AIX Version 6.1

IBM Workload Partitions Manager for AIX

SC23-5241-00

AIX Version 6.1

IBM Workload Partitions Manager for AIX

SC23-5241-00

Note

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

First Edition (November 2007)

This edition applies to AIX Version 6.1 and to all subsequent releases of this product until otherwise indicated in new editions.

A reader’s comment form is provided at the back of this publication. If the form has been removed, address comments to Information Development, Department 04XA-905-6C006, 11501 Burnet Road, Austin, Texas 78758-3493. To send comments electronically, use this commercial Internet address: aix6kpub@austin.ibm.com. Any information that you supply may be used without incurring any obligation to you.

Contents

About this document

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

Highlighting

The following highlighting conventions are used in this book:

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

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

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

Case-sensitivity in AIX

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

ISO 9000

ISO 9000 registered quality systems were used in the development and manufacturing of this product.

IBM Workload Partitions Manager for AIX

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

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

WPAR Manager overview

WPAR Manager is a platform management solution that provides multiple functions.

WPAR Manager includes the following features:

- Cross-system management of WPARs, including lifecycle management
- Global load balancing with application mobility
- Web-based administration of basic WPAR operations and advanced management tasks
- Monitoring and reporting of WPAR performance metrics

Accessibility features for WPAR Manager

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

Accessibility features

The following list includes the accessibility features in WPAR Manager:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers when used from a web browser on a remote Windows® system using assistive technology (AT) software

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

Keyboard navigation

This product uses standard Microsoft® Windows navigation keys when used from a web browser on a system running the Windows operating system.

Interface information

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

Related accessibility information

You can view the publications for AIX 6.1 in Adobe® Portable Document Format (PDF) using the Adobe Acrobat® Reader. The PDFs are provided on a CD that is packaged with the product, or you can access them in the *IBM Systems Information Center* by selecting **IBM Systems Information Center** → **Operating systems** → **AIX information** → **AIX PDFs** and clicking IBM Workload Partitions Manager for AIX.

IBM and accessibility

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

WPAR agent

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

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

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

Supported operating environments for WPAR Manager

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

WPAR Manager server requirements

The WPAR Manager server supports the following environment:

- AIX 6.1
- DB2® 9.1 for Linux®, UNIX®, and Windows, for database function

WPAR Manager agent requirements

The WPAR Manager agent can be installed on any AIX 6.1 system running on a physical server or in a logical partition on a POWER4 or later system.

WPAR Manager client requirements

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

Table 1.

Operating system	Supported browser version
AIX Version 6.1	Firefox 1.5 or later
Windows XP	Internet Explorer 6 or later Firefox 1.5 or later **Note:** Internet Explorer requires the SVG graphics plugin from Adobe. You can obtain this plugin from the following Web site: http://www.adobe.com/svg/viewer/install/

Memory and disk space requirements

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

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

Table 2. WPAR Manager memory and disk space requirements

Application	Memory requirement	Disk space requirement
WPAR Manager	125 MB	**/**, 5 MB **/var**, 100 MB **/opt**, 50 MB
DB2 server	256 MB	500 MB, minimum 2 GB, recommended /home, 200 MB /opt, 500 MB
Agent manager	50 MB when idle	30 MB
WPAR agent	45 MB when idle	27 MB

Planning for Application Mobility

When planning for Application Mobility, you should consider the compatibility of WPARs and your goal in relocating the WPARs.

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

Planning for Role Based Access Control

AIX 6.1 enhances Role Based Access Control (RBAC) to provide greater granularity in controlling access to AIX services based on roles and privileges granted to users.

WPAR Manager provides the capability to specify RBAC privileges to the WPAR during deployment. Because privileges can vary between managed systems, WPAR Manager queries the set of overall privileges on the system and the set of default privileges for a WPAR at registration time. This information is used to provide a set of valid RBAC privileges to choose from for the WPAR. You can also modify the RBAC privileges of a deployed WPAR. For a deployed WPAR, the WPAR Manager invokes the **chwpar -S** command through the agent to modify RBAC privileges.

Installing WPAR Manager

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

Installing WPAR Manager on the management server

You should install the WPAR Manager on a single AIX system that will be your management server.

1. Log in to the system as the root user.
2. If you are installing from media, insert the media containing WPAR Manager into the media drive.
3. Mount the media drive using the following command (where ***/mnt*** is the mount point for your media drive):

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

4. Run the **installp** command as follows to install WPAR Manager:

   ```
   installp -acqgXd mount_point wparmgt.mgr
   ```

Installing the WPAR Manager database

The WPAR Manager database is run by DB2 Version 9.1. You can install the database using an installation script.

1. Log in to the management server as the root user.
2. If you are installing from media, insert the media containing WPAR Manager into the media drive.
3. Mount the media drive using the following command (where */mnt* is the mount point for the media drive):
   ```
   /usr/sbin/mount -v cdrfs -p -r /dev/cd0 /mnt
   ```
4. Run the **installp** command as follows to install the WPAR Manager database:
   ```
   installp -acqgXd  mount_point wparmgt.db
   ```
5. Change directories to the directory where the installation script is located using the following command:
   ```
   cd  /opt/IBM/WPAR/manager/db/bin
   ```
6. Run the installation script using the following command:
   ```
   ./DBInstall.sh  -dbpassword your_password   -dbinstallerdir /mnt/db2
   ```

   Note: You will need the values you specified for this command when you configure WPAR Manager.

Configuring WPAR Manager server

You can configure WPAR Manager in GUI mode or console mode by running the **WPMConfig.sh** command. GUI mode provides a graphical user interface, while console mode uses a character-based interface for non-GUI terminals.

The **WPMConfig.sh** command will automatically starts in either GUI mode or console mode depending on whether you have the AIX X11 graphical environment. If you have the X11 environment on your system, and client access is graphical, then running the configuration wizard automatically starts the GUI mode. If there is not an X11 environment, then the configuration wizard starts in console mode. To run the configuration wizard in GUI mode or console mode, complete the following steps:

1. Log in to the system as the root user.
2. Run the **WPMConfig.sh** script in either of the following modes to begin the configuration:
   - To run the configuration in GUI mode, run the following command:
     ```
     /opt/IBM/WPAR/manager/bin/WPMConfig.sh
     ```
   - To run the configuration in console mode, run the following command:
     ```
     /opt/IBM/WPAR/manager/bin/WPMConfig.sh -i console
     ```

   The locale selection window opens.
3. Select the appropriate locale for your system.

You can now continue the configuration process in either GUI mode or console mode. If no parameters are specified, and the system has no graphical environment, the configuration wizard will start in console mode.

Configuring WPAR Manager server in silent mode

You can configure WPAR Manager in silent mode by running the **WPMConfig.sh** command.

To run the configuration in silent mode, complete the following steps.

1. Log in to the system as the root user.
2. Create a copy of the **/opt/IBM/WPAR/manager/config/wpmInstall.properties** file.
3. Edit the copy of the **wpmInstall.properties** file with your desired configuration values, including passwords.
4. Run the **WPMConfig.sh** command as follows:
   ```
   /opt/IBM/WPAR/manager/bin/WPMConfig.sh -f path_to_wpmInstall.properties -i silent
   ```

Note: You must provide a fully qualified file name for the **wpmInstall.properties** file.

A success code or failure code is returned. The success code value is zero, and the failure code value is any value other than zero.

Installing the WPAR agent on the managed system

The WPAR agent is software that runs on a managed system and communicates with the agent manager component of WPAR Manager. After you install the WPAR agent, it performs actions on the managed system.

The following files are prerequisites for installing the WPAR agent:

- **Java5.sdk** version 1.5.0.0
- **bos.wpars** version 6.1.0.0
- **perfagent.tools** version 6.1.0.0

The WPAR agent is packaged as a set of AIX **installp** file sets. The WPAR Manager CD includes the following WPAR agent file sets:

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

All file sets are required for installation.

To install the WPAR agent with the **installp** command, run the following command as the root user:

```
installp -acXYgd path_to_installp_images wparmgt.agent.rte
```

Substitute *path_to_installp_images* with the location of the WPAR Manager **installp** file sets. The location should either be the media drive or a local directory on the system.

Configuring the WPAR agent

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

The **/opt/IBM/WPAR/agent/bin/configure-agent** script supports the following syntax and parameters:

```
configure-agent -hostname amhost [ ... ]
```

-hostname *amhost*
Agent Manager Hostname (Required)

-pubport
port

-Agent Manager Public Port
(Default: 9513)

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

-agentport *port*
Agent Port (Default: 9510)

-force Reconfigure a previously configured agent

At a minimum, the host name of the agent manager is required to configure the WPAR agent. If the default port (9510) used by the agent conflicts with another product on the system, choose an alternate port.

The configuration script interactively prompts for the agent registration password. This password is specified when you configure the agent manager.

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

- The configuration process is not able to reach the agent manager at the specified host, port, or context root. This can occur if the agent manager is offline or unreachable, or the host name, public port, or context root parameters have been specified incorrectly.
- The WPAR agent is already configured to use an agent manager.
- The port specified for use by the WPAR agent is already in use on the system.

Starting and stopping the WPAR agent

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

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

To start the WPAR agent using the **wparagent** script, run the following command:

```
/opt/IBM/WPAR/agent/bin/wparagent start
```

To stop the WPAR agent using the **wparagent** script, run the following command:

```
/opt/IBM/WPAR/agent/bin/wparagent stop
```

Note: You can also use the **wparagent** script to restart the WPAR agent with the **restart** option.

Configuring WPAR agent logging

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

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

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

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

1. Open the **/etc/opt/IBM/WPAR/agent/wparagent_logging.properties** file in a text editor.
2. Modify the properties you want to change.
3. Restart the WPAR agent using the **/opt/IBM/WPAR/agent/bin/wparagent restart** command

Configuring WPAR Manager

You can configure different components of the WPAR Manager.

Configuring the environment for application mobility

There are restrictions on the environment set up to support application mobility.

The following restrictions apply to configuring the environment to support application mobility:

- Managed systems to be used as departure and arrival systems for mobility must be within the same subnet.
- Source and destination servers should not only be running on compatible hardware, but also have compatible software.

There are additional restrictions specific to system WPARs and application WPARs.

Configuring application mobility for system WPARs

In order to enable application mobility for system WPARs, you must specify a remote directory that will be the root mount point for the **/** directory, the **/var** directory, **/home**, and the **/tmp** directory.

Because the remote **/usr** directory and **/opt** directory are accessed over the network, you might experience slower performance than with local disk access. You should use these remote directories only if you need a private **/usr** directory and a private **/opt** directory.

The steps below for configuring application mobility for your system WPAR assume the following network topology:

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

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

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

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

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

1. Create a file system on the nfssrv1.*yourdomain*.com NFS server to host the system WPAR remote file systems. For example:

   ```
   crfs -v jfs2 -m /wparsfs -A yes -a size=1G -g rootvg
   ```

   Note: If you want to use an existing file system, you can skip this step.
2. Mount the file system you created (or the existing file system you plan to use) by running the following command:

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

   ```
    mkdir /wparsfs/wpars/wparhostname
   ```
4. Export the directory so all WPAR agents and WPAR host names have root access to write to the new file system by running the following command:

   ```
   # mknfsexp -d  /wparsfs/wpars/wparhostname -r wparagent1,wparagent2,wparhostname -B
   ```
5. Create a WPAR with the NFS server and root directory you specified using either the quick create method or the Create WPAR wizard.

Configuring application mobility for application WPARs

In order to enable application mobility for application WPARs, the WPAR Manager requires a shared file system to be created and configured.

You must grant root permissions for the shared file system to the global WPAR (the WPAR Agent) and the WPAR host name.

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

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

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

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

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

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

1. Create a file system, named **/sfs** in this example, on the nfssrv1.*yourdomain*.com NFS server where application WPARs states will be stored during checkpoint and restart operations. This file system does not have to be the same file system hosting the remote file systems for your system WPARs. For example:

   ```
   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 you plan to use) by running the following command:

   ```
   mount /sfs
   ```
3. Export the directory so that all WPAR agents and WPAR host names have root access to write to the new file system by running the following command:

   ```
   # mknfsexp -d  /sfs -r wparagent1,wparagent2,wparhostname -B
   ```
4. Mount the file system on all WPAR agent systems (wparagent1 and wparagent2) by running the following command:

   ```
   # mknfsmnt -f /var/adm/WPAR -d /sfs -h nfssrv1 -B
   ```

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

Configuring the WPAR agent to use a different agent manager

After you successfully configure the WPAR agent, you must run the configuration script with the **-force** flag to use a different agent manager.

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

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

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

Removing WPAR Manager

You can remove WPAR Manager from your system by using the **installp** command.

To remove WPAR Manager, complete the following steps.

1. Log in as root to the system where WPAR Manager is installed.
2. Run the **installp** command as follows to remove WPAR Manager and the agent manager:

   ```
   installp -ug wparmgt.mgr wparmgt.cas.agentmgr
   ```

   Several status messages display in the terminal window as the removal is initialized and launched.

Removing the WPAR Manager database

You can remove WPAR Manager database from your system by using the **DBUninstall.sh** script and the **installp** command.

To remove WPAR Manager database, complete the following steps.

1. Log in as the root user to the system where the WPAR Manager database is installed.
2. Change directories to the **/opt/IBM/WPAR/manager/db/bin** directory by running the following command:

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

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

   ```
   ./DBUninstall.sh
   ```

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

   ```
   installp -ug wparmgt.db
   ```

   Several status messages display in the terminal window as the removal is initialized and launched.

Removing the WPAR agent

To remove the WPAR agent, you must remove its **installp** file sets from the system using the **installp** command.

The following file sets must be removed:

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

To remove all of the WPAR agent file sets, run the **installp** command, as follows:

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

Note: The **installp** file set **tivoli.tivguid** is also required by the agent manager (**wparmgt.cas.agentmgr**). You will see requisite failure errors when attempting to remove this file set if the agent manager is installed on the same system.

Managing workload partitions with WPAR Manager

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

Managed systems

A managed system is an AIX image that has the WPAR agent installed, configured, and started.

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

Physical system
A POWER4or POWER5™ 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 the system appears as one logical partition that is using all of the system resources.

Virtual system
A logical partition (LPAR) on a POWER4 or POWER5 system where AIX is installed and running.

WPAR management in a logically partitioned environment

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

WPAR Manager does not recognize HMC or Integrated Virtualization Manager (IVM) configurations. If you are using the HMC or IVM to manage your environment, and you have created a WPAR within the logical partitions on your systems, you will not be able to view the entire environment from WPAR Manager. Logical partitions might not be viewable for the following reasons:

- They are running operating systems other than AIX.
- They do not have the WPAR agent software installed.
- They are not registered to your WPAR Manager server.

Defining a managed system

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

System profiles do not represent the actual managed systems, instead they represent a particular configuration, therefore at any time one or more managed systems can share the same system profile. If an existing profile from previous registrations already has the same characteristics as the system being registered, then the existing profile will be assigned to the system. If the system being registered has a unique set of hardware attributes, then a new profile will be created and assigned to the system.

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

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

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

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

The new managed system should automatically be discovered by the WPAR Manager after registration. If the new managed system is not automatically discovered, you can trigger the Discover task from the WPAR Manager in the Managed System Resource View. When a managed system is successfully discovered and registered, it is displayed in the WPAR Manager and is in the **Online** state.

Viewing managed system properties

WPAR Manager allows you to view configuration details and physical properties for managed systems that have been registered with the application.

1. Go to the **Resource Views** section of the navigation area.
2. Select **Managed Systems**.
3. In the table of managed systems, click the system's name. The Properties page displays.

Updating the profile for a managed system

System profiles are used by the WPAR Manager to determine possible relocation targets during an automated relocation event. When a managed system undergoes changes on the hardware configuration, the profile associated with it is no longer valid, and must be updated.

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

When a system configuration changes, and the server profile is updated, the process that performs the compatibility analysis starts again for that system. Any results from the compatibility analysis performed during registration are discarded.

Viewing performance metrics for a managed system

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

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

1. Go to the **Managed Systems** view in the WPAR Manager.
2. Select a system.
3. Select **Performance Metrics**. The Performance Metrics page displays.

From the Performance Metrics page, you can perform the following tasks:

- View recent performance trends for selected metrics
- View a graph of longer-term historical performance data

Removing a managed system

When a managed system is being redirected to other uses or being managed by another WPAR Manager, you might want to remove the managed system from the management environment of the WPAR Manager.

Before removing a managed system, the WPAR Manager provides options for WPARs that are defined on that system. You can select either the Preserving WPARs deployed on the system task, or the Removing all WPARs task before completing the Remove Managed System task.

When a managed system is removed from the WPAR Manager, the initial registration is revoked and the agent installed on the managed system can no longer communicate with the application. Note that although the agent is no longer registered to an instance of the WPAR Manager, it is still running on the system where it was installed. If you no longer need the agent on the machine, you must manually stop and uninstall the agent. If you want to re-register the agent with the same instance of the WPAR Manager or another instance, it can be reconfigured. For more information about reconfiguring, see ″Reconfiguring WPAR Agent to use a different WPAR Manager″.

Managing WPARs

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

Creating WPARs

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

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

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

There are two ways to create a WPAR:

Create a new WPAR

Configuration parameters for the WPAR are entered manually through the Create WPAR Wizard. You can also create a new WPAR using the **Quick Create** button in the WPAR.

Create a WPAR from an existing WPAR

Use another WPAR as a template to create the WPAR. The WPAR Manager allows you to review the WPAR configuration before the creation is completed so that you can modify settings that should be different for the new WPAR. This method uses the Create WPAR Wizard.

Creating a mobile WPAR:

Mobility is the capability of a WPAR to be relocated. WPARs that are going to be relocated require a special configuration that must be specified when the WPAR is created.

In order to create a WPAR that can be relocated, you must configure your WPAR as follows:

- A WPAR needs to explicitly be flagged to support relocation. This setting can be specified when the WPAR is created through the ″Enable relocation″ option. A WPAR that is enabled for relocation allows the application to capture the full context of the applications running within the WPAR. This information is then saved and used later to restore the WPAR to its original state.
- Specify a valid network configuration. WPARs without network connectivity cannot be relocated. If the name of your WPAR resolves to a valid network host name, the WPAR will connect to the network automatically. If the name of your WPAR does not resolve to valid network host name, you will have to provide connection information.

  Note: WPAR Manager does not check to see if a the name of a WPAR resolves to a valid network host name. You must verify this yourself.
- All the file systems specified for the WPAR must be mounted as remote file systems using NFS except for the **/usr** file system and the **/opt** file system, which can be mounted as namefs read-only file systems. File systems that are mounted remotely should be exported for the WPAR host name and the host name for any managed system to where the WPAR will be deployed.

  Related concepts

  "Configuring the environment for application mobility" on page 7
  There are restrictions on the environment set up to support application mobility.

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

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

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

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

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

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

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

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

Creating a WPAR from the command line:

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

Related information

Configuring system WPARs in IBM Workload Partitions for AIX

Configuring application WPARs in IBM Workload Partitions for AIX

Viewing or modifying WPAR properties

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

When a WPAR is not deployed in a Managed System, the WPAR Manager allows the modification of any of the properties for the WPAR. If the WPAR is currently deployed in one system, no configuration changes can take place unless the state of the WPAR allows the modification.

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

Modifying a WPAR on the command line:

Although the WPAR Manager provides a user interface to modify the configuration of WPARs, you can also use the command line to make modifications. When a change is completed through the command line, the WPAR Manager discovers the changes and the WPAR Manager database is updated to reflect the new configuration.

Deploying a WPAR

The WPAR Manager allows you to create and configure a WPAR without allocating the resources in an actual system.

This process is similar to creating a WPAR specification file, but the information is stored in the database of the application and can easily be used to create WPARs on any system managed by the WPAR Manager. WPARs that are not deployed in a particular system are in the Undeployed state. Once a WPAR is deployed, the state shown in the WPAR Manager should be consistent with the state of the WPAR in that system. After the WPAR is deployed, it cannot be deployed into any other system until the WPAR is deleted or the application running within an Application WPAR is completed.

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

To deploy a WPAR on a managed system, complete the following steps:

1. Locate the WPAR that you want to deploy. In the **Navigation** area, expand **Resource Views**, then select **Workload Partitions**. This displays a tabular view of all defined workload partitions, both deployed and undeployed.
2. Select the WPAR, then select **Deploy**. This displays the Deploy Workload Partition page.

Starting a WPAR

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

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

To start a system WPAR, complete the following steps:

1. From the Navigation area, open a view of the WPARs by selecting **Resource Views** → **Workload Partitions** or by selecting **Managed Systems** → ***Your System*** and then selecting **Show Workload Partitions** from the drop-down menu.
2. Select one or more WPARs that you want to start. These must be WPARs that are currently deployed on managed systems. From the drop-down menu, select **Start**.

Stopping a WPAR

System WPARs and Application WPARs can be stopped while they are active in a Managed System.

Depending on the type of the WPAR, the stop operation behaves differently. For both System WPARs and Application WPARs, the stop operation deactivates the running WPAR. System WPARs remain in the system but are inactive and the state changes to Defined. On the other hand, after an Application WPAR is stopped, all of its processes are terminated and the WPAR is removed from the system.

To stop a WPAR, complete the following steps:

1. Select an Active WPAR. You can do this either by selecting **Workload Partitions**, or by selecting **Managed Systems**, selecting a system, then selecting **Show Workload Partitions** from the drop-down action list.
2. Select one or more WPARs that you want to stop. From the drop-down menu, select **Stop**.

Pausing a WPAR

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

A WPAR can only be paused if it has been configured to enable relocation (checkpointable). When a WPAR is paused, all of its processes are locked, a snapshot of the state of the process is taken, network traffic is halted, and the state of the WPAR is changed. Because the state of the processes of the WPAR is saved, the WPAR can later resume operations from the point where it was paused. If a WPAR has active network connections when it is paused, the connections might expire if the WPAR remains paused for too long.

To pause a WPAR, use the following steps:

1. Select an Active WPAR. You can do this either by selecting **Workload Partitions**, or by selecting **Managed Systems**, selecting a system, then selecting **Show Workload Partitions** from the drop-down action list.
2. Select one or more WPARs that you want to pause. From the drop-down actions menu, select **Pause**.

Resuming a WPAR

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

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

To resume a WPAR, use the following steps:

1. Select an Active WPAR. You can do this either by selecting **Workload Partitions**, or by selecting **Managed Systems**, selecting a system, then selecting **Show Workload Partitions** from the drop-down menu.
2. Select one or more WPARs that you want to resume. From the drop-down menu, select **Resume**.

Ending WPAR processes

WPARs that are in the Paused state cannot be stopped from a managed system using the conventional stop mechanism.

If a WPAR in the paused state needs to be stopped, you must use the End Workload Partition Process action. Ending WPAR processes is similar to stopping a WPAR, but it only works for WPARs in the Paused state. The process state is lost for WPARs that are ended. Depending on the type of the WPAR, the End WPAR Process action will behave differently. For both WPAR types, the End Process action forces the deactivation of the running WPAR, however, system WPARs remain in the system but are inactive and their state changes to Defined. On the other hand, after an Application WPAR is ended, all of its processes are terminated and the WPAR is removed from the system.

To end the processes of a paused WPAR, complete the following steps:

1. Select an Active WPAR. You can do this either by selecting **Workload Partitions**, or by selecting **Managed Systems**, selecting a system, then selecting **Show Workload Partitions** from the drop-down action list.
2. Select one or more WPARs that you want to end. From the drop-down menu, select **End Processes**.

Removing a WPAR

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

When a WPAR is removed from a system, the configuration remains in the database of the WPAR Manager. A WPAR definition is similar to a WPAR specification but it is stored in the database of the WPAR Manager. WPARs that exist only as definitions are in the Undeployed state. If you try to remove a WPAR that is in the Undeployed state or if you select the option that allows you to remove the WPAR definition as well, you will completely remove the WPAR from the managed environment.

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

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

Managing WPAR groups

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

By default, workload partitions that you create are assigned to a default WPAR group, unless you reassign them to a different group. If you are implementing policy-based WPAR relocation, you might want to create WPAR groups and assign WPARs to them on the basis of ownership, application affinity, or other reasons. The definition of a WPAR group contains not only the list of the WPARs that belong to the group, but also the definition of the policy that governs the automated relocation of WPARs in response to various workload-related metrics.

The following graphic shows how WPAR groups are defined.

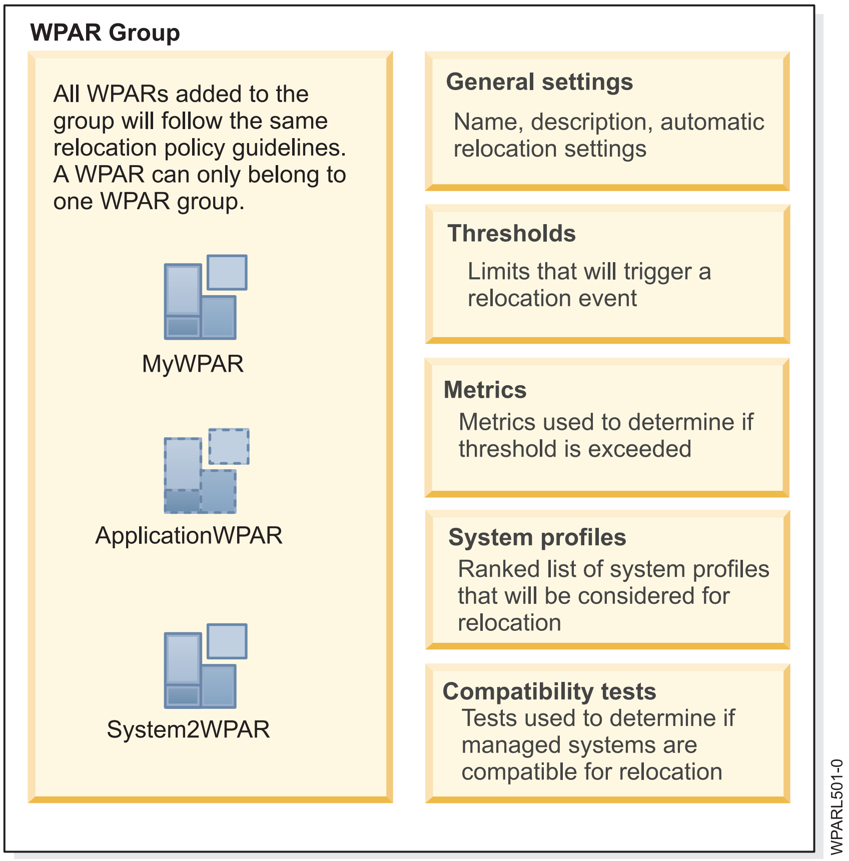

WPAR Group
All WPARs added to the group will follow the same relocation policy guidelines. A WPAR can only belong to one WPAR group.
MyWPAR
ApplicationWPAR
System2WPAR
General settings
Name, description, automatic relocation settings
Thresholds
Limits that will trigger a relocation event
Metrics
Metrics used to determine if threshold is exceeded
System profiles
Ranked list of system profiles that will be considered for relocation
Compatibility tests
Tests used to determine if managed systems are compatible for relocation
WPARL501-0

Figure 1. WPAR groups

Administering WPAR Manager

There are several administrative tasks you might need to perform to use WPAR Manager.

Administrative scripts

You can run the following scripts to perform useful administrative tasks.

Note: The actual locations of these scripts might differ if the default value was overridden at install time.

Script	Description	Default Location
lwilog.sh	Dynamically enables or disables the trace utility in the running application. • To enable the trace utility, run: `lwilog -addLogger -name package_name -level \ package_level` • To disable the trace utility, run: `lwilog -removeLogger -name package_name` Information is logged into the **/opt/IBM/WPAR/manager/lwi/logs/trace-log-#.xml** file, where # is replaced by numeral, with zero (0) representing the most recent trace log file written into. You can use a Web browser to review the resulting XML representation of the log file. This script is provided to assist with potential problem determination and typically is used by a support representative.	**/opt/IBM/WPAR/manager/lwi/bin/lwilog.sh**
lwiMapRole.sh	Maps users or groups to J2EE roles defined by the WPAR Manager. This script can be used to modify the users or groups that are authorized to log in to the WPAR Manager and the roles of each user or group. Run this script with no parameters for usage information.	**/opt/IBM/WPAR/lwi/bin/lwiMapRole.sh**
wparmgr start **wparmgr stop** **wparmgr restart** **wparmgr status**	Starts, stops, restarts, or provides status for WPAR Manager.	**/opt/IBM/WPAR/manager/bin/wparmgr**
db-offline-backup.sh	Performs an offline backup of the WPAR Manager database. An *offline* backup means that no applications can be using the DB2 database that is being backed up.	**/opt/IBM/WPAR/manager/db/bin/db-offline-backup.sh**
db-offline-restore.sh	Restores a copy of the WPAR Manager database that was previously backed up.	**/opt/IBM/WPAR/manager/db/bin/db-offline-restore.sh**

Changing the passwords for database IDs

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

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

```
/var/opt/IBM/WPAR/manager/lwi/bin/lwiencoder.sh -f path/wpmcfg.properties/
-keylist dswparmgt.dbpassword
```

5. Restart the WPAR Manager using the **wparmgr start** command.

Backing up the WPAR Manager database

WPAR Manager uses IBM DB2 Database for Linux, UNIX, and Windows Version 9 (DB2 Version 9) as its database engine. You can back up the database manually or automatically.

The setup for WPAR Manager creates a cron entry that schedules the DB2 database backup. This cron entry runs the **db-daily.sh** script. This script starts and stops WPAR Manager as needed to perform the daily incremental backups and one weekly full backup.

The default configuration for backing up is offline backup. This type of backup takes the WPAR Manager offline for a brief time during the backup phase. An offline backup is the most complete and offers the most assurance of successful data recovery if it is necessary. The WPAR Manager will be offline for only a few seconds.

Backups are configured to be stored in the **$INSTHOME/sqllib/backup** directory (where the $INSTHOME environmental variable is set to the ***/home/username*** directory). The filename looks similar to the following:

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

Each full backup can occupy 80 MB to 110 MB or more of disk space. Each incremental backup can occupy approximately 16 MB or more of disk space. The estimated total disk usage required to maintain one full week of backups using the strategy of one full backup and the remainder incremental backups is 190 MB.

Backing up the WPAR Manager database manually

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

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

1. Change to the directory for your user name using the **su** command.`db2wmgt`. For example, if your user name is *db2wmgt* you would run the following command:

   ```
   su - db2wmgt
   ```
2. Verify that $INSTHOME has been exported.
3. Change the directory to the WPAR Manager home by running the following command:

   ```
   cd /opt/IBM/WPAR/manager/db/bin
   ```
4. Run the **db-offline-backup.sh** script to perform a full backup.

Restoring the WPAR Manager database

The **db-restore-backup.sh** script uses a combination of the last full backup and the incremental backups.

Attention: Recovery replaces the existing database completely.

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

1. Change the directory to the WPAR Manager home by running the following command:

   ```
   cd /opt/IBM/WPAR/manager/db/bin
   ```
2. Run the **db-restore-backup.sh** script.

Security for WPAR Manager

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

User authentication

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

WPAR Manager supports the following four application roles:

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

WPARAdministrator
Provides access to all WPAR Manager windows and management actions.

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

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

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

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

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

Configuring authorization roles

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

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

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

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

The **lwiMapRole.sh** script provides mechanisms for mapping AIX groups to application roles, querying the role-mapping infrastructure, or deleting role access. This script is installed by default in the **/opt/IBM/WPAR/manager/lwi/bin** directory. If you changed the default installation root directory, the script can be located relative to the ***installroot*/WPAR/manager/lwi/bin** directory. You must have administrator access to run this script

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

```
# lwiMapRole.sh
lwiMapRole -add -role roleName [-user user1,user2,...] [-group group1,group2,...]
lwiMapRole -remove -role roleName [-user user1,user2,...] [-group group1,group2,...]
lwiMapRole -purge  -role roleName lwiMapRole -query criteria
Where criteria is one of:
                  getRoles
                  getRolesByUser userName
                  getRolesByGroup groupName
                  getUsersByRole roleName
                  getGroupsByRole roleName
                  getRolesByApplication appName
```

You must recycle the WPAR Manager server after running the **lwiMapRole.sh** script in order for the user ID role mappings to be available to the management console. Changes made with the Console User Authority window take effect immediately.

Configuring SSL support

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

You can configure the SSL subsystem by installing a certificate signed by a trusted certificate authority (CA) and generating a different private key. You can do this using the standard Java™ **keytool** command-line interface, or the ikeyman graphical user interface. These tools are located in the **/usr/java5/jre/bin** directory on most AIX systems. For more information about ikeyman, see *Secure Sockets Layer Introduction and ikeyman User's Guide* at the following Web site:

`ftp://www6.software.ibm.com/software/developer/jdk/security/142/GSK7c_SSL_IKM_Guide.pdf`

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

You can choose to accept the certificate, but this certificate does not provide an adequate level of security in a production environment. You should use ikeyman to replace the default certificate with your own self-signed or CA-signed certificate. You should also change the default keystore password to a value other than the default (`ibmpassw0rd`). You can also use ikeyman to periodically renew expired certificates.

Editing the webcontainer.properties file

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

If you did not default installation location, the **webcontainer.properties** file is located in the **/opt/IBM/WPAR/manager/lwi/conf** directory. The following lines show the default properties included in the **webcontainer.properties** file:

```
com.ibm.ssl.keyStorePassword.14443=[xor] 9MW08GTL+uut1b0\=
com.ibm.ssl.clientAuthentication.14443=false
com.ibm.ssl.trustStorePassword.14443=[xor] 9MW08GTL+uut1b0\=
com.ibm.ssl.trustStore.14443=/../../security/keystore/ibmjsse2.jts
com.ibm.ssl.keyStore.14443=/../../security/keystore/ibmjsse2.jks sslEnabled=true
```

The `keyStorePassword` property value and the `trustStorePassword` property value are encrypted and are not readable in this file.

Attention: You should not edit the **webcontainer.properties** file directly.

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

An example **conf/sslconfig** file contains the following lines:

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

In this example, the `keyStore` property and the `trustStore` property point to the same file. Client authentication is not enabled by default, so the `trustStore` property, which could contain the signer certificates that the Web container trusts, is not actually used. However, the WPAR Manager Web container requires that the `trustStore` property be set to a legitimate value. The default `keyStore` password is `ibmpassw0rd`.

Managing certificates with ikeyman

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

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

1. Start ikeyman. The ikeyman command is typically found in the **jre/bin** directory of the IBM JDK.
2. Open the keystore with the following steps:
   a. On the menu bar, select **Key Database File** → **Open**.

   b. Use the **Browse** button to locate the keystore under the **/opt/IBM/WPAR/manager/lwi/security** directory.
   c. Click **OK**. You will be prompted for the keystore password.
3. Create a certificate request with the following steps:
   a. On the menu bar, select **Create** → **New Certificate Request**.
   b. Enter a descriptive string for the **Key Label**.
   c. Enter the fully qualified host name for the **Common Name**.
   d. Enter appropriate values in the other fields.
   e. Enter the name of a file in which to store the certificate request. You will submit this file to a CA.
4. Send the certificate request file to a CA for signing.
5. Receive the signed certificate and complete the following steps:
   a. In the **Key** database content area, click **Personal Certificates**.
   b. Select the **Receive** button. You are prompted for the location of the signed certificate.
   c. Enter the location of the signed certificate.
   d. Click **OK**. The signed certificate is added to the keystore.
6. Add the CA's public key to the client browser's truststore. Most browsers already have the CA public keys of well-known CAs in their truststore, so this step is usually not necessary. If you find that it is necessary, your CA should provide you with instructions.

WPAR agent secure certificates

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

The following files are included in the directory:

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

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

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

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

Troubleshooting WPAR Manager

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

Log file locations

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

WPAR Manager logs

Table 3. WPAR Manager logs

Log file	Description
/var/opt/IBM/WPAR/manager/lwi/logs/error-log-*	WPAR Manager log files
/var/opt/IBM/WPAR/manager/lwi/logs/trace-log-*	WPAR Manager trace log files

Agent manager logs

Table 4. Agent manager logs

Log file	Description
/var/opt/IBM/WPAR/cas/agentmgr/logs/rcp.log.*	Agent manager log files

WPAR agent logs

Table 5. WPAR agent logs

Log File	Description
/var/opt/IBM/WPAR/agent/logs/WPARAgent.*	WPAR agent log files
/var/opt/IBM/WPAR/cas/agent/logs/rcp.log.*	Common agent log files

Checkpoint and restart logs

All mobility operations on the WPAR agent create log files on the system. You can use these log files to troubleshoot problems with relocating WPARs between managed systems. The WPAR agent creates a directory path to store the **mcr.log** file based on the following:

- The location you configured for state files
- The name of the WPAR you are migrating
- The host name of the source server

The log file path is also added to the beginning of the base directory for system WPARs.

For example, if the WPAR being relocated has the following specifications:

- Location of state file, **/var/adm/WPAR**
- Name, `wpar1`
- Source server hostname, `host1.domain.com`

The log file is located in the **/wpars/wpar1/var/adm/WPAR/wpar1/host1.domain.com/mcr.log** directory for system WPARs, and the **/var/adm/WPAR/wpar1/host1.domain.com/mcr.log** directory for application WPARs.

Table 6. Checkpoint and restart logs

Log file	Description
/wpars/wparname/state_path/wparname/ source_hostname/mcr.log	System WPAR checkpoint and restart log files
/state_path/wparname/source_hostname/mcr.log	Application WPAR checkpoint and restart log files

Verifying the agent manager is online

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

To view the agent manager configuration, go to the following URL:

```
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 URL:

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

Problem determination for checkpoint and restart

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

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.

Relocation fails for a system WPAR

Relocation fails for system WPARs.

Probable cause

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

Action

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

For more information about re-configuring the WPAR agent, see “Configuring the WPAR agent to use a different agent manager” on page 8.

Relocation fails for an application WPAR

Relocation fails for an application WPAR with the following message: `AKMWA0007E The operation failed due to an invalid state directory.`

Probable cause

The state file root directory is not NFS-mounted on either the departure managed system, the arrival managed system or both managed systems. The location of this directory is defined on the **Application Configuration** panel. The default location of the state file is **/var/adm/WPAR**.

Action

Refer to “Configuring application mobility for application WPARs” on page 7 for information on how to configure the environment to enable application mobility for application WPARs.

Managed system missing

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

Probable cause

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

Action

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

   Related tasks

   "Installing the WPAR agent on the managed system" on page 5
   The WPAR agent is software that runs on a managed system and communicates with the agent manager component of WPAR Manager. After you install the WPAR agent, it performs actions on the managed system.

Deploy operation of a WPAR fails because of permissions

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

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

```
mkwpar: Creating filesystems...

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

Probable cause

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

Action

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

Managed system marked offline

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

Probable cause

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

Action

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

1. Ensure the WPAR Manager can communicate with the agent HTTP port (the default is 9510) and is not blocked by a firewall.
2. Go to the **Managed Systems** view, select the managed system, and click **Update**.

3. Set **log.level** to `FINEST` in the **/opt/IBM/WPAR/agent/conf/wparagent_logging.properties** file and restart the agent. Tracing and debugging information is added to the agent log files in the **/opt/IBM/WPAR/agent/logs** directory.
4. Verify that the DB2 instance home directory file system is not full with the following command:

   ```
   df -m /home/db2wmgt
   ```
5. Uninstall and reinstall the agent.

Task fails in the Task Details page

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

Probable Cause

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

Action

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

Managed server discovery fails

The WPAR Manager fails to discover an agent.

Probable cause

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

Action

1. Verify that the agent is started on the managed system by viewing the **/opt/IBM/WPAR/agent/bin/wparagent** file.
2. Examine the **/opt/IBM/WPAR/agent/cas/logs/rcp.log.0** file for any error messages related to registration. For example, if the registration password is invalid, the log will contain the following error message:

   ```
   SEVERE: BTC5074E The common agent registration failed. The failure was caused by
    exception: Agent Manager returned: CTGEM0020E An agent registration request from
    <ip_address> was rejected because the password is not correct. The password
   that was specified is *****.
   ```
3. Verify that the WPAR agent can resolve the IP address of the host name passed to the **configure-cas** script.
4. Examine the log files in the **/opt/IBM/WPAR/manager/logs** directory for any error messages from registration.

   Related tasks

   "Configuring the WPAR agent to use a different agent manager" on page 8
   After you successfully configure the WPAR agent, you must run the configuration script with the **-force** flag to use a different agent manager.

Deploy operation fails because of incorrect IP address

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

The **Error** tab in the operations details displays the following error:

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

Probable cause

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

Action

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

Application mobility

Application mobility is the process of relocating a WPAR.

The relocation process includes the following steps:

1. Pausing running applications and other services within a WPAR
2. Performing a checkpoint to save execution states to a checkpoint file
3. Restoring the execution state on a different, compatible system or logical partition
4. Restarting the applications and other services from the restored execution state
5. Deleting the relocated WPAR on the old system

System compatibility

System compatibility refers to whether the departure and arrival systems are similar enough that you can relocate a WPAR from one system to another.

Compatibility is evaluated on the following criteria:

- Hardware levels (POWER4 or POWER5)
- Installed hardware features
- Installed devices
- Operating system levels and patch levels
- Other software or file systems installed with the operating system
- Additional user-selected tests

Compatibility testing for application mobility

Compatibility testing includes critical tests and optional tests. Each time a system is registered, the WPAR Manager starts a background process that compares the new system’s properties to the system properties of all previously registered systems. These compatibility tests help to determine if a WPAR can be relocated from one managed system to another.

All critical tests must pass for one managed system to be considered compatible with another. The critical compatibility tests check the following compatibility criteria:

- The operating system type must be the same on the arrival system and departure system
- The operating system version on the arrival system must be at least as high as the version on the departure system.
- The processor class on the arrival system must be at least as high as the processor class departure system.
- The operating system level on the arrival system must be at least as high as the level on the departure system.

- The version, release, modification, and fix level of the **bos.rte** file set on the arrival system must be at least as high as the level on the departure system.
- The version, release, modification, and fix level of the **bos.wpars** file set on the arrival system must be at least as high as the level on the departure system.
- The **bos.rte.libc** file must be the same on the arrival system and the departure system.
- There must be at least as many storage keys on the arrival system as on the departure system.

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

- NTP must be enabled on the arrival system and the departure system.
- The amount of physical memory on the arrival system must be at least as the amount on the departure system.
- The processor speed for the arrival system must be at least as high as the processor speed for the departure system.

Compatibility testing occurs in the background, starting when a system has registered, therefore the results for a particular system might not be immediately available. The amount of time required to complete testing for a system depends on the number of systems currently registered with the WPAR Manager. You can view a the compatibility status for a WPAR from the Managed System Properties view. A system will not be available for relocation in the WPAR Manager until compatibility testing is complete.

Compatibility states

Depending on the results of compatibility testing, two managed systems might be fully compatible, outbound compatible, inbound compatible, or incompatible.

The compatibility states are as follows:

Fully compatible

All critical and user-selected tests comparing the system properties of the departure system to the system properties of the arrival system pass. All tests comparing the properties of the arrival system to the departure system also 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.

Outbound compatible

Compatibility testing shows that a WPAR can be relocated from the departure system to the arrival system, but it cannot be relocated back from the arrival system to the departure system. Relocation to a newer hardware environment might require changes to an application that cannot be reversed, or the application might begin to exploit certain hardware features, causing a relocation back to an earlier hardware version to fail.

Inbound compatible

Compatibility testing shows that a WPAR can be relocated from the arrival system to the departure system, but it cannot be safely relocated from the departure system to the arrival system.

A system that is inbound compatible is not a good candidate for relocation. If the WPAR were already on the arrival system it could be moved back to the original system. A failure might occur if you try to move the WPAR to the inbound compatible system, but it is possible, in some cases, that the relocation might succeed.

Incompatible

Compatibility testing shows that a WPAR cannot be safely relocated either from the departure system to the arrival system, or from the arrival system to the departure system.

A failure will probably occur if you try to move the WPAR to the incompatible system, but it is possible, in some cases, that the relocation might succeed.

WPAR states

A WPAR can be in the defined, active, paused, or frozen state.

The characteristics of these states are as follows:

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 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 have not been saved. The WPAR can be resumed or checkpointed. The frozen state is indicated by an `F` when you run the **lswpar** command.

Relocation domains and system profiles

A relocation domain is a grouping of managed systems that you create. The relocation domain identifies a group of systems that serve the same purpose and is used to generate system profiles. Each relocation domain includes a separate system profile for the different hardware configurations of the managed systems in the relocation domain.

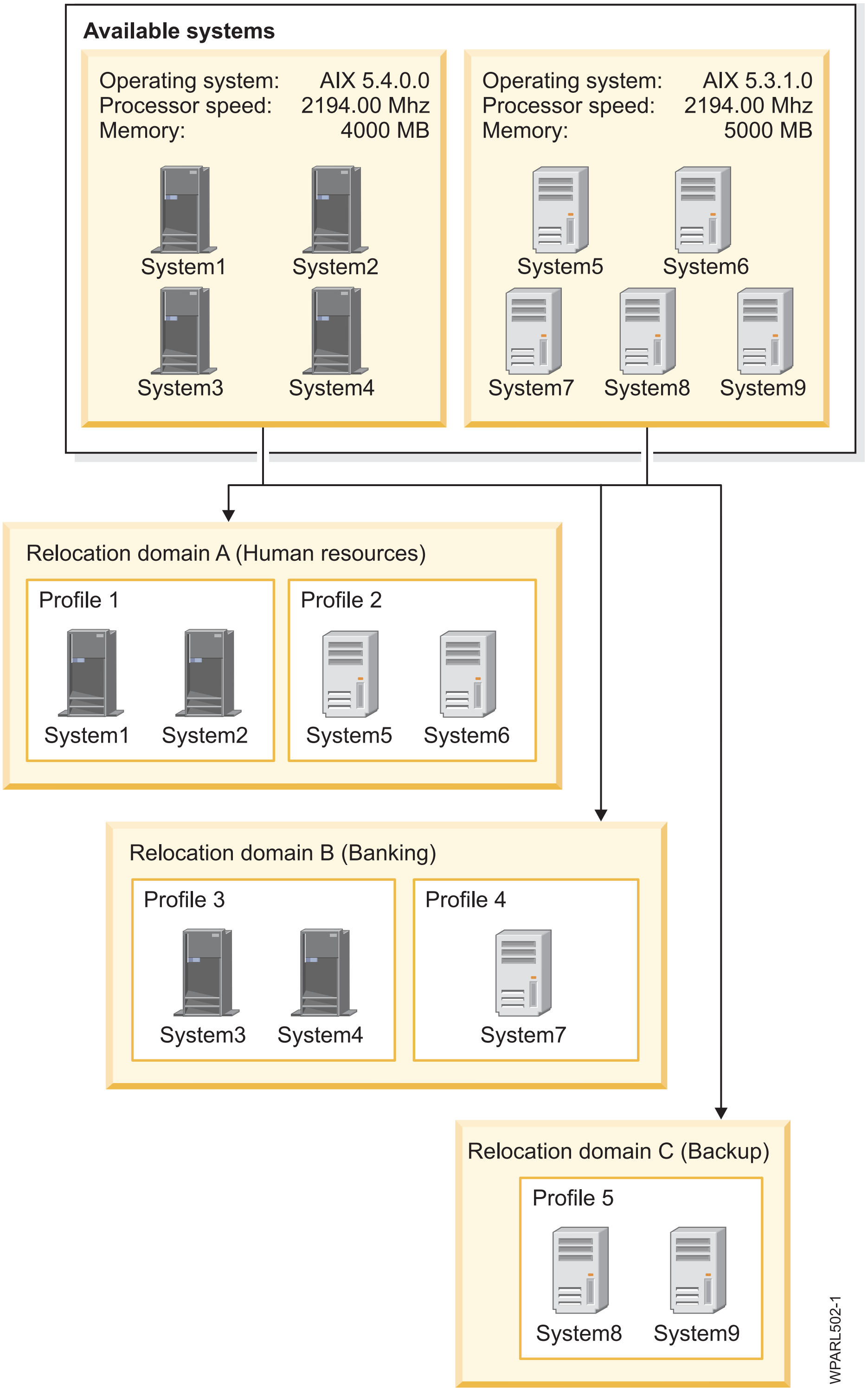
If you have multiple managed systems that are used for different purposes, you can tag each system with a relocation domain that matches its function, and tag similar systems with the same relocation domain. A managed system can belong to one relocation domain, and all managed systems are added to the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

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

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

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

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



Manual relocation

You can manually relocate WPARs that have been properly configured to support the relocation using WPAR Manager. When a WPAR is relocated, the full context of the applications running within the WPAR is captured so it can be restarted on a different system without interrupting the services provided by the WPAR.

Before you relocate a WPAR, you must complete the following tasks:

- Ensure your environment meets the requirements to support relocation
- Configure your environment appropriately so that mobile WPARs can be created
- Create a WPAR that can be relocated

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

Automatic selection
Automatic selection is based on the policy specified in the WPAR group to which the WPAR belongs, the current use of the systems that match the system profiles specified by the policy, and the current resource use of the WPAR. The system selection is also based on the compatibility status between the current system and the candidate. Only fully compatible systems are considered as candidates for hosting the WPAR. Managed systems that belong to the same relocation domain specified in the policy are analyzed and a system is selected as the best available fit for the WPAR being considered for relocation.

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

To start the relocation process, expand the **Guided Activities** section of the navigation area, and select **Relocate Workload Partition**. You can then use the wizard to guide you through the relocation process.

Policy-based relocation

WPAR mobility is governed by relocation policy settings that are contained within the definition of each WPAR group. The WPAR relocation policy defines the set of performance metrics that are analyzed to determine when a specific WPAR in a group is relocated.

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

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

Metric policy settings

For each performance metric that you select, you must configure metric policy settings for the WPAR Group relocation policy.

The metric policy settings are as follows:

Weight
Defines the relative strength of a metric compared to the other metrics in a relocation policy. The minimum value for this setting is zero, but at least one metric must have a weight greater than zero to calculate a performance state value. The WPAR Manager calculates the weighted average

of metrics in a relocation policy and uses the result to indicate performance state. If all metric weight properties are set to zero, then the weighted average calculation always returns a zero value.

Limit Represents either of the following:

Utilization metric
A percentage of utilization of some resource, such as CPU or memory. For a utilization metric, the value of the **limit** property cannot be changed from the default value of 1.

Rate metric
A measurement of some state value with no clearly-defined upper limit, such as process count, application response time, or disk throughput. In order to normalize all relocation policy metrics to calculate a weighted average performance state, the WPAR Manager must know what the maximum expected value should be for a performance metric of this second type. The WPAR Manager divides the measured value of the metric by the limit value that you specify to convert a rate or count metric into a percentage of the expected maximum value.

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

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

Group policy settings

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

The following group policy settings are required:

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

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

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

to the group maximum and minimum values. If the result of this calculation is above or below the maximum or minimum, then a WPAR relocation is ordered, adjusting the averaging period allows the user to tune how responsive the WPAR Manager is to load spikes. A short averaging period results in averaging fewer metric values and increased sensitivity to load spikes. A longer averaging period allows more metric samplings to be included in the performance state calculation, which decreases sensitivity to transient load.

Policy tuning

Relocation policy for WPAR Manager is based on the premise that the application's performance state is strongly correlated with the values of key performance metrics. When analyzed in the context of the total resources available in the hosting logical partition, these metrics can accurately indicate high or low resource demand by processes running in the WPAR.

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

```
(WPAR Utilization)/(1-(LPAR Utilization-WPAR Utilization))
```

In this example, this equation will resolve to 20% only when no other processes are consuming any cpu cycles on the LPAR. This allows the WPAR Manager to accurately determine when resources are constrained for a particular WPAR without instrumentation of the deployed application or the hosting LPAR. The primary consideration when selecting which metrics should be monitored in the WPAR group's policy settings is the magnitude of the linear correlation between the value of a specific performance metric and some key measurement of application performance. The most common measurement of application performance is application response time (ART). The WPAR Manager is designed to manage similar applications deployed within a WPAR group. Consequently, ART measurements for a WPAR group should come from source transactions that do not traverse multiple WPAR groups. What this means is that if a test transaction involves dynamic content generated by an application server cluster deployed within a WPAR group, the generated content should not be dependant upon data retrieved from a database deployed within a different WPAR group. Instead, the test transaction for the application server WPAR group should be set up so that the generated content is retrieved from the local file system, and a separate test transaction should be used to determine the ART for the database WPAR group. Separate WPAR relocation policies should be created for the two WPAR groups so that they can be managed independently, eliminating the need for instrumentation of the application stack.

Group averaging

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

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

Table 7. Group and policy structure of a 3-tiered enterprise application

Application tiers	Relocation policy
Transaction servers	Group 1 policy
Application servers	Group 2 policy
Database servers	Group 3 policy

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

Checkpoint and restart

The checkpoint and restart function is used to implement application mobility in the WPAR Manager, but you can also run checkpoint and restart commands from the command line to pause and resume WPAR operations without relocating the WPAR. Checkpoint and restart enables you to optimize and protect 32-bit and 64-bit applications running in system WPARs or application WPARs across multiple physical systems.

You can checkpoint and restart WPARs to protect them against failures or to balance loads across systems at a production site. Checkpoint and restart can be used with the following types of applications:

- Multi-processed and multi-threaded 32-bit applications
- Multi-processed and multi-threaded 64-bit applications
- Statically linked applications
- Dynamically linked applications
- Off-the-shelf applications and custom applications

Checkpoint and restart operates transparently at the application level, capturing the full context of the application memory, including the following:

- Resources
- Process hierarchies
- States
- Signals
- Inter-process communication pipes
- Semaphores
- Shared memory
- Open files
- TCP/IP sockets

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

Checkpointing a system WPAR and restarting it on the same physical system

You can create a system WPAR that can be checkpointed and restarted on the same system.

1. Create a system WPAR that can be checkpointed, named *mywpar*, by defining an IP address and by mounting its file system on NFS, as shown in the following example:

   ```
   mkwpar -c -N address=10.5.1.0 -M directory=/ vfs=nfs dev=/dir1 host=myhost -n mywpar
   ```

2. Start the WPAR, as shown in the following example:

   ```
   startwpar mywpar
   ```

3. Create a checkpoint directory, as shown in the following example. The directory must be accessible from within the WPAR.

```
mkdir /wpars/mywpar/tmp/chkpt
```

4. Checkpoint and kill this WPAR, as shown in the following example. You must run this command from the global environment.

   ```
   /opt/mcr/bin/chkptwpar -k -d /wpars/mywpar/tmp/chkpt mywpar
   ```

5. Restart the WPAR on the same system, as shown in the following example:

   ```
   /opt/mcr/bin/restartwpar -d /wpars/mywpar/tmp/chkpt mywpar
   ```

Checkpointing a system WPAR and restarting it on a different physical system

You can create a system WPAR that can be checkpointed and restarted on a different physical system and can take advantage of application mobility.

The following procedure demonstrates how to checkpoint a system WPAR from one physical system (*host1*) and restart it on a different physical system (*host2*):

1. On *host1*, create a system WPAR that can be checkpointed, named *mywpar*, by defining an IP address and by mounting its file system on NFS, as shown in the following example. Save the specification file for this WPAR in a shared directory that can be accessed by *host2*.

   ```
   mkwpar -c -N address=10.5.1.0 -M directory=/ vfs=nfs dev=/dir1 host=myhost\
   -o /dir1/tmp/specfile -n mywpar
   ```

2. On *host1*, create a checkpoint directory, as shown in the following example. The directory must be accessible from within the WPAR.

   ```
   mkdir /wpars/mywpar/chkpt
   ```

3. On *host2*, create the same WPAR using the specification file you created earlier, as shown in the following example:

   ```
   mkwpar -pf /dir1/tmp/specfile
   ```

4. On *host1*, start the WPAR, as shown in the following example:

   ```
   startwpar mywpar
   ```

5. On *host1*, checkpoint and kill this WPAR, as shown in the following example. You must run this command from the global environment.

   ```
   /opt/mcr/bin/chkptwpar -d /wpars/mywpar/chkpt -k mywpar
   ```

6. On *host2*, restart the WPAR on the same system, as shown in the following example. You must run this command from the global environment.

   ```
   /opt/mcr/bin/restartwpar -d /wpars/mywpar/tmp/chkpt mywpar
   ```

Checkpointing and restarting an application WPAR

You can start an application WPAR that can be checkpointed and restarted on the same system.

1. Start an application WPAR that can be checkpointed, named *mywpar*, as shown in the following example:

   ```
   wparexec -c -n mywpar -- /usr/bin/myapplication myargument
   ```

2. Checkpoint and kill this WPAR, as shown in the following example:

   ```
   /opt/mcr/bin/chkptwpar -k -d /tmp/checkpoint mywpar
   ```

3. Restart the WPAR on the same system, as shown in the following example:

   ```
   /opt/mcr/bin/restartwpar -d /tmp/checkpoint mywpar
   ```

Checkpointing and restarting an application WPAR that is running a command

You can checkpoint an application WPAR and call a command when the WPAR is restarted.

This procedure demonstrates how to call a command when you restart your application WPAR. The command is a script called *my_usercommand*.

1. Create a user command that can be called during the restart of the application WPAR, as shown in the following example:

   ```
   vi /tmp/my_usercommand
   ```

   ```
   #!/bin/sh
   echo -e "The application WPAR name is $1"
   exit 0
   ```

2. Start an application WPAR that can be checkpointed, named *mywpar*, as shown in the following example:

   ```
   wparexec -c -- /usr/bin/myapplication myargument
   ```

3. Checkpoint and kill this WPAR, as shown in the following example:

   ```
   /opt/mcr/bin/chkptwpar -k -d /tmp/checkpoint mywpar
   ```

4. Restart and pause the WPAR on the same system and call the previously defined user command, as shown in the following example:

   ```
   /opt/mcr/bin/restartwpar -p -u /tmp/my_usercommand -d /tmp/checkpoint mywpar
   ```

5. Resume the application WPAR, as shown in the following example:

   ```
   /opt/mcr/bin/resumewpar mywpar
   ```

Problem determination for checkpoint and restart

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

Restart of a system WPAR fails

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

Probable cause

Restart must always be processed from the Global Environment, not from within the WPAR.

Action

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

Restart of a system WPAR ends

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

Probable cause

The checkpoint directory that you supplied does not exist.

Action

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

Checkpointing a system WPAR fails

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

Probable cause

Checkpoints must always be processed from the Global Environment, not from within the WPAR.

Action

1. Verify that you are running the checkpoint while you are logged in to the WPAR. Checkpoints must always be processed from the Global Environment, not from within the WPAR.
2. If it is not the case, then check if the WPAR you are checkpointing exists on your server. It must exist and be active.

Checkpointing a system WPAR fails because of the checkpoint directory

Checkpointing a system WPAR fails with the following error: `Invalid statefile`.

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

Probable cause

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

Action

Make sure that the checkpoint directory can be reached from the Global Environment and from within the WPAR, otherwise the checkpoint will fail.

Checkpoint and restart commands references

There are several commands for checkpoint and restart that are unique to the WPAR Manager environment.

chkptwpar command

Purpose

Checkpoints a running workload partition (WPAR).

Syntax

To checkpoint an active WPAR

chkptwpar -d */path/to/statefile* [**-o** */path/to/logfile* [**-l** *debug* | *error*]] [**-k** | **-p**] *wparname*

To freeze an active WPAR

chkptwpar -f-d */path/to/statefile* [**-o** */path/to/logfile* [**-l** *debug* | *error*]] *wparname*

To checkpoint a frozen WPAR

chkptwpar [**-k** | **-p**] *wparname*

Description

The **chkptwpar** command checkpoints a WPAR into a state file. The checkpoint is achieved in three steps:

1. All kernel tasks in the WPAR are interrupted and synchronized to reach a quiescence point.
2. The context of the WPAR is written to the state file.
3. The WPAR resumes running or terminates if the user wants to migrate the WPAR to another node.

The **-f** flag, the **-p** flag and the **-k** flag allow fine-grained control on the checkpoint sequence. If none of these flags are used, the WPAR is check-pointed, and it resumes running.

Note: Processes running in a session initiated by the **clogin** command cannot be checkpointed.

Flags

-d /path/to/statefile
Specifies the path where all WPAR state files are stored. If the specified checkpoint directory does not exist, it is created. If the specified checkpoint directory already exists, it must be empty.
Note: This path belongs to the global environment namespace, but it should point to a directory that is accessible within the WPAR.

-f
Freezes all processes for *wparname* without performing a checkpoint. All processes remain frozen until you run the **resumewpar** command or the **chkptwpar** command.

-k
Stops all processes for *wparname* and stops the WPAR after the checkpoint is finished. This flag has the same effect as running the **stopwpar** command with the **-F** flag.

-l debug | error
Controls log level for error report. The possible values are:

ERROR

DEBUG

You must specify the **-o** flag if you use the **-l** flag. The default log level is ERROR. DEBUG enables verbose log messages. You should only use this level for debugging because it could affect performance.

-o /path/to/logfile
Specifies the path where log file are stored. There is no default value.
Note: This path belongs to the global environment namespace, but it should point to a directory that is accessible within the workload partition WPAR.

-p
Pauses all of the processes for *wparname* at the end of the checkpoint. The WPAR remains paused until you resume it with the **resumewpar** command or stop all of the processes with the **killwpar** command.

Exit status

This command returns the following exit values:

0	The command was successful.
1	Invalid command line arguments.
3	There is not enough free memory to checkpoint the WPAR. Run the command again.
4	An internal error occurred.
5	There are not enough free system resources to checkpoint the WPAR. Run the command again.
6	Some devices or processes temporarily cannot be checkpointed. Run the command again.

7	The resource cannot be checkpointed. Resources such as deleted, shared, mapped files, shared writable maps, and the NFS subsystem do not support mobility.
8	The command can only by run by root.
9	Some resources were altered during checkpoint. The WPAR execution is likely to be impacted.
10	Checkpoint failed because a process needed too many file descriptors. Raising the limit on opened files in the WPAR might resolve the error.
15	There is a version mismatch between the **chkptwpar** command and the currently loaded **MCRK** kernel extension. You should reload the kernel extension by running the **mcrk_admin** command or by rebooting.
16	Unknown WPAR name.
17	The WPAR is currently busy in a checkpoint and restart operation. Wait for the operation to complete and try to checkpoint again.
18	The application running in the WPAR exited before the checkpoint could begin.
19	The WPAR is not configured to be checkpointed.
21	The state file path is invalid. For system WPARs, remember that the state file must be accessible from within the WPAR.
22	There is not enough space in the state file.
23	The state file path should point to an empty directory. Delete all files in the state file and try again.
24	The state file could not be created because of incorrect access rights.
25	A state file entry could not be initialized correctly. Try again with a shorter state file name. This error can also occur if the state file has changed between a checkpoint pause and a checkpoint continue operation.
26	The log file path is invalid. For system WPARs, remember that the log file must be accessible from within the WPAR.
28	An error occurred while interacting with the DR subsystem. Check the DR logs.

Security

Only the root user can run this command.

Examples

1. To checkpoint and system WPAR named *wpar1*, run the following command:

   ```
   chkptwpar -d /wpars/wpar1/statefile wpar1
   ```

2. To checkpoint and pause an application WPAR named *wpar2*, run the following command:

   ```
   chkptwpar  -d /statefile -p wpar2
   ```

3. To freeze an application WPAR named *wpar3*, so it can be checkpointed later, run the following command:

   ```
   chkptwpar -d /statefile -f wpar3   # freezes the WPAR
   chkptwpar wpar3                    # checkpoints the frozen WPAR
   ```

killwpar command

Purpose

Kills a paused workload partition (WPAR).

Syntax

killwpar *wparname*

Description

The **killwpar** command kills all tasks in a WPAR that has been paused by the **chkptwpar -p** command or the **restartwpar -p** command. This command stops the WPAR in the same way as running the **stopwpar -F** command.

Exit status

This command returns the following exit values:

0	The command was successful.
3	There is not enough free memory to checkpoint the WPAR. Run the command again.
4	An internal error occurred.
7	The NFS subsystem do not support mobility.
8	The command can only be run by root.
15	There is a version mismatch between the **killwpar** command and the currently loaded **MCRK** kernel extension. You should reload the kernel extension by running the **mcrk_admin** command or by rebooting.
16	Unknown WPAR name.
17	The WPAR is not paused.
28	An error occurred while interacting with the DR subsystem. Check the DR logs.

Security

Only the root user can run this command.

Examples

To kill a paused system or application WPAR named *wpar1*, run the following command:

```
killwpar wpar1
```

restartwpar command

Purpose

Restarts a checkpointed workload partition (WPAR).

Syntax

restartwpar [**-a**] **-d** */path/to/statefile* [**-o** */path/to/logfile* [**-l** *debug* | *error*]] [**-p** [**-u** *userCommand*]] *wparname*

Description

The **restartwpar** command creates a WPAR from a state file created with the **chkptwpar** command. For application WPARs, the WPAR is created automatically with the **wparexec** command. The WPAR that is created is an exact replica of the checkpointed WPAR.

If the **-p** flag is specified, the WPAR is paused after the restart and before resuming execution.

For system WPARs, the **restartwpar** command returns an exit value as soon as the WPAR resumes execution. For application WPARs the **restartwpar** command returns an exit value only when the WPAR terminates. If the workload partition was correctly restarted, the exit value will be the same as the application that was running in the WPAR. However, if the restart failed, the exit status is one of the values for the **restartwpar** command. If you wants to differentiate restart failure exit values from application exit values, you can use the **-u** flag.

Flags

-a
: Specifies the **-a** flag to the underlying **wparexec** command. This flag is valid only for application WPARs. It directly refers to the **wparexec** command, which recreates the application WPAR. It automatically resolves erroneous or conflicting settings if required.

-d /path/to/statefile
: Specifies the path where all WPAR state files are stored.
Note: This path belongs to the global environment namespace, but it should point to a directory that is accessible within the WPAR.

-l loglevel
: Controls log level for error report. The possible values are:

ERROR

DEBUG

You must specify the **-o** flag if you use the **-l** flag. The default log level is ERROR. DEBUG enables verbose log messages. You should only use this level for debugging because it could affect performance.

-o /path/to/logfile
: Specifies the path where log files are stored. There is no default value.
Note: This path belongs to the global environment namespace, but it should point to a directory that is accessible within the workload partition WPAR.

-p
: Pauses all of the processes for *wparname* at the end of the checkpoint. The WPAR remains paused until you resume it with the **resumewpar** command or stop all of the processes with the **killwpar** command.

-u userCommand
: Runs the specified command when an application WPAR is successfully restarted and paused. The specified command is run with only one argument, the WPAR name. If the command does not complete successfully, it is considered an error and the application WPAR is terminated. The WPAR remains paused until you resume it with the **resumewpar** command or stop all of the processes with the **killwpar** command.
Note: The exit status of the user command is returned by the **restartwpar** command. The exit status must have a value greater than 100 to avoid confusion with exit status values for the **restartwpar** command. If an incorrect status is returned, the **restartwpar** returns 13.

Exit status

This command returns the following exit values:

0	The command was successful.
1	Invalid command line arguments.
3	There is not enough free memory to restart the WPAR. Run the command again.
4	An internal error occurred.
5	There are not enough free system resources to restart the WPAR. Run the command again.
7	The NFS subsystem do not support mobility.
8	The command can only be run by root.
9	The WPAR was restarted but some resources were altered. The WPAR execution is likely to be impacted.
10	Restart failed because a process needed too many file descriptors. Raising the limit on opened files in the WPAR might resolve the error.
11	A file could not be restored because the file system is read-only.
12	A file could not be restored because the file system is full.
13	The user command was called and terminated unexpectedly or returned a status smaller than or equal to 100. The WPAR is stopped.
14	A file expected by the **restartwpar** command could not be found on the file system.
15	There is a version mismatch between the **restartwpar** command and the currently loaded **MCRK** kernel extension. You should reload the kernel extension by running the **mcrk_admin** command or by rebooting.
16	The specified WPAR does not exist. The name of the WPAR might be different from the name in the state file. Run the command again with the same WPAR name.
17	The WPAR is currently busy in a checkpoint and restart operation. Wait for the operation to complete and try to checkpoint again.
19	The WPAR is not configured to be checkpointed. You cannot use it to restart a previously checkpointed WPAR.
20	The state file is incompatible with the WPAR mobility feature on the system.
21	The state file path is invalid. For system WPARs, remember that the state file must be accessible from within the WPAR.
24	The state file could not be processed because of incorrect access rights.
25	Corruption was detected in the state file.
26	The log file path is invalid. For system WPARs, remember that the log file must be accessible from within the WPAR.
27	For application WPARs, the layout of standard I/Os differs from what is in the state file.
28	An error occurred while interacting with the DR subsystem. Check the DR logs.
29	For system WPARs, devices were not initialized in the WPAR.
30	The WPAR file system structures were not restored.
31	The time at restart is earlier than the checkpoint time. You can resynchronize the host clock NTP.

Security

Only the root user can run this command.

Examples

1. To restart a system WPAR named *wpar1*, run the following command:
   ```
   restartwpar -d /wpars/wpar1/statefile wpar1
   ```
2. To restart and pause an application WPAR named *appwpar2* and to invoke a user command when the restart has succeeded run the following command:
   ```
   restartwpar -d /statefile -p -u ucmd appwpar2
   ```

   Related information

   wparexec command

resumewpar command

Purpose

Resumes execution of a paused or frozen workload partition (WPAR).

Syntax

resumewpar *wparname*

Description

The **resumewpar** command resumes execution of a WPAR that has been paused or frozen by the **chkptwpar** command or the **restartwpar** command.

Exit status

This command returns the following exit values:

0	The command was successful.
1	Invalid command line arguments.
3	There is not enough free memory to checkpoint the WPAR. Run the command again.
4	An internal error occurred.
7	The NFS subsystem do not support mobility.
8	The command can only be run by root.
9	The WPAR resumed execution, but some resources were altered during checkpoint. The WPAR execution is likely to be impacted.
15	There is a version mismatch between the **resumewparr** command and the currently loaded **MCRK** kernel extension. You should reload the kernel extension by running the **mcrk_admin** command or by rebooting.
16	Unknown WPAR name.
17	The WPAR is neither paused nor frozen.
28	An error occurred while interacting with the DR subsystem. Check the DR logs.

Security

Only the root user can run this command.

Examples

To resume a paused system WPAR or application WPAR named *wpar1*, run the following command:

```
resumewpar wpar1
```

mcrk_admin command

Purpose

Loads and unloads the **mcrk** kernel extension.

Syntax

Loading the kernel extension

mcrk_admin -l -f */path/to/mcrk* **-m** */path/to/mcrp* [**-q**]

Unloading the kernel extension

mcrk_admin [**-u**] {**-f** */path/to/mcrk* | **-i** *mid*}

Description

The **mcrk_admin** command allows you to load, set up, and unload the **mcrk** kernel extension. Using the **mcrk_admin** command to load the mcrk kernel extension enables application mobility for WPARs.

Flags

-f /path/to/mcrk
Specifies the absolute path to the **mcrk** kernel extension.

-i mid
Specifies the kernel extension ID.

-l
Loads the kernel extension. The **mcrk** kernel extension is registered in the operating system, and it is automatically loaded when you start a mobile WPAR.

-m /path/to/mcrp
Specifies the absolute path to the **mcrp.so** user mode module.

-q
Runs the command in silent mode.

-u
Unloads the kernel extension. The kernel extension is unregistered from the operating system. Reference counting conditions in the operating system might prevent a complete removal of the kernel extension. As a result, the **mcrk** kernel extension might still appear to be present to the **genkex** tool, even if the code is no longer called by the kernel. Running the **slibclean** utility after an indefinite amount of time might free unused kernel objects and make the unloading process effective.

Exit status

This command returns the following exit values:

0	The command was successful.
1	An error occurred.

Security

Only the root user can run this command.

Related information

The **genkex** command

The **slibclean** command

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 agent manager component of WPAR Manager and performs actions on the managed system.

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

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 to enable checkpoint, restart, and relocation at the application level. Application WPARs have less overhead on system resources and are lighter weight compared to system WPARs. Application WPARs do not require their own instance of system services.

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

B

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

C

Checkpoint
To save the state of an active WPAR and to enable relocation and later restart of the WPAR.

Compatibility
The degree of similarity between a potential arrival system, and the system currently hosting the WPAR (the departure system). Compatibility is evaluated in two directions: from the current system to a potential arrival system; and from the arrival system back to the original departure system.

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. In the initial release, there is only one global compatibility policy.

Critical metric
A critical metric is one which, if its value falls outside the specified maximum or minimum values, indicates that a managed system should be immediately relocated to other systems.

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.

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

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

Discovery
Refers to the WPAR Manager registering new managed systems in the environment. Discovery is usually an automatic process following configuration of a managed system, but can be initiated manually from the Managed Systems view.

E

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

L

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

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.

M

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

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

Mobility
The ability to relocate WPARs from one managed system to another. When creating a WPAR, you can specify that the WPAR is enabled for mobility, meaning that the WPAR is capable of being relocated.

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

O

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

P

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

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

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

R

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

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

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

Relocation policy
The set of metrics and rules that determine when a WPAR should be relocated. Relocation policy settings are contained within the properties of a WPAR group.

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

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

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

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

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

S

System WPAR

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

T

Task (event)

A significant WPAR management task initiated either by the WPAR Manager user or by the WPAR Manager in response to policy-driven trigger events. A task can initiate additional tasks, or lower-level workload management operations, as part of its processing.

Transitional state

A WPAR on which an administrative operation is in progress. The WPAR is in the process of being created, started, stopped, or configured.

U

Undeployed state

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

Use metric

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

W

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 in that 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.

WPAR group

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

Appendix. Notices

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

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

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

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

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.

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. 003
11400 Burnet Road
Austin, TX 78758-3498
U.S.A.

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

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

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

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

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.

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.

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.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX
DB2
IBM
PTX
WebSphere®

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

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

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

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

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

Index

Readers' Comments — We'd Like to Hear from You

AIX Version 6.1
IBM Workload Partitions Manager for AIX

Publication No. SC23-5241-00

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Submit your comments using one of these channels:

- Send your comments to the address on the reverse side of this form.
- Send your comments via e-mail to: aix6koub@austin.ibm.com

If you would like a response from IBM, please fill in the following information:

Name	Address
Company or Organization	
Phone No.	E-mail address

Readers' Comments — We'd Like to Hear from You

SC23-5241-00

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Information Development
Department 04XA-905-6C006
11501 Burnet Road
Austin, TX 78758-3493

Fold and Tape **Please do not staple** Fold and Tape

Cut or Fold
Along Line

Printed in U.S.A.

SC23-5241-00