR).

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

1. Log in as the root user to the system where WPAR Manager is installed.

2. In the IBM Systems Director, select **Resource Explorer**.

3. Select **Workload Partitions Groups** in the groups table. Select either the WPAR-capable systems link or the versioned WPAR-capable systems link in the **Workload Partitions Groups** table depending on the type of WPAR that you would like and are capable of creating.

   Select a managed system from the list where you would like the workload partition to be created.

4. Right-click the managed system and select **Workload Partitions Management** from the menu, and select the appropriate **Create Workload Partitions** wizard from the cascading submenu.

5. On the **Devices** tab in the **Device control** page, click **Add**. The **Devices for export** page is displayed. This page shows the available virtual shared 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. Select from the devices list the storage devices that you would like to allocate and export to the WPAR being created. To move the devices to the selected box, click Add.

7. Click OK to add the selected storage devices to the list of devices that are allocated to the WPAR and to close the Add Devices for Export page.

By default, the device is considered a standard storage device. If you are including the virtual shared storage device as part of the root volume group, select the rootvg option in the rootvg column. Only devices of type disk can be part of the root volume group.

Complete the remaining wizard as desired or needed.

8. When you are finished working in the wizard, click Finish to close the wizard and start the process of creating the specified WPAR on the selected managed system.

A new WPAR in the Defined state with the selected virtual shared storage 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, the WPAR successfully starts but an error message is displayed.

Exporting a virtual local storage adapter to an existing native system WPAR

The storage adapter and its attached devices are exported for the use of a WPAR when the WPAR is started or restarts if not in use in the global environment or by any other active WPAR. Use the Edit action in WPAR Manager to allocate configured storage adapters to an existing native system WPAR. Storage adapter support is not available for application WPARs or for versioned system WPARs.

To export a virtual local storage adapter and its devices to an existing WPAR by using the Edit action, complete the following steps:

1. Log in as the root user to the system where WPAR Manager is installed.

2. From the IBM Systems Director, select Resource Explorer.

3. Select the navigation link for the Workload Partitions Groups, and then select the link in the table for All System Workload Partitions to display a list of system WPARs.

4. Right-click the required native system WPAR and select Edit to launch the Modify Workload Partition wizard.

The WPAR must show a dash (·) in the versioned column to indicate that it is not a versioned WPAR.

If the managed system that hosts the WPAR is configured with the storage support (either virtual shared device support or virtual local adapter support), a Device Control tab is present in the Modify Workload Partition wizard.

The Device Control tab, if present, displays one or two subtabs, Devices and Adapters, depending on the storage support configured in the global environment. Use the Adapters subtab on the Device Control tab to allocate virtual local storage adapters to the WPAR.

5. Use the Adapters subtab on the Device Control tab to allocate virtual local storage adapters to the WPAR. Click the Add Adapters button. The Add Adapters dialog is displayed. This window shows the available storage
adapters on the managed system. For information on the devices attached to an adapter, click the link on the name of an adapter to display, in the same window, the list of adapter-attached storage devices. In this window, you can view the device type, device name, device ID, whether the device is currently exported to a WPAR, a list of WPARs that the device is allocated to, and the device capacity and subclass. If you have displayed adapter-attached devices, follow the breadcrumb link back to the list of adapters.

6. Select the check box next to each adapter you want to allocate and export to the WPAR.

7. Click OK to select the adapter and its attached devices. This closes the Add Adapters page and returns to the table that shows storage to be allocated to the WPAR. When modifying a WPAR, storage attached to the storage adapter can only be added to the WPAR for storage and cannot be added to the WPAR-owned root volume group if the WPAR is a rootvg WPAR.

8. Click OK in the Modify Workload Partition window to allocate the selected storage adapter to the WPAR.

If the Modify WPAR action is performed on a WPAR in the Defined state, the adapter and its attached devices are allocated to it. By performing a start action on the WPAR, attempts to export the allocated storage adapter and its attached devices from the managed system to the WPAR. If the adapter and its devices are not being used in the global environment or by another WPAR, the adapter and its devices are available for use within the WPAR. If the adapter or its devices are otherwise in use, 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 adapter and its attached devices automatically export if they are otherwise not in use.

**Exporting a virtual local storage adapter and devices to a new native system WPAR**

Use the Create Workload Partition wizard or the Deploy Workload Partition Definition wizard to export a virtual shared storage device to a new workload partition (WPAR) during creation or definition deployment.

Use the Create WPAR or Deploy WPAR Definition in WPAR Manager to allocate system-configured storage adapters to a newly created native system workload partition (WPAR). Storage adapter support is not available for application WPARs or for versioned system WPARs. The virtual local storage adapter and its attached devices are exported for the WPARs exclusive use when the newly created WPAR is started if the adapter and its devices are not in use in the global environment or not in use by any other active WPAR.

To export a virtual local storage adapter and its attached devices to a newly created WPAR using the Create action, complete the following steps:

1. Log in as the root user to the system where WPAR Manager is installed.
2. From IBM Systems Director, select Resource Explorer.
3. Select the navigation link for Workload Partitions Groups. Select the link in the table for WPAR capable systems to display a list of systems where WPARs might be created and hosted.
4. Right-click the system where the WPAR must be created, and click Workload Partitions Support > Create Workload Partition.

The Create Workload Partition wizard is launched.
5. If the managed system that hosts the WPAR is configured with storage support (either virtual shared device support or virtual local adapter support), a Device Control page is present in the Create Workload Partition wizard.

The Device Control page, if present, displays one or two tabs, Devices and Adapters, depending on the storage support configuration in the global environment.

6. Use the Adapters tab on the Device Control page to allocate virtual local storage adapters to the WPAR. Click Add Adapters to display the available storage adapters on the managed system. Click the name of an adapter to display, the list of adapter-attached storage devices.

7. Select the check box next to each adapter you want to allocate and export it to the WPAR being created.

8. Click OK to select the adapter and its attached devices. This closes the Add Adapters page and return to the table that shows the storage to be allocated to the WPAR.

   If the WPAR being created is a rootvg WPAR (a WPAR that owns its own root volume group), any of the virtual local adapter-attached devices that are to be included in the WPARs root volume group must be designated as such when the WPAR is being created. To identify an adapter-attached disk storage device as a member of the WPARs root volume group, use the Device Control column to identify the disk as a rootvg disk. By default, the adapter-attached disk devices are added to the list that is identified as storage devices that are not part of the WPARs root volume group (if there is one). This cannot be changed after the WPAR is created so must be configured when the WPAR is created, if required.

9. Click Finish in the wizard to create the WPAR and to allocate the selected storage adapter and adapter-attached devices to the WPAR.

   The Create Workload Partition action can also be initiated from any other view where WPAR-capable systems are displayed, for example, Workload Partitions and Hosts.

If the WPAR created by the Create WPAR action is not configured to start automatically, then:

   • The WPAR is created in the Defined state.
   • The adapter and its attached devices are allocated to the WPAR.

By performing a Start action on the WPAR, you can export the allocated storage adapter and its attached devices from the managed system to the WPAR. If the adapter and its devices are not being used in the global environment or by another WPAR, they are available for use within the WPAR. If the adapter or its devices are otherwise in use, the WPAR is successfully started but an error message is displayed.

Note: You can use the Deploy Workload Partition Definition wizard to create a WPAR by using a previously defined WPAR. Virtual local storage adapters and adapter-attached devices can be allocated and exported to the newly created and started WPAR using similar steps as outlined above by using the Deploy Workload Partition Definition wizard.

**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. In IBM Systems Director, click Resource Explorer in the console navigation page, and then click Workload Partitions Groups. Click WPAR capable systems.
3. In the table of managed systems, click the link for the name of a system.
4. Click WPAR-related properties.
5. Click the Devices tab. The following information about the devices configured on 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.

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

   **Capacity**
   Displays, in megabytes, the capacity of storage devices that are configured on the managed system. If the capacity column shows a dash (-) for a disk device, the disk is exported to another WPAR and is not available in the global environment. For any other device type (tape drive), the dash indicates that the capacity information is not reported.

   **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 a list of WPARs that the device is currently allocated to, if any.

The WPAR related properties of a WPAR-capable system can be viewed from any other view where WPAR-capable systems are displayed, for example, Workload Partitions and Hosts.

**Viewing performance metrics for a managed system**

IBM Systems Director automatically retrieves and displays the status of systems that have been discovered, including current and historical data for a selected set of performance metrics. In addition, current CPU and memory utilization are reported in the Workload Partitions and Host view.

**Related information:**

- Monitoring system status and health
- Adding a graphical monitor to the dashboard
- eLearning: Monitoring a system

**Viewing performance metrics for managed systems and WPARs**

IBM Systems Director provides capabilities to view current and historical data for selected performance metrics for managed systems.
In addition to this capability, you can view the current processor and memory use for both WPAR-capable systems and WPARs in the Workload Partitions and Hosts view. This helps you to determine whether systems and WPARs are overused or underused. This information can help you decide how to manage the WPARs.

For example, the metrics can help you decide whether adding a new WPAR or relocating a WPAR to another managed system would have a significant impact on the performance.

Related information:
Monitoring system status and health

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. The two types of relocation possible in WPAR Manager are live relocation and static relocation.

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 back up and restore capabilities.

When working with application mobility, ensure that you plan for it to ensure your environments meets the system requirements. In addition, ensure you are familiar with the various concepts and tasks associated with application mobility.

Related concepts:
"Configuring the environment for application mobility” on page 17

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 the AIX operating system.
• Update all WPAR Manager agent software to the same version.

System compatibility
System compatibility is the degree of similarity between two servers as it relates to 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**
You can use the compatibility tests 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.1ibc 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.
- A versioned WPAR requires version, release, modification, and fix-level checks of additional file sets.

**Note:** In addition to the devices test cases, the only additional critical test for static relocation is that the bos.rte.1ibc 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 Modify 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 x1C.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 feasibility 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 relocation domains
A relocation domain is a grouping of managed systems that you define which
represents a 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 Resource
   Explorer.
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 WPAR can be moved based on system compatibility. System compatibility status is determined by the type of relocation (static or live) being performed. While selecting a fully compatible system is the preferred option, you can override the compatibility option 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 17

**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.

**Related information:**

Security

---

**Command-line interface**

WPAR Manager functions can be accessed both from the IBM Systems Director graphical console and from the IBM Systems Director distributed 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 from the system where IBM Systems Director is running:

```
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 from the system where IBM Systems Director is running:

```
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 from the system where IBM Systems Director is running:

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

**Note:** You must run the commands in an administrator role.

**Related concepts:**
- “Accessibility features for WPAR Manager” on page 6

**Related information:**
- `smcli` - Systems Management command-line interface

---

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

### Agent manager logs

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

### WPAR Manager agent logs

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

<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>
<tr>
<td><code>/var/adm/ras/wpar.&lt;wparname&gt;.log</code></td>
<td>WPAR RAS-related log files</td>
</tr>
<tr>
<td><code>/var/adm/wpars/event.log</code></td>
<td>WPAR RAS-related 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 6. Live relocation logs

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

Verifying the agent manager is online

The agent manager provides configuration information to clients over an unsecured HTTP port. It can be useful in problem determination to verify 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:**

"The managed system does not appear in All Operating Systems group"

**The managed system does not appear in All Operating Systems group:**

If the managed system does not appear in the **All Operating Systems** group, you have a few courses of action to resolve this problem.

**Probable cause**

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

**Action**

1. Login to the managed system as the root user.
2. Verify that the agent manager is online. If the agent is not running, restart the agent.
3. Examine the log files on the system running IBM Systems Director in the `<director_install_location>/lwi/logs/` directory for any error messages generated during the system discovery process.
4. In the IBM Systems Director console navigation area, click **Inventory > System Discovery** to initiate the system discovery process again.

**Related concepts:**

"Managed system does not appear in WPAR-capable systems group" on page 50

**Related tasks:**

"Installing the WPAR Manager subagent on the managed system" on page 12

**Managed system does not appear in versioned WPAR-capable systems group**

The system anticipated to have versioned WPAR capabilities does not appear in the versioned WPAR-capable systems group.

**Probable cause**

- The required licensed program for versioned WPARs has not been installed on the managed system.
- All software inventory and extended WPAR inventory were not collected, or a failure occurred when collecting the inventories.
**Action**

**Note:** Perform the following steps in order. Only perform the next step in this procedure if this previous step did not produce the required 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. **Ensure that the required versioned WPAR support lpp software has been installed** on the managed system. This can be done by logging into the managed system and issuing the command `# lslpp -h | grep vwpar`. If the versioned WPAR support lpps are installed, the files sets will be listed in the output of this command.
   You can skip this step and go directly to the next step to find the information in a different fashion. After collecting the software inventory from the managed system, you can search the software inventory table for the versioned WPAR support licensed program file sets (search table for `vwpar`).
5. **Log in to the IBM Systems Director console** and click [View and Collect Inventory](#). Select the managed system and collect software inventory.
6. **Examine the Director server log files** in the `<Director_install_location>/lwi/logs` directory for any error messages reported by the USMi discovery service.
7. **After the software inventory is collected successfully,** select the managed system again and from the [View and Collect Inventory](#) window, collect WPAR Extended inventory.

**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:
   ```bash
   # cd /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/error-log-0.html` log file for any errors reported by the WPAR Manager extension.

**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 the issue, you can view the `/opt/IBM/WPAR/agent/logs/mcr/<wparname>.log` log file that contains detailed information about the files that failed the checksum test. The `ls1pp -w /path/to/filename` command can be used to search for the file set that is included a specific file. Ensure that the file set 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 the 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 back up 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 fails to restore the WPAR on the arrival system.
- The expected mount point for the shared location must match with the shared directory setting in the WPAR Manager Application Configuration page. The WPAR Manager Application Configuration page can be accessed from the WPAR Manager welcome page.
- 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 WPAR operation of an NFS-based WPAR fails because of permissions

The Create WPAR operation for an NFS-based WPAR that can be relocated fails with this message: AKMWA0002E. The command failed to run on the target system.

The failing job step for the Create WPAR operation in the IBM Systems Director Active and Scheduled Jobs portlet show the following output:
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.

Deploy WPAR Definition operation for an NFS-based WPAR fails because of permissions

The Deploy operation for an NFS-based WPAR that can be relocated fails with this message: AKMWA0002E. The command failed to run on the target system.

The failing job step for the Deploy WPAR operation in the IBM Systems Director Active and Scheduled Jobs portlet shows the following output:

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 WPAR definition 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.

**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.

On the job steps page, entries are displayed for the individual steps involved in the job request. The completion status for each individual step is listed in the status column of the table. Failed job steps show completion status as Complete with errors. Select the hyperlink on the name of the failing job step. A window opens that lists the relevant information regarding the command that was run on the managed system. Information on the command that was run and any output from the command directed to standard output or standard error as well as the return code provided by the command are available for your information.

**Deploy WPAR Definition operation fails because of an incorrect IP address**
The Deploy WPAR Definition operation fails with this message: AKMWA0002E. The command failed to run on the target system. As a result, the WPAR was not created on the selected managed system from the WPAR definition.

In the IBM Systems Director Active and Scheduled Jobs portlet, the status of the command issued is shown as Complete with errors. Select the Job Steps tab and select the link for the failing job step (Start WPAR). This displays the command issued as well as the return code for the command run on the agent and the information printed to standard error and standard output. The standard error information displays the following error:

```markdown
mkwpar: Failed to determine the appropriate interface for address <ip address="">.
```

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

**Action**
2. Select the WPAR Definition, and select Action.
3. Select Deploy from the menu to launch the Deploy Workload Partitions Definition wizard. Navigate through the pages making requisite changes until the Network page is reached.
4. On the Network page, ensure that you enter an IP address in the same subnet as the managed server where the WPAR is deployed.
5. Click **Finish**.
   This creates the WPAR on the selected managed system from the provided
   WPAR definition.

**Edit WPAR operation fails because of an incorrect IP address**

The edit WPAR operation fails with this message: **AKMWA0002E**. The command failed
to run on the target system. As a result, the WPAR was not modified on the
selected managed system.

In the IBM Systems Director **Active and Scheduled Jobs** portlet, the status of the
command issued is shown as **Complete with errors**. Select the **Job steps** tab and
select the link for the failing Job step (Start WPAR). This displays the command
issued as well as the return code for the command run on the agent and the
information printed to standard error and standard output. The standard error
information displays the following error:

```
chwpar: Failed to determine the appropriate interface for address <ip address="">.
```

**Probable cause**

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

**Action**

- Attempt to edit the WPAR task on the **Network** page again. Ensure that you
  enter an IP address that is in the same subnet as the managed system where the
  WPAR is deployed.
- Click **OK** to submit the changed information. This modifies the WPAR on the
  selected managed system from the provided information.

---

**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 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.
allocate storage
The process of adding a virtual local storage adapter or a virtual shared storage device to an inactive (not started) WPAR. The local adapter (and its attached devices) or the virtual shared storage device is exported to the WPAR for its exclusive use at start time if it is not currently in use by any other active WPAR. An adapter or device might be simultaneously allocated to multiple inactive WPARs but can only be exported to one active WPAR at a time.

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 use fewer 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.

B

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

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

C

checkpointable
WPAR attribute that indicates that the WPAR is capable of live mobility. When creating a WPAR, it is necessary to specify checkpoint support if live mobility of the WPAR is necessary. Toggling the checkpointable attribute imposes restrictions on the file system configuration settings; that is, the WPAR has to either own its root volume group or be an NFS-based WPAR.

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.

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

departure system
The managed system on which a WPAR is deployed 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 console.

E
export storage
The process of adding a virtual local storage adapter or a virtual shared storage device to the kernel structures for an active WPAR. This designates the adapter (and its attached devices) or the specified device as available to the WPAR for the exclusive use of the WPAR.

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

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

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

**maintenance state**
The WPAR has been started in maintenance mode; that is, networks that are associated with the workload partition are not configured. While in maintenance mode, the only access to the workload partition is from the global system.

**moving state**
The WPAR is transferring its memory contents to another system. When the memory transfer is complete, the WPAR stops and is removed from the system.

**managed system**
A server or logical partition running the AIX operating system 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 Explorer**. 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.

**MPIO**
Multiple Path I/O (MPIO) is an AIX operating system function that can be used to define alternate paths to a device for I/O failover purposes. I/O failover is a path-management algorithm that improves the reliability and availability of a device because the system automatically detects when one I/O path fails and reroutes I/O through an alternate path. Only MPIO storage devices are supported in WPAR Manager.

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

**N**

**native WPAR**
A system WPAR that was created with and runs the same version of the AIX operating system as the managed system where the WPAR was originally created and hosted.

**P**

**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.

R
recovery
An automatic action started by WPAR Manager when an error is detected while performing operations on managed systems or WPARs. The goal of any recovery action is to synchronize the information in the WPAR Manager database with the real state of the managed systems and WPARs. As an example, 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. In this case, 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.

Recovery actions initiated by WPAR Manager are logged in the **Job Steps** tab of the IBM Systems Director Active and Scheduled Jobs portlet just like any other step involved in a task execution.

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.

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.

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.

versioned workload partition
Versioned workload partitions are system WPARs that are created with and run a different version of the AIX runtime environment than the global system where the WPAR was originally created. This versioning support requires the purchase and installation of separate licensed program software.

Virtual I/O Server (VIOS)
The Virtual I/O Server facilitates the sharing of physical I/O resources among client logical partitions within a physical system. The VIOS
provides virtual SCSI target, virtual fibre channel, Shared Ethernet Adapter, PowerVM Active Memory™ Sharing, and PowerVM Client Partition Mobility capability to client logical partitions within the physical system.

**virtual local adapter**
An adapter that is configured in the global environment and exported to a WPAR.

**virtual shared adapter**
An adapter that is created in the WPAR as the parent of a storage device that is exported to the WPAR.

**VSCSI adapter**
A virtual adapter under the VIO bus. It is the parent of a VSCSI disk.

**VSCSI disk**
A virtual SCSI disk that is provisioned to a client LPAR from the VIOS.

**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.

**Related information:**

- [MPIO device management in AIX 7.1](#)
Notices

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

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

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

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

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

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

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

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites 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 IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Dept. LRAS/Bldg. 903
11501 Burnet Road
Austin, TX 78758-3400
U.S.A

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

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

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

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

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

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

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy,
modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

If you are viewing this information 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 registered trademark of Linus Torvalds in the United States, other countries, or both.

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

A
accessibility 6
agent
configuring 15
installing 13
agent manager 50
application mobility
configuring 17
planning 43

C
checkpoint and restart
states 31
compatibility
testing 44
configuring
agent 15
application mobility 17
logging 17
WPAR agent 17

I
installing 9
agent 13
server 10

L
legal notices 63
logical partitions 8

M
managed system
defining 23
problem determination 51, 53, 54, 55
properties 24
manual relocation 47
mobility
compatibility 44, 45

P
planning
application mobility 43
WPAR Manager agent 7
policy-based relocation 47
group policy settings 48
metric policy settings 48
problem determination
deploy 55
deploy operation 53
managed system 51, 53, 54, 55
missing managed system 51
offline 54
secure connection 55

R
relocation
manual 47
removing 13
WPAR Manager agent 13

S
server
installing 10
starting 33
WPAR agent 17
stopping 34
WPAR agent 17

W
WPAR
states 31
WPAR agent 7
configuring 17
starting 17
stopping 17
WPAR Manager 9
WPAR Manager agent
planning 7
removing 13