z/OS

IBM

MVS Capacity Provisioning User's Guide

Version 1, Release 13

z/OS

MVS Capacity Provisioning User's Guide

Version 1, Release 13

Contents

Figures

v

Tables

About this publication

This manual supports z/OS (5694–A01). This document contains information to help you use Capacity Provisioning and to make the most of the product.

Who should use this document

This document is intended for system administrators who want to use MVS™ Capacity Provisioning to manage Capacity on Demand, and for system programmers, system analysts, and systems engineers who are responsible for implementing MVS Capacity Provisioning.

Where to find more information

Where necessary, this document references information in other documents, by using shortened versions of the document title. For complete titles and order numbers of the documents for all products that are part of z/OS, see *z/OS Information Roadmap*.

Softcopy Title	Title	Order Number
z/OS Common Information Model User's Guide	z/OS Common Information Model User's Guide	SC33-7998
z/OS MVS Initialization and Tuning Guide	z/OS MVS Initialization and Tuning Guide	SA22-7591
z/OS MVS Initialization and Tuning Reference	z/OS MVS Initialization and Tuning Reference	SA22-7592
z/OS MVS JCL User's Guide	z/OS MVS JCL User's Guide	SA22-7598
z/OS MVS JCL Reference	z/OS MVS JCL Reference	SA22-7597
z/OS Planning for Installation	z/OS Planning for Installation	GA22-7504
z/OS MVS Planning: Workload Management	z/OS MVS Planning: Workload Management	SA22-7602
z/OS MVS Programming: Workload Management Services	z/OS MVS Programming: Workload Management Services	SA22-7619
z/OS MVS Programming: Callable Services for High-Level Languages	z/OS MVS Programming: Callable Services for High-Level Languages	SA22-7613
z/OS MVS Setting Up a Sysplex	z/OS MVS Setting Up a Sysplex	SA22-7625
z/OS MVS System Commands	z/OS MVS System Commands	SA22-7627
z/OS MVS System Messages, Vol 4 (CBD-DMO)	z/OS MVS System Messages, Vol 4 (CBD-DMO)	SA22-7634
System z10™ Enterprise Class Capacity on Demand User's Guide	System z10 Enterprise Class Capacity on Demand User's Guide	SC28-6871
zEnterprise System Capacity on Demand User's Guide	zEnterprise System Capacity on Demand User's Guide	SC28-2605
IBM z/OS Management Facility Configuration Guide	IBM z/OS Management Facility Configuration Guide	SA38-0652

Other Referenced Documents

Softcopy Title	Title	Order Number
z/OS® Security Server RACF® Security Administrators Guide	z/OS Security Server RACF Security Administrators Guide	SA22-7683
z/OS Security Server RACF Security Callable Services	z/OS Security Server RACF Security Callable Services	SA22-7691
z/OS RMF Report Analysis	z/OS RMF Report Analysis	SC33-7991
z/OS UNIX System Services Programming Tools	z/OS UNIX System Services Programming Tools	SA22-7805
z/OS UNIX System Services Planning	z/OS UNIX System Services Planning	GA22-7800
z/OS UNIX System Services Parallel Environment: Operation and Use	z/OS UNIX System Services Parallel Environment: Operation and Use	SA22-7810
PR/SM Planning Guide	PR/SM Planning Guide	GA22-7236
Support Element Operations Guide	Support Element Operations Guide	SC28-6802
System z Application Programming Interfaces	System z Application Programming Interfaces	SB10–7030

The Capacity Provisioning Web Page

For the latest information about capacity provisioning, see the Capacity Provisioning web page at:

`http://www.ibm.com/systems/z/os/zos/features/cpm/index.html`

How to read syntax diagrams

This section describes how to read syntax diagrams. It defines syntax diagram symbols, items that may be contained within the diagrams (keywords, variables, delimiters, operators, fragment references, operands) and provides syntax examples that contain these items.

Syntax diagrams pictorially display the order and parts (options and arguments) that comprise a command statement. They are read from left to right and from top to bottom, following the main path of the horizontal line.

For users accessing the Information Center using a screen reader, syntax diagrams are provided in dotted decimal format.

Symbols

The following symbols may be displayed in syntax diagrams:

Symbol	Definition
►►—	Indicates the beginning of the syntax diagram.
—→	Indicates that the syntax diagram is continued to the next line.
►—	Indicates that the syntax is continued from the previous line.
—►◄	Indicates the end of the syntax diagram.

Syntax items

Syntax diagrams contain many different items. Syntax items include:

- Keywords - a command name or any other literal information.

- Variables - variables are italicized, appear in lowercase, and represent the name of values you can supply.
- Delimiters - delimiters indicate the start or end of keywords, variables, or operators. For example, a left parenthesis is a delimiter.
- Operators - operators include add (+), subtract (-), multiply (*), divide (/), equal (=), and other mathematical operations that may need to be performed.
- Fragment references - a part of a syntax diagram, separated from the diagram to show greater detail.
- Separators - a separator separates keywords, variables or operators. For example, a comma (,) is a separator.

Note: If a syntax diagram shows a character that is not alphanumeric (for example, parentheses, periods, commas, equal signs, a blank space), enter the character as part of the syntax.

Keywords, variables, and operators may be displayed as required, optional, or default. Fragments, separators, and delimiters may be displayed as required or optional.

Item type	Definition
Required	Required items are displayed on the main path of the horizontal line.
Optional	Optional items are displayed below the main path of the horizontal line.
Default	Default items are displayed above the main path of the horizontal line.

Syntax examples

The following table provides syntax examples.

Table 1. Syntax examples
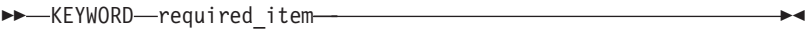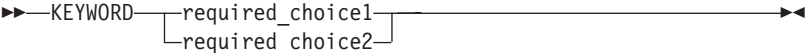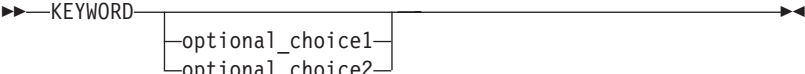
Item	Syntax example
Required item. Required items appear on the main path of the horizontal line. You must specify these items.	►►──KEYWORD──required_item────────────────────────────►◄
Required choice. A required choice (two or more items) appears in a vertical stack on the main path of the horizontal line. You must choose one of the items in the stack.	►►──KEYWORD──┬─required_choice1─┬──────────────►◄ 　　　　　　　　 └─required_choice2─┘
Optional item. Optional items appear below the main path of the horizontal line.	►►──KEYWORD──┬──────────────┬──────────────►◄ 　　　　　　　　 └─optional_item─┘
Optional choice. An optional choice (two or more items) appears in a vertical stack below the main path of the horizontal line. You may choose one of the items in the stack.	►►──KEYWORD──┬──────────────────┬──────────►◄ 　　　　　　　　 ├─optional_choice1─┤ 　　　　　　　　 └─optional_choice2─┘

Table 1. Syntax examples (continued)

Item	Syntax example
Default. Default items appear above the main path of the horizontal line. The remaining items (required or optional) appear on (required) or below (optional) the main path of the horizontal line. The following example displays a default with optional items.	▶▶──KEYWORD──┬─default_choice1─┬──────────────────▶◀ ├─optional_choice2─┤ └─optional_choice3─┘
Variable. Variables appear in lowercase italics. They represent names or values.	▶▶──KEYWORD──*variable*──────────────────────▶◀
Repeatable item. An arrow returning to the left above the main path of the horizontal line indicates an item that can be repeated. A character within the arrow means you must separate repeated items with that character. An arrow returning to the left above a group of repeatable items indicates that one of the items can be selected,or a single item can be repeated.	▶▶──KEYWORD──┬◀─repeatable_item─┬──────────────▶◀ ▶▶──KEYWORD──┬◀─,─repeatable_item─┬────────────▶◀
Fragment. The fragment symbol indicates that a labelled group is described below the main syntax diagram. Syntax is occasionally broken into fragments if the inclusion of the fragment would overly complicate the main syntax diagram.	▶▶──KEYWORD──┤ fragment ├──────────────────▶◀ **fragment:** ├──┬─,required_choice1──────────────────────────┤ └─,required_choice2──┬─,default_choice──┬── └─,optional_choice─┘

How to send your comments to IBM

We appreciate your input on this publication. Feel free to comment on the clarity, accuracy, and completeness of the information or give us any other feedback that you might have.

Use one of the following methods to send us your comments:

1. Send an email to s390id@de.ibm.com
2. Visit the Contact z/OS webpage at http://www.ibm.com/servers/eserver/zseries/zos/webqs.html
3. Mail the comments to the following address:
   IBM® Deutschland Research & Development GmbH
   Department 3272
   Schönaicher Str. 220
   D-71032 Böblingen
   Federal Republic of Germany
4. Fax the comments to us as follows:
   From Germany: 07031-16-3456
   From all other countries: +(49)+7031-16-3456

Include the following information:
- Your name and address
- Your email address
- Your telephone or fax number
- The publication title and order number:
  MVS Capacity Provisioning User's Guide
  SC33-8299–05
- The topic and page number related to your comment
- The text of your comment

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 use the personal information that you supply only to contact you about the issues that you submit.

If you have a technical problem

Do not use the feedback methods listed in "How to send your comments to IBM." Instead, do one of the following:
- Contact your IBM service representative.
- Call IBM technical support.
- Visit the IBM zSeries® support Web page at http://www.ibm.com/servers/eserver/support/zseries/.

Summary of Changes

Summary of Changes
for SC33-8299-05
z/OS Version 1 Release 13

The book contains information previously presented in *z/OS MVS Capacity Provisioning User's Guide, SC33-8299-04* which supports z/OS Version 1 Release 12.

This document contains terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change. Technical changes include:

- Support for user-defined capacity increments for activation of general-purpose capacity
- Support for recurring time conditions
- Usage of CIM Client for Java Version 2 instead of Version 1
- Support for Microsoft® Windows® 7 on the workstation running the Capacity Provisioning Control Center
- Integration of Capacity Provisioning in z/OS Management Facility

Summary of Changes
for SC33-8299-04
z/OS Version 1 Release 12

The book contains information previously presented in *z/OS MVS Capacity Provisioning User's Guide, SC33-8299-03* which supports z/OS Version 1 Release 11.

This document contains terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change. Technical changes include:

- Support for CICS® and IMS™ transaction service classes in workload conditions within a Capacity Provisioning policy
- Simplified setup of the Capacity Provisioning CIM provider
- RACF security definitions simplified and provided as sample
- Detailed status information about the Capacity Provisioning Manager within the Capacity Provisioning Control Center
- Support for management on behalf of averaged PI
- Support for Microsoft® Windows® Vista on the workstation running the Capacity Provisioning Control Center
- Support for new IBM zEnterprise System hardware with Power Save Function

Summary of Changes
for SC33-8299-03
z/OS Version 1 Release 11

The book contains information previously presented in *z/OS MVS Capacity Provisioning User's Guide, SC33-8299-02* which supports z/OS Version 1 Release 10.

You might notice changes in the style and structure of some content in this document. For example, headings that use uppercase for the first letter of initial

words only, and procedures that have a different look and format. The changes are ongoing improvements to the consistency and retrievability of information in our documents. This document contains terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change. The Capacity Provisioning messages were moved and are now available with z/OS MVS System Messages Volume 4, SA22-7634.

**Summary of Changes
for SC33-8299-02
z/OS Version 1 Release 10**

The book contains information previously presented in *z/OS MVS Capacity Provisioning User's Guide, SC33-8299-01* which supports z/OS Version 1 Release 10. Technical changes include:
- An internal BCPiibased communication to the hardware is supported.
- Changing the logical processors and the physical capacity is supported.

**Summary of Changes
for SC33-8299-01
z/OS Version 1 Release 10**

The book contains information previously presented in *z/OS MVS Capacity Provisioning User's Guide, SC33-8299-00* which supports z/OS Version 1 Release 9. Technical changes include:
- The REPORT LOG command was added. For more information, see "REPORT LOG" on page 158.

Part 1. Getting started

Provides an overview of Capacity Provisioning (CP) and how to implement it.

Chapter 1. Introducing z/OS Capacity Provisioning

Performance and capacity management on System z® must ensure that work is processed according to the service level agreements that are in place. Guaranteeing service levels continues to be a relatively static task as long as the workloads being considered are sufficiently stable. However, in many environments, workloads fluctuate considerably over time. Because the total workload or mixture of workloads varies, it can become increasingly difficult to guarantee service levels. With z/OS Workload Management (WLM), incoming work is classified with a performance goal and a business priority. WLM tries to accommodate the goals of all the work in the system. However, even with an ideal WLM service definition, it might not be possible to achieve all specified goals when the total workload increases. In this case, trade-offs must be made. WLM decides which goals can be compromised first, based on the assigned importance level. Discretionary work is displaced first, followed by low importance work.

At some point, however, this solution might not be acceptable, either because the displaced work is relevant from a business perspective, or because it interacts with resources that are required by more important work. When such situation occurs, the processing capacity is increased to accommodate the increased workload. This situation can result in a permanent capacity increase for planned growth or a temporary capacity increase for seasonal or unpredictable peak periods. IBM System z quickly and non-disruptively configures additional processor capacity. That capability is built directly into System z servers. It is provided by IBM Capacity Upgrade on Demand (CUoD) for a permanent increase in processing capability, and IBM On/Off Capacity on Demand (On/Off CoD) for temporary capacity increased.

On/Off Capacity on Demand allows the configuration, for example, of general-purpose processor (CP) capacity and specialty processors, such as zAAPs or zIIPs. Several models of System z10 are subcapacity models. On such models, additional general-purpose processor capacity can be provided by a different capacity level, additional processors, or a combination of the two.

For example, for the z10 EC server, the capacity levels for the CP engine are 7, 6, 5, and 4. Full capacity CP engine is indicated by 7; subcapacity CP engines are indicated by 6, 5, and 4. For the z10 BC server, the capacity levels for the CP engine are A-Z. A full capacity CP engine is indicated by the letter Z. The capacity setting is derived from both the capacity level and the number of CPs. For the z10 EC server, the capacity settings are 4xx, 5xx, 6xx, 7xx. For the z10 BC server, the capacity levels are Axx - Zxx.

What Capacity Provisioning can do for you

z/OS Capacity Provisioning helps you manage the CP, zAAP, and zIIP capacity of System z10 or zEnterprise servers that are running one or more z/OS systems. Based on On/Off CoD, temporary capacity is activated and deactivated with a policy that you define. z/OS Capacity Provisioning simplifies the monitoring of critical workloads, and its automation features can help activate additional resources faster than manual operation.

To accommodate changes to the physical capacity, you might need to change the configuration of logical processors. Capacity Provisioning can configure logical processors online or offline whenever such resources would block a change to the hardware capacity.

When you use Capacity Provisioning, you select different levels of automation to provide you with an appropriate level of control. For more information about these processing modes, see page 36.

For example, you can:
- Activate and deactivate temporary capacity through operator commands
- Activate and deactivate temporary capacity based on a defined schedule, without considering workload performance
- Have the Provisioning Manager suggest changes to the capacity of the System z10 based on the observation of workloads that you define
- Have the Provisioning Manager automatically implement changes to the capacity of the System z10 or zEnterprise server based on the observation of workloads that you define

Considerations for configuring capacity

Configuring additional capacity via On/Off Capacity on Demand can result in additional IBM hardware and software license charges. For more information, see the *System z10 Enterprise Class Capacity on Demand User's Guide*, SC28-6871, zEnterprise System Capacity on Demand User's Guide, SC28-2605,or your IBM sale representative.

There might be additional fees for non-IBM software. In addition, some non-IBM software packages might require new license keys to take advantage of the additional capacity. Check with your software vendor for details.

What are the components of Capacity Provisioning?

z/OS Capacity Provisioning is delivered as part of the z/OS MVS Base Control Program (BCP) component. Capacity Provisioning includes the following:

- Capacity Provisioning Manager (Provisioning Manager)
- Capacity Provisioning Graphical User Interface code
- Sample data sets and files

Capacity Provisioning configuration entities, such as policies and domain configurations, are defined through the Control Center on a workstation. The Provisioning Manager on the z/OS host observes workloads and interacts with the servers defined as part of Capacity Provisioning.

The Capacity Provisioning Manager

The Provisioning Manager monitors the workload on a set of z/OS systems and organizes the allocation of additional capacity to these systems when required. You define the systems to be observed in a domain configuration file. Details of additional capacity and the rules for its allocation are stored in a policy file. These two files are created and maintained through the Control Center.

The Capacity Provisioning graphical user interfaces

There are two graphical user interfaces for Capacity Provisioning:

- The Capacity Provisioning Control Center
- The Capacity Provisioning task in z/OSMF

The Capacity Provisioning Control Center

The Capacity Provisioning Control Center is a desktop application that runs on a Windows workstation. Administrators use this interface to work with provisioning policies and domain configurations.

You can set up a direct connection from the Control Center to the Provisioning Manager, and use it to transfer provisioning policies and domain configurations to the Provisioning Manager, or to query various status reports.

The Capacity Provisioning task in z/OSMF

z/OSMF provides a framework for managing various aspects of a z/OS system through a web browser interface. You use the Capacity Provisioning task in z/OSMF to work with the Capacity Provisioning Manager on your z/OS system. You can set up a connection to the Provisioning Manager and query various status reports.

Capacity Provisioning sample data sets and files

The Capacity Provisioning component includes several samples that simplify customization and speed-up the definition of your provisioning policies:

- Sample jobs for setting up and customizing the Capacity Provisioning component are placed in SYS1.SAMPLIB. The use of these sample members is described in Chapter 3, "Setting up a Capacity Provisioning domain," on page 43.
- The Control Center contains sample domain configurations and policies. These samples are used to illustrate concepts.

Prerequisites

z/OS Capacity Provisioning has certain hardware and software requirements. If your configuration does not meet all these requirements, you cannot use the full functionality of Capacity Provisioning. However, some functions can be used with fewer requirements.

System z hardware requirements

- One or more z10 or zEnterprise servers.
- If temporary capacity is to be controlled by the Provisioning Manager in confirmation or autonomic mode, or if provisioning actions are to be performed through Provisioning Manager commands, temporary capacity must be available. To make temporary capacity available, On/Off CoD must be enabled (feature code 9896 on System z10), as well as a valid On/Off CoD record for temporary general-purpose processor, zAAP, or zIIP capacity.
- Capacity Provisioning communicates with the hardware to get information about the permanent and temporary capacity of the server. The communication types include:
  - **Simple Network Management Protocol (SNMP)** A TCP/IP-based communication that requires a network connection from the z/OS system on which the Provisioning Manager runs to the Support Element (SE) or the Hardware Management Console (HMC). For more information, see *System z Application Programming Interfaces*.

    Note: If you use SNMP communication, support elements (SE) and the optional Hardware Management Console must be at driver level D73G or higher.
  - **BCPii**. A z/OS built-in communication that does not require a network connection. BCPii is the recommended protocol.
  - If more than one processor complex is to be controlled, an HMC is required. The available options are listed in Table 2.

  Note: SNMP support will be removed in a future release. During installation, select BCPii as your protocol. If you are migrating from a previous release and your domain is still configured to use SNMP protocol, the Provisioning Manager issues a warning message when you start. If you are using the z/OS Tracking Facility, you might also notice additional entries from the Capacity Provisioning Manager in there. Entries with the following text can appear: CPO-W:SNMP usage *domain name*.
  The domain name is substituted by the system with the actual name of the domain that is configured to use SNMP. You can configure the Tracking Facility to skip the Capacity Provisioning entries. A sample CNIDTRxx member content can be found in member CPODTR00 in your system SAMPLIB library.

Table 2. Support Element (SE) or Hardware Management Console (HMC) requirements for Capacity Provisioning configuration

Configuration	Communication through System z API (SNMP)	Communication through BCPii
All observed systems and hosting system on one processor complex	HMC (preferred) or SE	SE

Table 2. Support Element (SE) or Hardware Management Console (HMC) requirements for Capacity Provisioning configuration (continued)

Configuration	Communication through System z API (SNMP)	Communication through BCPii
All observed systems on one processor complex; hosting system on a different processor complex	HMC (preferred) or SE	HMC
Observed systems on multiple processor complexes	HMC	HMC

z/OS software requirements

- Monitored systems must use z/OS Release 9, with APAR OA20824 installed, or higher.
- z/OS Resource Measurement Facility™ (RMF™), an optional element of z/OS, must be enabled, or you can use an equivalent product.
- Your z/OS security product must support creation of PassTickets (R_GenSec) and evaluation through the SAF interfaces. If you are using a security product other than IBM Security Server (Resource Access Control Facility, or RACF), check with your vendor.
- Network (SNMP) connectivity from your hosting system to the HMC or SE, if you are using SNMP communication.

Supported LPAR and z/OS environments and restrictions

The IBM System z platform and z/OS provide for great flexibility. Capacity Provisioning supports a broad range of configurations, but certain configurations are not supported or are restricted. Restrictions include:

- Observed systems must be running z/OS Release 9 or higher. Other operating systems or the Coupling Facility Control Code (CFCC), can be active in other LPARs.
- Observed systems that are running as guests under z/VM® are not supported. Do not use a z/OS system running as a z/VM guest to run the Provisioning Manager.
- The version of the Control Center must be compatible with the version of the z/OS system.
- An observed system can run in a shared or dedicated LPAR. An LPAR with dedicated processors, however, can generate demand only for higher general-purpose processor capacity level. If the processor complex is not a subcapacity model but is already operating at its maximum capacity level, additional demand is not recognized. If the LPAR is dedicated, no demand for additional special purpose processors is recognized.
- Demand for additional physical processors, as opposed to increased capacity level, for shared general purpose (CP), zAAP, or zIIP processors can be recognized only if the current sum of logical processors is greater than the number of physical processors in the respective processor pool, or the Capacity Provisioning policy allows for configuring logical processors online.
- Observed systems might have general-purpose CPs, zAAPs, and zIIPs that are configured.
- The additional physical capacity provided through Capacity Provisioning is distributed through PR/SM™ and the operating systems. In general, the additional capacity is available to all LPARs, but facilities such as defined capacity (soft capping) or initial capping (hard capping) can be used to control the use of capacity.
- Do not define provisioning conditions for service classes associated with resource groups for which a capacity maximum is in effect.
- If a system has IRD Vary CPU Management turned on, no logical processors are configured by Capacity Provisioning.
- Logical processors are managed only for systems with shared processors.
- Monitored systems cannot use "initial capping" (hard capping).

- All active LPARs on a CPC must be loaded with an operating system. Active unused LPAR processor resources are recognized as potential absorbers of processor capacity and could result in activation of additional temporary processors that cannot be used.

Workstation requirements

The workstation on which the Control Center runs must meet the following minimum requirements:

- An INTEL Pentium or equivalent processor with 512 MB memory (1 GB recommended)
- At least 150 MB of available disk space
- Microsoft Windows XP Professional, Service Pack 2 or higher or Microsoft® Windows® Vista Version 6.0 or Microsoft® Windows 7. For Windows 7 both 32 and 64 bit versions are supported
- Screen resolution 1024x768 or higher
- If the Control Center is used to connect to the Provisioning Manager, a TCP/IP connection to the z/OS system which is hosting the Provisioning Manager

Chapter 2. Capacity Provisioning basics

It is assumed that the user knows the main Capacity Provisioning concepts and the terms related to them. Capacity Provisioning basics is intended to provide basic knowledge of terms and concepts related to the topic. Capacity Provisioning operates in the following environment:

Field of operation

The scope of a z/OS Capacity Provisioning system is referred to as a Capacity Provisioning Domain, or simply a domain. The domain configuration describes the scope of management within a provisioning domain. The domain includes hardware and software elements. The hardware elements are one or more central processor complexes (CPCs) where temporary capacity can be activated or deactivated by Capacity Provisioning. The software elements are z/OS operating systems that can run on one or more of these CPCs. These elements are monitored by Capacity Provisioning to determine the hardware requirements.

Rules of operation

Provisioning Management is controlled by a Capacity Provisioning Policy, or simply a policy. This policy defines the actions to be performed on the hardware and software elements in response to the demands of the observed software elements. A policy contains rules, which define workload conditions that trigger intervention, resources that can be activated, and time periods during which the rule is applied.

The domain is controlled by the Provisioning Manager. The Provisioning Manager runs in a z/OS system and controls the domain in real time. It observes the software elements and monitors workload demands. It recommends hardware configuration changes to the system operator, or can activate or deactivate hardware and software elements to satisfy these demands.

The Capacity Provisioning software also includes a graphical user interface for the Provisioning Manager, the Control Center.

These concepts are expanded in the overview section. The domain is described on page 13, policies on page 14, the Provisioning Manager on page 15 and the Control Center on page 15.

More information about key points is provided in "Capacity Provisioning in detail" on page 16.

Overview

This information describes the following elements:

- The environment of Capacity Provisioning, or the Capacity Provisioning Domain
- The processing rules, or the Capacity Provisioning Policy
- The program used to run Capacity Provisioning, or the Capacity Provisioning Manager
- The program used to manage Capacity Provisioning, or the Capacity Provisioning Control Center

Capacity Provisioning Domain

The domain consists of:

- Observed systems that can trigger provisioning, as described in "Observed systems" on page 16, and where the number of logical processors can be changed, and
- Central Processor Complexes (CPCs) on which the configuration can be changed, as described in "CPCs" on page 17.

Capacity Provisioning can maintain the configuration of more than one domain for different purposes. Each domain is identified by a unique name.

An example of a domain is:
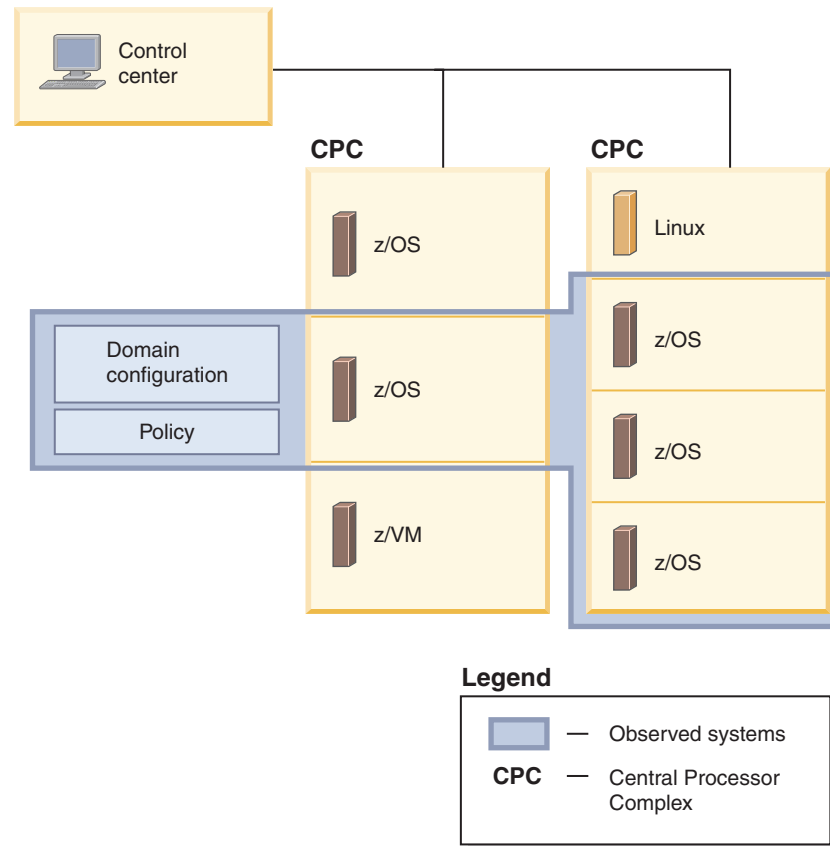
Figure 1. Capacity Provisioning domain

Figure 1 shows an example domain configuration with two CPCs being managed and four systems being observed. Capacity Provisioning can be performed for one or more CPCs. If a sysplex consists of multiple systems, all observed systems of this sysplex must belong to the same Capacity Provisioning domain. One CPC cannot belong to multiple domains. Each system in the domain configuration is identified by its z/OS system name and the name of the sysplex to which it belongs. Systems keep the same name even if they move across LPARs and CPCs.

Capacity Provisioning Policy

The policy describes the scope of management within a provisioning domain. The policy controls the provisioning of additional capacity. Different policies can be created for different circumstances, but only one of these policies can be used by the Provisioning Manager at a time. The policy defines:

- How much additional capacity can be activated
- When this additional capacity can be activated
- What triggers the activation of additional capacity

Each policy has a maximum provisioning scope that defines the total amount of resources that can be activated:

- Maximum amount of general-purpose capacity, in MSU
- Maximum number of Application Assist Processors (zAAPs)
- Maximum number of Integrated Information Processors (zIIPs)

General-purpose capacity can be provided by either additional general-purpose processors (CPs) or by increased processor capabilities.

In the policy, you can optionally specify a logical processor scope that determines the z/OS systems for which the number of logical processors can be changed. For each system, you can either specify the maximum number of processors that can be online at once, or specify that the limit of the LPAR definition applies. If you omit the logical processor definition, the number of processors for an observed system is not managed by Capacity Provisioning.

A policy contains one or more provisioning rules. These rules define limits, or provisioning scope, to the capacity that can be activated, time periods, or time conditions, when activation is possible, and triggers, or workload conditions, that can cause activation.

Rules contain provisioning conditions that describe the situations in which the Provisioning Manager can activate temporary resources under the rule. These situations can include time conditions that indicate periods in which provisioning is allowed, and workload conditions that indicate demand, which in turn triggers activation. Workload conditions are expressed in terms of the z/OS WLM service class model.

Additional capacity can be activated by z/OS Capacity Provisioning only when business critical work is negatively affected. This work is identified at the planning stage and must be specified in the workload conditions of a policy.

Capacity Provisioning Manager

The Provisioning Manager controls a domain. It monitors the observed systems and can activate or propose manual activation of temporary capacity, based on the settings in your active domain configuration and policy.

The specifications of the CPCs to be managed and the systems to be observed are included in a domain configuration. The Provisioning Manager must be able to access these CPCs from every host system it runs on. Information from available CPCs is obtained through a connection to the hardware console. This console can be a service element (SE) or a hardware management console (HMC).

Note: Unless otherwise indicated, the assumed console is HMC. At certain points, however, if it is possible to interchange the two consoles, the term HMC can be replaced with the term SE.

Management of the domain is controlled by a policy that specifies the workload conditions that can trigger provisioning, and the resources that can be allocated under these conditions.

Domain configurations are part of a domain configuration repository, and policies are located in a policy repository. Because these repositories can contain more than one domain configuration or policy, each configuration or policy must be given a unique name. At any given time, only one configuration and one policy can be active in the domain. See "Defining the runtime data sets" on page 49 for more information about repository files.

The Provisioning Manager operates in any one of four processing modes, each with varying powers of autonomy. These modes are described in detail on page 36.

Only temporary capacity activated by the Provisioning Manager is managed by the Provisioning Manager. Resources that are activated manually, either by using Provisioning Manager commands or by using the interfaces available on the HMC, are not managed by the Provisioning Manager.

Capacity Provisioning Control Center

The Control Center is a program that runs under Windows. It holds information in a workspace directory. You can prepare domain configurations and policies in the workspace and transmit these directly from the Control Center to the Provisioning Manager if a communication channel for this is set up. You can also inspect the details of the Provisioning Manager status. When a communication channel is set up, the Control Center connects to the Common Information Model (CIM) server on the system where the Provisioning Manager is active, using the CIM HTTP or CIM HTTPS protocol.

For more information about the Control Center, see page 38, and for the workspace, see page 39.

Capacity Provisioning in detail

Provides details about the Capacity Provisioning domain and policy, Central Processor Complexes, provisioning, and processor scopes, rules, conditions, configurations etc.

Capacity Provisioning Domain

The CPCs to be managed and the systems to be observed are specified in the domain configuration. You can create and edit the domain configuration by using the Control Center. For more information, see page 38. Before you can activate the domain configuration, you must add it to the domain configuration repository of the Provisioning Manager. You can store multiple domain configurations for different purposes in the repository, but only one domain configuration can be active in the domain.

Observed systems

To get information about the workload that is running on a system or to manage the number of processors on that system, the Provisioning Manager must be connected to the system. The information is provided by a CIM server on the system. The domain configuration includes attributes that describe how to connect to each system. One attribute is the host address of the system, another attribute is the protocol to be used, and a third specifies the port on which the CIM server is listening.

Each system has an enabled attribute that specifies whether the Provisioning Manager is allowed to connect to the system and retrieve the information. You can switch this attribute on or off at runtime by using the Provisioning Manager commands ENABLE CONFIGURATION and DISABLE CONFIGURATION described on pages 150 and 146.

CPCs

Temporary capacity must be installed on a CPC before it can be activated. Installed capacity is described in a capacity record, as described in *System z10 Enterprise Class Capacity on Demand User's Guide*. The Provisioning Manager can activate the residual capacity only in this record within limits that are defined during the order process of the record. Some CPCs in a domain might not have temporary capacity. In this case, the Provisioning Manager still reports resource shortages on these CPCs.

The provisioning domain contains a set of logical partitions (LPARs). They can be part of a stand-alone system (a monoplex), or can be part of a sysplex. A z/OS system runs within each LPAR. When you define the domain configuration, you specify the set of z/OS systems to be observed. Each z/OS system is identified by name. If the system is part of a sysplex, the name also includes the name of the sysplex. A system can be observed and considered for capacity changes only if it runs on a CPC in the provisioning domain.

Each CPC in the domain configuration is identified by its logical name, which defines it on the support element (SE) of that processor complex. Each CPC has an enabled attribute that specifies whether the CPC is to be considered for temporary capacity changes. If it is enabled, the Provisioning Manager can change the temporary capacity of that CPC. If it is disabled, only manual capacity changes by using Provisioning Manager commands are allowed. You can switch the enabled attribute on or off at runtime by using Provisioning Manager commands. For more information about the commands, see ENABLE CONFIGURATION and DISABLE CONFIGURATION described on pages 150 and 146.

The temporary capacity on a CPC includes multiple capacity records that are identified with unique record IDs. Only one of these records can be used by the Provisioning Manager at any one time. You can specify the ID of the record to use in the domain configuration, or if there is only one record, you can let the Provisioning Manager find it.

For CPCs that support static power save mode, the Provisioning Manager does not add capacity based on the active policy while static power save is enabled. However, already activated temporary capacity can be deactivated by the Provisioning Manager based on your policy. ACTIVATE RESOURCE and DEACTIVATE RESOURCE commands are not affected by power save mode.

You can enable or disable static power save mode by using the Provisioning Manager commands ENABLE POWERSAVE or DISABLE POWERSAVE or by using the Support Element or Hardware Management Console application.

Capacity Provisioning Policy

The management of temporary resources is based on a policy that contains rules for activation and deactivation. You can create and edit a policy by using the Control Center. When the policy is complete, install it into the policy repository of the domain before it can be activated. You can have multiple policies for different purposes in the policy repository, but at any one time only one policy can be active in the domain.

Figure 2 shows the basic structure of a policy.

Capacity provisioning policy

Logical processor scope

Processor limits

Maximum provisioning scope

Processor limits

Rule

Condition

Time condition

Workload condition

Provisioning scope
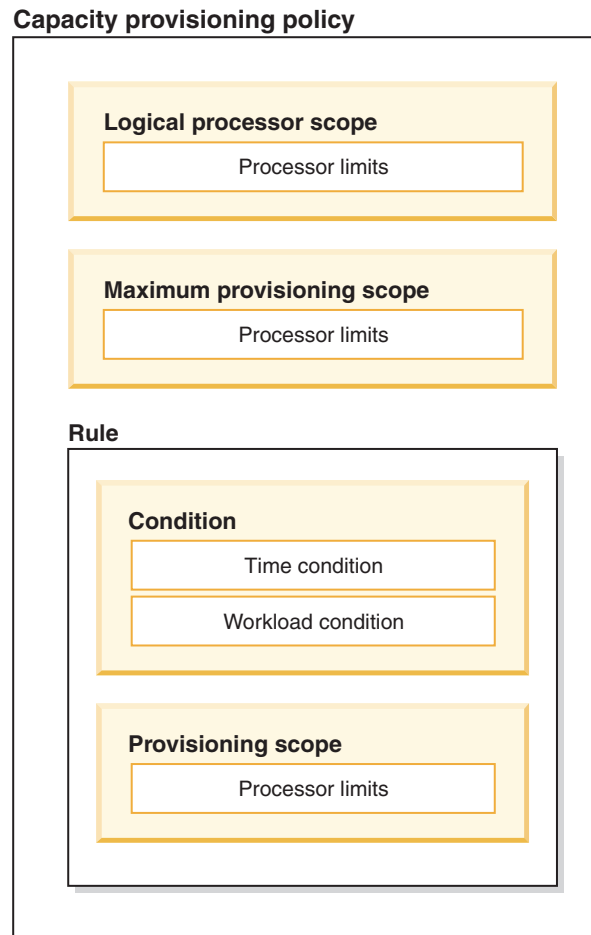
Processor limits

Figure 2. Capacity Provisioning policy structure

The policy contains:

A logical processor scope

Defines the systems in which Capacity Provisioning manages the number of logical processors and which processor limits apply for those systems.

A maximum provisioning scope

Limits the amount of additional resources that can be activated on behalf of the contained rules, and defines the amount in which capacity is incremented.

A set of provisioning rules

A rule contains provisioning conditions and a provisioning scope

limiting the additional capacity that can be provisioned based on the rule. Two types of conditions are supported:

- *Time condition* specifies time periods during which additional capacity can be activated.
- *Workload condition* identifies work which is eligible to cause an activation, and the conditions under which activation can be triggered. Eligible work is specified according to the workload model of the z/OS Workload Manager (WLM).

Each provisioning policy is identified by name. Within a policy, identify rules, provisioning conditions, time conditions, and workload conditions with unique names. These names are used in commands to the Provisioning Manager (for example to enable or disable a rule or a provisioning condition), and in reports from the Provisioning Manager that reference these policy elements.

Maximum Provisioning Scope

Table 3 shows an example of a provisioning scope in which limits are defined for two CPCs, named CPC0 and CPC1. The first definition specifies that 200 MSU and four additional zIIPs can be activated on CPC0, but no zAAPs can be activated on it. The second definition specifies that a maximum of 300 MSU, two zIIPs, and three zAAPs can be activated on CPC1.

Table 3. Provisioning scope

CPC	Maximum MSU	Maximum zAAP processors	Maximum zIIP processors	Primary activation (MSU)	Secondary activations (MSU)
CPC0	200	0	4	1	1
CPC1	300	3	2	70	50

For each CPC, you can also specify the increments in which general-purpose capacity is to be added. There is one increment for the first activation (primary activation) and one increment for all further activations (secondary activations). The capacity increments are specified in MSU and denote the minimum capacity that can be added. The default increment is one MSU, meaning the software model with the next higher capacity. The capacity increments are used for workload-based capacity activation. Each of the increments should not be higher than the maximum capacity specified as maximum MSU. If you specify primary and secondary increments and the next activation would exceed the capacity of either the defined On/Off Capacity on Demand record for the CPC or the capacity of the provisioning scope, the next increment is reduced to activate the maximum allowed remaining capacity.

A Capacity Provisioning policy includes a maximum provisioning scope which defines the total capacity that can be activated at any time by all the rules contained in the policy. Each rule also contains a provisioning scope that restricts the capacity that can be activated by that rule. If the provisioning scope of a rule includes restrictions on CPCs, they must also be included in the maximum provisioning scope, otherwise no additional capacity is activated for these CPCs.

For example, suppose you want to allow one additional zAAP to be activated when an online service class is affected, and one or two additional zAAPs when a batch service class is affected, but you do not want to have more than two additional zAAPs active at the same time. To model this scenario, you define a maximum provisioning scope of two zAAPs and two rules: one for the online

service class with a provisioning scope of one zAAP and one for the batch service class with a provisioning scope of two zAAPs. With these rules, if two additional zAAPs are requested for a batch application and one additional zAAP is requested for an online application at the same time, one of the requests is unfulfilled. Either the batch service class is allocated only one additional zAAP, or the online service class is allocated no additional zAAPs. In total, no more than two additional zAAPs are active at the same time.

Logical Processor Scope

With the logical processor scope, you can define the systems on which Capacity Provisioning manages the number of logical processors, which processor limits apply for these systems, and the type of action to take when changes are required. Table 4 shows an example of logical processor limits:

Table 4. Logical processor scope

System	Sysplex	Maximum CP Processors	Maximum zAAP Processors	Maximum zIIP Processors	Action
SYS1	PLEX1	7	5	3	Message on runtime system
SYS2	PLEX2	*	0	0	Message on managed system

The fields in Table 4 have the following meaning:

System System is identified by its z/OS system name and by the name of the sysplex that it belongs to

Sysplex The name of the sysplex the system belongs to

Maximum CP Processors
The maximum number of CP processors that can be active for the system. The system must allow this number of processors. Alternatively, an asterisk (*) stands for as many logical processors as allowed by the z/OS and LPAR configuration.

Maximum zAAP Processors
The maximum number of zAAP processors that can be active for the system. The system must allow this number of processors. Alternatively, an asterisk (*) stands for as many logical processors as allowed by the z/OS and LPAR configuration.

Maximum zIIP Processors
The maximum number of zIIP processors that can be active for the system. The system must allow this number of processors. Alternatively, an asterisk (*) stands for as many logical processors as allowed by the z/OS and LPAR configuration.

Action The action to be taken by the Provisioning Manager whenever more or fewer processors are required. You can choose between the following actions:

- Message on runtime system. The Provisioning Manager issues a message on the system on which the Provisioning Manager runs. If this message is displayed, follow the recommendation and perform the activation and deactivations on the affected system yourself.

- Message on managed system. The Provisioning Manager issues a message on the system on which the change needs to be performed. If this message is displayed, perform the activation and deactivation on the affected system yourself.

To configure additional logical processors online and offline, your system must have offline logical processors. You can vary these processors offline or define them as reserved processors in the LPAR in which the system is running.

The logical processor scope is observed if the system is running with WLM LPAR CPU management turned off and has shared processors.

Capacity Provisioning puts logical processors online if the number of logical processors puts a limit on the consumption of physical capacity. This situation can occur when only logical processors need to be configured online or offline or when the action is performed in combination with a physical activation. Logical processors are configured offline if the number of logical processors of a system prevents a change to the physical capacity of the CPC on which the system is running. In this case, physical resources deactivation is postponed until logical processors are configured offline. Capacity Provisioning does not attempt to optimize the number of logical processors for the consumed capacity. However, the HiperDispatch function can be used for that purpose.

Systems that are not defined for logical processor management are not considered for offline configuration of logical processors when activating or deactivating physical capacity on the CPC.

Requests to take additional logical processors online or offline are issued in confirmation and autonomic processing modes.

Rules

A rule can be associated with a particular service class. In the provisioning scope, you can limit the additional capacity that can be allocated to applications. You can use time conditions to select periods when you expect significant capacity shortages, and you can identify triggers such as the WLM service class to be associated with an application. Additional capacity is then only activated within periods specified by the time conditions, and when at least one of the associated service classes is negatively affected. Rules are defined for all applications to which additional temporary capacity can be allocated.

A rule can be enabled or disabled. Only enabled rules are considered by the Provisioning Manager. You can specify whether a rule is initially enabled or disabled. This status can be changed at runtime by using the Provisioning Manager commands ENABLE POLICY and DISABLE POLICY. In this way, you can specify different scenarios in the policy and activate only those scenarios that are relevant at any time, or you can temporarily disable provisioning, for example if a maintenance period overlaps with a time condition in the policy.

Provisioning conditions

The workload conditions apply to all time conditions of the provisioning condition. For example, a workload condition can be defined for a service class SC1 associated with month-end jobs, and time conditions can be defined to cause provisioning on January 31st, February 28th, and so on. To consider workloads running on different sysplexes or systems, several workload conditions can be specified. For example, service class SC2 could be specified to trigger provisioning when running in sysplex PLEX1 and service class SC3 to trigger provisioning on system SYS2 only when running in sysplex PLEX2.

All the resources included by the provisioning scope of a rule are shared by all provisioning conditions within that rule. If you want to allocate a different set of resources for a provisioning condition, create a new rule to include this condition.

Provisioning conditions can be enabled or disabled in the same way as rules. Only enabled provisioning conditions are considered by the Provisioning Manager. You can specify in the policy whether a provisioning condition is initially enabled or disabled. This status can be changed at runtime, in the same way as rules, by using the Provisioning Manager commands ENABLE POLICY and DISABLE POLICY. In this way, you can specify different scenarios in the policy and activate only those scenarios that are relevant at a particular time. You can also temporarily disable part of the policy, for example, if a maintenance period overlaps with a time condition.

Time conditions

A time condition defines one or several periods during which the activation of additional resources is allowed.

You can choose between two different types of time conditions:
- Nonrecurring time conditions specify a period with a well-defined beginning and end
- Recurring time conditions describe regularly repeating periods on a weekday basis

Nonrecurring time condition: A nonrecurring time condition specifies one period that has a clear start and end point in time. It is defined by the following parameters:

Name
The time condition identifier within the policy. It must be unique across all nonrecurring and recurring time conditions.

Start time
The time at which the Provisioning Manager can start to activate additional capacity if one of the associated workloads is negatively affected.

Deadline
The latest time when activation of additional capacity is allowed. Additional capacity that has already been activated can remain activated until the end time or until the capacity is no longer needed.

End time
The time at which the Provisioning Manager starts to deactivate additional capacity.

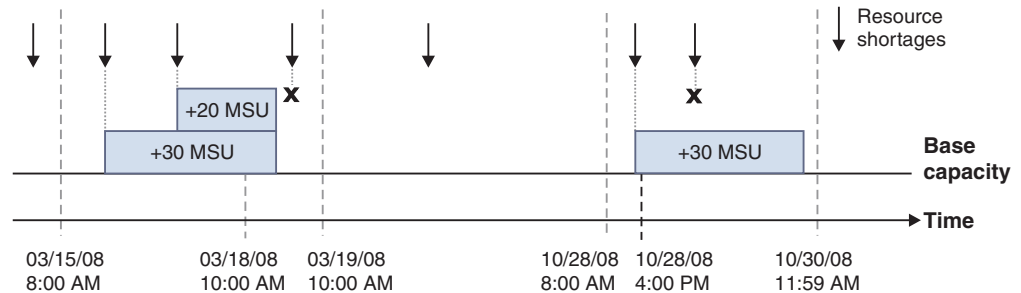| Name	Start time	Deadline	End time
TC1	03/15/08 8:00 AM	03/18/08 10:00 AM	03/19/08 10:00 AM
TC2	10/28/08 8:00 AM	10/28/08 4:00 PM	10/30/08 11:59 AM

Figure 3. Nonrecurring time condition semantics

Figure 3 describes two nonrecurring time conditions and shows how the Provisioning Manager interprets them. On the left, you see the effect of time condition TC1. Resource shortages are only considered between the start time and the deadline; resource shortages between the deadline and the end time cannot trigger activation of additional resources. The boxes represent additionally provisioned general-purpose capacity. On the right, you see the effect of time condition TC2. In this condition, the period between the start time and the deadline is very short compared to the period between the deadline and the end time. This means that additionally provisioned capacity can remain active for a longer period but cannot be increased after the deadline.

Recurring time condition: A recurring time condition describes weekly repeating periods. The periods describe the time of the day when provisioning of resources are allowed and the days of the week to which these times apply.

A recurring time condition is defined by the following parameters:

Name
The time condition identifier within the policy. It must be unique across all nonrecurring and recurring time conditions.

Start date
The date of the first day on which the Provisioning Manager can activate additional capacity.

End date
The date of the last day on which the Provisioning Manager can activate additional capacity.

Allowed days of the week
One or several days of the week that are eligible for activation of additional capacity by the Provisioning Manager.

Start time
The time of the selected day at which the Provisioning Manager can activate additional capacity if one of the additional workloads is negatively affected.

Deadline time The time of the selected day when no further capacity is activated. Additional capacity that is already active remains active until the end time or until the capacity is no longer needed.

End time
The time of the selected day at which the Provisioning Manager starts to deactivate additional capacity.

Deactivation of temporary resources assumes that they have been active for at least a minimum activation time, as specified in the Capacity Provisioning control parameters in Table 14 on page 52. If not, deactivation is delayed to fulfill that duration.
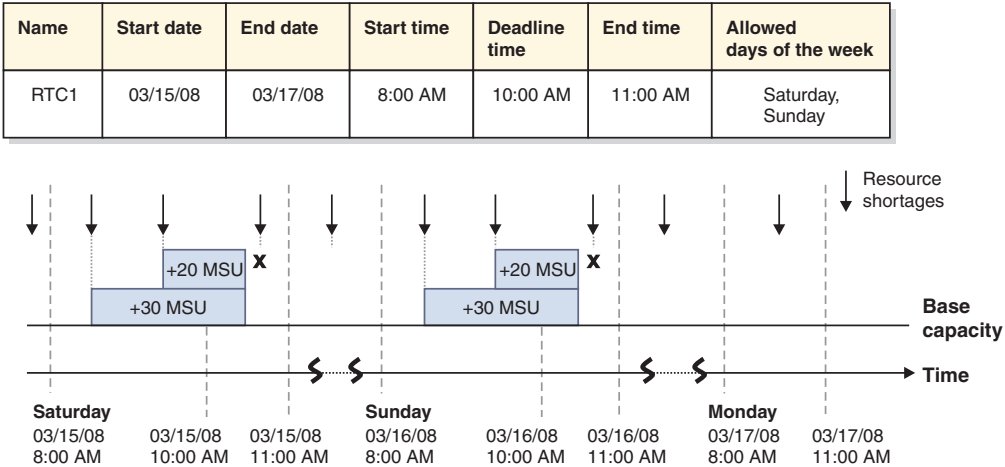
Name	Start date	End date	Start time	Deadline time	End time	Allowed days of the week
RTC1	03/15/08	03/17/08	8:00 AM	10:00 AM	11:00 AM	Saturday, Sunday

Figure 4. Recurring time condition semantics

Figure 4 describes a recurring time condition that covers the weekends: all Saturdays and Sundays from start date until end date are eligible for activation of resources. Activations can occur on any of these days between the start time and the deadline time. Resource shortages that occur at a different day of the week than the selected ones or outside the range that is specified by start date and end date do not trigger resource activations. Activated resources are deactivated as soon as the end time is reached. The example assumes that minimum activation time is short enough to allow deactivations not later than at end time.

Workload conditions

If time conditions are defined in a provisioning condition, but workload conditions are not, the Provisioning Manager schedules the activation and deactivation of additional capacity as specified. The maximum additional allowed resources in the provisioning scope are activated at start time and deactivated at the specified end time.

You use Capacity Provisioning to define business-critical work as being eligible for provisioning by using workload conditions. The concept of a workload condition is based on the WLM service class model:

In a Workload Manager (WLM) service definition, work is assigned to WLM service classes, which are associated with goals, such as a response time.

A service class period describes how an amount of work is managed by WLM. It includes a duration, a goal, and an importance. A service class can be comprised of multiple periods. If the work is not completed within the specified duration, it falls through to the next period.

The importance of a service class period describes its business importance. If not all goals can be met, service classes with a lower importance are provided with less capacity to the benefit of service classes with higher importance.

Service classes are defined for the entire sysplex. The same or different service definitions can be active on different sysplexes.

For more information about WLM service classes, see *z/OS MVS Planning: Workload Management*.

You use a workload condition to activate temporary capacity for business critical service class periods. A workload condition specifies these eligible periods with several parameters:

Name The name of the workload condition uniquely identifies it within the policy and allows Provisioning Manager reports to reference it.

Sysplex
A set of z/OS systems that specifies the set of z/OS systems in which the workload can run.

You use a * to specify that the workload condition apply to all sysplexes observed by the Provisioning Manager.

System
The z/OS system to which the workload condition applies.

You use a * to specify that the workload condition apply to all systems observed on the specified sysplex.

Importance Filters
Eligible service class periods are ranked by their importance. They allocate service class periods by importance level to sets of provisioning criteria; for more information, see "Provisioning criteria" on page 26. The Provisioning Manager checks for temporary resources for all service class periods with an importance level that is equal to or higher than the specified value. You can define separate provisioning criteria for each importance level.

The specification of the importance filter is optional; as an alternative, you can specify included service classes.

For more information about importance filters, see "Importance filter" on page 30.

Included Service Classes
This optional parameter specifies eligible service class periods or additional eligible service class periods by name and period. The Provisioning Manager monitors these periods and takes any required provisioning action. Separate provisioning criteria can be defined for each service class period.

Included Service Classes are specified by service class period filters; see "Service class period filter" on page 30.

Excluded Service Classes Filter
You use the filter to exclude ineligible service class periods which would otherwise be included through an importance filter. They identify sets of service class periods that are not to be considered by the Provisioning Manager.

Excluded Service Class Filters are specified by service class period filters; see "Service class period filter" on page 30.

At least one importance filter or included service class period must be defined for a workload condition to take effect.

The Provisioning Manager determines service class periods to be considered for temporary additional resource as follows:

1. Service class periods with the specified or a higher importance on the specified system in the specified sysplex are chosen first.
2. This set is then extended with the periods contained in the included service classes.
3. Service class periods contained in the excluded service classes are then removed from the set.
4. The Provisioning Manager then checks for temporary additional resources for those service class periods remaining in the set.

Whenever a new WLM service policy is activated, the set of observed service class periods is redetermined.

Because all work running in an eligible service class period can trigger provisioning, verify if the service classes and classification rules in the WLM service definition are properly defined before using these service classes to trigger Capacity Provisioning.

Provisioning criteria: To detect when a service class period is affected by insufficient processing capacity, the Provisioning Manager uses two major indications: the performance index (PI), and the resource demand of the service class period. The resource demand of a service class period can be detected automatically by the Provisioning Manager. You define PI thresholds in the provisioning policy as provisioning criteria that are associated with importance filters or included service classes.

The PI provided by WLM is calculated as the ratio of the specified goal of a service class period to the measured response time or velocity of the work running in this period. A PI of 1.0 indicates that the work is meeting the goal. A PI lower than 1.0 indicates that the work in the service class period exceeds the goal. A PI higher than 1.0 indicates that the goal is not fulfilled. In practice, a PI greater than 1.0 might be adequate for your installation, so you can assign a sufficient or appropriate target PI threshold to each service class period. Capacity Provisioning considers an action if the PI of a defined service class period is greater than the target PI for a specified amount of time. The PI that exceeds the limit for the specified amount of time indicates that WLM or, when active, Intelligent Resource Director (IRD), have not been able to resolve the bottleneck by shifting access to processor resources. The speed at which the Provisioning Manager is to react if a PI exceeds tolerance is also installation-dependent. Individual provisioning criteria can be defined for eligible service classes within the workload condition.

Importance filters and included service classes filters have the following parameters in common:

Table 5. Provisioning criteria

Provisioning criteria	Explanation
Provisioning PI	The value of the performance index, at or above which the Provisioning Manager considers the service class period to be negatively affected.
Provisioning duration	The duration (in minutes) that the performance index must exceed the specified provisioning PI before the Provisioning Manager considers the service class period as being negatively affected. The actual reaction time can be slightly longer than the specified duration. For example, when the performance monitor sampling interval is not aligned with the specified duration.

Table 5. Provisioning criteria (continued)

Provisioning criteria	Explanation
Deprovisioning PI	The value of the performance index which the Provisioning Manager considers the service class period to no longer be negatively affected. The deprovisioning PI must be lower than the provisioning PI.
Deprovisioning duration	The time (in minutes) that the performance index must be less than the deprovisioning PI before the Provisioning Manager considers the service class period to no longer be negatively affected.

PI Scope	Indicates whether the provisioning PI and deprovisioning PI values refer to the sysplex PI or the system PI of the service class period.
	
	System The system PI is the performance index of the service class period on each system in the sysplex. It is also referred to as the local performance index (local PI).
	
	This is the default setting.
	
	Sysplex
	The sysplex PI is the performance index of the service class period within the sysplex. A sysplex PI is only considered if all systems that are joining the sysplex are defined to the provisioning domain.
	
	If you choose PI scope "Sysplex", in addition to monitoring the sysplex PI, the Provisioning Manager monitors the system PI. The Provisioning Manager takes action only if the monitored system is negatively affected.
	
	Note: Some system monitoring products can only display the sysplex PI.
	
	If you use z/OS RMF, you can find the local PI in the
	• RMF Monitor III Data Portal SYSINFO report
	• RMF Monitor III as metric 0x8D1020
	• RMF WLMGL report if
	  – The SYSTEMS option is in effect
	  – Data from a single system only is provided

Provisioning PI and provisioning PI duration are used by the Provisioning Manager to detect whether observed service class periods require help. Before any actions are taken, the Provisioning Manager considers the resource demand of the service class period to ensure that the activation of additional processing capacity can improve the PI. Deprovisioning PI and deprovisioning PI duration are used by the Provisioning Manager to detect when a service class period no longer needs help.

For example, assume that a workload condition is specified including ONLINE service class. This condition is defined with one period of WLM service definition WLMSD, a provisioning PI of 1.8, and duration of 10 minutes, and a deprovisioning PI of 1.2 and duration of 10 minutes. If the PI of the service class period changes within a defined time condition, as shown in Figure 5 on page 28, the Provisioning Manager detects three instances in which the provisioning PI criteria are fulfilled. For the first two instances, the Provisioning Manager activates additional capacity. The third instance is ignored, because it occurs after the deadline. The Provisioning Manager also detects an instance in which the

deprovisioning PI criteria are fulfilled. The Provisioning Manager then decides that ONLINE service class no longer needs additional capacity and deactivates it.

Provisioning criteria parameters

Name:
PT1

Sysplex:
PLEX1

System:
SYSA

Importance Filter:
Importance <= 2 with PI >= 1.8 for 10 min until PI <= 1.2 for 20 min

Included Service Class Periods:
ONLINE.1 in WLMSD with PI >=1.8 for 10 min until PI <= 1.2 for 10 min

Excluded Service Class Periods:
BACKUP.1 in WLMSD
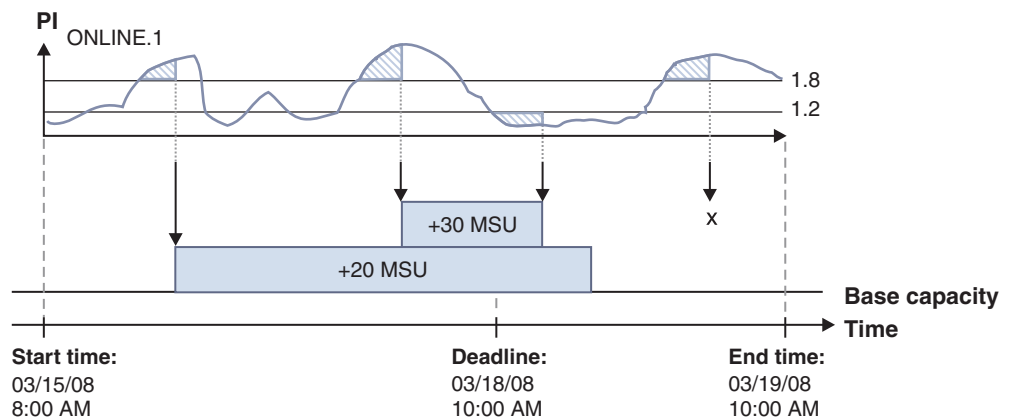
Figure 5. Provisioning criteria semantics

Moving average PI: The performance index of many workloads can change rapidly, for example because the amount of work varies, or because additional capacity becomes available in the system. If the provisioning duration includes several observation intervals, such as RMF MINTIME intervals, it is unlikely that you encounter a contiguous number of monitoring intervals so that the PI exceeds the provisioning PI for the entire provisioning duration.

Managing a workload via moving average PI can account for that behavior. When the actual performance index of a workload decreases below the provisioning PI for a short time the moving average PI can still exceed that limit. Consequently, high PI values in the provisioning duration might be recognized more reliably.
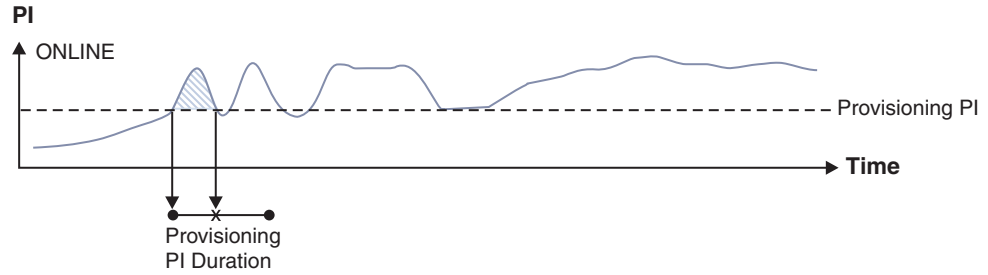
Figure 6. Fluctuating workload missing provisioning criteria

Figure 6 shows a fluctuating workload that does not meet the provisioning criteria because during the specified provisioning PI duration, the PI temporarily drops below the provisioning PI.

Optionally, the Provisioning Manager can average the PI provided by the monitoring component for a service class period. In this case the Provisioning Manager calculates a *moving average PI*. The actual PI pattern is averaged by using an exponentially weighted moving average (EWMA) function. The calculation considers current PI observations (interval t in the formula) as well as all preceding PI observations (as far as back to the first observed interval 0 in the formula) of a continuous time series, and weights the values with a user-specified smoothing factor as shown in Figure 7.

$$ PI_t^{mov.avg.} = \omega \sum_{i=0}^{t-1} (1-\omega)^i PI_{t-i} + (1-\omega)^t PI_0 $$

Figure 7. Exponentially weighted moving average (EWMA) PI formula

The graph that results from moving average smoothening is characterized by a more evenly value pattern; it might allow for activations in situations that would not be taken into account without the additional smoothening.
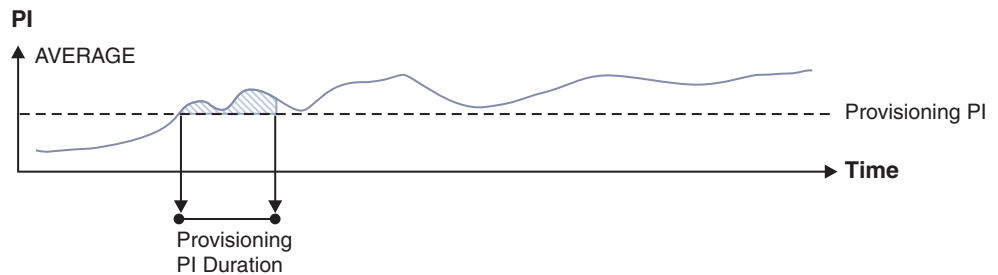

Figure 8. EWMA smoothened PI pattern with workload meeting provisioning criteria

Figure 8 shows the PI pattern, smoothened by the EWMA PI formula.

The smoothening algorithm delays the moments when the provisioning PI limit or the deprovisioning PI limit are being crossed; the smaller the smoothing factor, the more PI limit crossings are delayed. Hence, related capacity activations or deactivations are also delayed. Reducing provisioning or deprovisioning PI durations adequately can compensate for this delay.

The formula assumes that a contiguous series of PI values (time interval i=0 to t) is available, meaning that PI values are reported for every interval. For patterns with short gaps in workload, the formula disregards all PI observations that precede the last gap. The series of contiguous PI values can also be interrupted after subcapacity changes to the managed hardware, when the monitoring component, such as RMF, needs to recalculate the provided data.

To prevent high PI values from distorting the computed moving average PI pattern, a maximum capping PI value must be specified. This value limits the PI values that are considered to the maximum value specified by the capping PI. PI values that exceed that limit are replaced by the capping PI during computation of the moving average PI. That protects the resulting moving average PI graph from very high PI values that would have long-term effects. By default, the PI is capped at 5.5. If needed, it can be set to a different value, or moving average PI capping can be disabled.

Management on behalf of moving average PI and the capping value of the maximum capping PI is set globally. Hence, both values, the smoothing factor and the maximum capping PI, apply to all observed workloads.

For setting the moving average weight factor, see key "SystemObservation.MovingAveragePiWeight" in Table 14 on page 52

For setting the moving average capping, see key "SystemObservation.MovingAveragePiCapping" in Table 14 on page 52

Importance filter: An importance filter selects service class periods based on their importance. It includes the following parameter.

`Importance`
> The relative importance of the service class periods. All service class periods with an importance value equal or smaller than that specified match the filter unless another importance filter applies.

An importance filter also includes Provisioning Criteria PI values indicating when service class periods that match the importance filter are considered to be negatively affected. For more information about Provisioning Criteria PI values, see "Provisioning criteria" on page 26.

For example, if you specify importance value 3 in a filter, all service class periods with importance values 3, 2, and 1 match the filter and the specified provisioning criteria is applied to them. To define different provisioning criteria only for service class periods of importance value 1, you define another importance filter with the new criteria. The filter for importance value 3 then applies only to service class periods with importance values 3 and 2, and the filter for importance value 1 applies only to service class periods with importance value 1.

Service class period filter: Included and excluded service class periods are identified by service class period filters, which contain criteria that a service class period must match to be considered or ignored by the Provisioning Manager. These filters include the following parameters:

`Service Definition`
> The name of the WLM service definition. The specified service class periods are only considered if this WLM service definition is installed. You can specify '*' to include all WLM service definitions.

Service Policy

The name of the service policy within the WLM service definition. The specified service class periods are considered if a service policy with that name is activated. You can specify '*' to include all service policies matching the other criteria.

Service Class

The name of the service class. You can specify '*' to include all service classes matching the other criteria.

Period

The period of the service class to be considered. In an included service class filter, this period and all periods with a lower period number are considered eligible to trigger provisioning. If a service class has fewer periods than this number, all periods are considered.

In an excluded service class filter, this period and all periods with a higher period number are excluded from provisioning.

Capacity Provisioning Manager

The Provisioning Manager program is located in SYS1.SIEALNKE and in the file system under /usr/lpp/cpo. It must be activated through a started task procedure. It works with the resource definitions from the domain configuration and the workload and time conditions from the policy. These elements are created by using the Control Center.

The Provisioning Manager observes z/OS systems by connecting to the CIM servers on these systems, and uses these connections:
- To retrieve the required capacity and performance metrics
- To configure logical processors online or offline

To monitor and control resources, a connection to the HMC must be established. You have the following options:
- An SNMP protocol. To use this protocol, a network path to the console must be available. For more information, see "Defining the connection to the hardware" on page 65.
- An internal connection. To use this connection, the BCPii component of z/OS must be set up and configured. For more information, see "Defining the connection to the support elements for BCPii" on page 65.

The processing mode of the Provisioning Manager (see "Processing modes" on page 36) is controlled by operator commands. The processing actions available are described in "Processing activations and deactivations" on page 37. For the method of entering these commands, see "Provisioning Manager commands" on page 118, and for the actual commands, see Chapter 9, "Provisioning Manager command reference," on page 139.

To ensure availability, you can install and set up the Provisioning Manager on more than one system. Run the Provisioning Manager on a system that is included in the domain. Only one instance of the Provisioning Manager can be active at a time. You can define a restart policy for situations when the Provisioning Manager needs to stop, or when you need to shut down the system on which the Provisioning Manager is currently running. You can use your automation product or the z/OS Automatic Restart Manager (ARM) for this purpose.

Processing the domain configuration

When connected to the HMC, the Provisioning Manager retrieves a list of available CPCs. This list is correlated to the list of CPCs that is defined in the active domain configuration. Any CPCs that are defined in the domain configuration that are not listed as available by the HMC are marked as "not correlated." The Provisioning Manager regularly checks for additional CPCs. When finds them, it checks whether they can be correlated to CPCs that are defined in the domain configuration.

After the CPC lists have been correlated, the Provisioning Manager retrieves specific information about all CPCs that are common to both lists. When this information shows that a CPC has temporary capacity that can be managed by the Provisioning Manager, the CPC is considered valid for activation and deactivation requests. There can be multiple On/Off CoD records installed on a CPC. You can specify that a specific record be used. Otherwise the Provisioning Manager chooses an arbitrary one.

The Provisioning Manager can automatically activate or deactivate temporary capacity on a CPC that is enabled. If the capacity is disabled, it can only be activated or deactivated manually by using Provisioning Manager commands.

When the Provisioning Manager is in the processing modes `analysis`, `confirmation` or `autonomic`, and the observed system is enabled, the Provisioning Manager tries to connect to the CIM server on the observed system. A network connection to the observed system must be available, and all required services on this system must be configured and running. These services include the CIM server itself and the providers of workload metrics. If RMF supplies the CIM providers, RMF and the distributed data server (DDS) must be operating and the RMF CIM provider must have a connection to the DDS.

After data has been retrieved through the connection, the Provisioning Manager verifies that the responding z/OS system is the one specified and that it is running on a CPC that is defined in the domain configuration. Performance information relating to the CPC, the LPAR, and the WLM service classes is then retrieved for the workload that is defined in the policy. Because this information changes regularly, the rate at which the values are retrieved is synchronized with the change intervals. If RMF is used, this interval is the value of the RMF MINTIME option.

There are some situations when the metric data is not valid. In particular, changes to the WLM policy can cause disruption. Such changes are due to updating and reactivating the current WLM policy, or to installing a new WLM service definition. In these situations, the Provisioning Manager must reevaluate the workload situation. This might result in some history no longer being valid, and if resources are currently activated by the Provisioning Manager they might be deactivated.

The state information about the domain configuration and observed systems and managed CPCs is reported by the Provisioning Manager in the domain configuration report. For more information about this report, see page 126. The enabled state of the system and the CPC domain configuration elements can be changed by using Provisioning Manager commands. For more information about these commands, see "ENABLE CONFIGURATION" on page 150 and "DISABLE CONFIGURATION" on page 146.

Processing policy time conditions

The provisioning condition that contains the time condition can also contain workload conditions. Based on the provisioning PI durations of all associated workload conditions, the Provisioning Manager calculates the time at which observation of the workload must start in order to allow activation at the start time if necessary. This calculated time is referred to as the observation start time.

Note: The Provisioning Manager can run at different times on different systems, and it normally observes several other systems. Because these systems can be running in different time zones, the Provisioning Manager calculates and reports all times based on a common time zone. This common time zone is the Coordinated Universal Time (UTC).

One of the parameters of a nonrecurring time condition is the start time, which defines when the activation of temporary resources can start. For a recurring time condition, start time is the start time and a selected day of the week that occurs between the start date and the end date. Recurring time conditions are processed as a set of nonrecurring time conditions.

The state of time conditions at runtime is calculated based on the current time. A time condition can be in any of the states in the following list, depending on the current time, the enabled state of the time condition, and the enabled state of the policy. The enabled state of the time condition depends on the enabled states of the provisioning condition, rule, and policy that contain this time condition. If all of these policy elements are enabled, the time condition is also enabled.

Table 6. Time condition states

Time condition state	Meaning
Pending	The current time is before the start time of the condition and no system observation is necessary.
Observing and enabled	The current time is after the observation start time and before the start time of the condition. The time condition and policy are enabled, and one or more workload conditions is defined that requires systems to be observed. Systems that are referenced by associated workload conditions might be contacted to get performance information for further processing.
Observing and disabled	The current time is after the observation start time and before the start time of the condition. The time condition is disabled.
Active and enabled	The current time is after the start time and before the deadline of the condition, and the time condition is enabled. The Provisioning Manager might change the activation level of the managed CPCs based on the provisioning condition that contains the time condition.
Active and disabled	The current time is after the start time and before the deadline of the condition, and the time condition is disabled. The activation level of the managed CPCs cannot be changed by the Provisioning Manager based on the provisioning condition that contains the time condition.
Drained and enabled	The current time is after the deadline and before the end time of the condition; the time condition is enabled. The Provisioning Manager cannot not activate additional temporary resources but can maintain the current activation level of the managed CPCs based on the provisioning condition that contains the time condition.

Table 6. Time condition states (continued)

Time condition state	Meaning
Drained and disabled	The current time is after the deadline and before the end time of the condition, and the time condition is disabled. The activation level of the managed CPCs cannot be changed by the Provisioning Manager based on the provisioning condition that contains the time condition.
Inactive	The current time is after the end time of the condition; for recurring time conditions the current time is after the end time of the last selected day of the week between the start date and the end date. The activation level of the managed CPCs cannot be changed by the Provisioning Manager based on the provisioning condition that contains the time condition.

The states of time conditions in the active provisioning policy can be reported by the Provisioning Manager in the policy report. For more information about this report, see page 123. The enabled or disabled states of the rule and provisioning condition policy elements can be changed by using Provisioning Manager commands. For more information about these commands, see "ENABLE POLICY" on page 151 and "DISABLE POLICY" on page 147. The state of the active policy itself depends on the processing mode of the Provisioning Manager; for more information, see page 36. The policy is disabled in manual mode and enabled in all other processing modes.

Processing modes

The Provisioning Manager must collect different amounts of information,
depending on the processing mode. The possible processing modes are:

Table 7. Processing modes

Mode	Explanation
Manual	In this mode, you can issue manual activation and deactivation commands to the Provisioning Manager, but the Provisioning Manager does not activate or deactivate by itself. You use this processing mode if you want to maintain your systems and CPCs yourself, or if you want to quiesce the Provisioning Manager. The active policy and the active domain configuration are not processed.
Analysis	In this mode, you are informed through console messages if any additional resources are required. The Provisioning Manager processes the active policy, analyzes the workload on all accessible systems, and sends the messages. The messages contain details on the maximum resources allowed by the policy that can be provisioned to help the current workload situation. In this mode, like in manual mode, the Provisioning Manager does not activate or deactivate by itself. **Note:** In this mode, the Provisioning Manager does not check whether the CPC on which the workload is running allows activation. It might report the need for additional resources for CPCs that do not in fact have any temporary resources that can be activated by the Provisioning Manager.
Confirmation	In this mode, you are informed of proposed changes to the capacity settings of the CPCs through console messages, and you are asked to confirm the changes. The Provisioning Manager processes the active policy and the active domain configuration, analyzes the current workload situation on the observed systems, calculates which resources are needed, and sends the proposals. You can either accept or deny the proposed action. If you accept the proposal, the Provisioning Manager performs the action and continues processing based on the new activation level. If you deny the proposal, the Provisioning Manager does not consider the CPC for additional changes for a period of time, typically two hours. After this time, the Provisioning Manager considers the CPC again and proposes the same or other actions according to the new situation. While the answer to the request message is pending, the Provisioning Manager continues to check for any necessary changes. If the old requirement no longer exists, the request is canceled. If a new requirement has arisen, a new proposal is to be issued. If you need more information to answer the proposal, you can request reports from the Provisioning Manager, for example to show the actual workload situation as observed by the Provisioning Manager, or the current activation level of the CPC.
Autonomic	In this mode, the Provisioning Manager autonomically adjusts the capacity settings of the CPCs as determined through analysis of the workload situation on the observed systems. The Provisioning Manager processes the active policy and the active domain configuration. When any activation or deactivation is performed, it issues a message to the console to inform you which activities have been performed.

You can switch between these processing modes while the Provisioning Manager is
running. Information about activation level changes that were performed based on

the policy is preserved in all modes. If you switch to a mode that allows the activation level to be changed, the Provisioning Manager continues to manage those resources that it has activated.

When you start the Provisioning Manager, you can pass the initial processing mode as a parameter. You can change the processing mode at any time by using the Provisioning Manager SET DOMAIN command. For more information about this command, see page 164. The current processing mode is reported by the Provisioning Manager in the domain report, described on page 122.

Table 8 shows the requirements for each mode and the functions available in each mode.

Table 8. Processing modes: requirements and functions supported

Requirement/Function	Manual	Analysis	Confirmation	Autonomic
Domain configuration required	Yes	Yes	Yes	Yes
Policy definitions required	No	Yes	Yes	Yes
RMF DDS and CIM server required	No	Yes	Yes	Yes
Provisioning and deprovisioning through Provisioning Manager commands	Yes, if the CPC is defined in the domain configuration	Yes	Yes	Yes
Observation of defined workloads	No	Yes	Yes	Yes
Provisioning and deprovisioning recommen- dations or actions	No	Recommen- dations through console messages.	Console messages (WTOR) that might be accepted, rejected, or ignored.	Actions are implemented immediately.
On/Off Capacity on Demand record required to be installed	No	No	Yes	Yes

Processing of configuration online or offline

Configuring logical processors online or offline is independent of the processing mode. These actions are only based on the activation and deactivation of physical resources at the CPC. Logical operations never need to be accepted or rejected by an operator. Instead, the intended mode is defined in the policy. For more information, see "Logical Processor Scope" on page 20.

Processing activations and deactivations

The actions defined in a provisioning policy can be based on a schedule alone, on workload conditions, or on a combination of the two.

Schedule-based provisioning actions are defined by provisioning conditions that do not have workload condition. All available associated resources are activated at the start. If there are not enough resources available for activation at the start time, resources that become available later, for example by replenishing the record of the managed CPC or by deactivating resources that are not managed by the

Provisioning Manager, can be activated at any time up to the deadline. All activated resources are deactivated at the end time of the condition.

Workload-based provisioning actions define workload targets for the observed systems. If the workload is affected due to insufficient resources, the Provisioning Manager activates temporary resources, one by one, until the situation is resolved or the supply of resources is exhausted. For this resolution, the Provisioning Manager considers the performance index, as described in the provisioning conditions, and assesses which resources are needed and how they would help the workload. For example, it considers whether the LPAR that contains the system has sufficient logical processors or whether the processing weight is high enough to absorb more capacity.

The Provisioning Manager performs activation level changes based on the active policy and the workload situation on the observed systems, and monitors the effect these changes have on the workload situation. There are multiple mechanisms that need to adjust to the new capacity situation, for example PR/SM on the hardware side and WLM and IRD on the software side. These mechanisms take time to distribute the available capacity, so the Provisioning Manager blocks the CPC for a period of time, referred to as the blocking time. During this period of time, the Provisioning Manager does not consider it for further changes after any activation or deactivation of temporary capacity.

Temporary resources are not deactivated by the Provisioning Manager until they have been active for a minimum activation time, even if the workload situation of the observed systems no longer requires them, or if rules in the provisioning policy become inactive. This solution is designed to ensure that short-term fluctuations in the workload situation do not cause too many changes in the activation level.

Information about the provisioning actions that are performed by the Provisioning Manager based on the workload situation and the active policy is reported in the activity report. For more information about this report, see page 132.

Note: Manual changes to the activation level are not listed in the activity report.

Provisioning Manager manages the record describing the temporary capacity. If necessary, you can manually activate and deactivate temporary resources contained in this record. If you manually activate resources, they are not managed by the Provisioning Manager and you must deactivate them manually as needed. If you manually deactivate resources that have been activated by the Provisioning Manager, it is detected and reported. The Provisioning Manager continues to manage from the new activation level of the CPC, and, if needed, the resources can be activated again. You can manually change the activation level of the record at the HMC or by using Provisioning Manager commands.

Capacity Provisioning Control Center

The Control Center is the graphical user interface for Capacity Provisioning. You use this interface to work with provisioning policies and domain configurations. If there is a connection to the Provisioning Manager, you can transfer the policies and configurations to the Provisioning Manager and view the status of the Provisioning Manager, for example, to view which policy is active. The interface is described in Chapter 4, "Using the Capacity Provisioning Control Center," on page 73.

Workspace

The Control Center maintains a workspace, which includes the Provisioning Manager connections, a set of domain configurations, and a set of provisioning policies. The workspace is stored on the file system in a `Workspace` directory. The `workspace` directory contains three subdirectories:

- `Connections`
- `DomainConfigurations`
- `ProvisioningPolicies`

When you leave the Control Center, you are prompted to save any changes you made to the workspace. Provisioning policies are saved in the **ProvisioningPolicies** directory, domain configurations in **DomainConfigurations**, and the connection definitions for the Provisioning Manager in **Connections** directory.

You can have several workspace directories, for example a separate one for each provisioning domain, but you can work only on one workspace at a time. During startup of the Control Center, you are prompted to select a workspace. If you want to switch to a different workspace, start the Control Center again with the different workspace.

During installation, a workspace directory is created. To create an additional workspace directory, start the Control Center and when asked, specify the directory for the new workspace. If the directory does not exist, it is created. Under the specified directory, a subdirectory with the name `workspace` and its three subdirectories are created. These directories contain sample files that you can use as models to copy into your own definition files. Do not to use these samples because service updates to the Control Center can replace the sample files.

The Control Center time zone

The Control Center displays times in different contexts:

- within the workspace in time conditions
- in status reports retrieved from the Provisioning Manager.

You can choose which time zone the Control Center uses to display all times. The setting does not influence the way in which times within the time conditions of workspace policies are stored on the file system. The times when the status information is generated are documented in the Connection Report. The default time zone is UTC. When you switch the Control Center to a different time zone, all dates and times are adjusted. When you switch the Control Center to a different time zone, all dates and times are adjusted.

The time zone setting for displayed times does not affect how times are stored in the policy files; they are always stored in UTC.

Policies contain time conditions that define time periods during which additional capacity can be activated. Recurring time conditions define weekly repeating periods. They describe the time of the day when provisioning of resources are allowed and the days of the week to which these times apply.

The Control Center time zone is used to display the dates and times contained in the time conditions. If a time zone with daylight saving time is specified, the actual date and time values used might be one hour later or earlier than the values displayed.

When you switch the Control Center to a different time zone, all dates and times are adjusted. If the start time of a recurring time condition moves to a different day, the checks for the selected days of the week are moved accordingly.

Naming conventions

Policy names and configuration names must be unique within the workspace. If the name you specify for a new policy or configuration already exists in the workspace, the name is altered by the Control Center to make it unique. The names of policy elements must be unique within that policy, and these names too are altered if necessary.

The length of names and the character set that can be used are restricted.

Named elements within a provisioning policy or a domain configuration, and elements referencing external entities such as a system name or the logical name of a CPC must conform to the rules defined in Table 9. In this table, the hyphen (-) indicates that any ASCII character within the range is valid.

Table 9. Naming restrictions

Name	Minimum length	Maximum length	Initial character	Subsequent characters
Domain	1	8	A - Z	A - Z, 0 - 9, #
Provisioning policy	1	8	A - Z	A - Z, 0 - 9, #
Provisioning rule	1	12	A - Z, a - z	A - Z, a - z, 0 - 9, #, _
Provisioning condition	1	12	A - Z, a - z	A - Z, a - z, 0 - 9, #, _
Time condition	1	12	A - Z, a - z	A - Z, a - z, 0 - 9, #, _
Workload condition	1	12	A - Z, a - z	A - Z, a - z, 0 - 9, #, _
WLM service definition	1	8	A - Z, a - z, 0 - 9, #, $, %, @	A - Z, a - z, 0 - 9, #, $, %, @, _
WLM service policy	1	8	A - Z, a - z, 0 - 9, #, $, %, @	A - Z, a - z, 0 - 9, #, $, %, @, _
WLM service class	1	8	A - Z, a - z, 0 - 9, #, $, %, @	A - Z, a - z, 0 - 9, #, $, %, @, _
Domain configuration	1	8	A - Z	A - Z, 0 - 9, #
System	1	8	A - Z, 0 - 9, #, $, @	A - Z, 0 - 9, #, $, @
Sysplex	1	8	A - Z, 0 - 9, #, $, @	A - Z, 0 - 9, #, $, @
CPC	1	8	A - Z, 0 - 9, #, $, @	A - Z, 0 - 9, #, $, @
CPC record ID	8	8	A - Z, 0 - 9	A - Z, 0 - 9
Description	0	128	A - Z, a - z, 0 - 9, #, $, %, @, _, blank, nl, period	A - Z, a - z, 0 - 9, #, $, %, @, _, blank, nl, period

Chapter 3. Setting up a Capacity Provisioning domain

Capacity Provisioning Domain configuration specifies the CPCs to be managed and the systems to be observed. The domain configuration can be created and edited through the Control Center.

To set up a domain follow these steps:

- Plan the domain set up: Define your configuration settings such as the name of the domain, prepare your security and collect information about your system.
- Define the Provisioning Manager: Prepare your z/OS system to start up a Provisioning Manager.
- Install the Control Center: Check the prerequisites and install the Control Center on a workstation.

Note: The second and third steps can be performed in either order.

Before customizing Capacity Provisioning, set up the prerequisite components:

- Customize your monitoring product, such as z/OS Resource Measurement Facility (RMF), including the Distributed Data Server (DDS). For more information, see the z/OS RMF User's Guide.
- Customize the z/OS Common Information Model (CIM) element, including the RMF CIM Monitoring providers.

When you set up the Provisioning Manager, you must create security definitions and CIM definitions. For more background information about the security definitions, see *z/OS RACF Security Administrators Guide*, and for CIM definitions, see *z/OS Common Information Model User's Guide*.

Planning the domain set-up

Plan the domain set-up before performing any other actions. It requires that you collect information, specify your goals, and revisit your corporate conventions.

To plan the domain set-up consider the following points:

- What naming conventions to use
- Which z/OS system to run the Provisioning Manager on
- Where the prerequisites are located

Choosing names

Capacity Provisioning includes samples that you can use to set up a new domain. These samples contain default values for element names. If you are satisfied with these defaults, do not change them when you set up the domain. If you choose a different naming convention, replace all occurrences of the default names with the names you select during the actual definition steps. Table 10 on page 45 includes space for you to record the names you choose. The following paragraphs describe the element names, their default values, and their meaning.

Each domain is identified by a domain name. If you use multiple domains, each name must be unique. For more information about the rules for a valid domain name, see "Naming conventions" on page 41.

The Provisioning Manager runs as a started task, by using an entry setup for this purpose in the procedure data set for started tasks used in your installation (normally SYS1.PROCLIB). A sample started task procedure, CPOSERV, is delivered in SYS1.SAMPLIB. Copy this procedure or an equivalent to your started task procedure data set. If you choose a name other than CPOSERV for the started task, you must name the member in this data set accordingly.

When the Provisioning Manager starts, a useris assigned to the started task. This user must be defined and authorized for all resources accessed by the Provisioning Manager. Because the Provisioning Manager user is authenticated with PassTickets, it requires a unique UNIX identifier (UID) and it cannot be defined as a protected user, it must be assigned a password. You also must define a default group for the user, and an OMVS segment that specifies a home directory.

The Provisioning Manager contains status and configuration data in data sets. The names of these data sets use the same high-level qualifier, to make security definitions easier.

Provisioning policies and domain configurations are defined by using the Control Center. If a connection is set up between the Control Center and the Provisioning Manager, you can install policies and domain configurations directly from the Control Center. In this case, the user of the Control Center must connect to the CIM server on the system where the Provisioning Manager runs. Different security definitions are needed according to the operations required:

- If a Control Center user wants only to query the Provisioning Manager, the user must be a member of the Provisioning Manager query security group.
- If the user can modify the runtime behavior of the Provisioning Manager, the user must also be a member of the Provisioning Manager control security group.

The Provisioning Manager and the Control Center communicate by using the CIM protocol. The CIM server user is required to set up security definitions for the communication.

Table 10 contains a list of names to be chosen and their default values. If you do not use the defaults, make a note of the names you use.

Table 10. Name information for a new domain

Name	Default	Your value
Domain name	DOMAIN1	
Started task procedure name	CPOSERV	
High-level qualifier for runtime data set	CPO	
Provisioning Manager user	CPOSRV	
Control Center user[1]	CPCCUSR	
Provisioning Manager query security group	CPOQUERY	
Provisioning Manager control security group	CPOCTRL	
Default group for CIM user ID	CFZUSRGP	

Notes:

1. The Control Center user can be any z/OS user that is authorized to interact between the Control Center and the Provisioning Manager. The Control Center user must be set up with a password (to authenticate through the Control Center).

Defining the runtime environment

Once you define your names, define the environment for the Provisioning Manager. To start with, identify the primary z/OS system on which you run the Provisioning Manager, and select alternative systems on which a backup of the Provisioning Manager can run if the primary system becomes unavailable. All of these systems need access to the Provisioning Manager data sets.

To allow a restart on an alternative system, the runtime information shown in Table 11 on page 47 and all paths listed in Table 12 on page 48 must be identical on the two systems. The term *runtime systems* refers to all systems on which the Provisioning Manager can run, but note that only one instance of the Provisioning Manager can run at any one time.

Note: All runtime systems must be on the same z/OS level. If the Provisioning Manager is able to restart on a system that is running with a previous z/OS release, configuration or status data might not be readable for the Provisioning Manager and the program might stop processing.

You can use z/OS Automatic Restart Manager (ARM) to restart the Provisioning Manager in the event of failure. To use ARM, define the ARM restart policy, element name, and element type. You can also use any other automation product that can restart the Provisioning Manager when needed.

The Provisioning Manager uses either the SNMP protocol or z/OS BCPii
(INTERNAL) to communicate with the hardware. You must define your
communication protocol. The two protocols are set up differently.

When using the Simple Network Management Protocol (SNMP) to communicate
with the hardware, you need the address of the hardware console. The hardware
console can be either a CPC support element (SE) or a Hardware Management
Console (HMC). The SE or HMC that serves the Provisioning Manager must be
identified. Note that you need an HMC to manage multiple CPCs. The term HMC
is used to mean HMC or SE, unless otherwise noted. The address can be either the
host name or the TCP/IP address of the HMC. A TCP/IP connection from your
runtime system to the HMC must be possible.

BCPii is a method of communicating with the CPC support elements that does not
require a network connection from the runtime system to the HMC. Instead, you
must create security definitions on your runtime systems.

For both protocols, you need the name of the community that the Provisioning
Manager uses to access the hardware console. It is possible to use the default
community name ("public") but it is better to define a new community name for
Capacity Provisioning. Note that BCPii requires an uppercase community name.
This community name must be authorized to issue read and write operations and
to issue commands to change the temporary capacity. When using SNMP
communication, the community name must be defined only at the HMC. When
you use the BCPii, you must set up a community name for each CPC that is
managed by Capacity Provisioning and all CPCs on which the Provisioning
Manager can run.

To create service information, the Provisioning Manager can write trace and log
data. Because the data is temporary, it is usually written to the /tmp directory on
the runtime system. If you want this data to be written to another location, you
can redirect it to another file system. The selected path must be available on the
runtime system, and the Provisioning Manager user must be authorized to write to
this location. Service data can be deleted after it is sent to IBM. Do not delete the
data while the Provisioning Manager is still running.

Use the Control Center to define the policies and domain configurations for the
Provisioning Manager. A workstation is required to run the Control Center
program.

Table 11 contains a list of all necessary environment information, and the default values where applicable. Record any values you change for your domain in the table.

Table 11. Provisioning Manager runtime environment

Name	Default	Your value
Primary runtime system	-	
Alternative runtime systems	-	
ARM restart needed	no	
ARM element type	SYSCPM	
ARM element name	SYSCPO	
Hardware console protocol (SNMP or INTERNAL) The preferred protocol is INTERNAL.	SNMP	
SNA (System Network Architecture) names of managed CPC (only when using INTERNAL protocol)	-	
HMC address (only when using SNMP)	-	
SNMP community name	public	
Log data location	/tmp	
Trace data location	/tmp	
Control Center workstation	-	

Collecting information about prerequisites

To set up the Provisioning Manager you need information about other components and products on your runtime system. The information required is:

- The installation directory for the Java product
- The installation directory for the CIM server
- The location of the CIM Clients for Java
- The location of the System Authorization Facility (SAF) libraries
- The location of the SAF Java library for secured sign-on function

Table 12 contains a list of prerequisite components and products and their default locations. Record the locations that are defined on your runtime systems here.

Table 12. Prerequisites information

Product or Component	Default location	Your location
IBM 31-bit SDK for z/OS, Java 2 Technology Edition, V6 (5655-R31)	`/usr/lpp/java/J6.0`	
CIM server	`/usr/lpp/wbem`	
CIM Client for Java Version 2	`/usr/lpp/wbem/jclient/sblim-cim-client2.jar`	
SAF library	`/usr/lib`	
SAF JAR file	`/usr/include/java_classes/IRRRacf.jar`	

Preparing the Provisioning Manager

The prerequisites must be satisfied before you can successfully start the Provisioning Manager. These prerequisites include the runtime system and the systems that are observed by the Provisioning Manager. The runtime system can also be one of the observed systems. On the runtime system, you must:

- Define data sets used for the runtime data
- Set the configuration parameters to your chosen values
- Create a started task procedure
- Provide APF authorization
- Define the security
- Define a restart policy

If you defined alternative runtime systems that share the same resources, for example a common RACF database, you create the definitions only once.

On the observed systems, security must allow the Provisioning Manager user to connect to the system and to query the information for management purposes.

Note: The following definitions and examples use the default values for all the data that you collected in the planning step. If you chose different values, adjust the examples accordingly. For more information about the different values and their defaults, see "Planning the domain set-up" on page 44.

Defining the runtime data sets

The Provisioning Manager stores permanent and temporary data in data sets. You define these data sets only once for each domain. The data sets must be accessible on all runtime systems. Table 13 contains a list of the required data sets and their attributes:

Table 13. Provisioning Manager data sets

	Restart data set	**Policy repository**	**Domain configuration repository**	**Provisioning Manager parameters**
Data set	*prefix*`.RESTART`	*prefix*`.POLICIES`	*prefix*`.DOMCFG`	*prefix*`.PARM`
DSORG	PO	PO	PO	PO
DSNTYPE	LIBRARY (preferred) or PDS	LIBRARY (preferred) or PDS	LIBRARY (preferred) or PDS	LIBRARY (preferred) or PDS
RECFM	VB	VB	VB	VB
LRECL	16384	512	512	512
BLKSIZE	32760	32760	32760	32760
Directory blocks (if DSNTYPE=PDS)	20	20	20	20
Primary allocation	1 MB	1 MB	1 MB	300 KB
Secondary allocation	2 MB	2 MB	2 MB	600 KB

The *prefix* for the data set names is the high-level qualifier and the name of the domain defined in Table 10 on page 45. For example, with the default values, the

restart data set name would be `CPO.DOMAIN1.RESTART`.

After you create the data sets, copy two sample files from the Capacity Provisioning installation file system to the data sets for Provisioning Manager parameters. The files are `env` and `parm` from directory `/usr/lpp/cpo/samples`. Copy them as members `ENV` and `PARM`.

Capacity Provisioning provides a sample job to define these data sets and copy the files. The sample job is available as member `CPOMKDSN` in library `SYS1.SAMPLIB`. Note that this job deletes any existing data sets that have the same name as the ones to be defined.

Adapting the Provisioning Manager parameters

Some parameters of the Provisioning Manager might need to be adapted to your environment. These parameters are part of the Provisioning Manager parameters data set, *prefix*`.PARM`, in the members `ENV` for the Provisioning Manager runtime environment data and `PARM` for the Provisioning Manager configuration information.

The `ENV` member contains information about the runtime processing environment for your Provisioning Manager. Modify the following paths to match your installation settings:

LIBPATH

> This entry must contain:
> - The path `/usr/lib` for SAF libraries
> - The Java installation paths `/usr/lpp/java/J6.0/bin` and `usr/lpp/java/J6.0/bin/classic`
> - The Capacity Provisioning installation path `/usr/lpp/cpo/lib`

CLASSPATH

> This entry must contain the Capacity Provisioning JAR file cpom.jar from the installation directory `/usr/lpp/cpo/classes`, and the SAF JAR file `/usr/include/java_classes/IRRRacf.jar`.
>
> Optionally, if your Capacity Provisioning installation directory or your CIM installation directory are not at the default locations, you might need to add the CIM Client for Java `/usr/lpp/wbem/jclient/sblim-cim-client2.jar`
>
> Add the CIM Client for Java Version 2 before adding the CIM Client for Java Version 1 if your Provisioning Manager is defined to be restarted on a system that has a lower release.

For example:

```
LIBPATH=/usr/lib:/usr/lpp/java/J6.0/bin:usr/lpp/java/J6.0/bin/classic:...
        /usr/lpp/cpo/lib
CLASSPATH=/usr/lpp/cpo/classes/cpom.jar:...
          /usr/include/java_classes/IRRRacf.jar
```

Note: The information for each path must be on one line, and there must be no blanks between the path values.

The `PARM` member contains configuration information for the Provisioning Manager. It has the structure of a Java property-file with keyword-value pairs. Both

keywords and values are case-sensitive. Comment lines must start with a hash character (#). In the PARM member, you can enter keywords for:

Hardware access

The Provisioning Manager must access a hardware console to get information about the available CPCs and available temporary capacity, and to activate and deactivate the temporary capacity, if required. You must specify access information for the HMC. The primary information is the protocol. The protocol is specified by using the configuration key Topology.Protocol. The value can be either SNMP for the SNMP protocol, or INTERNAL for BCPii. For BCPii, the information would look like:

```
# Topology settings
Topology.Protocol = INTERNAL
```

If the protocol is SNMP, you also specify the host name or IP address of the HMC, and the community name under which all operations are performed. Specify the HMC host address by using the configuration key Topology.Address. Specify community name by using the key Topology.Community. The syntax for SNMP is:

```
# Topology settings
Topology.Protocol = SNMP
Topology.Address = HMC_address
Topology.Community = community_name
```

Automatic Restart Manager setting

To use ARM to monitor availability of the Provisioning Manager, you must set the value ARM.Register to *Yes*. You can do this simply by removing the comment symbol from this statement in the sample member provided. If this key is not specified, or is given any value other than *Yes*, the Provisioning Manager is not registered with ARM. The value is not case-sensitive.

If you use ARM to monitor the Provisioning Manager, you must define ARM policy. This policy specifies an ARM element type and an ARM element name. If you chose the default element type and name, SYSCPM and SYSCPO, no changes are needed. If you changed these values, you must replace the values of the keys ARM.ElementType and ARM.ElementName with the ones you have chosen. The defaults are:

```
# ARM settings
ARM.Register    = No
ARM.ElementType = SYSCPM
ARM.ElementName = SYSCPO
```

Security groups for Control Center commands authorization

To allow the Control Center user to communicate with the Provisioning Manager, you must define the Provisioning Manager query security group and the Provisioning Manager control security group in the configuration keys CIM.ReadGroup and CIM.ModifyGroup. In this case, the defaults are:

```
# Command authorization definitions
CIM.ReadGroup=CPOQUERY
CIM.ModifyGroup=CPOCTRL
```

Trace and Log data

If you chose directories other than the defaults for the trace and log data, you must set configuration keys Trace.Path and Log.Path accordingly. The directories must exist and the Provisioning Manager must have write access to them. The default entries are:

```
                    # Service data location
                    Trace.Path = /tmp
                    Log.Path = /tmp
```

Additional parameters to control provisioning management

In addition to the configuration parameters described above, the PARM member can also contain optional directives that influence the operation of the Provisioning Manager. When these values are specified, they override the default values of the Provisioning Manager. Specify a value if you need to override the default.

Table 14. Additional control parameters

Key	Default value	Description
`Planner.BlockingTime`	15	Number of minutes the provisioning Manager waits after detection of a CPC capacity change before any new capacity change action is initiated. This time allows the workload to be redistributed after a capacity change. If faster provisioning or deprovisioning is warranted, the value can be lowered. The recommended range is a value of 5 - 15 minutes.
`Planner.ProvisioningRejectTime`	120	Number of minutes a CPC is not considered for Provisioning Manager actions after a provisioning request made in confirmation mode has been rejected.
`Planner.DeprovisioningRejectTime`	120	Number of minutes a CPC is not considered for Provisioning Manager actions after a deprovisioning request proposed by the CPM has been rejected in confirmation mode.
`Planner.MinimumActivationTime`	240	Number of minutes a temporary resource must remain active before it is considered for deactivation. This time interval starts again with any new activation and applies to all active resources. When specified, the minimum activation time must be greater than the blocking time.
`Analyzer.Threshold.` `Decision001TotalSharedPhysicalUtilCp`	95	Lower limit of physical utilization on shared CPs that must be exceeded before additional general-purpose capacity is considered. In some environments, severe processor contention occurs at lower levels of processor utilization. In such environments you can specify a lower percentage value, such as 90.

Table 14. Additional control parameters (continued)

Key	Default value	Description
`Analyzer.Threshold.` `Decision001TotalSharedPhysicalUtilZaap`	95	Lower limit of physical utilization on shared zAAPs that must be exceeded before additional zAAP capacity is considered. In some environments, severe processor contention occurs at lower levels of processor utilization. In such environments you can specify a lower percentage value, such as 90.
`Analyzer.Threshold.` `Decision001TotalSharedPhysicalUtilZiip`	95	Lower limit of physical utilization on shared zIIPs that must be exceeded before additional zIIP capacity is considered. In some environments, severe processor contention occurs at lower levels of processor utilization. In such environments you can specify a lower percentage value, such as 90.
`Analyzer.Threshold.Decision002MvsUtilCp`	95	Lower limit of MVS utilization on CPs that must be exceeded before additional general-purpose capacity is considered. In some environments, severe processor contention occurs at lower levels of MVS utilization. In such environments you can specify a lower percentage value, such as 90.
`Analyzer.Threshold.` `Decision002MvsUtilZaap`	95	Lower limit of MVS utilization on zAAPs that must be exceeded before additional zAAP capacity is considered. In some environments, severe processor contention occurs at lower levels of MVS utilization. In such environments you can specify a lower percentage value, such as 90.
`Analyzer.Threshold.` `Decision002MvsUtilZiip`	95	Lower limit of MVS utilization on zIIPs that must be exceeded before additional zIIP capacity is considered. In some environments, severe processor contention occurs at lower levels of MVS utilization. In such environments you can specify a lower percentage value, such as 90.
`Analyzer.CycleTime`	200	The Capacity Provisioning management cycle time in seconds. This time interval is used to analyze capacity metrics whether the capacity requirements have changed.

Table 14. Additional control parameters (continued)

Key	Default value	Description
SystemObservation.MovingAveragePiWeight	100	Percentage from 1 to 100 that expresses the weight applied to the calculation of the moving average PI. The weight applies both to calculation of system and sysplex PI calculation. Smaller key-values increase smoothing by giving more weight to older PI data, while larger key-values discount older data in benefit of the latest PI data and produce a less smoothened moving average PI. Values below 100 enable the calculation of moving average PI for all observed workloads. The average is also the basis for the management process. The default value of 100 leaves moving average management disabled.
SystemObservation.MovingAveragePiCapping	5.5	Maximum PI limit that is considered for calculating the moving average PI. Prevents extremely high PI values from distorting computed moving average PI in the long term. Zero indicates that capping is disabled. Other allowed values are 1.3 - 55.
SystemObservation.PollingSpreadLimit	0	The default value of zero optimally times system observation requests. The value can be changed if it is important to distribute monitoring work more evenly over the observation cycle. If multiple systems are observed, the value helps limit the overflow of work eligible for specialty processor to general-purpose processors. Allowed values are 0 - 100. The default is zero (polling spread disabled).

Creating started task procedures

You can create started task procedures by copying member CPOSERV from data set SYS1.SAMPLIB to the started task procedure data set. The data set is normally SYS1.PROCLIB. If you have not chosen to use the default name for the started task, CPOSERV, you must rename the member appropriately. In the header section of the procedure, change the following values to the ones you chose:

HLQ   High-level qualifier of the runtime data sets

DOMAIN   Name of the domain

CPODIR   Home directory of the Provisioning Manager user

OUTCLS   Suitable output class

RGNSIZE   Region size allowed by the server

The sample procedure supplied is:

```
//*****************************************************
//* Licensed Materials - Property of IBM
//* 5694-A01
//* Copyright IBM Corp. 2007, 2010
//* Status = HPV7770
//* Change Activity:
//* $P1=OA31072 HPV7770 091118 3272HS: Increase default heap size
//*********************************************
//CPOSERV PROC PMODE='*',
// POLICY='*'
//*****************************************************
//* This section of variables may require customization.
//* Changing RGNSIZE may also require a change to the maximum Java heap
//* size (-Xmx) in the member allocated to STDENV below.
//HLQ SET HLQ=CPO HLQ of runtime datasets
//DOMAIN SET DOMAIN=DOMAIN1 provisioning domain name
//CPODIR SET CPODIR='/u/cposrv' home directory of cposrv
//OUTCLS SET OUTCLS=A output class
//RGNSIZE SET RGNSIZE=512M Server region.See note above. @P1C
//*
```

Providing APF authorization

First, ensure that data set `SYS1.SIEALNKE` is in the link list. The system automatically places this data set at the beginning of the link list, unless it is overridden by a `SYSLIB` statement in `PROGxx`. The default `IEASYSxx` value `LNKAUTH=LNKLST` must also be in effect, or `SYS1.SIEALNKE` must be APF authorized.

The next steps in this process are optional. They are only required if you copied the Capacity Provisioning files or the Java files on your runtime system.

On any runtime system, the Provisioning Manager must run with APF authorization. In this case the code must be authorized; the main program is located in a program library data set (PDSE) and the libraries are located in the file system.

If you have copied the Capacity Provisioning library files from the UNIX file system, make sure that all Provisioning Manager libraries and the Java libraries are sufficiently authorized. The Provisioning Manager libraries are located in `/usr/lpp/cpo/lib`. You can check the authorization by entering the command:

`extattr /usr/lpp/cpo/lib/*`

at a UNIX shell prompt.

The following libraries require `APF authorized = YES`:
- `libcpoarm.so`
- `libcpoconsole.so`
- `libcposocket.so`
- `libcpostream.so`
- `libcpoii.so`

The Java library is in `/usr/lpp/java/J6.0/bin/classic`, and is named `libjvm.so`. If you have copied the Java SDK code, you must ensure that its APF authorization is the same as the one of the Provisioning Manager libraries.

Securing the runtime system

Set up security on the runtime system and on the observed systems. Because an observed system can also be a runtime system, you might have to perform both definitions on these systems. On the runtime system the steps to take are:

- Define the started task
- Define ARM access
- Define access for the Provisioning Manager user
- Define the secured sign-on function
- Define access for the Control Center user
- Define access to the hardware

The following examples assume that your external security manager is z/OS Security Server (RACF). If you have installed a different external security manager, modify the examples accordingly. These examples also assume that the Provisioning Manager user and the Control Center user are already defined to the security manager, and that an OMVS segment is defined for both users.

All RACF security definitions that are required for a runtime system that is also an observed system are contained in member CPOSEC1 in SYS1.SAMPLIB. You can copy and change this sample job to match your needs. All security definitions required for additional observed systems that are not sharing the same security database are listed in sample member CPOSEC2.

The RACF security definitions listed in this document and contained in the members CPOSEC1 and CPOSEC2 assume a prior CIM setup. Detailed information about CIM setup can be found in *z/OS Common Information Model User's Guide*.

Defining the started task

The Provisioning Manager started task on the runtime system must be assigned to the Provisioning Manager user. Here is an example definition for RACF:

```
RDEFINE STARTED CPOSERV.* STDATA(USER(CPOSRV))
SETROPTS RACLIST(STARTED) REFRESH
```

Defining ARM access

If Automatic Restart Manager (ARM) is used, a FACILITY class profile must be defined and the Provisioning Manager user must have an UPDATE access. If you change the default ARM element type, ARM element name or Provisioning Manager user you must replace the values SYSCPM, SYSCPO, or CPOSRV in the following example with the values you chose. An example definition is:

```
RDEFINE FACILITY IXCARM.SYSCPM.SYSCPO UACC(NONE)
PERMIT IXCARM.SYSCPM.SYSCPO CLASS(FACILITY) ID(CPOSRV) ACC(UPDATE)
SETROPTS RACLIST(FACILITY) REFRESH
```

Defining security for the Provisioning Manager user

The Provisioning Manager user requires access to local resources on your runtime system. The local resources include:

- Membership in the Provisioning Manager security groups CPOQUERY and CPOCTRL
- UPDATE access to the Provisioning Manager data sets CPO.DOMAIN1.*
- READ access to the profile BPX.CONSOLE in the FACILITY class
- CONTROL access to the Provisioning Manager user data sets CPOSRV.*
- If the FACILITY class does not exist, you can create it using the RDEF FACILITY BPX.CONSOLE UACC(NONE) command

You can define these access rights as follows:

```
ADDGROUP CPOQUERY OMVS(GID(...))
ADDGROUP CPOCTRL OMVS(GID(...))

CONNECT (CPOSRV) GROUP(CPOQUERY) AUTH(USE)
CONNECT (CPOSRV) GROUP(CPOCTRL) AUTH(USE)

ADDSD ('CPO.DOMAIN1.*') GENERIC UACC(NONE)
PERMIT 'CPO.DOMAIN1.*'  GENERIC ID(CPOSRV) ACCESS(UPDATE)
ADDSD ('CPOSRV.**')     GENERIC UACC(NONE)
PERMIT 'CPOSRV.**'      GENERIC ID(CPOSRV) ACCESS(CONTROL)
SETROPTS GENERIC(DATASET) REFRESH
```

Optionally, grant the Provisioning Manager access to BPX.CONSOLE in the FACILITY class.

If this access is not granted, all messages issued by the Provisioning Manager are prefixed with a BPXM023I message.

```
RDEFINE FACILITY BPX.CONSOLE UACC(NONE)
```

```
PERMIT 'BPX.CONSOLE' CLASS(FACILITY) ID(CPOSRV) ACCESS(READ)
SETROPTS RACLIST(FACILITY) REFRESH
```

Note that you need to complete the OMVS information for the Provisioning Manager security groups before entering these definitions.

In addition, the Provisioning Manager user needs access to files and directories in the local file system of the runtime system. These access rights are usually sufficient by default. The following access is needed for the Provisioning Manager user:

- Read and execute access to the Capacity Provisioning installation directory /usr/lpp/cpo and all its subdirectories
- Read and execute access to the Java installation directory /usr/lpp/java and all its subdirectories
- Read access to the CIM Client for Java/usr/lpp/wbem/jclient/sblim-cim-client2.jar
- Read access to the SAF library /usr/include/java_classes/IRRRacf.jar
- Read and write access to trace and log data in file system path /tmp
- Read and write access to file system path /var
- Read and write access to the home directory of the Provisioning Manager user /u/cposrv

If the current access rights are insufficient, set the "other" read, write, and execute access permissions of the directories and files accordingly by using the UNIX command chmod, for example:

```
chmod -R o+rx /usr/lpp/cpo
```

These permissions allow all users to read and execute files and directories starting with /usr/lpp/cpo.

Note: This command must be issued by a user with appropriate access rights.

Defining the secured sign-on function on the runtime system

Communication between the runtime system and the observed systems requires authentication and authorization. These processes are implemented by using the secured sign-on function, which generates PassTickets when the Provisioning Manager logs on to an observed system. The logon is performed as the Provisioning Manager user, so this user must be defined on the runtime system and all observed systems.

The following definitions are needed to use the secured sign-on function and to generate PassTickets:

To activate the PTKTDATA class

Use the definitions:

```
SETROPTS CLASSACT(PTKTDATA)
SETROPTS RACLIST(PTKTDATA)
```

To use PassTickets

If it is not already implemented as part of the CIM server setup, define the profile CFZAPPL in the PTKTDATA class. The Provisioning Manager user must have at least READ access to this profile. If a common cryptographic architecture (CCA) product is installed on the systems with the secured sign-on function you can encrypt the secured sign-on application keys. If not, mask the secured sign-on application key by using the SSIGNON operand and a 64-bit KEYMASKED value. For example:

```
RDEFINE PTKTDATA CFZAPPL SSIGNON(KEYMASKED(XXXXXXXXXXXXXXXX))+
APPLDATA('NO REPLAY PROTECTION')
PERMIT CFZAPPL CLASS(PTKTDATA) ID(CPOSRV) ACCESS(READ)
SETROPTS RACLIST(PTKTDATA) REFRESH
```

To generate PassTickets

To enable the Provisioning Manager user to generate PassTickets, create the security profile IRRPTAUTH.CFZAPPL.CPOSRV in the PTKTDATA class giving the Provisioning Manager user at least UPDATE access authority. Then create the profile IRR.RTICKETSERV in the FACILITY class, giving this user at least READ access authority. For example:

```
RDEFINE PTKTDATA IRRPTAUTH.CFZAPPL.CPOSRV
PERMIT IRRPTAUTH.CFZAPPL.CPOSRV CLASS(PTKTDATA) ID(CPOSRV) ACCESS(UPDATE)
SETROPTS RACLIST(PTKTDATA) REFRESH

RDEFINE FACILITY IRR.RTICKETSERV
PERMIT IRR.RTICKETSERV CLASS(FACILITY) ID(CPOSRV) ACCESS(READ)
SETROPTS RACLIST(FACILITY) REFRESH
```

For more information about configuring RACF to use PassTicket services, see *z/OS Security Server RACF Security Administrators Guide*.

Defining security for hardware access

This step is only required if your communication to the hardware console is based on BCPii. If you are using BCPii communication, the Common Event Adapter (CEA) must run in full function mode and the Provisioning Manager user must be authorized for to some Common Event Adapter (CEA) services and for the CPCs that need to be managed. Instructions for setting the CEA into full function mode are provided in *z/OS Planning for Installation*.

For the CEA services, the Provisioning Manager user needs READ authority to the following profiles in the SERVAUTH class:

- CEA.CONNECT
- CEA.SUBSCRIBE.ENF_0068*

If you previously defined access through more generic profiles, such as CEA.*, you might want to use those profiles also to permit the Capacity Provisioning user.

A sample definition would look like the following:

```
SETROPTS CLASSACT(SERVAUTH)
RDEFINE SERVAUTH CEA.CONNECT UACC(NONE)
RDEFINE SERVAUTH CEA.SUBSCRIBE.ENF_0068* UACC(NONE)
PERMIT CEA.CONNECT CLASS(SERVAUTH) ID(CPOSRV) ACCESS(READ)
PERMIT CEA.SUBSCRIBE.ENF_0068*  CLASS(SERVAUTH) ID(CPOSRV) ACCESS(READ)
SETROPTS RACLIST(SERVAUTH)  REFRESH
```

The Provisioning Manager user needs the following authorizations to access information about the hardware and perform activation and deactivation requests for temporary capacity on a CPC:

- READ access to profile HWI.APPLNAME.HWISERV in the FACILITY class
- CONTROL access to profile HWI.TARGET.*netid.name* in the FACILITY class. The net ID and name represent the SNA (System Network Architecture) name of the CPC as defined at the SE. The APPLDATA of the security definition must contain the uppercase community name for the Provisioning Manager as defined in Table 11 on page 47. The profiles must cover all CPCs to be managed by Capacity Provisioning and all CPCs on which the Provisioning Manager can run.
- READ access to profile HWI.CAPREC.netid.nau.* in the FACILITY class. The net ID and name represent the SNA name of the CPC as defined at the support element. The profiles must cover all capacity records.

For example, if you have a CPC with SNA Name IBMNET.CPC1, the definitions would look as follows:

```
RDEFINE FACILITY HWI.APPLNAME.HWISERV UACC(NONE)
RDEFINE FACILITY HWI.TARGET.IBMNET.CPC1 APPLDATA(...) UACC(NONE)
RDEFINE FACILITY HWI.CAPREC.IBMNET.CPC1.* UACC(NONE)

PERMIT HWI.APPLNAME.HWISERV CLASS(FACILITY) ID(CPOSRV) ACCESS(READ)
PERMIT HWI.TARGET.IBMNET.CPC1 CLASS(FACILITY) ID(CPOSRV) ACCESS(CONTROL)
PERMIT HWI.CAPREC.IBMNET.CPC1.* CLASS(FACILITY) ID(CPOSRV) ACCESS(READ)

SETROPTS RACLIST(FACILITY)  REFRESH
```

For more information about BCPii setup, see *z/OS MVS Programming: Callable Services for High-Level Languages*.

Defining security for the Control Center user

The Control Center user must be authorized to connect the Control Center to the Provisioning Manager. Define this user on the runtime system with an OMVS segment, and add the user to the appropriate Provisioning Manager security group, depending on which administration and operation commands the user is allowed.

Define the control center users with a non-zero z/OS UNIX identifier (UID). When using a UID of zero, the "enableRemotePrivileged UserAccess" configuration property must be enabled in the CIM server. All control center users need to have execute permission to the /var directory. You can grant all users execute permission via the command chmod o+x /var.

At this time, the CIM server must be set up as described in *z/OS Common Information Model User's Guide*.

The Control Center user must have UPDATE access to the CIMSERV profile in the WBEM class. If your system is set up to use z/OS UNIX level security, for example, if BPX.SERVER is defined, define the CIM server user as a surrogate of the Control Center user. To do it, a profile BPX.SRV.** in the SURROGAT class is required. It is accomplished by the CIM setup. The CIM server user requires access to this profile. The next step depends on the authorization to be given to the Control Center User.

If the Control Center user is only authorized to query information from the Provisioning Manager, add this user to the Provisioning Manager query security group CPOQUERY, and grant UPDATE access to the CIMSERV profile by connecting it to the CIM users ID default group CFZUSRGP, which was defined during the CIM setup:

```
CONNECT (CPCCUSR) GROUP(CPOQUERY) AUTH(USE)

CONNECT (CPCCUSR) GROUP(CFZUSRGP) AUTH(USE)
```

If instead the Control Center user is authorized to change the processing characteristics of the Provisioning Manager, add this user to both Provisioning Manager security groups, CPOQUERY and CPOCTRL, and grant UPDATE access to the CIMSERV profile by connecting it to the CIM users ID default group CFZUSRGP, which has been defined during the CIM setup:

```
CONNECT (CPCCUSR) GROUP(CPOQUERY) AUTH(USE)
CONNECT (CPCCUSR) GROUP(CPOCTRL) AUTH(USE)

CONNECT (CPCCUSR) GROUP(CFZUSRGP) AUTH(USE)
```

Securing the observed systems

When a system is observed, the Provisioning Manager connects to the CIM server on that system and retrieves configuration and performance information about the workload. To enable this communication, establish a connection for the Provisioning Manager user and authorize it with a PassTicket. The steps to take are:

- Define the Provisioning Manager user on the observed systems with the same password as on the runtime system
- Enable the secured sign-on function
- Authorize the Provisioning Manager user to access the CIM server

The following definitions assume that the Provisioning Manager user is already defined and OMVS segment is assigned. These definitions must be effective on all observed systems.

Defining the secured sign-on function on the observed systems

This feature must be set up on the observed systems in the same way it was set up on the runtime system, which is described in "Defining the secured sign-on function on the runtime system" on page 59. Note that the KEYMASKED value must match the runtime system, and PassTicket generation is only performed on the runtime systems.

Defining access to the CIM server

RACF must be configured as follows to allow the Provisioning Manager user to access the CIM server on all observed systems. This configuration assumes that the CIM server user is already defined and the CIM setup is complete.

- Give the Provisioning Manager user access to the CIMSERV profile in the WBEM class by connecting it to the CIM users ID default group CFZUSRGP, which was defined in the CIM setup:

  ```
  CONNECT (CPOSRV) GROUP(CFZUSRGP) AUTH(USE)
  ```

For more information, see *z/OS Common Information Model User's Guide*.

Setting up Automatic Restart Manager

This step is only needed if you use ARM to restart the Provisioning Manager.

The Provisioning Manager requires the following conditions to use the ARM capability:

- The element name is SYSCPO, unless you chose another value in Provisioning Manager runtime environment.
- The element type is SYSCPM, unless you chose another value in Provisioning Manager runtime environment.
- The Provisioning Manager normally restarts with the policy and processing mode used the last time it ran, together with any modifications to the policy that are triggered by console commands. To achieve such a restart, the policy name and the processing mode on the restart command must be specified as '*'.
- The Provisioning Manager can be restarted on another system of the sysplex, if this system has access to the runtime data sets and the required file systems used by the previous system.

An example setup is supplied in member CPOARMPO of SYS1.SAMPLIB. For more information about ARM, see *z/OS MVS Setting Up a Sysplex*.

Preparing the connection to the CIM server

The Provisioning Manager and the Control Center communicate through a CIM server.In order to communicate from the Control Center to the Provisioning Manager, a connection via CIM is needed. Use the following steps to prepare the communication: You can establish connections through the server by using either the HTTP protocol or the HTTPS protocol, if the CIM server is configured to support the chosen protocol. For more information about configuring the CIM server, see the *z/OS Common Information Model User's Guide*.With the HTTPS protocol, you use an AT-TLS configuration. The Provisioning Manager and the Control Center do not support authentication based on SSL certificates.

Note: Ensure that the configured portof the CIM server matches the definitions that you make in your domain configuration and the Control Center.

Required settings for the RMF Distributed Data Server

The GPMSRVxx member that is used by the RMF Distributed Data Server must specify a higher value for MAXSESSIONS_HTTP than the default of 20. The recommended value is 60 or greater.

```
MAXSESSIONS_HTTP(60)            /* MaxNo of concurrent HTTP requests */
```

Preparing the connection to the Provisioning Manager

Logon to a z/OS UNIX session as a CIM administrator user.

1. Copy the Capacity Provisioning CIM provider properties file to the `/etc` directory:

   `cp /usr/lpp/cpo/provider/cpoprovider.properties /etc`

2. If your domain name is not the default (DOMAIN1), edit the file you copied, for example by using `oedit /etc/cpoprovider.properties` to change the `DomainNames = DOMAIN1` line to reflect the name of your domain.

3. Ensure that the file is readable:

   `chmod a+r /etc/cpoprovider.properties`

4. Verify that the program-controlled flag is set in the extended file attributes for the Capacity Provisioning CIM provider library:

   `ls -E /usr/lpp/cpo/lib/libcpoprovider.so`

   If the attribute is not set, use the following command to set the program-controlled flag manually:

   `extattr +p /usr/lpp/cpo/lib/libcpoprovider.so`

5. Verify that a link to the Capacity Provisioning CIM provider library is created in the CIM server provider directory:

   `ls -l /usr/lpp/wbem/provider/libcpoprovider.so`

   If the link does not exist, use the following command to create the link manually:

   `ln -s /usr/lpp/cpo/lib/libcpoprovider.so`
   `     /usr/lpp/wbem/provider/libcpoprovider.so`

6. If the cpoprovider.properties was changed, restart the CIM server.

Defining the connection to the hardware

Depending on the selected communication type, prepare the hardware that interacts with the Provisioning Manager. The communication types can be SNMP and BCPii (INTERNAL).

Defining the connection to the HMC for SNMP

When using SNMP communication between the Provisioning Manager and the hardware, ensure that there is a network connection between the runtime system and the HMC, that a firewall between the two permits access, and that the HMC is configured for remote API operations. The first step is to define the community name that you chose when you configured the Provisioning Manager. For more information, see Table 11 on page 47. Note that the address and network mask of the community name must be defined so that all runtime systems can use that name. The community name must be authorized for read and write operations. The next step is to allow external programs remote operation by using the API. If there are firewalls installed between the HMC and the network that your runtime systems belong to, allow communication for SNMP (port 161) and on port 3161 from the runtime system to the HMC.

For more information about the configuration of an HMC for API programs, see *System z Application Programming Interfaces*.

Defining the connection to the support elements for BCPii

For the BCPii communication, define the community name that you chose in your configuration of the Provisioning Manager. For more information, see Table 11 on page 47. Note that the community name needs to be specified by using the loopback device. The loopback device is used by specifying the address 127.0.0.1 and a network mask of 255.255.255.255. The community name must be authorized for read and write operations. The next step is to allow external programs remote operation by using the API. You need to define on the SE of each CPC that is to be managed by the Provisioning Manager and all CPCs on which the Provisioning Manager can run. For more information about the configuration of an SE for API programs, see *Callable Services for High-Level Languages*.

Tuning and workload classification for Capacity Provisioning

Your Workload Management (WLM) service definition for the observed systems ensures that monitors run at a higher priority than the work being monitored. The Provisioning Manager, together with the infrastructure it uses, must be prioritized so that they perform reliably even in a capacity-constrained situation. On the runtime systems, ensure that the Provisioning Manager started task CPOSERV is classified appropriately.

Either classify the Provisioning Manager and the supporting subsystems into SYSSTC, or give them an aggressive single period velocity goal at an importance level that is higher than the work that is defined in your provisioning policy. In particular, the following subsystems and address spaces are required:

On the runtime system:
- The Provisioning Manager (CPOSERV)
- The TCP/IP infrastructure
- The CIM server, if the Control Center is used to control the Provisioning Manager

On the observed systems:
- The RMF address spaces
- The RMF Distributed Data Server (GPMSERVE)
- The TCP/IP infrastructure
- The CIM server

Network latency in the CIM protocol can be minimized by specifying numeric IP addresses or by defining entries in the hosts file for the observed systems.

Other contention factors that could affect the ability of the Provisioning Manager to operate efficiently must be minimized. The Provisioning Manager and the CIM servers rely on the z/OS UNIX file system. Severe contention must be relieved by appropriate tuning measures to allow capacity provisioning to operate reliably.

Resource consumption considerations

The consumption of resources (processor or virtual storage) by the Provisioning Manager largely depends on the domain and policy definitions. The following factors increase resource consumption by the server:
- Many observed systems
- Many monitored service class periods
- A small RMF MINTIME
- Use of the HTTPS protocol for communication with the CIM server
- Activated traces

Most Provisioning Manager processing is zAAP-eligible. zAAPs are used automatically on systems configured with them and no additional definitions are required.

Installing the Control Center

You must use a CPCC with the same version as the z/OS system on which your provisioning manager runs. For example, run the z/OS V1R13 CPCC on your workstation when interacting with the z/OS V1R13 Capacity Provisioning Manager, and run the z/OS V1R12 CPCC on your workstation when you are interacting with the z/OS V1R12 Capacity Provisioning Manager.

The new CPCC can coexist with older versions of the CPCC on a workstation.

There are two stages to the installation of the Capacity Provisioning Control Center:
- Installing the CIM client
- Running the Control Center installation wizard

Installing the CIM client

The Control Center requires that the CIM client for Java Version 2 is installed on the workstation. The location of the corresponding JAR file in the host file system is given in the prerequisites information in Table 12 on page 48. Download the `sblim-cim-client2.jar` file in binary mode from the host to your workstation, and make a note of its location on the workstation. The file is required when you configure the Control Center. If you use the defaults, you can download the file by using FTP as follows:

```
cd "C:\Program Files\IBM\CIMClient"
ftp <host>
ftp> cd /usr/lpp/wbem/jclient
ftp> binary
ftp> get sblim-cim-client2.jar
ftp> bye
```

Installing the Control Center by using the installation wizard

The Control Center is installed by using the Microsoft installer. Before running the installer:
- Download the installation wizard to the workstation from the host
- Execute the installation wizard on the workstation

Retrieving the Control Center Installation Package

The installation program is located in the `pws` subdirectory of the Capacity Provisioning installation directory on the host. Download the file `/usr/lpp/cpo/pws/cpccinstall.msi` in binary mode to a temporary directory on your workstation, for example:

```
cd "C:\Temp"
ftp <host>
ftp> cd /usr/lpp/cpo/pws
ftp> binary
ftp> get cpccinstall.msi
ftp> bye
```

Starting the initial installation

Note: You must have administrator access rights on your Windows system to install and use the Control Center.

Start the installation by executing the file `cpccinstall.msi`, for example

```
cd "C:\Temp\cpccinstall"
cpccinstall.msi
```

Follow the steps specified by the installation wizard. Specify the directory of Capacity Provisioning workspace;for more information, see "Workspace" on page 39.

If you want to continue by using the existing policies and configurations, you have the following options:

- Point to the wanted existing workspace during the installation. You can also switch the workspace at a later time by navigating to the workspace when the CPCC starts.
- Create a new workspace during the CPCC installation and copy the existing policy, domain configuration, and connection XML files from the old workspace to the respective directories of the newly created workspace.

After finishing the installation, you can delete `cpccinstall.msi`.

After you install the Control Center, you must make certain configuration changes to allow the CIM Client for Java to connect to the Provisioning Manager; see "PreferencesDialog" on page 80.

Updating an existing Control Center installation

Updates are received via the host system, and must then be applied on the workstation.

Receiving an update for the Control Center: The Control Center is serviced through the Capacity Provisioning component on the z/OS host. A service, such as a PTF, is flagged with a `++HOLD...SYSTEM REASON(DOWNLD)` action to indicate that a new version of the Control Center is available. SMP/E reports the `++HOLD` requirements when the service is received. Apply the service in SMP/E and then download the updated `/usr/lpp/cpo/pws/cpccinstall.msi` binary to a temporary directory on your workstation, as described in "Retrieving the Control Center Installation Package" on page 67.

Unless a particular APAR documents a different requirement, the Provisioning Manager does not require a particular service level of the Control Center within the same z/OS release.

Applying an update for the Control Center: Stop the Control Center before starting the update. For more information, see "Stopping the Control Center" on page 83. Start the update by executing the file `cpccinstall.msi`, as described in "Starting the initial installation" on page 67.

Start the update installation by running the file `cpccinstall.msi` to reinstall the application with the settings you selected during the first installation. The new version of Control Center and workspace is installed to the directories you chose in the initial installation. The workspace is reset to the one you specified during the initial installation.

Repairing an existing Control Center installation: If the same version of the installation program is launched again on a system in which the Control Center is installed, the installation wizard Welcome screen gives you the option to 'Repair or remove the program.' The repair option reinstalls the application with the settings you selected during the first installation. Select **Repair** on the panel. The Control Center and the workspace are reinstalled to the directories you have chosen in the initial installation. The workspace is set to the one you specified during the initial installation.

Uninstalling the Control Center

If you no longer require the Control Center on a workstation, you can remove the IBM Capacity Provisioning Control Center program.

On Windows XP:

Either

- Click "Add or Remove Programs" on the Windows Control Panel.

or

- Click the **Uninstall IBM Capacity Provisioning V1R13** in the **IBM Capacity Provisioning** program group.

On Windows Vista and Windows 7:

Either

- Use the "Programs->Programs and Features" option on the Windows control panel

or

- Click the **Uninstall IBM Capacity Provisioning V1R13** in the **IBM Capacity Provisioning** program group.

The installation wizard tracks the installation and any updates and maintains a corresponding uninstallation. Stop the Control Center before starting uninstall. For more information, see "Stopping the Control Center" on page 83. The Control Center code is removed from your workstation. You can remove also the Control Center workspace, which contains the connection definitions, the domain configurations, and the provisioning policies.

Note: The file `settings/Unity.Toolkit.User.ser` in the directory in which you originally installed the Control Center is not removed and must be deleted manually.

Part 2. Operating Capacity Provisioning

Describes the use of Provisioning Management.

Chapter 4. Using the Capacity Provisioning Control Center

The Control Center is the graphical user interface for Capacity Provisioning. It is a desktop application that runs on a Windows workstation. As an administrator, you can work with provisioning policies and domain configurations through this interface. You can also use it to transfer these policies and configurations to the Provisioning Manager or to query the status, for example, to see which policy is active. The Control Center provides the following functions:

Provisioning Manager

Define the connection to the Provisioning Manager and show the status of the Provisioning Manager.

Domain Configurations

Manage domain configurations, defining the CPCs to be managed and the systems to be observed. Transfer the domain configurations to the Provisioning Manager.

Provisioning Policies

Manage provisioning policies, defining how much additional capacity can be activated on each CPC. Transfer the provisioning policies to the Provisioning Manager.

The Control Center window layout

The Control Center is a graphical user interface, with a screen layout as shown:
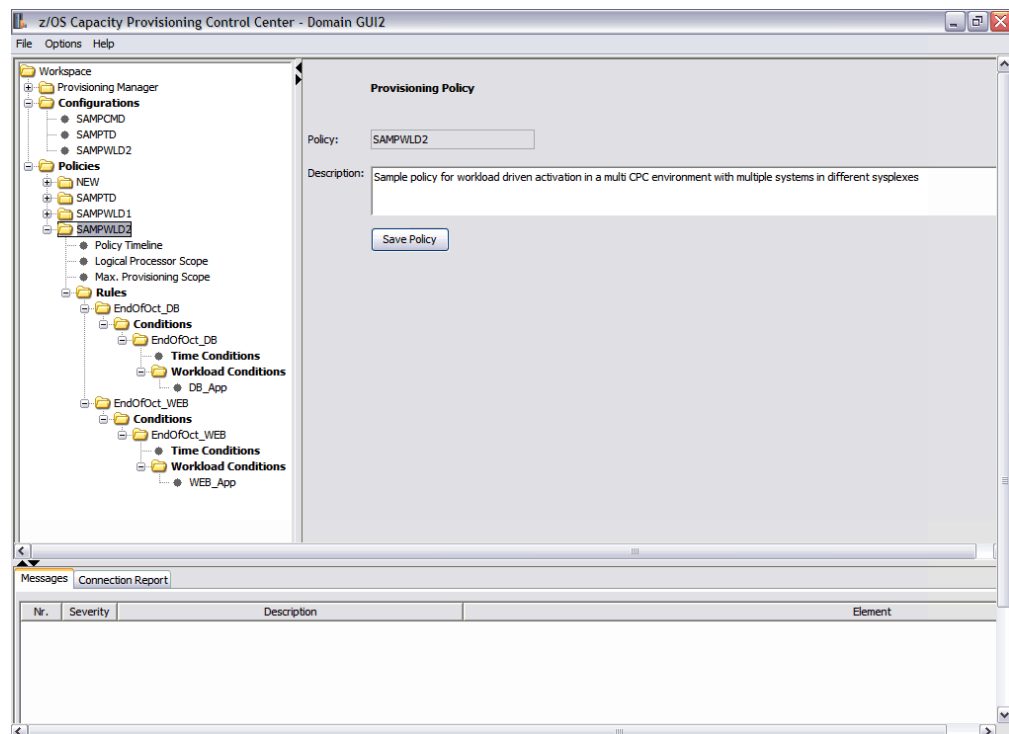
Figure 9. Layout of the graphical user interface

The menu bar at the top is used for general actions. The main window below the menu bar is divided into three panels: the tree navigation on the left, the details view on the right, and the information view at the bottom.

- The **tree navigation** displays the workspace and its contents as a tree.
- Details of the object selected in the tree are displayed in the **details view**.
- Information about the selected object is displayed in the **information view**.

The tree navigation

The tree navigation shows the structure of the Capacity Provisioning workspace. It contains the **Provisioning Manager** folder, the **Configurations** and the **Policies** folder. The **Provisioning Manager** folder manages connections to and reports from a Provisioning Manager. The **Configurations** folder contains one entry for each defined configuration. The **Policies** folder is structured hierarchically. For each policy, it contains an entry for the **Logical Processor Scope**, the **Maximum Provisioning Scope**, and a **Rules** folder. A rule contains **Conditions**, which can be **Time Conditions**, **Workload Conditions**, or both.

In the tree navigation, folders are always preceded by a ⊞ or ⊟ symbol. Clicking these symbols expands or collapses the folder. Nodes that cannot be expanded are indicated by a bullet symbol. Note that a folder can be empty, in which case clicking the ⊞ symbol does not show any more detail.

The help buttons at the bottom offer context-sensitive help.

Operations on the tree

A left-click on an item in the tree selects the object and displays the details of the selected object in the **Details view** on the right.

A right-click on an item in the tree opens the menu with commands for the selected object. If the menu exists, the object is also selected and its details are displayed the **Details view**.

Note: The characters '...' following a command name indicate that the command opens a dialog. This dialog might require further input.

The context commands are:

Command	Action
New...	Creates a new object and prompts for a name.
	This command creates a child object in any folder that has a name in bold type in the tree navigation.
	The **New** command is available on the **Configurations**, **Policies**, **Rules**, **Conditions**, and **Workload Conditions** folders.
Copy	Copies an object to the Control Center clipboard.The object can then be pasted to another position. Only one object can be stored in the clipboard; a second copy command overwrites the previous one.
	The **Copy** command is available for a selected configuration, policy, rule, condition, or workload condition.
Paste	Pastes a copied object to the selected folder if the type of the copied object allows it. For example, a rule can be pasted only in a **Rules** folder. The object remains in the clipboard, so that it can be pasted more than once. If an object with the name of the copied object exists in the selected policy, the name of the pasted object is altered by the Control Center to make it unique.
	The **Paste** command is available in the **Configurations**, **Policies**, **Rules**, **Conditions**, and **Workload Conditions** folders. Rules and conditions can be pasted only to the same policy.
Delete	Deletes an object from the workspace. Policies and configurations are deleted immediately. Policy elements are deleted when the policy is saved.
	The **Delete** command is available for a selected configuration, policy, rule, condition, or workload condition.
Rename	Prompts for a name and renames an existing object. If the new name exists, you are prompted to specify a different one. If a policy or configuration is renamed and it has changed, you are prompted to save it before renaming.
	The **Rename** command is available for a selected configuration, policy, rule, condition, and workload condition.
Save...	Saves the selected object or object group in the workspace.
	Save commands are available in the **Provisioning Manager** and in the **Configurations** and **Policies** folders, and for selected configurations and policies.

Command	Action
Install	Transfers a policy or a configuration to the Provisioning Manager. A connection to the Provisioning Manager must be established and you must be a member of the Provisioning Manager control security group; see "Adapting the Provisioning Manager parameters" on page 50. Domain configurations are installed in the domain configuration repository and policies in the policy repository; see "Defining the runtime data sets" on page 49. The **Install** command is available for a selected configuration or policy.

The details view

The details view shows the properties of the capacity provisioning object that is selected in the tree navigation. This view also shows related elements for some objects.
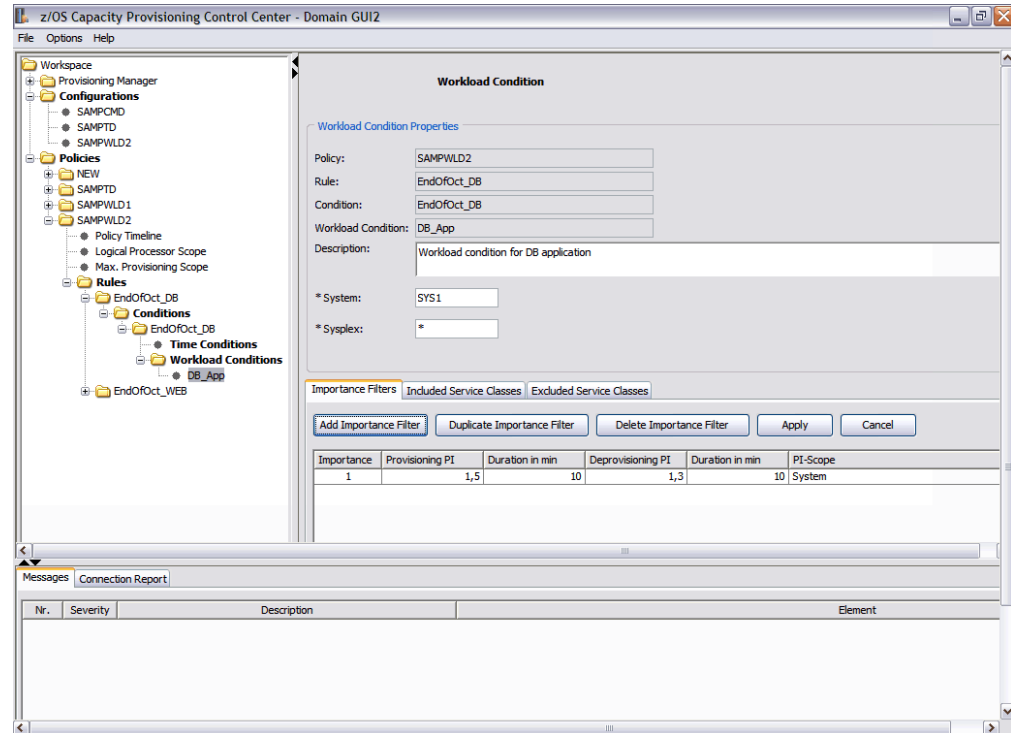
Figure 10. Details view showing the details of a workload condition.

The properties displayed in the upper part of the panel depend on the type of object selected. Figure 10 shows the properties of a **Workload Condition**. For your reference you can add a textual description for most objects.

The lower part of the panel might show a table that contains additional elements of the displayed object, which are not shown in the tree navigation. On some panels, the lower part contains tabs that you can click to switch between multiple tables.

Operations on tables

Buttons below a table allow you to modify the table. The actions performed are:

Button	Action
Add...	Adds a new row after the selected row
Delete...	Deletes the selected row
Apply	Accepts changes to the properties and the contents of the table, and checks for errors. If you click a different tab or node in the tree, **Apply** is executed automatically.
Cancel	Rejects any changes that have been made to the properties and the table since the last **Apply** action.

You can also perform actions directly on rows of the table:

Action	Method
Select a table row	To select a row, left-click anywhere in the row.
Edit a table cell	To edit a cell, click the cell. The cursor is placed to the left of the cell, and as soon as you start to type the background color of the cell changes. If you double-click the cell the color changes immediately and you can position the cursor in the cell.
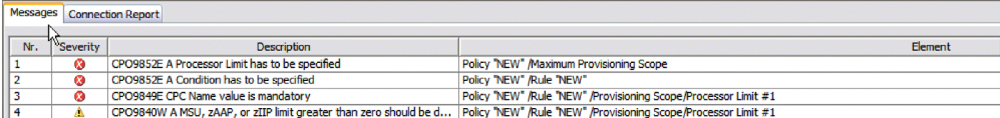
The information view

This view shows one of two panels: one for **Messages** and one for the **Connection Report**. These panels are identified by tabs. Left-click on these tabs to switch from one panel to the other.

Messages

The Messages panel shows a list of messages that are related to the selected object in the tree navigation. If the object belongs to a provisioning policy, messages relating to the complete policy are shown. The list is refreshed when the **Apply** action is executed or when a different object is selected in the tree navigation.

Messages indicate that a policy or domain configuration is not complete or that it contains incompatible specifications. Error messages are displayed if required parts are missing or the specifications are incompatible. Warning messages are displayed if optional but recommended parts are missing. Error messages and warning messages indicate the next steps you should take. An example messages report is:

Nr.	Severity	Description	Element
1	❌	CPO9852E A Processor Limit has to be specified	Policy "NEW" /Maximum Provisioning Scope
2	❌	CPO9852E A Condition has to be specified	Policy "NEW" /Rule "NEW"
3	❌	CPO9849E CPC Name value is mandatory	Policy "NEW" /Rule "NEW" /Provisioning Scope/Processor Limit #1
4	⚠	CPO9840W A MSU, zAAP, or zIIP limit greater than zero should be d...	Policy "NEW" /Rule "NEW" /Provisioning Scope/Processor Limit #1

Figure 11. Messages

Connection Report

The connection report contains information about the interaction between the Control Center and the Provisioning Manager. An entry is added whenever one of the following actions is performed on the Provisioning Manager panel:

- **Connect**
- **Disconnect**
- **Refresh Status**

An entry is also added to the connection report when a policy or a domain configuration is installed. You can remove all entries from the connection report by clicking the **Clear Connection Report** button.

The columns in this report show:

Time   The time the message was generated

Severity   The types of messages include:

                For informational messages. These messages report that the executed operation was successful.

                For warning messages.These messages are issued in situations that can prevent successful completion. Check whether the situation is OK or if you need to take corrective action.

                For error messages.For error messages. These messages are issued when the Control Center could not connect to the Provisioning Manager of the domain, or a policy or domain configuration could not be installed. In these situations, check that the Provisioning Manager and the CIM server are running on the specified host.

Description   The message number and a description of the message

Host Address The address to which the Control Center tried to connect or connected successfully

An example connection report is:

Figure 12. Connection report

The menu bar

The menu bar contains three pull-down menus: **File**, **Options**, and **Help**.

The choices on the **File** menu are:

The File Menu

New Configuration...
> You are prompted to specify a name for a new domain configuration, which is then created.

New Policy...
> You are prompted to specify a name for a new provisioning policy, which is then created.

Save Connections
> Saves all connection definitions in the local workspace.

Save Configurations
> Saves all domain configurations in the local workspace.

Save Policies
> Saves all provisioning policies in the local workspace.

Save All
> Saves all the above in the local workspace.

Refresh Workspace
> Reloads all locally stored connection definitions, domain configurations, and policies. Before reloading, you are asked if you want to save your changes. If you do not save the changes, they are overwritten.

Exit Closes the Control Center. Asks whether to save any changes before closing.

The Options Menu

The **Options** menu contains the **Preferences** dialog, where you can configure the Control Center:

Display Times in Time Zone

The time zone specified here determines the offset with which times are displayed and entered. Click the time zone field to open a list of time zones. The list contains standard time zone abbreviations and descriptions such as Europe/London. You can scroll quickly to a section of the list by typing the initial letter of that section, and can then scroll to and select the time zone of your choice.

CIM Client for Java

The Control Center requires a CIM Client for Java Version 2 archive file (jar) on the workstation. If the sblim-cim-client2.jar is not installed at the default location, you can specify where the file is installed.

Control Center Tracing

If you are advised by IBM service representatives to enable tracing for the Control Center, select the box **enable Tracing** and provide other details as advised. For normal operation, the **enable Tracing** box must be clear.

The Help Menu

The **Help** menu contains the following actions:

Welcome

Shows an introduction to the Control Center that contains links to more detailed information.

About Capacity Provisioning Control Center

Shows the version of the installed Control Center. This information is required if you send a problem report to IBM.

The information displayed is:

Version	The version of the Control Center installed
Driver Level	The build level of the code
APAR Level	The latest update applied to the program after installation
CIM Client Version	The version of the CIM client that interfaces between the Control Center and the Provisioning Manager

The Help Buttons

The help buttons in the lower left corner of the Control Center open a relevant help topic. The **Help** button opens a separate help window, which shows an introduction to the Control Center. Clicking "?" changes the shape of the mouse pointer so that you can click any panel of the Control Center to get help for the selected item.

Starting the Control Center

To start the Control Center, click the **IBM Capacity Provisioning V1R13** icon on your desktop or in the **IBM Capacity Provisioning** program group. When the Control Center V1R13 starts, you are asked which directory contains your workspace. The default is the most recently used directory. When you start the Control Center for the first time, the default is the directory that was specified during installation.
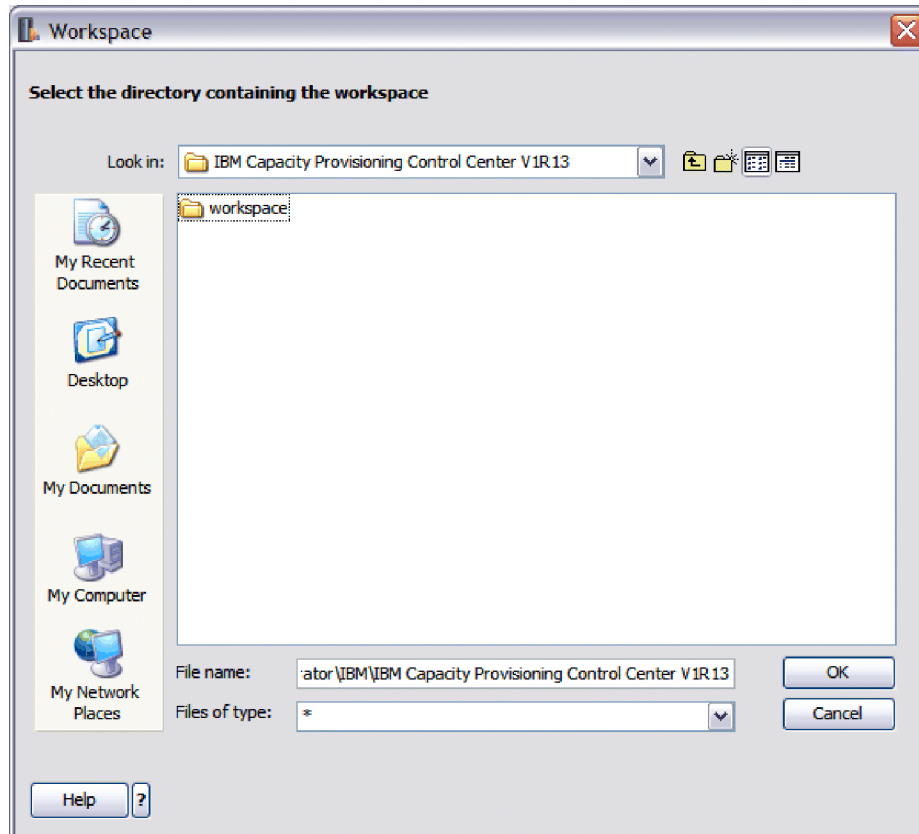
Figure 13. Starting the Control Center. Workspace browser

You can have several workspace directories, for example, one for each provisioning domain, but you can work in only one directory at a time. If you want to switch to a different workspace directory, you must restart the Control Center and specify a new workspace at startup. If the directory does not exist, it is created.

Note: Directories containing the workspace can be flagged as hidden files. If the Windows folder options are set to "Do not show hidden files and folders," they do not appear in the workspace dialog.

Stopping the Control Center

To stop the Control Center, close the window or select **Exit** from the **File** menu. If you have modified any provisioning policies, domain configurations or the connection definition, you are asked whether you want to save your changes before you leave.

Accessing the Provisioning Manager

The Provisioning Manager is the component of Capacity Provisioning which, based on your active policy and domain configuration, monitors the domain and performs activation and deactivation requests for temporary capacity. When the Control Center is connected to the Provisioning Manager you can view the status of the Provisioning Manager and install provisioning policies and domain configurations. This section describes:

1. How to define the connection to the Provisioning Manager.
2. How to work with the Provisioning Manager.
3. How to obtain the Provisioning Manager Status.

Defining connections

To enable a connection to the Provisioning Manager, you must define three elements: the host address where the Provisioning Manager is running, the port to connect to on this system, and the protocol to be used. The procedure to follow is:

1. Click **Provisioning Manager** in the navigation tree.
2. Click the **Add Connection** button. A new entry is created in the Connections table.
3. Click the field in the **Host Address** column and type either the host name or the IP address of the system on which the Provisioning Manager is running.
4. To change the default protocol, select the arrow in the **Protocol** column. Choose either HTTP or HTTPS protocol.
5. To change the default port, click the field in the **Port** column and enter the port number.
6. Click the **Apply** button and check the messages in the information view to ensure that the connection definition does not contain any errors.
7. Click the **Save Connections** buttonto save the connection definitions in the workspace.

Here is an example of a Control Center with one host connection defined and an entry for the second one.
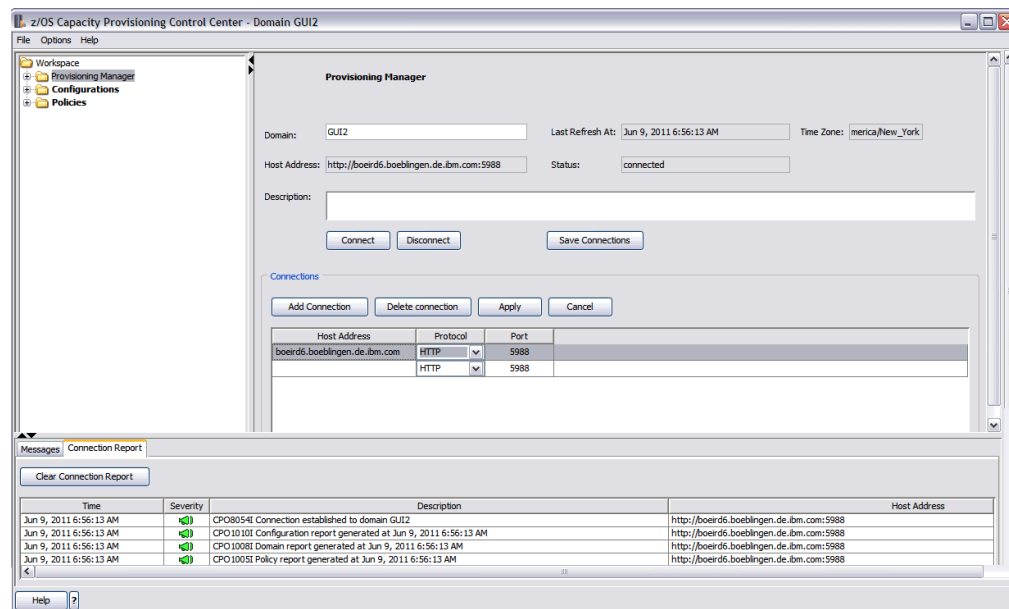
Figure 14. Provisioning Manager screen

If the Provisioning Manager can be started on more than one system, you must create more than one connection definition. Only one connection can be active at any time.

Working with the Provisioning Manager

To connect to the Provisioning Manager on a domain, some prerequisites must be met:

- Your Control Center user must be a member of the Provisioning Manager query security group. If you want to install policies or domain configurations, your Control Center user must also be a member of the Provisioning Manager control security group.
- The Control Center can only be connected to a Provisioning Manager that delivers report information. A Provisioning Manager can deliver report information if it runs on a system with z/OS Release 12 or higher.

To connect to a Provisioning Manager:

1. Enter the name of the domain in the **Domain** field on the Provisioning Manager screen. Use the name you used in Table 10 on page 45.
2. Click the connection you want to use in the Connections table.
3. Click the **Connect** button. A panel asking for the login information opens.
4. Enter your **User** name and **Password** for the system you want to connect to, and click the **OK** button.

The Control Center now checks that a Provisioning Manager for the specified domain is running on the host selected in the Connections table, and tries to connect to it by using the specified protocol and port. If you are unable to connect, try an alternative connection through another entry in the Connections table. If you still cannot connect, check the **Connection Report** in the information view for the cause. See page 79.

The status of the connection between the Control Center and the Provisioning Manager is shown in the **Status** field in the details view of the Provisioning Manager screen. The **Status** field displays:

disconnected   The Control Center is not connected to the Provisioning Manager.

connecting   The Control Center is trying to establish a connection to the Provisioning Manager.

connected   The connection is established and the Provisioning Manager is running.

connectionLost

It was not possible to execute a user request through the existing connection.

When the status is **Connected**, you can install policies and domain configurations into the repositories of the domain, and more information is displayed about the **Active Configuration, Active Policy**, and the **Domain** in the **Status** folder.

The **Last Refresh At** field shows the date and time when information was last gathered. All reported times are displayed in the time zone indicated in the **Time Zone** field. The time zone can be changed through the Preferences dialog described on page 80.

To close the connection, click the **Disconnect** button.

Switching to another domain

If you want to work on a different provisioning domain, first disconnect from the domain you are connected to. Then, change the name in the **Domain** field.

The next time you start the Control Center, the last domain you worked with is the new default.

How to obtain the Provisioning Manager Status

To view the Provisioning Manager Status, you must be connected to the Provisioning Manager for the specified domain. When you connect the Control Center to the Provisioning Manager of a domain, the reports for **Active Configuration**, the **Active Policy**, and the **Domain** are generated. To view a detailed status, proceed as follows:

1. Connect to the Provisioning Manager whose status you want to inspect. The **Status** field shows that the Control Center is **Connecting**.
2. When the **Status** changes to **Connected**, inspect the details of the Provisioning Manager status.
3. In the tree navigation, click '+' to the left of **Provisioning Manager**, and then click '+' to the left of **Status**.
4. Select **Active Configuration, Active Policy**, or **Domain** to display the detailed status of each.
5. The status differs depending on when the information was gathered. Click the **Refresh** button to get the latest information. The **Last Refresh At** field is updated to show the date and time the information was last gathered.
6. Check the **Connection Report** in the information view for the success of Connect and Refresh actions.

If the Control Center was not connected to a Provisioning Manager, the **Status** panels show empty fields. If the connection is lost after the status information was obtained, the information is displayed until it is successfully refreshed, or until the user disconnects from the Provisioning Manager.

The Status of the Active Configuration
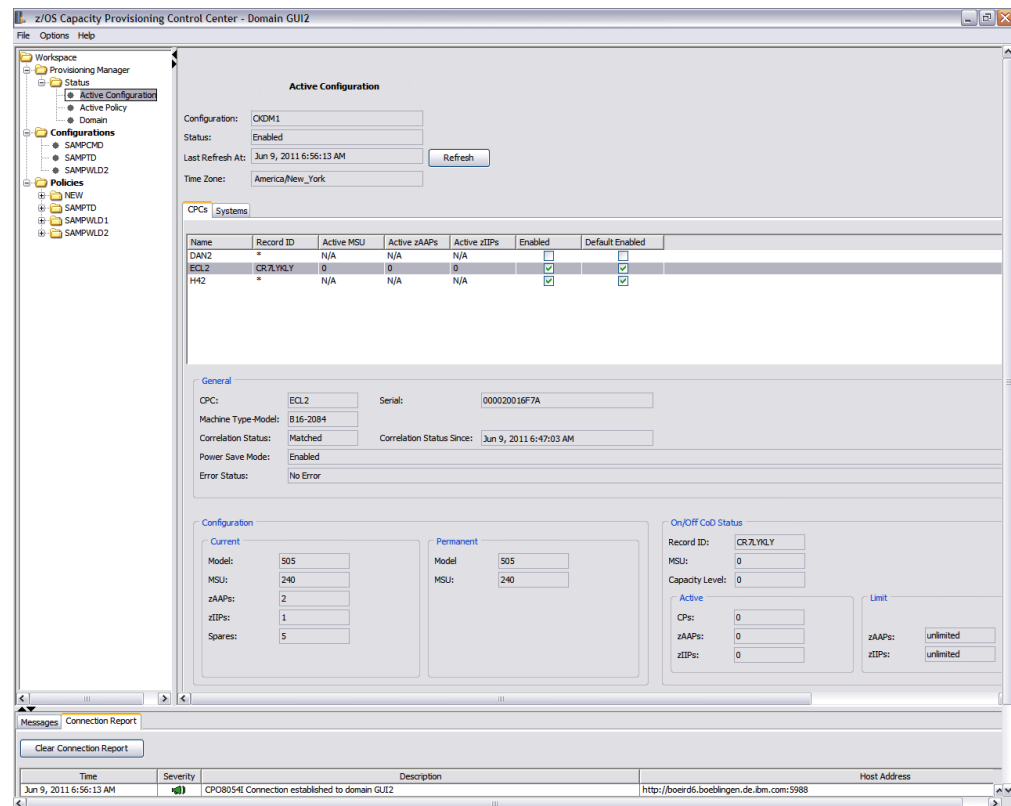
Figure 15. Active Configuration screen

This panel shows information about the active domain configuration on the connected Provisioning Manager and the status of its elements. The information reported indicates:

- The name of the active domain configuration
- Its current enabled or disabled status.
  A domain configuration is disabled if the Provisioning Manager is running in MANUAL processing mode. In all other processing modes, the domain configuration is enabled
- The CPCs defined in the domain configuration
- The systems defined in the domain configuration

The information about the Active Configuration is not refreshed automatically. To update the information click the **Refresh** button. The **Last Refresh At** field is updated to show the date and time the information was last gathered.

All reported times are displayed in the time zone indicated in the **Time Zone** field. The time zone can be changed in the **Preferences** dialog as described on page 80.

CPCs: To inspect the CPCs of the Active Configuration, perform the following steps:

1. Click the **CPCs** tab.
2. Select a CPC in the table to display the details of the selected CPC.

For each CPC, the table shows the following status information:

- The name of the CPC
- Its record ID
- How many MSU are currently active for the record
- How many zAAPs are currently active for the record
- How many zIIPs are currently active for the record
- Its current enabled or disabled status
- The default status defined in the domain configuration when it was activated

You must select a CPC in the table to see detailed information.

General: shows runtime information about the CPC:
- Optionally, if Power Save Mode is supported by the CPC, its current Power Save Mode.

The detailed information shows runtime information about the CPC:
- The name of the CPC
- The serial number of the CPC
- The CPC hardware model and type.
  If the CPC hardware model and type are supported, detailed capacity information about the CPC follows in the **Configuration** and optionally in the **On/Off CoD Status** group.
- The correlation status of the CPC at the support element or HMC. This status can be:
  - Not Correlated

    The CPC was not yet detected at the support element or HMC. CPC cannot be used to activate temporary capacity.
  - Correlated

    The CPC was detected at the support element or HMC, but detailed information about it is not yet available to the Provisioning Manager. It cannot be used to activate temporary capacity.
  - Matched

    The CPC was detected at the support element or HMC and detailed information about it is available. Temporary capacity can be activated on it if a valid record exists.
- The time when the correlation status was reached
- Power Save Mode
- Whether the CPC is supported for capacity management

  No Error
  Indicates that the CPC is supported.

  Any other value
  Indicates why it is not supported. Possibly, the record has expired or the configuration of the CPC does not allow commands to perform the temporary capacity change.

Configuration If the CPC is at a supported hardware level, detailed information about the CPC is displayed here:
- For the current CPC model, the capacity in MSU, number of zAAPs, number of zIIPs, and the number of spare processors
- The permanent model and capacity in MSU

On/Off CoD Status: This group displays detailed information about the On/Off CoD record that is used by the Provisioning Manager to manage temporary capacity. If no usable record is detected, N/A is shown.

- The record ID used by the Provisioning Manager for managing temporary capacity.
- The number of active MSU of the record.
- The number of increases in the capacity settings of the record.
- The number of CPs of the record.
- The number of zAAPs of the record.
- The number of zIIPs of the record.
- The number of zAAP processors allowed to be active for this record. If there is no activation limit in the record a value of unlimited is reported.
- The number of zIIP processors allowed to be active for this record. If there is no activation limit in the record, a value of unlimited is reported.
- The remaining number of MSU days for general-purpose capacity. If there is no limit for MSU days defined in the record, a value of unlimited is reported.
- The remaining number of processor days for zAAPs. If there is no limit for processor days defined in the record, a value of unlimited is reported.
- The remaining number of processor days for zIIPs. If there is no limit for processor days defined in the record, a value of unlimited is reported.

Systems: To inspect the systems from the Active Configuration, perform the following steps:

1. Click the **Systems** tab
2. Select a System in the table to display the details of the selected system

For each system, the table shows the following status information:

- The system name
- The name of the sysplex it belongs to
- The connection status that can be one of the following:
  - Not connected

    The connection to the system is not yet established. The Provisioning Manager is trying to connect to the system at the related host address.
  - Available

    The connection to the system is established.
  - Temporarily unavailable

    The connection to the system was suspended after successfully establishing a connection. The Provisioning Manager tries to reestablish the connection.
  - Unavailable

    The connection to the system has broken down. Provisioning Manager tres to connect to the system again.
- The system status information. This status can be:
  - Unknown

    The system is not identified. Either the name of the system or the name of the sysplex, or both are not yet retrieved.
  - Found

    The system is not correlated. The Provisioning Manager has not yet detected whether the name of the system and the name of the sysplex the system belongs to match the names in the domain configuration. Both names are reported in the message.
  - Correct

    The version of this system is not available. The version of the operating system is not yet retrieved.
  - Incorrect

    This system is not the defined system. Either the name of the system, or the name of the sysplex, or both do not match the definition of these names in the domain configuration.
  - UnsupportedVersion

    The version of this system is not supported. The version of the system is not supported by the Provisioning Manager.
  - CPCUnknown

    The CPC serial number is not available. The serial number of the CPC on which the system is running is not yet retrieved.
  - CPCNameMatched

    The CPC is not correlated. The CPC is not yet correlated. The Provisioning Manager has not detected if the CPC the system is running on is defined in the domain configuration.
  - CPCNotInDomain

    The CPC is not part of the domain. The CPC the system is running on is not defined in the domain configuration.

- SysplexUnknownMintime

  Insufficient information for retrieving metric values. The information for retrieving metric values has not yet been retrieved, or could not be retrieved.

- SysplexUnknown

  The information about the WLM service definition is not available. The name of the installed WLM service definition, the name of the active WLM policy, or the activation time of this policy have not yet been retrieved.

- SysplexUnknownSCP

  The information about WLM service class periods is not available. The service class periods defined in the active WLM policy have not yet been retrieved.

- SysplexValid

  The installed WLM service definition and active WLM policy are displayed in the WLM group.

- The observation status information. The system can be observed if the domain configuration is enabled and the system is enabled. This status can be:

  - PrimaryObserved

    The Provisioning Manager retrieves information from the system at the primary host address.

  - AlternateObserved

    The Provisioning Manager retrieves information from the system at the alternate host address.

  - BothObserved

    The Provisioning Manager retrieves information from the system at the primary host address and from the system at the alternate host address. Both systems are observed as long as they are unavailable.

  - NoneObserved

    The Provisioning Manager does not retrieve information from the system at the primary host address or the system at the alternate host address. The system is not observed if the domain configuration is disabled or the system is disabled.

- The enabled or disabled status
- The default status that was defined in the domain configuration when it was activated

Select a system in the table to show detail information:

Connection: Shows Connection information for the selected system.
- The system name
- The protocol and the port

The Primary Host: Shows information about the system at the primary host address:
- The related host address
- The connection status
- The time when the connection is changed into this status
- The system status
- The observation status
- The CPC where the system is running

The Alternate Host: Shows information about the system at the alternate host address:
- The related host address
- The connection status
- The time when the connection is changed into this status
- The system status
- The observation status
- The CPC where the system is running

WLM: Shows additional information about the system:
- The installed WLM service definition
- The active WLM policy

The Status of the Active Policy
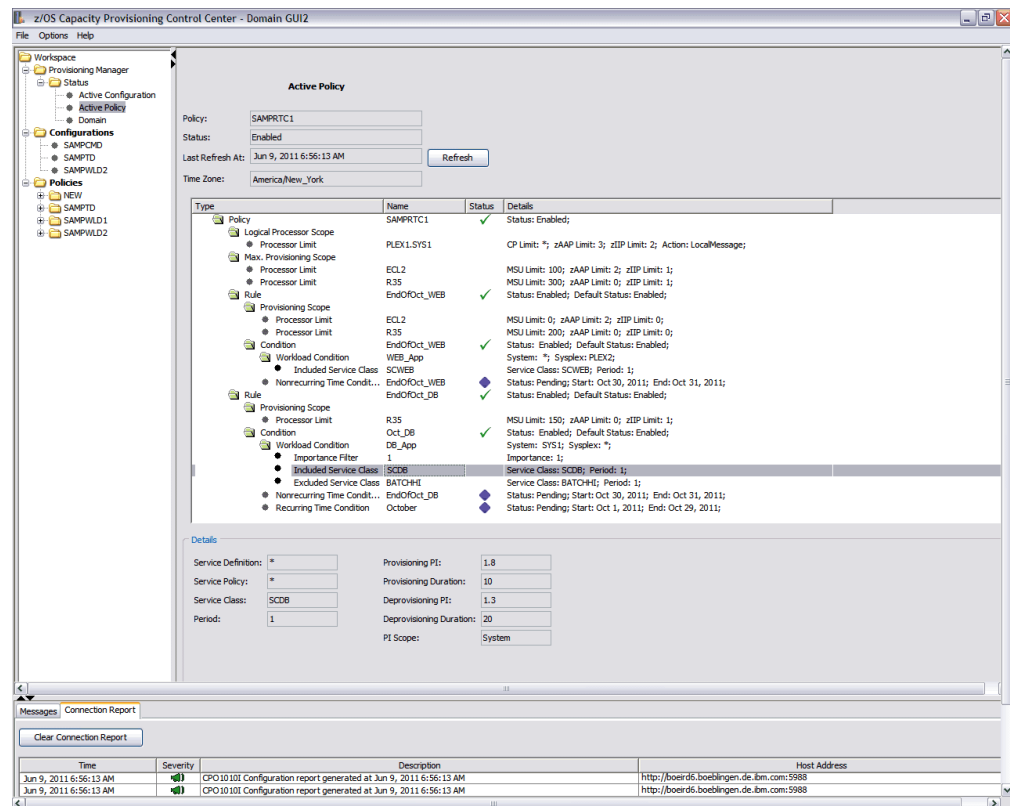
Figure 16. Active Policy screen.

This panel shows information about the active policy and the status of its elements. The information reported is:

- The name of the active policy
- Its current enabled or disabled status. A policy is disabled if the Provisioning Manager is running in MANUAL processing mode. In all other processing modes, the policy is enabled.
- The information about the Active Policy is not refreshed automatically. To update the information, click the **Refresh** button. The **Last Refresh At** field is updated to show the date and time when the information was last gathered.
- All reported times are displayed in the time zone indicated in the **Time Zone** field. The time zone can be changed through the Preferences dialog described on page 80.

The table shows the elements of the policy and their status. Select an element in the table to show detailed information below the table.

For each element, the table shows the following status information:

- The type of element and its position in the hierarchy of the policy
- The name of the element
- The status of the element, which can be:

![check] Enabled

Enabled policy elements are considered by the Provisioning Manager for activations of temporary capacity.

![red] Disabled

Disabled policy elements are not considered by the Provisioning Manager for activations of temporary capacity.

![diamond] Pending

The current time is before the start time of the condition and system observation is not necessary.
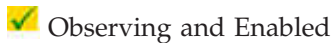
![yellow check] Observing and Enabled

The current time is after the observation start time and before the start time of the condition, the time condition and policy are enabled, and one or more workload conditions are defined. The workload conditions require systems to be observed if possible. To get performance information for further processing, the Provisioning Manager contacts systems that are referenced by associated workload conditions.
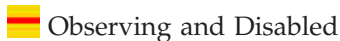
![yellow] Observing and Disabled

The current time is after the observation start time and before the start time of the condition. The time condition is disabled.

![gray check] Active and Enabled
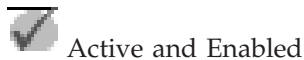
The current time is after the start time and before the deadline of the condition, and the time condition is enabled. The Provisioning Manager can change the activation level of the managed CPCs based on the provisioning condition that contains the time condition.

![red] Active and Disabled

The current time is after the start time and before the deadline of the condition, and the time condition is disabled. No changes to the activation level of the managed CPCs can be performed by the Provisioning Manager based on the provisioning condition that contains the time condition.

![green check] Drained and Enabled

The current time is after the deadline and before the end time of the condition; the time condition is enabled. The Provisioning Manager cannot activate additional temporary resources. It can maintain the current activation level of the managed CPCs based on the provisioning condition that contains the time condition.

Drained and Disabled

The current time is after the deadline and before the end time of the condition, and the time condition is disabled. The Provisioning Manager cannot change the activation level of the managed CPCs based on the provisioning condition that contains the time condition.

Inactive

The current time is after the end time of the condition. The Provisioning Manager cannot change the activation level of the managed CPCs based on the provisioning condition that contains the time condition.

- Details of the policy element are shown in short form. Select a policy element in the table to display all detailed information. Depending on the type of policy element, the following details are displayed:

Details of the Policy Status: Shows the details about the status of the active policy:
- The name of the active policy
- The enabled or disabled status of the active policy: A policy is disabled if the Provisioning Manager is running in MANUAL processing mode. In all other processing modes, the policy is enabled.

Processor Limit Details of Logical Processor Scope: If the active policy contains a Logical Processor Scope, details about processor limits are displayed. The details contain the sysplex and the system name, the maximum number of processors that can be online, and the defined action. An asterisk ('*') stands for as many logical processors as allowed by the z/OS and LPAR configuration.

The processor limit information contains:
- The system name
- The name of the sysplex that the system belongs to
- The maximum amount of logical CP processors that can be online
- The maximum number of zAAP processors that can be online
- The maximum number of zIIP processors that can be online
- The type of action to take, when required changes are detected

Processor Limit Details of Max. Provisioning Scope: Shows the details about the status of a processor limit in the Maximum Provisioning Scope of the active policy. The details contain the CPC name, the maximum resources that can be activated by all provisioning rules, and the capacity increments defined for the CPC.

The processor limit information contains:
- The name of the CPC
- The maximum amount of MSU to be activated
- The maximum number of zAAP processors to be activated
- The maximum number of zIIP processors to be activated
- The minimum amount of MSU for the first activation
- The minimum amount of MSU for all further activations

Details of the Rule Status: Shows details about the status of a selected rule in the active policy, including:

- The name of the selected rule
- Its current enabled or disabled status
- The default status defined in the policy when it was activated

Processor Limit Details of Provisioning Scope: Shows the details about the status of a processor limit in the Provisioning Scope of the active policy. The details contain the CPC name and the maximum resources that can be activated by the selected rule.

- The name of the CPC
- The maximum amount of MSU to be activated
- The maximum number of zAAP processors to be activated
- The maximum number of zIIP processors to be activated

Details of the Condition Status: Shows details about the status of a selected condition in the active policy, including:

- The name of the selected condition
- Its current enabled or disabled status
- The default status defined in the policy when it was activated

Details of the Nonrecurring Time Condition Status: Shows details about the status of a selected time condition in the active policy, including:

- The name of the selected time condition
- Its status; for more information, see Table 6 on page 34.
- The start time at which the Provisioning Manager activates additional capacity if one of the associated workloads is negatively affected
- The deadline, which is the latest time when activation of additional capacity is allowed. Additional capacity that has already been activated can remain activated until the end time or until the capacity is no longer needed
- The end time which is the latest time when the Provisioning Manager starts to deactivate additional capacity.

Details of the Recurring Time Condition Status: Shows details about the status of a selected recurring time condition in the active policy, including:

- The name of the selected recurring time condition
- Its status; for more information, see Table 6 on page 34.
- The start date is the first day on which the Provisioning Manager can activate additional capacity
- The end date is the last day on which the Provisioning Manager can activate additional capacity
- The days of week on which activation of additional capacity is allowed. The time when additional capacity can be activated on the selected day is displayed in the **Start time** field. The deadline and end time can be on the following day if these times are before the start time.
- The start time is the time of the selected day at which the Provisioning Manager can activate additional capacity, if one of the associated workloads are negatively affected.
- The deadline is the time of the selected day when no further capacity is activated. Additional capacity that is already active can remain active until the

end time or until the capacity is no longer needed. Remember that the deadline can be before start time, which means it occurs on the next day.

- The end time is the time of the selected day at which the Provisioning Manager starts to deactivate additional capacity. Remember that the end time can be before start time, which means it occurs on the next day.

Note: If a time zone with daylight saving time is specified, the date and time values used might be one hour later or earlier than the displayed values.

Details of the Workload Condition Status: Shows details about the status of a selected workload condition in the active policy. For each workload condition, the following information is given:

- The name of the selected workload condition
- The name of the system to which the workload condition applies
- The name of the sysplex to which the workload condition applies

Details of the Importance Filter: Shows details about the status of a selected importance of the Importance Filter. For each importance, the following information is given:

- The importance
- The provisioning performance index limit
- The duration of the provisioning performance index limit
- The deprovisioning performance index limit
- The duration of the deprovisioning performance index limit
- The scope for the performance index

Details of the Included Service Classes: Shows details about the status of a selected included service class. For each included service class, the following information is given:

- The Workload Management (WLM) service definition name
- The Workload Management (WLM) service policy name
- The service class name
- The period number of the service class to be observed
- The limit of the provisioning performance index
- The duration of the provisioning performance index limit
- The limit of the deprovisioning performance index
- The duration of the deprovisioning performance index limit
- The scope for the performance index

Details of the Excluded Service Classes: Shows details about the status of a selected excluded service class. For each excluded service class, the following information is given:

- The Workload Management (WLM) service definition name
- The Workload Management (WLM) service policy name
- The service class name
- The service class period to be excluded

The Status of the Connected Domain

The Connected Domain panel shows information about the current setup of the domain that is managed by the Provisioning Manager. This information includes:

- The name of the provisioning domain
- Information about the active configuration. This information is not refreshed automatically. To update the information click the **Refresh** button. The **Last Refresh At** field is updated to show the date and time when the information was last gathered.
- The time zone used for all reported times, as specified in the Preferences dialog.
- The time when the Provisioning Manager for the specified domain was started
- The active processing mode. The possible values for the processing mode are:
  - MANUAL
  - ANALYSIS
  - CONFIRMATION
  - AUTONOMIC
- The time when the processing mode was activated.
- The active domain configuration. A domain configuration name of "*none" indicates that the default domain configuration is active because you never activated your own domain configuration
- The time the active domain configuration was activated. If the domain configuration is "*none", the reported time is the time when the Provisioning Manager first ran
- The name of the active provisioning policy. A policy name of "*none" indicates that the default policy is active because you never activated your own policy
- The time the policy was activated. If the policy is "*none", the reported time is the time when the Provisioning Manager first ran
- Service information about the code level of the running Provisioning Manager

Note: The processing mode, domain configuration, and policy might have been activated in a previous run of the Provisioning Manager and can be earlier than the current start time of the Provisioning Manager.

Working with Domain Configurations

A domain configuration describes the managed CPCs and observed systems in a domain. You use the Control Centerto define domain configurations, and to install them. An installed domain configuration can be activated for the domain by the Provisioning Manager command SET DOMAIN described on page 164.

This section describes:

- How to create a new domain configuration
- How to define the set of CPCs for which the Provisioning Manager can activate additional capacity
- How to specify the z/OS systems to be observed by the Provisioning Manager
- How to install and activate a domain configuration

Creating a domain configuration

A domain configuration lists a set of z/OS systems that can be monitored by the Provisioning Manager, and a set of CPCs for which temporary capacity can be activated or deactivated. To create a domain configuration follow these steps:

1. Right-click on the **Configurations** folder in the tree navigation of the Control Center.
2. Select **New Configuration...**
3. Enter a name for the new configuration. If a configuration with this name already exists in the workspace, the name of the new configuration is altered by the Control Center to make it unique. For information about valid names, see "Naming conventions" on page 41. Characters must be uppercase.
4. Click **OK**. The new configuration is displayed. Since more steps are needed to complete the domain configuration, follow prompts that are displayed in the **Messages** panel at the bottom of the screen.
5. In the **Description** field, enter a description of this configuration for your reference. To leave the description field with keystrokes, type Ctrl + TAB.

In the next steps, you define the observed systems and the controlled CPCs.

Defining the systems

The set of all z/OS systems to be monitored by the Provisioning Manager for resource shortages is defined on the **Systems** panel. The systems are identified by sysplex name and a system name.

To define the systems perform the following steps:

1. On the details view of the domain configuration, click the **Systems** tab.
2. Click the **Add System** button. A new entry is created in the systems table.
3. Click the field in the **System** column and type the name of the z/OS system.
4. Click the field in the **Sysplex** column and type the name of the sysplex to which this z/OS system belongs.
5. Click the field in the **Primary Host Address** column and type either the host name or the IP address of this system.
6. If the system has an alternate address to be used if the primary address is not working, click the field in the **Alternate Host Address** column. Type either the alternate host name or the alternate IP address of the system.
7. If the entry for the protocol of the CIM server that is running on the z/OS system is not correct, click the arrow in the **Protocol** column and choose the protocol to use. To open the protocol combination box by using keystrokes, select the cell in the Protocol column and type F2 + Down Arrow.
8. If the port to be used is not the default (5988), click the field in the **Port** column. Type the number of the port that the CIM server is listening to.
9. Systems are enabled by default. If you want to disable a system, click the check box in the **Enabled** column to clear it. You can also enable or disable systems at run time by using the Provisioning Manager commands ENABLE CONFIGURATION described on page 150 and DISABLE CONFIGURATION described on page 146.
10. Click the **Apply** button. The Control Center checks the specifications for errors. If any errors are found, they are reported in the **Messages** panel at the bottom of the screen.

    Note: To complete the domain configuration, you must specify at least one system.
11. To add more systems, repeat the steps starting from **Add System**.

Defining the CPC

In the **CPCs** panel, you define the set of CPCs that the Provisioning Manager is responsible for. These CPCs must be known at your HMC.

To define the CPCs perform the following steps:

1. On the details view of the domain configuration, click the **CPCs** tab.
2. Click the **Add CPC** button. A new entry is created in the CPCs table.
3. Click the field in the **CPC** column and type the name of the processor complex. This name is the logical name by which it is identified at the support element (SE) of that processor complex.
4. If you want the Provisioning Manager to use a specific On/Off CoD record, click the field **Record ID** column. Enter the identifier of the record that describes the temporary capacity that can be activated on that CPC. If you have just one On/Off CoD record, you can enter an asterisk (*) in this field. The Provisioning Manager will find the record. If you specify an asterisk and you have multiple On/Off CoD records, the Provisioning Manager selects an arbitrary one.

5. CPCs are enabled by default. To disable the CPC, click the check box in the **Enabled** column to clear it. You can also enable or disable CPCs at runtime by using the Provisioning Manager commands "ENABLE CONFIGURATION" on page 150 and "DISABLE CONFIGURATION" on page 146.

6. Click the **Apply** button. The Control Center checks the specifications for errors. If any errors are found, they are reported in the **Messages** panel at the bottom of the screen.
   Note: You must specify at least one CPC.

7. To add more CPCs, repeat the steps starting from **Add CPC**.

The domain configuration is now complete. Select the domain configuration in the tree navigation and click the **Save Configuration** button to save the configuration to the workspace.

Installing and activating a domain configuration

To activate the domain configuration when it is complete and error free, install it to the domain configuration repository of the Provisioning Manager. To install a domain configuration by using the Control Center, perform the following steps:

1. In the tree navigation, click **Provisioning Manager** and ensure that the **Status** field shows **connected**.

2. If the Control Center is not connected, click the **Connect** button and check that the status changes to **connected**.

3. In the tree navigation, right-click on the name of the domain configuration.

4. Select **Install**.

To activate a domain configuration, perform the following steps:

1. Log on to the host where the Provisioning Manager is running.

2. Issue the Provisioning Manager command:
   SET DOMAIN CFG=*domain_configuration_name*

For more information, see "SET DOMAIN" on page 164.

Working with Provisioning Policies

A provisioning policy is used by the Provisioning Manager to determine when and under which conditions additional capacity is activated and deactivated. You can define provisioning policies by using the Control Center. A completed provisioning policy can be installed and activated for the domain by using the Provisioning Manager command ENABLE POLICY described on page 151. Working with Provisioning Policies explains:

- How to create a new provisioning policy
- How to define the components of a provisioning policy
- How to install and activate a provisioning policy
- How to display the policy timeline to see an overview of the time periods when provisioning is allowed

Creating a provisioning policy

A provisioning policy contains a set of provisioning rules that define the time periods during which additional capacity can be activated. The rules also define the work that can trigger the activation of additional capacity. The policy contains a logical processor scope, which defines the z/OS systems in which the number of logical processors can be changed, and a maximum provisioning scope, which places restrictions on the resources that can be activated.

To create a provisioning policy, perform the following steps:

1. Right-click on the **Policies** folder in the tree navigation of the Control Center.
2. Select **New Policy...**
3. Enter a name for the new policy. If a policy with this name exists in the workspace, the name of the new policy is altered by the Control Center to make it unique. For information about valid names, see "Naming conventions" on page 41. Characters must be uppercase.
4. Click **OK**. The new policy is created with entries for the **Policy Timeline**, the **Logical Processor Scope**, the **Max. Provisioning Scope**, and a **Rules** folder. Because further steps are needed to complete the policy, follow the prompts displayed in the **Messages** panel at the bottom of the screen.
5. In the **Description** field, you can enter a description of this policy for your reference.

The next steps are to define the logical processor scope, the maximum provisioning scope, and to create provisioning rules for the policy.

Defining the Logical Processor Scope

A policy contains a single Logical Processor Scope element that defines the z/OS systems for which the number of logical processors can be changed. For each system, you can either specify the maximum number of processors that can be online or specify that the limit of the LPAR definition applies. The Provisioning Manager cannot configure additional processors online, when this limit is reached.

Specifying a logical processor scope is optional. However, the Provisioning Manager will only configure logical processors online or offline if a limit is defined for the system.

The following resources are controlled by the Logical Processor Scope:
- The number of logical Central Processors (CPs)
- The number of logical z Application Assist Processors (zAAPs)
- The number of logical z Integrated Information Processors (zIIPs)

The Logical Processor Scope restricts how many logical processors can be configured online for each system. You cannot define two different maximum values for one system in the same Logical Processor Scope.

To define the Logical Processor Scope for your provisioning policy, perform the following steps:

1. In the tree navigation, click '+' to the left of the name of the policy for which you want to specify the logical processor scope.
2. Click Logical Processor Scope. The Logical Processor panel is shown in the details view of the Control Center.
3. Click the **Add Limit** button to define a limit for a system. A new entry is created in the Logical Processor Scope table. This entry contains the default values for the additional limit.
4. Click the field in the **System** column and type the name of the z/OS system this limit applies to. For information about valid names, see "Naming conventions" on page 41.
5. Click the field in the **Sysplex** column and type the name of the sysplex to which this z/OS system belongs.
6. To specify a limit for the number of logical CP processors, click the field in the **Max. CP Processors** column. Type the maximum number of processors that can be online. An asterisk ('*') indicates a specification of as many logical processors as allowed by the z/OS and LPAR configuration.
7. To specify a limit for the number of logical zAAP processors, click the field in the **Max. zAAP Processors** column and type the maximum number of processors that can be online. An asterisk ('*') indicates a specification of as many logical processors as allowed by the z/OS and LPAR configuration.
8. To specify a limit for the number of zIIP processors, click the field in the **Max. zIIP Processors** column and type the maximum number of processors that can be online. An asterisk ('*') indicates a specification of as many logical processors as allowed by the z/OS and LPAR configuration.
9. By default, the Provisioning Manager sends messages to the system on which the Provisioning Manager runs. To change this default, select the arrow in the **Action** column. You can send messages to the console of the managed system.
10. Click the **Apply** button. The Control Center checks that the specifications are correct.

To add a provisioning limit for another system, repeat these steps.

Defining the Maximum Provisioning Scope

A policy contains a single Maximum Provisioning Scope element that defines the maximum number of additional resources that can be activated at one time on behalf of all rules, and defines the amount in which capacity is to increment. Only resources that are activated through a Capacity Provisioning policy are considered in this limit. Resources that are activated manually, by using either Provisioning Manager commands or the interfaces available on the HMC, are not managed by the Provisioning Manager.

The resources controlled by the Maximum Provisioning Scope are:

- The general-purpose capacity in MSU
- The number of z Application Assist Processors (zAAPs)
- The number of z Integrated Information Processors (zIIPs)

For each CPC in the table, you can also specify the increments in which general-purpose capacity is added:

- One increment for the first activation, the Primary Activation in MSU
- Another increment for all further activations, the Secondary Activations in MSU

The capacity increments denote the minimum capacity that is to be added, if possible. Capacity increments are used for workload-based capacity activation. Both increments must not be higher than the maximum capacity specified as the Maximum MSU.

The Maximum Provisioning Scope limits how much additional capacity can be activated for each CPC. You cannot define two different limits for a single CPC in the policy.

To define the Maximum Provisioning Scope for your provisioning policy, perform the following steps:

1. In the tree navigation, click the '+' to the left of the name of the policy for which want to specify the maximum provisioning scope.
2. Click **Max. Provisioning Scope**. The Maximum Provisioning Scope panel is shown in the details view of the Control Center.
3. To define a provisioning limit for a processor complex, click the **Add Limit** button. A new entry is created in the Maximum Provisioning Scope table is created.
4. Click the field in the **CPC** column and type in the name of the processor complex. This name is the logical name by which it is identified at the support element (SE) of that processor complex.
5. Optionally, to allow the Provisioning Manager to activate additional general-purpose capacity, click the field in the **Max. MSU** column and type the maximum amount of MSU to be activated by all rules of the policy.
6. Optionally, to allow the Provisioning Manager to activate additional zAAP processors, click the field in the **Max. zAAP Processors** column and type the maximum number of processors to be activated.
7. Optionally, to allow the Provisioning Manager to activate additional zIIP processors, click the field in the **Max. zIIP Processors** column and type the maximum number of processors to be activated.
8. Optionally, to change an increment for the first activation click the field in the **Primary Activation (MSU)** column and type the minimum amount of MSU to be activated.

9. Optionally, to change an increment for the second and all following activations, click the field in the **Secondary Activations (MSU)** column and type the minimum amount of MSU to be activated.
10. Click the **Apply** button. The Control Center checks that the specifications are error free.
    Note: At least one processor limit for a CPC must be specified, and each limit must define at least one type of capacity.
11. To add a provisioning limit for another processor complex repeat the steps starting from **Add Limit**.

Creating provisioning rules

A provisioning rule contains a provisioning scope and provisioning conditions. The provisioning scope restricts the capacity that can be activated by the conditions in the rule. Each rule must have a unique name within the policy.

A rule can be enabled or disabled. Disabled rules are ignored by the Provisioning Manager.

To create a provisioning rule, perform the following steps:
1. Right-click on **Rules** in the tree navigation of the policy.
2. Select **New Rule...**
3. Enter the name of the new rule. If a rule with this name exists in the policy, the name of the new rule is altered by the Control Center to make it unique. For information about valid names, see "Naming conventions" on page 41.
4. Click **OK**. The new rule is created including a **Conditions** subfolder.
5. In the **Description** field, you can enter a description of this rule for your reference.
6. Rules are enabled by default. If you want to disable the rule, click the **Enabled** check box to clear it. If the rule is disabled, the Provisioning Manager does not consider it for triggering activation or deactivation of additional resources. You can also enable or disable rules at runtime by using the Provisioning Manager commands "ENABLE POLICY" on page 151 and "DISABLE POLICY" on page 147.

You can now define the provisioning scope and provisioning conditions for the rule.

Defining the provisioning scope for a rule: A rule contains a provisioning scope element, which defines the maximum number of resources that can be activated by all the contained conditions. The provisioning scope is defined in a similar way to the maximum provisioning scope.

If you define restrictions for CPCs in the provisioning scope of a rule, limits for these CPCs must also be defined in the maximum provisioning scope. If they are not defined, additional capacity is not activated. The values in the provisioning scope for each rule must be less than or equal to the values in the maximum provisioning scope.

Creating a provisioning condition for a rule: A provisioning condition contains two parts:
• **Time conditions** define time periods during which additional capacity can be activated.

- **Workload conditions** define the work that is eligible to activate additional capacity and the conditions under which the work can activate additional capacity. Workload conditions are optional.

A provisioning condition is either enabled or disabled. Disabled provisioning conditions are not considered by the Provisioning Manager.

To specify a provisioning condition, perform the following steps:

1. In the tree navigation, click to the left of the name of the rule to which you want to add the condition.
2. Right-click on **Conditions**.
3. Select **New Condition...**
4. Enter the name of the new condition. If a condition with this name already exists in the policy, the name of the new condition is altered by the Control Center to make it unique. For information about valid names, see "Naming conventions" on page 41.
5. Click **OK**. The new condition is created and an entry for the **Time Conditions** and a **Workload Conditions** folder are created under it in the tree navigation.
6. Conditions are enabled by default. If you want to disable the condition, click the **Enabled** check box to clear it. If the condition or the rule for the condition is disabled, the Provisioning Manager does not consider this condition for triggering activation of additional resources. You can also enable or disable conditions at runtime by using the Provisioning Manager commands "ENABLE POLICY" on page 151 and "DISABLE POLICY" on page 147.
7. In the **Description** field, you can enter a description of this condition for your reference.

The next step is to define a time condition for the provisioning condition.

Specifying a time condition: A time condition defines one or several periods during which the activation of additional resources is allowed.

The format of the date and time that is accepted by the Control Center is determined by the regional options of your workstation.

Note: If the regional options determine that seconds are displayed, they can be specified, but they are not used by the Control Center.

All dates and times are entered and displayed by using the time zone that is displayed in the **Times displayed in Time Zone** field. The time zone can be changed by using the **Options** menu, as described in "The menu bar" on page 80. A time zone change affects the display of all policies. The actual date and time values are stored in the workspace as Coordinated Universal Time (UTC).

To specify a time condition, perform the following steps:

1. In the tree navigation, click [+] to the left of the name of the condition to which you want to add a time condition.
2. Click **Time Conditions**.

The next step is to specify one or more periods during which the activation of additional resources is allowed. The lower part of the time conditions panel contains two tabs. The tabs are:

Nonrecurring

> Used to specify one period that is limited by a start and end point in time.

Recurring

> Used to specify weekly repeating periods. These periods describe the time of the day when provisioning of resources is allowed, and the days of the week for which these times apply.
>
> The provisioning period can start on one day and end on the following day.

Specifying a nonrecurring time condition: The specification of nonrecurring time conditions is optional. However, a valid condition must include at least one nonrecurring time condition or one recurring time condition.

To specify a nonrecurring time condition, perform the following steps:

1. Click the **Nonrecurring** tab.
2. Click the **Add Time Condition** button. A new row is added to the table where you can specify the new time condition.
   - In the **Name** column, enter the column and type a name for the new time condition. If a time condition with this name exists in the policy, the name of the new time condition is altered by the Control Center to make it unique. For information about valid names, see "Naming conventions" on page 41. The name is used in Provisioning Manager reports to reference the time condition.
   - In the **Start Time** column, enter the date and time for the provisioning period to begin.
   - In the **Deadline** column, enter the latest date and time when activation of additional capacity is allowed. The date and time must be after the start time.
   - In the **End Time** enter the date and time for the Provisioning Manager to start deactivating the additional capacity. The date and time must be on or after the deadline.
3. If you want to add another time condition, repeat the entire procedure.
4. Click the **Apply** button. The Control Center checks the specifications for errors. If any errors are found, they are reported in the Messages panel at the bottom of the screen.

Specifying a recurring time condition: The specification of recurring time conditions is optional. However, there must be at least one nonrecurring time condition or one recurring time condition for a valid condition.

To specify a recurring time condition, perform the following steps:

1. Click the **Recurring** tab.
2. Click the **Add Time Condition** button. A new row is added to the table where you can specify the new time condition.
   - In the **Name** column, type a name for the new time condition. If a time condition with this name already exists in the policy, the name of the new time condition is altered by the Control Center to make it unique. For information about valid names, see "Naming conventions" on page 41.

     The name is used in Provisioning Manager reports to reference the time condition.
   - In the **Start Date** column, enter the date of the first day on which the Provisioning Manager can activate additional capacity.

- In the **End Date** column, enter the date of the last day on which the Provisioning Manager can activate additional capacity. The date must be after the start date.
- Check the boxes for the days of the week on which activation of additional capacity is allowed. The time when additional capacity can be activated on the checked day is defined in the **Start Time** column. Deadline and end time can be on the following day if these times are before the start time.
- In the **Start Time** column, enter the time of day at which the Provisioning Manager can activate additional capacity, if one of the associated workloads is negatively affected.
- In the **Deadline** column, enter the time of day at which no further capacity is activated. Additional capacity that is already active can remain active until the end time or until the capacity is no longer needed. The deadline must be between the start and the end of the provisioning period. If the time is before start time, the deadline is on the following day.
- In the **End Time** column, enter the time of day at which the Provisioning Manager starts to deactivate additional capacity. If end time is before start time, the provisioning period ends on the following day.

3. If you want to add more time conditions, repeat the entire procedure.
4. Click the **Apply** button. The Control Center checks the specifications for errors. If any errors are found, they are reported in the **Messages** panel at the bottom of the screen. If a time zone with daylight saving time is used, the Control Center checks whether the conditions contain one or more daylight saving time adjustments. If the conditions are met, a warning indicates that the date and time values used might be one hour later or earlier than the values displayed.

Note: If a time zone with daylight saving time is specified, the date and time values actually used might be one hour later or earlier than the values displayed. The times are always converted to UTC based on the daylight savings situation on the start date.

Note: When you switch the Control Center to a different time zone, all dates and times are adjusted. If the start time of a recurring time condition moves to a different day, the checks for the selected days of the week are moved accordingly.

You can now define a workload condition. If time conditions are defined but no workload conditions, the Provisioning Manager performs a scheduled activation and deactivation of additional capacity. At the start of a time condition, the maximum allowed additional resources are activated, as restricted by the provisioning scope. At the end time of the time condition, any activated capacity is deactivated.

Creating a workload condition: A workload condition identifies work which is eligible to cause an activation of additional capacity, and the conditions under which activation can be triggered. Eligible work is specified according to the workload model of the z/OS Workload Manager (WLM).

To create a workload condition, perform the following steps:
1. In the tree navigation right-click on **Workload Conditions**.
2. Select **New Workload Condition...**

3. If a condition with this name already exists in the provisioning policy, the name of the new workload condition is altered by the Control Center to make it unique. For information about valid names, see "Naming conventions" on page 41.

4. Click **OK**. The new workload condition is displayed. Since further steps are needed to complete the policy, follow the prompts displayed in the **Messages** panel at the bottom of the screen.

5. In the **Description** field, you can enter a description of this workload condition for your reference.

6. Enter a name in the **Sysplex** field. To apply the condition to all sysplexes in the domain configuration, insert an asterisk (*) here. Otherwise only workload on the named sysplex is considered to trigger provisioning for this workload condition.

7. Enter the name of a z/OS system in the **System** field. To apply the condition to all systems in the named sysplex or the domain configuration, insert an asterisk (*). Otherwise only workload on the named system is considered to trigger provisioning for this workload condition.

8. Click the **Apply** button. The Control Center then checks the specifications for errors. If any errors are found, they are reported in the **Messages** panel at the bottom of the screen.

The next step is to identify the workload on the specified system based on the z/OS WLM service class model. Depending on the work that is running on a system, different service classes can be business-critical. The lower part of the **Workload Condition** panel contains three tabs. These tabs can be used to identify potentially critical service class periods. For more information, see "Workload conditions" on page 24. The tabs are:

Importance Filters   Used to specify service class periods to be monitored, based on their importance, and the performance index values and durations to trigger intervention.

Included Service Classes   Used to specify service classes to be monitored in addition to any identified by importance filters, and the triggers for the included service classes.

Excluded Service Classes filter
Used to specify service classes to be excluded from importance filters, or subsets of Included Service Classes to be excluded.

Note: You must specify at least one importance filter or included service class filter for a workload condition.

Specifying an importance filter: The specification of importance filters is optional. However, there must be at least one importance filter or one included service class filter for a valid workload condition. All service class periods with an importance level that is equal or higher than the specified value are monitored for resource shortages by the Provisioning Manager. For each specified importance level, additional provisioning criteria must be defined.

To specify an importance filter, perform the following steps:

1. In the tree navigation of the Control Center, click the name of the workload condition for which you want to specify an importance filter.

2. Click the **Importance Filters** tab.

3. Click the **Add Importance Filter** button.A new entry is created in the Importance Filters table that contains default values for the filter. All fields are required. If any of the defaults are not suitable, correct them as follows:

- Click the **Importance** column to change it. Service class periods with the specified importance level or higher are observed.
- In the **Provisioning PI** column, enter a value between 1.3 and 10. If the performance index of a service class period with at least the importance level is equal to or higher than the specified value, the Provisioning Manager considers the service class period to be negatively affected.
- In the first **Duration in min**column, enter a value between 1 and 1440. A service class period with at least the importance level must exceed the provisioning PI for at least that duration in minutes before the Provisioning Manager considers the service class period to be negatively affected.
- In the **Deprovisioning PI** column, enter a value between 1.1 and 9.8. The value must be at least 0.2 lower than the Provisioning PI limit, and must be not less than 1.1. If the performance index of a service class period with at least the importance level is equal to or higher than the specified value, the Provisioning Manager considers the service class period to be negatively affected.
- In the second **Duration in min** column, enter a value between 1 and 1440. A service class period with at least the importance level needs to fall below the deprovisioning PI for at least that duration in minutes before the Provisioning Manager considers that the service class is no longer negatively affected. It must have a value of 5 - 1440 minutes.

  Short times for the provisioning and deprovisioning duration require adequate configuration for the data gathering interval of your monitoring product, such as the MINTIME in RMF Monitor III and Capacity Provisioning management cycle time. The data gathering interval and the Capacity Provisioning management cycle time need to be short enough to support the duration value. If a duration of less than 4 minutes is specified, a warning message is issued.

- In the **PI-Scope** column, you can introduce changes. This scope indicates which PI other criteria apply to. The possible values are **System** and **Sysplex**. The default is **System**.

4. To add another importance filter, repeat the steps starting from the **Add Importance Filter** step.

5. Click the **Apply** button. The Control Center checks the specifications for errors. If any errors are found they are reported in the **Messages** panel at the bottom of the screen.

Specifying an included service class: The specification of included service classes filters is optional. However, there must be at least one importance filter or one included service class filter for a valid workload condition. Any service class listed on the **Included Service Classes** panel can trigger provisioning when it is in the defined service class period. For each specified service class period, additional provisioning criteria must be defined.

To add a service class on the **Included Service Classes** panel, perform the following steps:

1. Click the **Included Service Classes** tab.
2. Click the **Add Service Class Filter** button. A new entry is created in the included service classes table that contains the default values for the additional provisioning criteria. All fields of a service class filter are required.
   - In the **Service Definition** column, specify the name of the WLM service definition. To specify all service definitions insert an asterisk (*).
   - In the **Service Policy** column, specify the name of the WLM service policy. To specify all service policies insert an asterisk (*).
   - In the **Service Class** column, specify the name of the WLM service class to consider. To specify all service classes insert an asterisk (*).

   If any of the defaults are not suitable correct them as follows:
   - In the **Period** column, specify the number of the highest period of service class to be considered. All periods with a period number less than or equal to this period are considered.
   - In the **Provisioning PI** column, enter a value of 1.3 - 10. If the performance index of a service class period with at least the importance level is equal to or higher than the specified value, the Provisioning Manager considers the service class period to be negatively affected.
   - In the first **Duration in min** column, enter a value between 1 and 1440. A service class period with at least the importance level must exceed the provisioning PI for at least that duration in minutes before the Provisioning Manager considers the service class period to be negatively affected.
   - In the **Deprovisioning PI** column, enter a value between 1.1 and 9.8 but at least 0.2 lower than the Provisioning PI. If the performance index of a service class period with at least the importance level is equal to or higher than the specified value, the Provisioning Manager considers the service class period to be negatively affected.
   - In the second **Duration in min** column, enter a value between 1 and 1440. A service class period with at least the importance level must fall below the deprovisioning PI for at least that duration in minutes before the Provisioning Manager considers that the service class is no longer negatively affected.
   - In the **PI-Scope** column, you can introduce changes. This scope indicates which PI the other criteria apply to. The possible values are **System** and **Sysplex**. The default is **System**.
3. If you want to add service class, proceed starting from the step **Add Service Class Filter**.
4. Click the **Apply** button. The Control Center checks the specifications for errors. If any errors are found, they are reported in the **Messages** panel at the bottom of the screen.

Specifying an excluded service class: The specification of excluded service classes filters is optional and is used to exclude selected service classes that would

otherwise be included in an importance filter. The service classes listed on the **Excluded Service Classes Filter** panel do not trigger provisioning, even if they match the importance filters or the included service classes criteria.

To exclude a service class on the **Excluded Service Classes** panel, perform the following steps:

1. Click the **Excluded Service Classes** tab.
2. Click the **Add Service Class Filter** button.A new entry is created in the excluded service classes table that contains the default values for the additional provisioning criteria. All fields of a Service Class Filter are required.
   - In the **Service Definition** column, specify the name of the WLM service definition. To specify all service definitions, insert an asterisk (*).
   - In the **Service Policy** column, specify the name of the WLM service policy. To specify all service policies, insert an asterisk.
   - In the **Service Class** column, specify the name of the WLM service class to consider. To specify all service classes, insert an asterisk.

   If the default period is not suitable correct it as follows:
   - In the **Period** column, specify the number of the maximum period of the service class that is considered for provisioning. All periods with a number equal to or higher than the specified number are not considered.
3. If you want to exclude additional service classes, repeat from the **Add Service Class Filter** step.
4. Click the **Apply** button. The Control Center checks the specifications for errors. If any errors are found, they are reported in the **Messages** panel at the bottom of the screen.

The provisioning policy is now complete. Select the policy in the tree navigation and click the **Save Policy** button to save the policy to the workspace.

Installing and activating a provisioning policy

To activate the provisioning policy when it is complete and error free, install it to the provisioning policy repository of the domain. To install a provisioning policy by using the Control Center, perform the following steps:

1. In the tree navigation, click **Provisioning Manager** and check that the **Status** field shows **Connected**.
2. If the Control Center is not connected, click the **Connect** button and check that the status changes to **Connected**.
3. In the tree navigation, right-click on the name of the provisioning policy.
4. Select **Install**.

To activate a provisioning policy,perform the following steps:

1. Log on to the host on which the Provisioning Manager is running.
2. Issue the following Provisioning Manager command:
   ```
   SET DOMAIN POL=policy_name
   ```

For more information, see "SET DOMAIN" on page 164.

Displaying the policy timeline

To see an overview of the times when additional capacity can be activated and deactivated, display the timeline of the policy.

The procedure for displaying the timeline of a policy is the following:

1. In the tree navigation, click the "+" sign to the left of the name of the policy for which you want to display the timeline.
2. Click Policy Timeline. The Policy Timeline pane is shown in the details view of the Control Center.
3. Select the start and end dates for the time period for which you want to view possible activations. Only years for which time conditions exist in the selected policy are selectable.
4. Click one of the radio buttons to see either all known rules or all known conditions for the policy and to later select a subset of those to be displayed.
5. Select the rules or conditions you want to display. The screen shows whether the rules or conditions are enabled or disabled in the policy. The buttons below the table are provided for your convenience to select or clear groups of entries:

   All   All rules or conditions are to be displayed.

   None   All rules or conditions are cleared and none is displayed.

   Enabled   All enabled rules or conditions are to be displayed.

   Disabled   All disabled rules or conditions are to be displayed.
6. When you have selected the rules or conditions that you want to include, click the **Show Timeline** button.

A window opens that shows the selected time period and the included time conditions of the selected rules or conditions, for example:
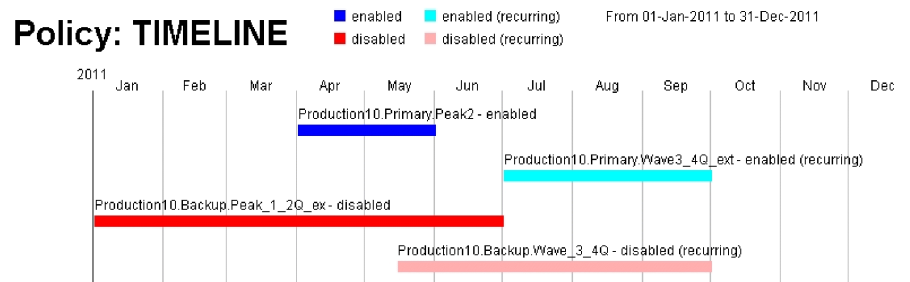
Figure 17. Policy timeline screen

Chapter 5. Using Capacity Provisioning in z/OS Management Facility

IBM z/OS Management Facility (z/OSMF) provides a framework for managing various aspects of a z/OS system through a Web browser interface. By streamlining some traditional tasks and automating others, z/OSMF can simplify some areas of system management and reduce the level of expertise that is needed for managing a system.

Capacity Provisioning provides a plug-in for z/OSMF that offers the following functionality:

Manage connections to your Provisioning Manager
Create, modify, and delete connections that you use to connect to your Provisioning Manager.

View reports
Request a domain status, active configuration, or active policy report.

Getting started with z/OSMF

After z/OSMF is installed and configured, you can log in with a Web browser. You see a navigation area on the left and a working area on the right. Depending on the installed plug-ins, z/OSMF offers a number of traditional system programmer tasks for which the user is authorized. The tasks belong to different categories. The Capacity Provisioning task is in the Performance category. When you click the Capacity Provisioning task, it opens in the working area.

Working with the Capacity Provisioning task

The initial page of the Capacity Provisioning task is called Provisioning Manager. The page contains a table with connections that you can use to connect to your Provisioning Manager. Connecting to a Provisioning Manager includes communication with the CIM server on the system where the Provisioning Manager runs. You can manage those connections by creating, modifying, and deleting them. The connections are stored in a shared repository on the z/OSMF server. You can use both local Provisioning Managers running on the same system on which z/OSMF is running and remote Provisioning Managers.

The connections are used to query the status of your Provisioning Manager. The following status reports are available:

- Domain Status
- Active Configuration
- Active Policy

To view a report for a specific domain that is managed by your Provisioning Manager, perform the following steps:

1. If a connection is not defined, add a connection by clicking **Actions** and then **New...** Specify the host address, port, and protocol; then click **OK**.

2. Select a connection and click **Actions**, and then **View**. A submenu opens that contains the choices **Domain status, Active configuration**, and **Active policy**. Select one of the entries to view the corresponding report.

3. A dialog opens to select a domain that is managed by the Provisioning Manager you are connected to. Select a domain and click **OK**.

The z/OSMF Capacity Provisioning task queries the Provisioning Manager to retrieve the requested report.

Additional information

You can find further information about z/OSMF and the Capacity Provisioning task in the *z/OS Management Facility Configuration Guide*.

Chapter 6. Controlling the Provisioning Manager

The Provisioning Manager is the server component in a Capacity Provisioning domain that manages the activation and deactivation of temporary capacity on your CPCs. It can be accessed from the MVS console or from any console device.

Starting the Provisioning Manager

The Provisioning Manager runs as a z/OS started task. You use the MVS start command to start the program.

Syntax

```
►►─┬─START─┬─CPOSERV─────────────────────────────────────────────►◄
   └─S─────┘         └─,POLICY=─┬─*────┬─┘  └─,PMODE=─┬─*────────┬─┘
                               └─name─┘               ├─MAN──────┤
                                                      ├─ANALYSIS─┤
                                                      ├─CONF─────┤
                                                      └─AUTO─────┘
```
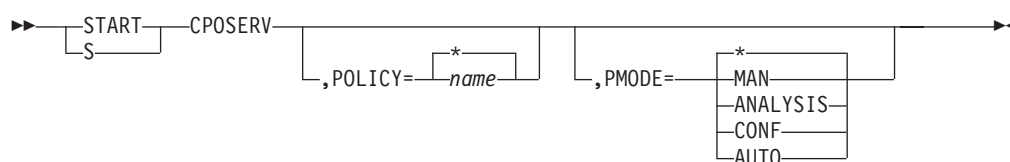
Parameters

POLICY=_name_

Specifies the name of the policy to be activated when the Provisioning Manager starts. A policy with this name must be available in the policy repository that is accessible to the Provisioning Manager. If the Provisioning Manager cannot activate the new policy, it stops.

You can specify an asterisk (*) instead of a policy name. In this case, the last recently active policy for the provisioning domain is used and no policy is retrieved from the policy repository. POLICY=* is the default for this parameter.

PMODE=_mode_

Specifies the initial processing mode of the Provisioning Manager. The following processing mode values are supported:

MAN	Manual mode, which disables policies
ANALYSIS	Analysis mode
CONF	Confirmation mode
AUTO	Autonomic mode

If the Provisioning Manager cannot activate the processing mode, it stops immediately.

You can specify an asterisk (*) instead of a processing mode. In this case, the lat recently active processing mode for the provisioning domain is used. PMODE=* is the default for this parameter.

If you start the Provisioning Manager for the first time without specifying start parameters, it starts with the default policy and the default processing mode. The

default policy is indicated by the policy name "*none". This policy is an empty policy that contains no rules. The default processing mode is manual (MAN).

When you start the Provisioning Manager for the first time, the default domain configuration is activated. The default domain configuration is indicated by the name "*none". This configuration is empty and contains no CPCs and no systems.

For more information about how to activate a new policy, a new domain configuration or a new processing mode, see "SET DOMAIN" on page 164.

Provisioning Manager commands

When the Provisioning Manager is running, it responds to MVS MODIFY and STOP commands. You pass commands to the provisioning manager by using MODIFY. These commands are processed sequentially.

The syntax for issuing Provisioning Manager commands is:

```
►►──┬─MODIFY─┬──CPOSERV──,──APPL=Provisioning Manager command───────────►◄
    └─F──────┘
```

For more information about the Provisioning Manager commands, see Chapter 9, "Provisioning Manager command reference," on page 139.

Stopping the Provisioning Manager

Two commands are used to end Provisioning Manager processing:

- The Provisioning Manager `stop manager` command. For more information, see page 168.
- The MVS STOP command. This command is equivalent to the Provisioning Manager command `stop manager mode=normal`. The format of the MVS command is:

```
►►──┬─STOP─┬──CPOSERV─────────────────────────────────────────►◄
    └─P────┘
```
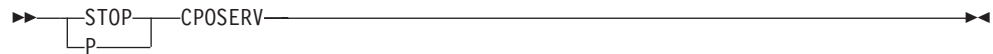
After the Provisioning Manager stop command is issued, it does not accept any further commands. While the Provisioning Manager runs, it writes status data to a restart data set, so that, when it is restarted, it continues to manage resources from the point where it stopped. This function allows for short breaks, for example, if you need to transfer the Provisioning Manager to another system. If you expect a longer interruption to processing, end the program only when there are no temporary resources activated by the Provisioning Manager.

Note: After a restart, the Provisioning Manager needs time to collect all the data required to decide on actions related to workload conditions. The minimum time required for this is the provisioning duration of all the specified and active workload conditions. Until this data is gathered, the Provisioning Manager assumes that no additional capacity is needed for workload conditions.

Temporary capacity that is activated by the Provisioning Manager is not automatically deactivated when the Provisioning Manager stops. If you have to deactivate temporary resources, do it manually before you issue the stop command. To find out which temporary resources are currently active, issue the `REPORT CONFIGURATION` command; see page 156. After the Provisioning Manager stops, temporary resources can be deactivated only by using the hardware interface at the HMC.

Answering operator messages

In some situations, the Provisioning Manager issues operator messages that you can reply to. These situations can occur:

- When the Provisioning Manager runs in confirmation mode and asks whether the proposed actions are allowed
- If inconsistencies with the hardware are detected

If the Provisioning Manager is running in confirmation mode, it checks the policy and the workload on the systems that are defined in the domain configuration to see whether temporary resources must be activated or deactivated. The Provisioning Manager proposes a change to the activation level and issues a message that asks whether you want to allow the proposed action. If you allow the action, the Provisioning Manager attempts to apply it to the CPC. If you deny the action, the CPC is not considered again for activation or deactivation for a few hours.

Until you respond, the Provisioning Manager continues to check the policy and workload to see whether the proposed action is still necessary. If the action is no longer necessary, the outstanding message is canceled. If another action is proposed instead, a new message is issued. While the Provisioning Manager is waiting for an answer, you use report commands to help you decide how to respond.

In some situations, there might be inconsistencies between the status of the Provisioning Manager and the CPC, for example, if an activation is triggered and the expected change in the activation level of the On/Off CoD record did not complete. In such situations, the Provisioning Manager issues a request message to the console asking how to resolve this situation. If the situation is resolved by any new information from the hardware, the request message is canceled.

Chapter 7. Working with reports

You can request various reports about the status of the Provisioning Manager. The content varies depending on the type of report. The following reports can be requested:

- Domain report
- Policy report
- Domain configuration report
- Workload report
- Activity report
- Trace report
- Log report

These reports can be written to the console or to a file in the file system by using Provisioning Manager commands. If the report is sent to the console, the command response message includes the type of report, date, and time in UTC, for example:

```
CPO1008I Domain report generated at 12/22/2007 08:45:01
```

If the report is written to a file, this information is included in the first line of the file, for example:

```
Domain report generated at 12/22/2007 08:45
```

In both cases, the report data follows this line. Sections described in the **Working with reports** chapter contain a description of the different reports and how to interpret the information.

Note: If the report is written to the console, the amount of information written is limited. If the data exceeds the limit, information is truncated or missing. In this case, direct the report to a file to get complete information.

The domain report

To create a domain report, issue a REPORT DOMAIN command. For the syntax of this command, see page 157. The report contains information about the current setup of the domain managed by the Provisioning Manager. The information is listed in the following order, and includes:

- The name of the provisioning domain and the time when the Provisioning Manager was started
- The active processing mode and the time it was activated. The possible values for the processing mode are:
  - MANUAL
  - ANALYSIS
  - CONFIRMATION
  - AUTONOMIC
- The active domain configuration and the time it was activated. A domain configuration name of "*none" indicates that the default domain configuration is active, because you never activated your own domain configuration. In this case, the reported time is the time when the Provisioning Manager first ran.
- The name of the active provisioning policy and the time it was activated. A policy name of "*none" indicates that the default policy is active, because you never activated your own policy. In this case, the reported time is the time when the Provisioning Manager first ran.
- Service information about the code level of the running program.

All reported times are in UTC.

Note: The activation times for the processing mode, domain configuration, and policy might have occurred in a previous run of the Provisioning Manager and might be earlier than the current start time of the Provisioning Manager.

An example of a domain report is:

```
Domain report generated at 12/22/2007 08:45
Provisioning Manager for domain DOMAIN1 started at 12/22/2007 08:40:53
Active processing mode is AUTONOMIC since 12/22/2007 08:40:54
Active domain configuration is DCSAMPLE since 12/22/2007 08:40:54
Active policy is EXAMPLE since 12/22/2007 08:40:54
Code level is 200712201
```

The policy report

To create a policy report, issue a REPORT POLICY command. For the syntax of this command, see page 159. The report contains information about the active policy and its status. Indentation is used in the report to group related items together. The reported information indicates:

- The name of the active policy, and its enabled or disabled status. A policy is disabled if the Provisioning Manager is running in MANUAL processing mode. In all other processing modes, the policy is enabled.

- The logical processor scope of the policy, if limits exist. For each limit, the system and sysplex names, the processor limits, and the defined action are displayed. An asterisk (*) signifies the limit as defined by the LPAR.

- The maximum provisioning scope of the policy. Two lines are displayed for each entry. The first line contains the CPC name and the maximum resources that can be activated by all provisioning rules. The second line denotes the primary and secondary capacity increments that are defined for the CPC.

- The provisioning rules that are contained in the policy. The information displayed about each rule includes:

  - The rule name, the current enabled or disabled status, and the default status as defined in the policy when it was activated

  - The provisioning scope for the rule. One line is displayed for each entry. It contains the CPC name and the resources that are eligible to be activated by this rule.

  - The provisioning conditions. For each provisioning condition, the following information is given:

    - The provisioning condition name, the current enabled or disabled status, and the default status as defined in the policy when it was activated.

    - The workload conditions, if any. For each workload condition, the following information is given:

      - The workload condition name and the name of the sysplex this condition is for.

      - The name of the system to which the workload condition applies.

      - The importance filters that are defined in the workload condition, if any. For each importance filter, the following information is given:

        - The importance (I), the provisioning performance index limit (PL), the provisioning performance index limit duration (PD), the deprovisioning performance index limit (DL), the deprovisioning performance index limit duration (DD), and the scope for the performance index (S).

      - The included service classes that are defined in the workload condition, if any. For each included service class, the following information is given:

        - The Workload Management (WLM) service definition name, policy name, service class name, and service class period number to be observed.

        - The provisioning performance index limit (PL), the provisioning performance index limit duration (PD), the deprovisioning performance index limit (DL), the deprovisioning performance index limit duration (DD), and the scope for the performance index (S).

        - The excluded service classes that are defined in the workload condition, if any. For each excluded service class, the following information is given:

- The Workload Management (WLM) service definition name, policy name, service class name, and service class period number not to be observed.
- The time conditions. All dates and times are reported in UTC. For nonrecurring and recurring time conditions, the information is different.
  - For nonrecurring time conditions, the following information is given:
    – The time condition name and status. The status might include:
      - Pending
      - Observing and enabled
      - Observing and disabled
      - Active and enabled
      - Active and disabled
      - Drained and enabled
      - Drained and disabled
      - Inactive

      For more information about the time condition status, see page 34. Because time conditions cannot be enabled or disabled, the status reflects the enabled or disabled status of all the elements it is contained in. A time condition is enabled if the policy, the rule, and the provisioning condition are all enabled. Otherwise it is disabled.
    – The start, deadline, and end time of the time condition.
  - For recurring time conditions, the following information is given:
    – The recurring time condition name and status. The status might include:
      - Pending
      - Observing and enabled
      - Observing and disabled
      - Active and enabled
      - Active and disabled
      - Drained and enabled
      - Drained and disabled
      - Inactive

      For more information about the time condition status, see page 34. Because time conditions cannot be enabled or disabled, the status reflects the enabled or disabled status of all the elements it is contained in. A time condition is enabled if the policy, the rule, and the provisioning condition are all enabled. Otherwise it is disabled.
    – The start date, end date, and the selected days of the week. The days of the week are marked with "X" if the day of the week is allowed and with a "-" if the day of the week is not allowed. The days are reported from Monday to Sunday.
    – The start time, deadline time, and end time of the recurring time condition.

Here is an example of a policy report:

```
Policy EXAMPLE is enabled
Logical processor scope:
 System SYS1 sysplex SYSPLEX scope is 4/7/3 Action: local message
 System SYS2 sysplex SYSPLEX scope is */*/* Action: remote message
Maximum provisioning scope:
 Limit for CPC SAMPCPC is 150 MSU, 3 zAAPs, 3 zIIPs
activation of 7/5 MSU
Rule SampleRule is enabled (default enabled)
 Provisioning scope:
  Limit for CPC SAMPCPC is 30 MSU, 0 zAAPs, 0 zIIPs
 Provisioning condition SampleCS is enabled (default enabled)
  Workload condition "SampleWLC" for sysplex "SYSPLEX"
   System name "*"
   I/PL/PD/DL/DD/S 1 1.5 10 1.2 10 System
   Included: SAMPLESD/SAMPLEP/SAMPSC.1
    PL/PD/DL/DD/S 2.0 15 1.2 7 Sysplex
   Excluded: SAMPLESD/SAMPLEP/SC2
  Time condition SampleTime is active and enabled
   s/d/e: 01/01/2010 00:00 / 12/31/2010 16:00 / 12/31/2010 20:00
  Recurring time condition Sample2 is active and enabled
   s/e/w days : 01/01/2010 / 12/31/2010 / -XXXXXX
   s/d/e times: 11:30 / 12:30 / 13:30
```

The domain configuration report

To create a domain configuration report, issue a REPORT CONFIGURATION command. For the syntax of this command, see page 156. The report contains information about the active domain configuration and the status of its elements. Indentation is used in this report to group related items. The reported information indicates:

- The name of the active domain configuration and its enabled or disabled status. A domain configuration is disabled if the Provisioning Manager is running in MANUAL processing mode. In all other processing modes, the domain configuration is enabled.
- Information about the CPCs that are defined in the domain configuration. For each CPC, such information contains:
  - The name of the CPC, its record ID, its current enabled or disabled status, and the default status that was defined in the domain configuration when it was activated.
  - Runtime information about the CPC:
    - The status of the CPC at the support element (SE) or hardware management console (HMC):

      not correlated
      The CPC is not yet detected at the support element or hardware management console. It cannot be used to activate temporary capacity.

      correlated
      The CPC is detected at the support element or hardware management console, but detailed information about it is not yet available to the Provisioning Manager. It cannot be used to activate temporary capacity.

      matched
      The CPC is detected at the support element or hardware management console, and detailed information about it is available. Temporary capacity can be activated on it if a valid record exists.

    - The CPC hardware type and model. If the CPC is not supported for capacity management, it is indicated at the end of the line. If it is supported, then detailed information about the CPC follows in separate lines:
      - The current CPC model, capacity in MSU, number of zAAPs, and number of zIIPs.
      - The permanent model and capacity in MSU.
      - If a usable record was detected:
        - If the record ID in the domain configuration is defined as '*' in the domain configuration, the record ID used by the Provisioning Manager for managing temporary capacity is displayed.
        - The remaining capacity: either the number of processors available that can still be activated as general purpose, zAAP, or zIIP, or the remaining capacity tokens followed by the number of available processors. If capacity tokens are available, they are reported in MSU days for general-purpose capacity and in processor days for zAAPs and zIIPs.

- The activation limits: the number of zAAP and zIIP processors allowed to be active for this record. If there is no activation limit in the record, a value of -1 is reported.
- The active resources: the number of resources currently active for the record. The resources are displayed in MSU, followed by the number of additional processors, the number of increases of the capacity level, the number of zAAPs, and the number of zIIPs.
  - If no usable record was detected:
    - A note that no record for capacity management is available.
  - If the record ID in the domain configuration is not defined as "*":
    - A note that the record ID is not valid.
  - If the CPC cannot be used for capacity management:
    - The reason that capacity cannot be activated or deactivated. For example, the record has expired or the configuration of the CPC does not allow commands to perform the temporary capacity change.
- If the CPC supports static power save function whether the function is enabled or disabled. In the disabled state, it is also reported when it is allowed to enable static power save mode.
- Information about the systems in the domain configuration. For each system, it contains:
  - The system name, the name of the sysplex it belongs to, its enabled or disabled status, and the default status as defined in the domain configuration when it was activated
  - The primary host address
  - The alternate host address, if defined
  - The protocol and the port
  - Information about the system at the primary host address:
    - The observation status information. This status can be:

      observed
      The Provisioning Manager retrieves information from the system at the reported host address. The system can be observed if the domain configuration is enabled and the system is enabled. If the alternate host address is not defined, the system at the primary host address is observed. If both host addresses are defined, at least one of the two systems is observed. This depends on the runtime status of the system at the other host address.

      not observed
      The Provisioning Manager does not retrieve information from the system at the reported host address. The system is not observed if the domain configuration is disabled or if the system is disabled. If the domain configuration is enabled and the system is enabled, and if both host addresses are defined, the system does not need to be observed. Whether one or more systems are observed depends on the runtime status of the system at the other host address.
- If the system is observed, the following lines contain runtime information about the system at the reported host address. The first piece of information is the connection status and the time when the connection changed into this status. The connection status can be one of the following:

not connected

> The connection to the system has not yet been established successfully. The Provisioning Manager is trying to connect to the system at the related host address.

available

> The connection to the system has been successfully established.

temporarily unavailable

> The connection to the system is no longer available. The Provisioning Manager tries to reestablish the connection.

unavailable

> The connection to the system has been broken. The Provisioning Manager tries to connect to the system again.

- If additional information about the system is available, it is reported as follows:
  - The date and time the system became available
  - The CPC where the system is running
  - The installed WLM service definition and active WLM policy
- If the Provisioning Manager does not yet have all required information about the system at the related host address, the following messages are generated:
  - A note indicating that the information is unavailable
  - A message indicating which initialization step has not yet finished or was not able to finish successfully. If the step was not able to finish successfully, a corresponding message is sent to the console the first time it occurs. This message is one of the following:

    The system is not identified

    > Either the name of the system and the name of the sysplex or the name of the system or the name of the sysplex has not yet been retrieved.

    The system is not correlated

    > The Provisioning Manager has not yet detected whether the name of the system and the name of the sysplex that the system belongs to match the names in the domain configuration. Both names are reported in the message.

    The version of this system is not available

    > The version of the operating system has not yet been retrieved.

    The CPC serial number is not available

    > The serial number of the CPC where the system is running has not yet been retrieved.

    The CPC serial number is not correlated

    > The serial number of the CPC has not yet been correlated with the name of the CPC. The serial number of the CPC is reported in the message.

    The CPC is not correlated

    > The CPC has not yet been correlated. The Provisioning Manager has not detected whether the CPC the system is running on is defined in the domain configuration.

    Insufficient information for retrieving metric values

    > The information for retrieving metric values has not yet been retrieved, or could not be retrieved.

The information about the WLM service definition is not available
> The name of the installed WLM service definition, the name of the active WLM policy, or the activation time of this policy have not yet been retrieved.

The information about WLM service class periods is not available
> The service class periods defined in the active WLM policy have not yet been retrieved.

- Even if all data can be successfully initialized, other conditions might prevent further processing. If so, the condition that is not fulfilled is reported. This condition might be:

The system is not the defined system
> Either the name of the system and the name of the sysplex or the name of the system or the name of the sysplex this system belongs to, does not match the definition of these names in the domain configuration. Both names are reported in the message.

The version of this system is not supported
> The version of the system is not supported by the Provisioning Manager.

The CPC is not part of the domain
> The CPC the system is running on is not defined in the domain configuration.

An example of a domain configuration report is:

```
Domain configuration DCSAMPLE for domain DOMAIN1 is enabled
CPC SAMPCPC with record * is enabled (default enabled)
 CPC is matched with serial 000020016F7A since 01/16/2008 16:51:06
 Hardware is of type 2097 with model E12
 Current model is 705 with 342 MSU, 2 zAAPs, and 3 zIIPs
 Permanent model is 704 with 281 MSU
 Active record ID is A0123456
 Hardware has 6 spare processors
 Activation limits are 3 zAAPs, and 1 zIIP
 Active resources GP/zAAP/zIIP 61(1/0)/0/0
System SYSTEM1 in sysplex SVPLEX is enabled (default enabled)
 Primary host address: system1.ibm.com
 Alternate host address: 9.99.99.99
 Protocol: HTTP, port: 5988
 The system at primary host address is observed
  This system is available since 04/27/2008 16:46:32
  This system is running on the CPC SAMPCPC
  WLM service definition: SAMPLESD, active policy: SAMPLEP
 The system at alternate host address is not observed
```

The workload report

To create a workload report, issue a REPORT WORKLOAD command. For the syntax of this command, see page 160. The report contains information the workload that is currently being observed. The reported information indicates:

- The number of systems for which the workload can be observed.
- For each system that is observed:
  - The name of the system, the name of the sysplex the system belongs to, and the name of the CPC the system is running on.
  - For each WLM service class period that is observed on the system:
    - The name and number of a service class period, for example, SAMPSC.1, followed by the provisioning performance index limit (PL), the provisioning performance index limit duration (PD), the deprovisioning performance index limit (DL), the deprovisioning performance index limit duration (DD), and the scope for the performance index (S).
    - The last measured performance index and the time of this measurement. A dash (-) is displayed whenever the performance index is not available at the time of measurement; for example, this situation can occur when the workload that is running in the observed service class has been displaced. To show how long the performance index has been at this level, the line also indicates the last time the performance index crossed the provisioning or deprovisioning performance index limit. Both times are shown in UTC.
    - If a detailed workload report is issued (TYPE=DETAILED), it also lists the types of temporary resources that are needed for a service class that is negatively affected, or, optionally, the reason why an additional temporary resource is not needed by a negatively affected service class.

An example of a workload report is:

```
Workload is analyzed for 1 system(s)
Workload for system SYSTEM1 of sysplex SYSPLEX on CPC SAMPCPC
 SAMPSC.1 PL/PD/DL/DD/S 1.4 10 1.2 10 Sysplex
  PI from 01/16/2008 16:55 is 1.6. Last limit crossing was 01/16/2008 16:55
   Demand for additional logical zIIPs not recognized
    Lack of spare logical zIIPs
   Demand for additional physical zAAPs not recognized
    Shared logical zAAPs not available on LPAR
   Demand for additional logical CPs recognized
   Demand for capacity level increase only recognized.
   Demand for additional physical CPs not recognized
    Amount of logical online CPs outnumbers amount of physical CPs
```

If management with moving average PI is enabled, the workload report lists the user-settings that are being used for the moving average PI calculation, such as weight and capping. The report also lists the PI as it has been reported by WLM for each observed WLM service class period, as well as the alternate moving average PI that is calculated by Capacity Provisioning.

An example of a workload report is:

```
Workload is analyzed for 1 system(s)
average PI management enabled: weight 57%, capping PI 2.79
Workload for system SYSTEM1 of sysplex SYSPLEX on CPC SAMPCPC
 SAMPSC.1 PL/PD/DL/DD/S 1.4 10 1.2 10 Sysplex
  average PI from 08/11/2009 16:55 is 1.46
   Last limit crossing was 08/11/2009 16:51
  PI from 08/11/2009 16:55 is 1.6
   Last limit crossing was 08/11/2009 16:49
```

For setting the moving average weight, see key
SystemObservation.MovingAveragePiWeight in Table 14 on page 52

For setting the moving average capping, see key
SystemObservation.MovingAveragePiCapping in Table 14 on page 52

The activity report

To create an activity report, issue a REPORT ACTIVITY command. For the syntax of this command, see page 155. The report contains information about the activation and deactivation of temporary resources that are initiated by the Provisioning Manager based on the policy and workload status.

This activity is displayed in reverse chronological order, with the latest actions displayed at the top of the list, so that when the list is truncated, only the oldest data is not displayed. Activation and deactivation are processed asynchronously by the CPC. The activity report may also show whether failures to activations and deactivations have been detected.

The reported information includes:
* A summary line that shows the time period reported and the number of activities performed by the Provisioning Manager.
* Optionally, if failures have been detected for the requested period, a summary line containing the number of failures in the report.
* Information about each of these activities includes:
  – The type of activity (activation or deactivation), the CPC affected and the time the activity took place
  – The target activation level. This includes the target model for general-purpose capacity and the numbers of temporary zAAP and zIIP processors
  – The activation level of the CPC at the time the activity was initiated, in the same format as the target activation level
  – If the activity was an activation of temporary resources, for each workload that triggered the activation:
    - The policy element that triggered the activation: the policy name, the provisioning rule, the provisioning condition, and the time condition
    - The system that was negatively affected and the sysplex it belongs to
    - The service class period that was negatively affected: the active WLM service definition and policy name and the service class name and period number.
* Information about command failures that have been asynchronously reported. Such information includes the time when the failure was detected, the name of the affected CPC, and the code of the cause of failure reported by the hardware.

An example of an activity report is:

```
Number of activities between 11/14/2007 and 01/16/2008 was 2
Deactivation for CPC SAMPCPC at 01/16/2008 21:26:29
Deactivation to model 505, 0 zAAPs, 0 zIIPs
Active resources before deactivation: model 506, 0 zAAPs, 0 zIIPs
Activation for CPC SAMPCPC at 01/16/2008 17:26:25
Activation of model 506, 0 zAAPs and 0 zIIPs
Active resources before activation: model 505, 0 zAAPs, 0 zIIPs
Inducing policy element is policy EXAMPLE, rule SampleRule,
provisioning condition SampleCS, time condition SampleTime
Inducing system is SYSTEM1 in sysplex SYSPLEX
Inducing workload is WLM service definition SAMPLESD,
policy SAMPLEP, service class period SAMPSC.1
```

The trace report

To create a trace report, issue a REPORT TRACE command. For the syntax of this command, see page 160. The report contains information about the current trace level settings and trace file settings:

- A header "Trace level settings" that includes:
  - The value for the default level
  - The values for each individual trace component
- A header "Trace file settings" that includes:
  - The prefix of the trace file name. The full file name is constructed from this by adding a dot (.) and the sequence number of the trace, starting from zero. For example, the first trace file might be /tmp/cpotrace_20080127134147469.log.0.
  - The maximum file size and number of trace files. When the file size limit is reached, a new file is started. When the maximum number is reached, the sequence number begins again at zero and the old files are reused and overwritten.

An example of a trace report is:

```
Trace level settings
 Default level is set to INFO
 Level for component BASE is set to default
 Level for component UTIL is set to default
 Level for component POLICY is set to ALL
 Level for component CONFIGURATION is set to ALL
 Level for component ANALYZER is set to default
 Level for component PLANNER is set to default
 Level for component CONSOLESERVER is set to default
 Level for component CIMOBSERVER is set to default
 Level for component CIMCLIENT is set to OFF
 Level for component HMCCLIENT is set to OFF
Trace file settings
 Trace is written to /tmp/cpotrace_20080127134147469.log
 Limit=100000000, count=1
```

The log report

To create a log report, issue a REPORT LOG command. For the syntax of this command, see page 158. The report contains information about the current log and log file settings, including:

- A header line that shows the configured destination for log files
- A line for each log that states if data writing is active for this log

An example of a log report is:

```
Default destination is /tmp
Writing for log NotificationLog is inactive
Writing for log ErrorLog is active
Writing for log AnalyzerLog is inactive
Writing for log SystemObservationLog is inactive
```

Managing reports

The Provisioning Manager reports only the status information that is currently in memory, and does not keep a history. If you require a history,you must create it yourself by regularly requesting the reports you are interested in. Specify a unique file name for each report, because the Provisioning Manager overwrites the content of a file if it already exists.

Chapter 8. Considerations for defining policies and domains

You should consider several points when you are setting parameters in a Capacity Provisioning policy or domain configuration.

Choosing service class periods

z/OS Capacity Provisioning uses the performance index (PI) of service class periods as the primary trigger for provisioning and deprovisioning actions. For example, the Capacity Provisioning Manager considers a provisioning action only if the actual PI of any included service class period is worse than the defined PI. You must select appropriate service class periods for which the performance index is correlated to the performance of your business application.

For example, an important business application can consist of multiple service classes that are defined with importance 2 and 3 in the WLM service definition. Somewhat simplified, the goal attainment of those service classes primarily depends on other work that is classified as importance 1, SYSSTC or SYSTEM. When system resources such as processing capacity become constrained, WLM attempts to help the most important work first and assign fewer resources to other work. In this example, resources are taken from the service class periods with an importance of 3 first, and they in turn show a higher (worse) PI.

It is best practice in WLM not to activate too many service class periods at any point in time. There must be a substantial service measurement in any period so that WLM has sufficient sample data. Having sufficient amounts of sample data is especially important for service class periods that are defined with average response times or response time with percentile goals. The same objective applies to Capacity Provisioning. The number of transaction endings should be high enough to allow RMF to compute a performance index. At least one transaction ending is required for each RMF MINTIME, and preferably more.

You can specify service class periods with importance levels of 1 - 5 only. SYSTEM, SYSSTC, SYSSTC1 to SYSSTC5 and DISCRETIONARY work cannot trigger a provisioning action and is ignored, if included. Do not include any service classes that are associated with a maximum capacity for a resource group. If a service class is capped, Capacity Provisioning avoids provisioning on behalf of it, if possible.

135

Choosing provisioning criteria

The PI limits that you specify in your provisioning criteria depend on what you would consider tolerable when capacity is constrained. If you define the goal for the service class period so that the goal can still be achieved in times of peak demand, and additional capacity does not need to be active, the provisioning PI could be set just above 1. In other cases, with more aggressive goals in effect, a provisioning PI would need to be higher.

The provisioning duration determines how fast the Provisioning Manager activates additional capacity when the PI of that service class period is consistently above the limit. The duration must be viewed relative to RMF MINTIME, the default of which is 100 seconds. In general, the duration is to be greater than 3 minutes, to prevent a short-term disturbance from triggering a provisioning action. It can also take some time for WLM to resolve a PI problem by reassigning resources.

The specified duration is not a guaranteed reaction time. Certain events cause the Provisioning Manager to block some time to allow WLM to readjust. Events that can trigger a block include, for example, the activation of a new WLM service definition or policy, or a capacity change in the observed CPC.

Part 3. Reference

Provides an overview of Provisioning Manager commands.

Chapter 9. Provisioning Manager command reference

Describes the Provisioning Manager commands and their syntax. For information about how to pass commands to the Provisioning Manager, see page 118.

Introduction

The Provisioning Manager command syntax is based on the z/OS command syntax shown in the following diagram:

```
>>--action--object--+----------------------------+------><
                    |  <-------------------------+ |
                    |                        (1)   |
                    +--+--------+--parameter------+
                       +--,-----+
```
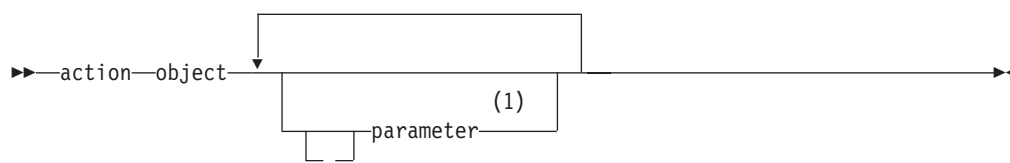
Notes:

1   Parameters can be required, optional or nonexistent, depending on the specific action and object.

For information about these diagrams, see "How to read syntax diagrams" on page x.

Commas are optional, and any number of blanks are allowed to separate action, object, and parameters. A comment is allowed at any place where a blank is allowed. Comments have the following form:

```
/* comment */
```

Parameters have the following form:

```
>>--parameter_name=value------------------------------------><
```

You can specify the parameters in any order. A value can be any sequence of characters. If special characters are needed, such as spaces or commas, the parameter value must be enclosed in quotation marks (*'value'*). Within these quotation marks, any character is allowed. To specify an apostrophe (') within the parameter value, enclose it in quotation marks. For example, "parm1='*It''s mine*'" assigns the value "*It's mine*" to the parm1 parameter. Actions, objects, and parameter names are not case-sensitive. Values can be case-sensitive if they are not keywords. In this case the value must be enclosed in quotation marks.

The commands fall into three types:

- Control commands, which alter the operation of the Provisioning Manager
- Status commands, which report the current situation
- Debug commands, which can be used to give diagnostic information to IBM service personnel

The supported commands, such as actions and objects, are listed in the tables together with a short form of the command and the page on which each command is described. The short forms can be used to save typing; note that the short forms are not abbreviations.

    139

Table 15. Control commands

Command	Short form	Page
ACTIVATE RESOURCE	a r	143
DEACTIVATE RESOURCE	i r	145
DISABLE CONFIGURATION	d c	146
DISABLE POLICY	d p	147
DISABLE POWERSAVE	d ps	148
ENABLE CONFIGURATION	e c	150
ENABLE POLICY	e p	151
ENABLE POWERSAVE	e ps	152
RESET CONFIGURATION	t c	162
RESET POLICY	t p	162
SET DOMAIN	s d	164
STOP MANAGER	p m	168

Table 16. Status commands

Command	Short form	Page
LIST CONFIGURATION	l c	153
LIST POLICY	l p	154
REPORT ACTIVITY	r a	155
REPORT CONFIGURATION	r c	156
REPORT DOMAIN	r d	157
REPORT LOG	r l	158
REPORT POLICY	r p	159
REPORT TRACE	r t	160
REPORT WORKLOAD	r w	160

Table 17. Debug commands

Command	Short form	Page
ACTIVATE LOG	a l	141
DEACTIVATE LOG	i l	144
DUMP MANAGER	none	149
SET TRACE	s t	166
RESET TRACE	t t	163
WRITE LOG	w l	169

ACTIVATE LOG

Use the ACTIVATE LOG command to start recording log data to a file. Log data is always collected in memory. If the log is activated, whenever the log buffer is full, the buffer is written to a file. The default location for this file is the /tmp directory. This location can be overridden as described in "Planning the domain set-up" on page 44. You must ensure that there is sufficient space in the active location.

The data is written until the log is deactivated or the Provisioning Manager terminates. See "DEACTIVATE LOG" on page 144. When the Provisioning Manager is started for the first time, all logs are in their default state. The default state for the error log is activated. For all other logs, it is deactivated.

Note: This command is to be used only if instructed to do so by IBM service personnel.
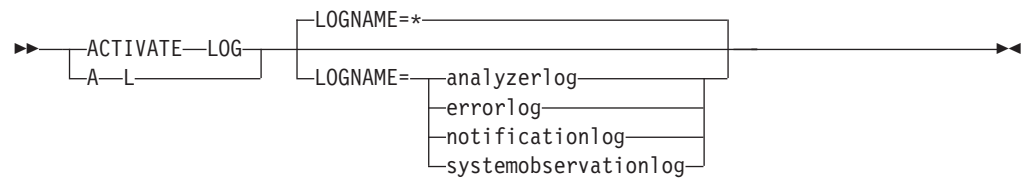
Syntax

```
                              ┌─LOGNAME=*────────────────────────┐
►►──┬─ACTIVATE──LOG─┬──────┼──────────────────────────────────┼────────►◄
    └─A──L──────────┘      └─LOGNAME=──┬─analyzerlog──────────┬┘
                                       ├─errorlog─────────────┤
                                       ├─notificationlog──────┤
                                       └─systemobservationlog─┘
```

Parameters

The command has the following parameter:

LOGNAME=_name_
> The type of data to be recorded:
>
> **analyzerlog**
>> Workload analysis results
>
> **errorlog**
>> Unexpected errors detected during processing
>
> **notificationlog**
>> Communications with the Provisioning Manager
>
> **systemobservationlog**
>> Monitored metrics from the observed systems
>
> You can also specify LOGNAME=* to indicate that writing is activated for all logs. It is the default if you omit the LOGNAME parameter; _name_ is not case-sensitive.

Example

To record communications with the Provisioning Manager, issue the following command:

```
MODIFY CPOSERV,APPL=ACTIVATE LOG LOGNAME=NotificationLog
```

or:

```
F CPOSERV,APPL=A L LOGNAME=NotificationLog
```

The response on the console is:

```
CPO1031I Logging successfully activated for log NotificationLog
```

ACTIVATE RESOURCE

Use the ACTIVATE RESOURCE command to manually activate temporary resources of a CPC in the provisioning domain. The temporary resources can be activated only for the On/Off CoD record that is identified in the domain configuration.

Note: The number that is supplied as a parameter is the total number of resources that you want to have active, not the number of resources that you want to add to the already active resources.

Before performing the activation, the Provisioning Manager checks that the specified resource level is an activation, that is it has more capacity, and that the target record allows the requested change. The resources are not managed by the Provisioning Manager and they are not deactivated automatically.

Syntax
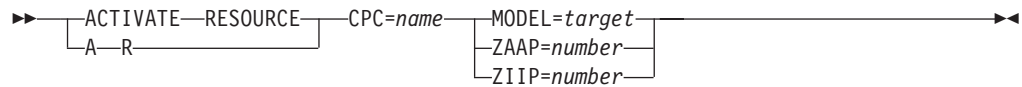
```
►►──┬─ACTIVATE──RESOURCE─┬──CPC=name──┬─MODEL=target──┬──────────────────►◄
    └─A──R───────────────┘            ├─ZAAP=number───┤
                                      └─ZIIP=number───┘
```

Parameters

The command has the following parameters:

CPC=_name_
: The name of the CPC on which you want to activate the temporary resources. A CPC with this name must be part of the active domain configuration. The CPC must be at the supported hardware level, there must be an On/Off CoD record on the CPC that is managed by the Provisioning Manager, and this record must allow for the requested activation level.

MODEL=_target_
: The model capacity identifier that you want to make active on the CPC. The target model must have more general-purpose capacity measured in MSU than the current model. The On/Off CoD record managed by the Provisioning Manager must also allow for the capacity that is defined by the requested model.

ZAAP=_number_
: The number of temporary zAAP processors that you want to have active. The target number must be higher than the number of active zAAP processors, and is limited by the number of spare processors on the machine, the maximum number of zAAP processors allowed by the On/Off CoD record, and the remaining capacity for zAAP processors of this record.

ZIIP=_number_
: The number of temporary zIIP processors that you want to have active. The target number must be higher than the number of active zIIP processors, and is limited by the number of spare processors on the machine, the maximum number of zIIP processors allowed by the On/Off CoD record, and the remaining capacity for zIIP processors of this record.

Example

To activate one zAAP for CPC G14, issue the following command:

```
MODIFY CPOSERV,APPL=ACTIVATE RESOURCE CPC=G14 ZAAP=1
```

or:

```
F CPOSERV,APPL=A R CPC=G14 ZAAP=1
```

The response on the console is:

```
CPO1026I Activation level change to 1 zAAPs successfully initiated for CPC G14
```

DEACTIVATE LOG

Use the DEACTIVATE LOG command to stop recording log data to a file. Even though the data is no longer recorded in a file, it continues to be collected in memory. If the log was active, the current log buffer is written to the file. The default location for this file is the /tmp directory. This location can be overridden as described in "Planning the domain set-up" on page 44.

Note: This command should be used only if instructed to do so by IBM service personnel.

Syntax

```
                        ┌─LOGNAME=*──────────────────────┐
►►──┬─DEACTIVATE─LOG─┬──┼────────────────────────────────┼──►◄
    └─I─L────────────┘  └─LOGNAME=─┬─analyzerlog────────┬─┘
                                   ├─errorlog───────────┤
                                   ├─notificationlog────┤
                                   └─systemobservationlog┘
```
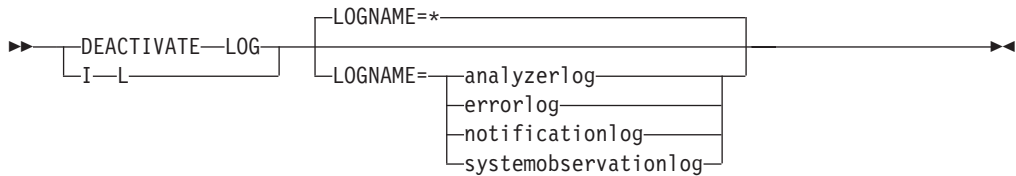
Parameters

The command has the following parameter:

LOGNAME=_name_
> The type of data to stop recording:

> **analyzerlog**
>> Contains workload analysis results

> **errorlog**
>> Contains unexpected errors that are detected during processing

> **notificationlog**
>> Contains communications with the Provisioning Manager

> **systemobservationlog**
>> Contains monitored metrics from the observed systems

> You can also specify LOGNAME=* to indicate that writing be deactivated for all logs. If you omit the LOGNAME parameter, the default is that writing is deactivated for all logs. _Name_ is not case-sensitive.

Example

To stop recording monitored metrics for the observed systems, issue the following command:

```
MODIFY CPOSERV,APPL=DEACTIVATE LOG LOGNAME=NotificationLog
```

or:

```
F CPOSERV,APPL=I L LOGNAME=NotificationLog
```

The response on the console is:

```
CPO1031I Logging successfully deactivated for log NotificationLog
CPO2030I Log information written to file
                  /tmp/cpoNotificationLog_20071024131732469.log
```

DEACTIVATE RESOURCE

Use the DEACTIVATE RESOURCE commandto manually deactivate temporary resources of a CPC in the provisioning domain. The temporary resources can be deactivated only for the On/Off CoD record identified in the domain configuration.

Use this command to deactivate resources that you activated manually, for example, by using the `activate resource` command; see page 143).

Note: The number that is supplied as a parameter represents the total number of resources that you want to keep active, not the number of resources that you want to remove from resources that are already active.

Before deactivating, the Provisioning Manager checks that the specified resource level is below the currently active resources within the managed record.

Syntax
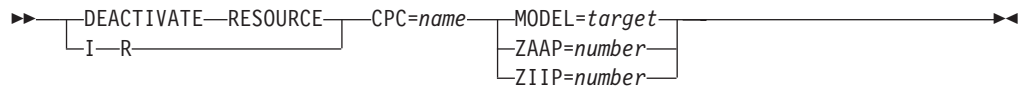
```
►►──┬─DEACTIVATE─RESOURCE─┬──CPC=name──┬─MODEL=target──┬──────────────────────►◄
    └─I─R─────────────────┘            ├─ZAAP=number───┤
                                       └─ZIIP=number───┘
```

Parameters

The command has the following parameters:

CPC=_name_
: The name of the CPC on which you want to deactivate the temporary resources. A CPC with this name must be part of the active domain configuration. The CPC must be at the supported hardware level and there must be an On/Off CoD record on the CPC that is managed by the Provisioning Manager.

MODEL=_target_
: The model capacity identifier that you want to keep active on the CPC. The target model must have less general-purpose capacity in terms of MSU than the current model. The On/Off CoD record managed by the Provisioning Manager must also allow for the requested model.

ZAAP=_number_
: The number of temporary zAAP processors that you want to have active. The target number must be less than the current number of active zAAP processors for this record.

ZIIP=_number_

The number of temporary zIIP processors that you want to have active. The target number must be less than the current number of active zIIP processors for this record.

Example

To deactivate all zAAPs for CPC G14, issue the following command:

```
MODIFY CPOSERV,APPL=DEACTIVATE RESOURCE CPC=G14 ZAAP=0
```

or:

```
F CPOSERV,APPL=I R CPC=G14 ZAAP=0
```

The response on the console is:

```
CPO1028I Activation level change to 0 zAAPs successfully initiated for CPC G14
```

DISABLE CONFIGURATION

Use the DISABLE CONFIGURATION command to disable a CPC or a system within the active domain configuration. If a system is disabled, the Provisioning Manager no longer observes the system. If a CPC is disabled, the Provisioning Manager no longer considers it for activation and deactivation of temporary resources.

If the command completes successfully, the selected CPC or system is listed as disabled in the domain configuration report.

Syntax

```
►►──┬─DISABLE──CONFIGURATION─┬──┬─CPC=name──────────────┬──────────────►◄
    └─D──C─────────────────┘  └─PLEX=name──SYS=name─┘
```

Parameters

The command has the following parameters:

CPC=_name_

Specifies the name of the CPC that you want to disable. A CPC with this name must be part of the active domain configuration.

PLEX=_name_

Specifies the name of the sysplex that includes the system that you want to disable. A sysplex with this name must be in the active domain configuration.

SYS=_name_

Specifies the name of the system that you want to disable. A system with this name must exist in the specified sysplex within the active domain configuration.

Example

To disable CPC G14, issue the following command:

```
MODIFY CPOSERV,APPL=DISABLE CONFIGURATION CPC=G14
```

or:

```
F CPOSERV,APPL=D C CPC=G14
```

The response on the console is:

```
CPO1012I CPC G14 in current configuration successfully disabled
```

DISABLE POLICY

Use the DISABLE POLICY command to disable an entire provisioning rule or a specific provisioning condition within a provisioning rule in the active provisioning policy. If resources are already activated because of affected time conditions, these resources are deactivated.

If the command completes successfully, the selected rule or provisioning condition is listed as disabled in the policy report.

Syntax

```
►►──┬─DISABLE──POLICY─┬──R=rule_name─────────────────────────────────────►◄
    └─D──P───────────┘            └─PC=name─┘
```

Parameters

The command has the following parameters:

R=_rule_name_
> The name of the rule that you want to disable. A rule with this name must exist in the active policy. If the name contains lowercase characters, your console might require that the name be enclosed in quotation marks.

PC=_name_
> The name of the provisioning condition that you want to disable. A provisioning condition with the specified name must be part of the _rule_name_ specified. If the name contains lowercase characters, your console might require that the name be enclosed in quotation marks.

Example

To disable rule CP160106R, issue the following command:

```
MODIFY CPOSERV,APPL=DISABLE POLICY R=CP160106R
```

or:

```
F CPOSERV,APPL=D P R=CP160106R
```

The response on the console is:

```
CPO1003I Rule CP160106R successfully disabled
```

DISABLE POWERSAVE

Use the DISABLE POWERSAVE command to initiate the transition of a CPC out of static power save mode. Only zEnterprise Systems and later support static power save mode. Disabling static power save resumes nominal capacity of the CPC model. The Provisioning Manager considers the CPC for activation of additional temporary capacity.

Transition into or out of power save mode takes some time. A subsequent Provisioning Manager message informs you when the operation is complete.

Syntax

```
►►──┬─DISABLE──POWERSAVE─┬──CPC=name────────────────────────────────────────►◄
    └─D──PS──────────────┘
```

Parameters

The command has the following parameters:

CPC=*name*
> This parameter specifies the name of the CPC on which you want to disable static power save. A CPC with this name must be part of the active domain configuration.

Example

To disable the static power save function for CPC G14, issue the following command:

```
MODIFY CPOSERV,APPL=DISABLE POWERSAVE CPC=G14
```

or:

```
F CPOSERV,APPL=D PS CPC=G14
```

The response on the console is:

```
CPO1093I Static power save mode for CPC G14 successfully disabled
```

DUMP MANAGER

Use the DUMP MANAGER command to request dumps from the Provisioning Manager. Different types of dumps can be requested:

- Heap dumps
- Java dumps
- Java system dumps

The dumps are created in the home directory of the Provisioning Manager user.

Note: This command is to be used only if instructed to do so by IBM service personnel.

Syntax

```
►►──DUMP──MANAGER────TYPE=──┬─HEAP────┬──────────────────────────────────────►◄
                           ├─JAVA────┤
                           └─SYSTEM──┘
```

Parameters

The command has the following parameter:

TYPE=_type_
    Specifies the type of dump. The following types are supported:

    HEAP   Requests a Java heap dump

    JAVA   Requests a Java dump

    SYSTEM
          Requests a Java system dump

    The type values are not case-sensitive.

Example

To perform a snap dump, issue the following command:
```
MODIFY CPOSERV,APPL=DUMP MANAGER TYPE=HEAP
```

The response on the console is:
```
CPO1088I Dump manager command for dump type HEAP successfully performed
```

ENABLE CONFIGURATION

Use the ENABLE CONFIGURATION command to enable a CPC or a system within the active domain configuration.If a system is enabled, the Provisioning Manager starts to observe it and resources are activated based on the workload situation of this system. If a CPC is enabled, the Provisioning Manager considers it for activation and deactivation of temporary resources.

If the command is successful, the selected CPC or system is listed as enabled in the domain configuration report.

Syntax

```
►►──┬─ENABLE─CONFIGURATION─┬──┬─CPC=name──────────────┬───────────────────────►◄
    └─E─C──────────────────┘  └─PLEX=name─SYS=name─────┘
```

Parameters

The command has the following parameters:

CPC=_name_
> Specifies the name of the CPC that you want to enable. A CPC with this name must be part of the active domain configuration.

PLEX=_name_
> Specifies the name of the sysplex which includes the system which you want to enable. A sysplex with this name must be in the active domain configuration.

SYS=_name_
> Specifies the name of the system that you want to enable. A system with this name must exist in the specified sysplex in the active domain configuration.

Example

To enable CPC G14, issue the following command:

```
MODIFY CPOSERV,APPL=ENABLE CONFIGURATION CPC=G14
```

or:

```
F CPOSERV,APPL=E C CPC=G14
```

The response on the console is:

```
CPO1011I CPC G14 in current configuration successfully enabled
```

ENABLE POLICY

Use the ENABLE POLICY command to enable an entire provisioning rule or a specific provisioning condition within a provisioning rule in the active provisioning policy. If time conditions are enabled by this command, temporary resources can be activated.

If the command is successful, the selected rule or provisioning condition is listed as enabled in the policy report.
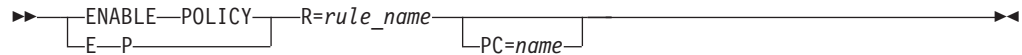
Syntax

```
►►─┬─ENABLE──POLICY─┬──┬─R=rule_name──────────────┬──────────────────────►◄
   └─E──────P───────┘               └─PC=name─┘
```

Parameters

The command has the following parameters:

R=_rule_name_
> The name of the rule that you want to enable. A rule with this name must exist in the active policy. If the name contains lowercase characters, then your console might require that the name be enclosed in quotation marks.

PC=_name_
> The name of the provisioning condition that you want to enable. A provisioning condition with the specified name must be part of the _rule_name_ specified. If the name contains lowercase characters, then your console might require that the name be enclosed in quotation marks.

Example

To enable rule CP160106R, issue the following command:

```
MODIFY CPOSERV,APPL=ENABLE POLICY R=CP160106R
```

or:

```
F CPOSERV,APPL=E P R=CP160106R
```

The response on the console is:

```
CPO1001I Rule CP160106R successfully enabled
```

ENABLE POWERSAVE

Use the ENABLE POWERSAVE command to initiate the transition of a CPC into static power save mode. Only zEnterprise and later support static power save mode. Because static power save mode reduces the total capacity of a CPC, the Provisioning Manager no longer considers the CPC for activation of additional temporary capacity.

The CPC must be configured to allow for a certain command in order for it to complete successfully. For more information about how to set up a CPC for static power save mode, see the appropriate hardware documentation.

Transition into or out of power save mode takes some time. A Provisioning Manager message informs when the operation is complete.

Syntax

```
►►──┬─ENABLE──POWERSAVE─┬──CPC=name───────────────────────────────────────►◄
    └─E──PS─────────────┘
```

Parameters

The command has the following parameters:

CPC=_name_
    Specifies the name of the CPC for which you want to enable static power save. A CPC of this name must be part of the active domain configuration.

Example

To enable static power save function for CPC G14, issue the following command:

```
MODIFY CPOSERV,APPL=ENABLE POWERSAVE CPC=G14
```

or:

```
F CPOSERV,APPL=E PS CPC=G14
```

The response on the console is:

```
CPO1092I Static power save mode for CPC G14 successfully enabled
```

LIST CONFIGURATION

Use the LIST CONFIGURATION command to list the entries in the domain configuration repository for the domain.

Syntax

```
►►──┬─LIST──CONFIGURATION─┬──────────────────────────────────────────────────────►◄
    └─L──C────────────────┘
```

Parameters

None.

Example

To list the domain configuration, issue the following command:

```
MODIFY CPOSERV,APPL=LIST CONFIGURATION
```

or:

```
F CPOSERV,APPL=L C
```

The response on the console might be:

```
CPO1049I Domain configuration list generated at 01/17/2006 02:14:08
  DS
```

LIST POLICY

Use the LIST POLICY command to list the entries in the policy repository of the
domain.

Syntax

```
►►──┬─LIST──POLICY─┬──────────────────────────────────────────────►◄
    └─L──P─────────┘
```

Parameters

None.

Example

To list the available policies, issue the following command:

```
MODIFY CPOSERV,APPL=LIST POLICY
```

or:

```
F CPOSERV,APPL=L P
```

The response on the console might be:

```
CPO1048I Policy list generated at 01/17/2006 02:38:39
  BERLINP
```

REPORT ACTIVITY

Use the REPORT ACTIVITY command to display the activation and deactivation operations that have been performed by the Provisioning Manager. Information about activations and deactivations is retained for approximately two months. You can select the time period to be reported.

For information about what is contained in the report, see page 132.

Note: Manual activations and deactivations are not recorded by the Provisioning Manager in the activity log.

Syntax
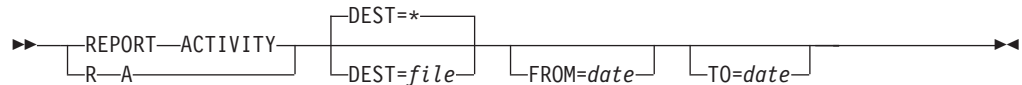
```
>>─┬─REPORT──ACTIVITY─┬──┬───────────┬──┬─────────────┬──┬───────────┬──><
   └─R──A─────────────┘  │ ┌─DEST=*─┐ │  └─FROM=date─┘  └─TO=date─┘
                         └─┴─DEST=file─┘
```

Parameters

The command has the following parameters:

DEST

Specifies the destination of the activity report. The following destinations are supported:

*   (Default) specifies that the report should be written to the console that is issuing the command.

file   Specifies a file where the information is to be stored. If the name includes lowercase characters, this parameter must be enclosed in single quotation marks ('). The file must be in the hierarchical file system. You can specify either an absolute path or a relative path to the file. If this is not absolute, the path is relative to the home directory of the user who is running the Provisioning Manager. You must ensure that there is sufficient space in the selected location. The Provisioning Manager user must be authorized to write to this location.

FROM=*date*

Specifies the start date of the report. All activations and deactivations executed from the beginning of that day are reported. If the parameter is omitted, the start date of the log is used. The start date of the report must be before the end date of the report specified in the TO parameter.

The format for the start date is mm/dd/yyyy, where mm is the month, dd is the day, and yyyy is the year. For example April, 20th, 2006 is 4/20/2006.

TO=*date*

Specifies the end date of the report. All activations and deactivations executed before the end of that day are reported. If the end date is omitted, the current date is used. The end date of the report must be after the start date of the report specified in the FROM parameter.

The format for the end date is the same as the one for the start date.

REPORT CONFIGURATION

Use the REPORT CONFIGURATION command to display the active domain configuration.

For information about what is contained in the report, see page 126.

Syntax
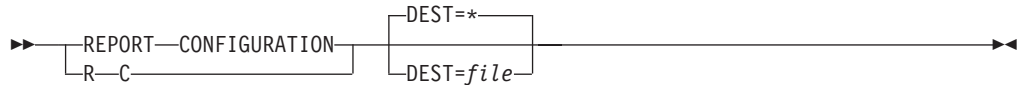
```
                              ┌─DEST=*────────┐
►►──┬─REPORT──CONFIGURATION─┬─┤               ├──────────────────►◄
    └─R──C──────────────────┘ └─DEST=file─────┘
```

Parameters

The command has the following parameter:

DEST

Specifies the destination of the domain configuration report. The following destinations are supported:

* (Default) specifies that the report should be written to the console that is issuing the command.

file Specifies a file where the information is to be stored. If the name includes lowercase characters, this parameter must be enclosed in single quotation marks ('). The file must be in the hierarchical file system. You can specify either an absolute path or a relative path to the file. If this is not absolute, the path is relative to the home directory of the user who is running the Provisioning Manager. You must ensure that there is sufficient space in the selected location. The Provisioning Manager user must be authorized to write to this location.

REPORT DOMAIN

Use the REPORT DOMAIN command to display the status of the current domain.

For information about what is contained in the report, see page 122.

Syntax
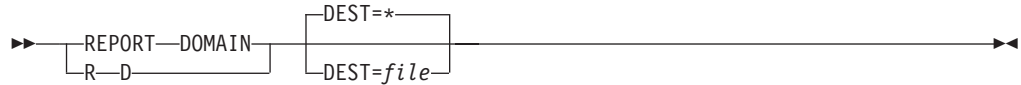
```
                        ┌─DEST=*──────┐
►►──┬─REPORT──DOMAIN─┬──┼─────────────┼────────────────────────────────────►◄
    └─R──D───────────┘  └─DEST=file───┘
```

Parameters

The command has the following parameter:

DEST

(Default) specifies the destination of the domain report. The following destinations are supported:

* (Default) specifies that the report should be written to the console that is issuing the command.

file Specifies a file where the information is to be stored. If the name includes lowercase characters, this parameter must be enclosed in single quotation marks ('). The file must be in the hierarchical file system. You can specify either an absolute path or a relative path to the file. If this is not absolute, the path is relative to the home directory of the user who is running the Provisioning Manager. You must ensure that there is sufficient space in the selected location. The Provisioning Manager user must be authorized to write to this location.

REPORT LOG

Use the REPORT LOG command to display the status of the current log write settings.

For information about what is contained in the report, see page 133.

Syntax

```
>>──┬─REPORT──LOG─┬──┬──────────DEST=*─────────┬──────────────────────><
    └─R──L────────┘  └─DEST=file─┘
```

Parameters

The command has the following parameter:

DEST

(Default) specifies the destination of the log report. The following destinations are supported:

*   (Default) specifies that the report should be written to the console issuing the command.

file   Specifies a file where the information is to be stored. If the name includes lowercase characters, this parameter must be enclosed in single quotation marks ('). The file must be in the hierarchical file system. You can specify either an absolute path or a relative path to the file. If this is not absolute, the path is relative to the home directory of the user that is running the Provisioning Manager. You must ensure that there is sufficient space in the selected location. The Provisioning Manager user must be authorized to write to this location.

REPORT POLICY

Use the REPORT POLICY command to display the active provisioning policy.

For information about what is contained in the report, see page 123.

Syntax
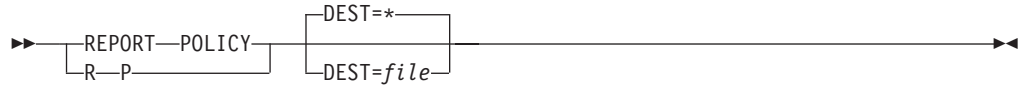
```
                      ┌─DEST=*─────┐
►►──┬─REPORT─POLICY─┬─┼────────────┼──────────────────────────────────►◄
    └─R───P─────────┘ └─DEST=file──┘
```

Parameters

The command has the following parameter:

DEST

Specifies the destination of the policy report. The following destinations are
supported:

*   (Default) specifies that the report should be written to the console
         issuing the command.

file   Specifies a file where the information is to be stored. If the name
         includes lowercase characters, this parameter must be enclosed in
         single quotation marks ('). The file must be in the hierarchical file
         system. You can specify either an absolute, path or a relative path to
         the file. If this is not absolute the path is relative to the home directory
         of the user who is running the Provisioning Manager. You must ensure
         that there is sufficient space in the selected location. The Provisioning
         Manager user must be authorized to write to this location.

REPORT TRACE

Use the REPORT TRACE command to display the active trace configuration.

For information about what is contained in the report, see page 133.
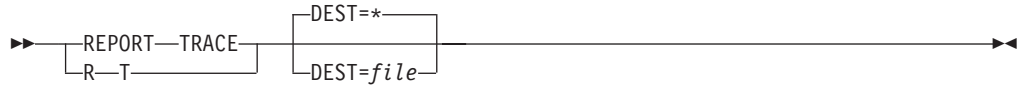
Syntax

```
>>--+--REPORT--TRACE--+--+----------------+----------------------------><
     +--R-----T--------+  +--DEST=*---------+
                          +--DEST=file------+
```

Parameters

The command has the following parameter:

DEST

Specifies the destination of the trace report. The following destinations are supported:

*   (Default) specifies that the report should be written to the console issuing the command.

file   Specifies a file where the information is to be stored. If the name includes lowercase characters, this parameter must be enclosed in single quotation marks ('). The file must be in the hierarchical file system. You can specify either an absolute, path or a relative path to the file. If this is not absolute the path is relative to the home directory of the user that is running the Provisioning Manager. You must ensure that there is sufficient space in the selected location. The Provisioning Manager user must be authorized to write to this location.

REPORT WORKLOAD

Use the REPORT WORKLOAD command to display the WLM service class periods that are currently being monitored on the observed systems.

For information about what is contained in the reporta, see page 130.

Syntax
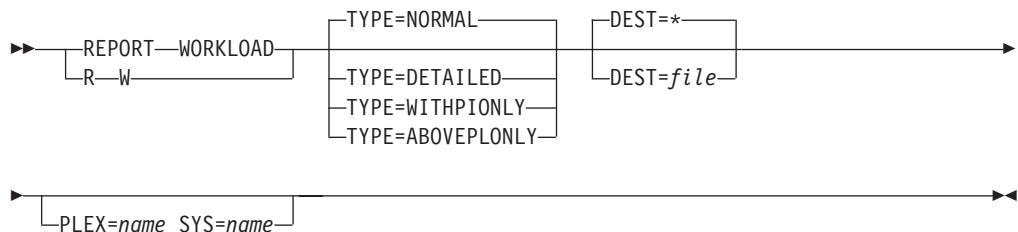
```
>>--+--REPORT--WORKLOAD--+--+--TYPE=NORMAL--------+--+--DEST=*-------+-->
     +--R-----W-----------+  +--TYPE=DETAILED------+  +--DEST=file----+
                            +--TYPE=WITHPIONLY----+
                            +--TYPE=ABOVEPLONLY---+

>--+-------------------------+-------------------------------------------><
   +--PLEX=name SYS=name------+
```

Parameters

The command has the following parameters:

DEST

   Specifies the destination of the workload report. The following destinations are supported:

   *   (Default) specifies the report should be written to the console issuing the command.

   file   Specifies a file where the information is to be stored. If the name includes lowercase characters this parameter must be enclosed in single quotation marks ('). The file must be in the hierarchical file system. You can specify either an absolute, path or a relative path to the file. If this is not absolute the path is relative to the home directory of the user who is running the Provisioning Manager. Make sure that there is sufficient space in the selected location. The Provisioning Manager user must be authorized to write to this location.

TYPE=type

   Specifies the type of report to display. The following types are supported:

   NORMAL
      Displays a short workload report

   DETAILED
      Displays a workload report that includes detailed information about WLM service class periods that are negatively affected. For each service class period, the report lists which type of temporary resource is needed, or why an additional temporary resource is not needed.

   WITHPIONLY
      Displays a detailed workload report that lists workloads with a recent PI measurement only.

   ABOVEPLONLY
      Displays a detailed workload report that lists only workloads with a PI that is above the corresponding provisioning limit (PL), as specified in the provisioning policy.

PLEX=name

   Specifies the name of the sysplex that includes the system whose workload you want to list exclusively. A sysplex with this name must be in the active domain configuration.

SYS=name

   Specifies the name of the system whose workload you want to list exclusively. A system with this name must exist in the specified sysplex in the active domain configuration. It must also be one of the currently observed systems.

RESET CONFIGURATION

Use the RESET CONFIGURATION command to undo all configuration changes that have been issued since the domain configuration was activated.

Syntax

```
►►──┬─RESET──CONFIGURATION─┬──────────────────────────────────────────►◄
    └─T──C────────────────┘
```

Parameters

None.

Example

To reset the configuration, issue the following command:

```
MODIFY CPOSERV,APPL=RESET CONFIGURATION
```

or:

```
F CPOSERV,APPL=T C
```

The response on the console might be:

```
CPO1019I Current configuration successfully reset
```

RESET POLICY

Use the RESET POLICY command to reset all elements in the active provisioning policy to their default states as defined in the policy at the time of activation.

Syntax

```
►►──┬─RESET──POLICY─┬──────────────────────────────────────────────────►◄
    └─T──P─────────┘
```

Parameters

None.

Example

To reset the current policy, issue the following command:

```
MODIFY CPOSERV,APPL=RESET POLICY
```

or:

```
F CPOSERV,APPL=T P
```

The response on the console might be:
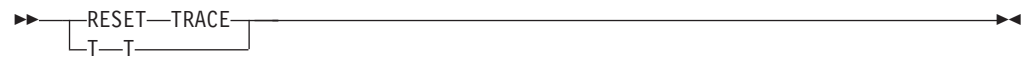
```
CPO1018I Current policy successfully reset
```

RESET TRACE

Use the RESET TRACE command to reset the tracing parameters of the Provisioning Manager. The default trace level and the trace level for all trace components are reset to the defaults delivered with the product.

Note: This command is to be used only if instructed to do so by IBM service personnel.

Syntax

```
►►──┬─RESET──TRACE─┬──────────────────────────────────────────►◄
    └─T──T────────┘
```

Parameters
None.

Example
To reset the current trace configuration issue the following command:
```
MODIFY CPOSERV,APPL=RESET TRACE
```

or:
```
F CPOSERV,APPL=T T
```

The response on the console might be:
```
CPO1070I The trace configuration has been reset
```

SET DOMAIN

Use the SET DOMAIN command to change the global processing information of the domain. This information includes the active provisioning policy, the active domain configuration, and the active processing mode.

The information supplied is validated before processing. If the command cannot be processed for any reason, the previous information remains active.

Note: If any resources are active when you change a policy or configuration, these resources might be deactivated.

Syntax

Set domain command syntax

```
>>--+--SET--DOMAIN--+--+--CFG=name----------+------------------------><
    +--S----D-------+  +--POL=name----------+
                       +--MODE=--+--MAN------+
                                 +--ANALYSIS-+
                                 +--CONF-----+
                                 +--AUTO-----+
```
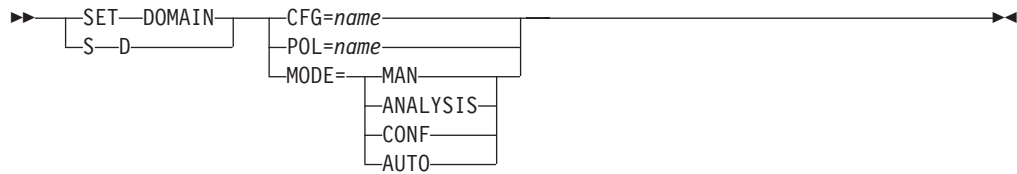
Parameters

The command has the following parameters:

CFG=_name_
   Specifies the name of the domain configuration that you want to activate. A domain configuration with the specified name must be installed in the domain configuration repository of the Provisioning Manager. Before the policy is activated, the content is validated.

POL=_name_
   Specifies the name of the policy that you want to activate. A policy with the specified name must be installed in the policy repository of the Provisioning Manager. Before the domain configuration is activated, the content is validated.

MODE=_mode_
   Specifies the new processing mode for the Provisioning Manager. The following processing mode values are supported:

   MAN   Manual mode (policies are disabled)

   ANALYSIS
         Analysis mode

   CONF   Confirmation mode

   AUTO
         Autonomic mode

   The processing mode values are not case-sensitive.

Example

To activate configuration DS, issue the following command:
```
MODIFY CPOSERV,APPL=SET DOMAIN CFG=DS
```

or:
```
F CPOSERV,APPL=S D CFG=DS
```

The response on the console might be:

```
CPO1041I Domain configuration DS successfully activated
```

To change the policy to BERLINP, issue the following command:

```
MODIFY CPOSERV,APPL=SET DOMAIN POL=BERLINP
```

or:

```
F CPOSERV,APPL=S D POL=BERLINP
```

The response on the console might be:

```
CPO1020I Policy successfully changed to BERLINP
```

To set the processing mode to autonomic, issue the following command:

```
MODIFY CPOSERV,APPL=SET DOMAIN MODE=AUTO
```

or:

```
F CPOSERV,APPL=S D MODE=AUTO
```

The response on the console might be:

```
CPO1009I Processing mode successfully changed to AUTO
```

SET TRACE

Use the SET TRACE command to change the tracing parameters of the Provisioning Manager. You can set a default trace level and also separate trace levels for individual trace components. Setting the default trace level does not overwrite a trace level set for an individual component.

Note: This command is to be used only if instructed to do so by IBM service personnel.

Syntax

```
►►─┬─SET─TRACE─┬─ LEV=─┬─OFF─────┬──┬─────────────────────────────────────────┬─►◄
   └─S───T─────┘       ├─SEVERE──┤  └─COMP=─┬─BASE──────────┬─────────────────┘
                       ├─WARNING─┤          ├─UTIL──────────┤
                       ├─INFO────┤          ├─POLICY────────┤
                       ├─FINER───┤          ├─CONFIGURATION─┤
                       └─ALL─────┘          ├─ANALYZER──────┤
                                            ├─PLANNER───────┤
                                            ├─CONSOLESERVER─┤
                                            ├─CIMOBSERVER───┤
                                            ├─CIMCLIENT─────┤
                                            └─HMCCLIENT─────┘
```
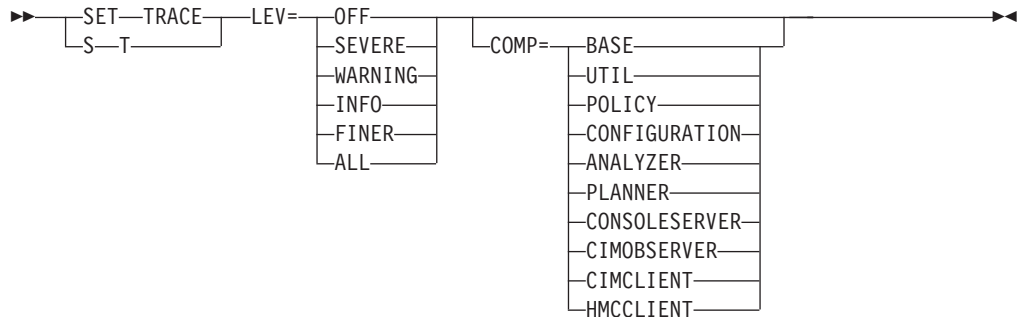
Parameters

The parameter names and trace values are not case-sensitive. This command has the following parameters:

LEV
Name of the trace level you want to activate. The following trace levels are supported:

OFF   Do not trace

SEVERE
Trace severe information

WARNING
Trace warnings or severe information

INFO   Trace general information

FINER
Trace at a finer information level

ALL   Trace all information

COMP
The name of a component of the Provisioning Manager for which you want to alter the trace level. The supported component names are:

BASE   Base processing

UTIL   Utility classes

POLICY
Policy-relevant processing

CONFIGURATION
Domain configuration-relevant processing

ANALYZER
Analysis of the metrics retrieved from the observed systems

PLANNER

Processing that is relevant to planning

CONSOLESERVER

Command processing

CIMOBSERVER

CIM requests processing

CIMCLIENT

CIM client API

HMCCLIENT

HMC or SE client API

If COMP is not specified, the overall trace level is changed.

Example

To set the global trace level to ALL, issue the following command:

```
MODIFY CPOSERV,APPL=SET TRACE LEV=ALL
```

or:

```
F CPOSERV,APPL=S T LEV=ALL
```

The response on the console might be:

```
CPO1060I The global trace level has been set to ALL
```

STOP MANAGER

Use the STOP MANAGER command to stop processing of the Provisioning Manager. After the Provisioning Manager is requested to stop, it does not accept any other commands. The state of resources does not change. Any active resources remain active.

Syntax

```
                      ┌─MODE=NORMAL─┐
►►─┬─STOP─MANAGER─┬───┼─────────────┼──────────────────────────────────►◄
   └─P──M─────────┘   └─MODE=FORCE──┘
```
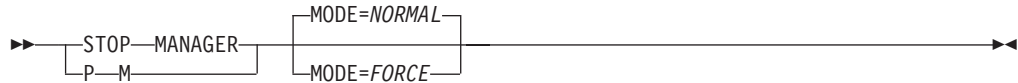
Parameters

The command has the following parameter:

MODE

Mode in which you want to end the Provisioning Manager. There are two supported stop modes:

NORMAL

The default stop mode is to terminate all processing and to unregister the Provisioning Manager from ARM if applicable

FORCE

To stop processing immediately. If the Provisioning Manager is registered with ARM, the process restart.

The mode values are not case-sensitive.

Example

To stop the Provisioning Manager, issue the following command:

```
MODIFY CPOSERV,APPL=STOP MANAGER
```

or:

```
F CPOSERV,APPL=P M
```

The response on the console might be:

```
CPO1007I Stop command for the Provisioning Manager accepted
```

WRITE LOG

Use the WRITE LOG command to save the current data for a specific log to a file.

Note: This command is to be used only if instructed to do so by IBM service personnel.

Syntax

```
►►──┬─WRITE─LOG─┬──LOGNAME=─┬─analyzerlog────────┬──┬─DEST=*────┬──────►◄
    └─W─────L───┘           ├─errorlog───────────┤  └─DEST=file─┘
                            ├─notificationlog────┤
                            └─systemobservationlog┘
```
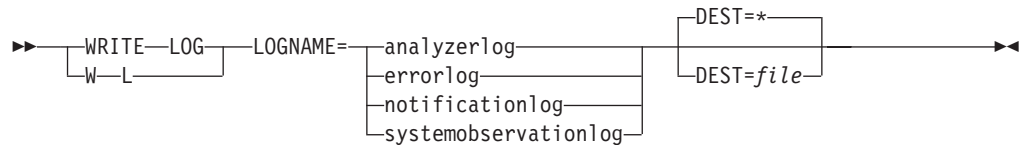
Parameters

The command has the following parameters:

LOGNAME=_name_

The type of data to be recorded might be:

analyzerlog
> Workload analysis results

errorlog
> Unexpected errors that are detected during processing

notificationlog
> Communications within the Provisioning Manager

systemobservationlog
> Monitored metrics from the observed systems

The log names are not case-sensitive.

DEST

Specifies the destination of the log. The following destinations are supported:

*   (Default) specifies that the report be written to the standard log file in the log path specified during setup. This option can be used if logging is already active for the specified log and data is available in the log.

file   Specifies a file where the information is to be stored. If the name includes lowercase characters, this parameter must be enclosed in single quotation marks ('). The file must be in the hierarchical file system. You can specify either an absolute path or a relative path to the file. If this is not absolute the path is relative to the home directory of the user who is running the Provisioning Manager. You must ensure that there is sufficient space in the selected location. The Provisioning Manager user must be authorized to write to this location. This option can always be used and does not require that log writing be activated for the specified log.

Example

To write the notification log to file `nl.log`, issue the following command:

```
MODIFY CPOSERV,APPL=WRITE LOG LOGNAME=NotificationLog DEST='nl.log'
```

or:

```
F CPOSERV,APPL=W L LOGNAME=NotificationLog DEST='nl.log'
```

The response on the console might be:

```
CPO1040I Log NotificationLog successfully written to file nl.log
```

Part 4. Appendixes

171

Glossary

A

Application Assist Processor. See zAAP.

ARM. See Automatic Restart Manager.

Automatic Restart Manager (ARM). A z/OS recovery function that can automatically restart tasks after they or the system on which they are running end unexpectedly.

B

Base Control Program (BCP). A program that provides essential services for the MVS and z/OS operating systems. The program includes functions that manage system resources. These functions include input or output, dispatch units of work, and the z/OS UNIX System Services kernel.

BCP. See Base Control Program.

C

capacity. See temporary capacity.

Capacity Provisioning Control Center. A Windows application installed on a workstation that provides a graphical user interface to Capacity Provisioning. Administrators use this interface to can work with provisioning policies and domain configurations and can transfer them to the Provisioning Manager.

Capacity Upgrade on Demand (CUoD). The capability of permanently activating one or more inactive processors without having to restart the server or interrupt the data flow of the business, through the purchase of a permanent processor activation. This capability adds significant value by enabling a fast and economical way of adding capacity for new workloads, enabling the server to adapt to unexpected performance demands.

CDT. See class descriptor table.

Central Processor Complex (CPC). A physical collection of hardware that consists of main storage, one or more central processors, timers, and channels.

CFCC. See Coupling Facility.

CIM. See Common Interface Module.

CIU. See Customer Initiated Upgrade.

class descriptor table (CDT). A table in RACF that contains class descriptors. The CDT contains descriptors with default class names for CICS resources. Users can modify the supplied descriptors and add new ones.

Common Interface Module (CIM). An implementation-neutral, object-oriented schema for describing network management information. The Distributed Management Task Force (DMTF) develops and maintains CIM specifications.

condition. See time condition, workload condition.

control center. See Capacity Provisioning Control Center.

Coupling Facility. A special logical partition that provides high-speed caching, list processing, and locking functions in a sysplex.

CPC. See Central Processor Complex.

CUoD. See Capacity Upgrade on Demand.

Customer Initiated Upgrade (CIU). A permanent upgrade ordered, downloaded, and installed by using the IBM CIU web-based application on Resource Link®.

D

deadline. The time during a time condition after which activation of additional capacity is no longer allowed. Additional capacity that is activated as part of the activated in the time condition before the deadline remains activated until the end time or until the capacity is no longer needed. See also start time, end time.

deprovisioning PI. The minimum of the performance index range for a service class period, at or below which the Provisioning Manager considers the service class period not to be negatively affected.

domain configuration. Manage domain configurations, defining the CPCs to be managed and the systems to be observed. Transfer the domain configurations to the Provisioning Manager.

E

end time. The end of a time condition, after which the Provisioning Manager starts to deactivate any additional capacity activated in the time condition. See also start time, deadline.

H

hardware management console (HMC). A system that controls managed systems, including the logical partitions and use of Capacity Upgrade on Demand. Using service applications, the HMC communicates with managed systems to detect, consolidate, and send information to IBM for analysis.

HMC. See hardware management console.

I

importance filter. A table that assigns importance levels to sets of provisioning criteria.

Integrated Information Processor. See zIIP.

Intelligent Resource Director (IRD). A z/OS facility enhances the ability of an installation to dynamically move resources to the most important work.

IRD. See Intelligent Resource Director.

L

logical processor. A processor that is defined in an LPAR profile. It can be either configured online, offline, or be reserved. Only online logical processors are dispatched on physical processors.

logical processor limit. The number of logical processors that can be configured online for the systems in the provisioning domain.

M

maximum provisioning scope. The total amount of resources that can be additionally activated for a domain. See also provisioning scope.

monoplex. A sysplex that consists of one system that uses a sysplex couple data set (CDS).

O

On/Off Capacity on Demand (On/Off CoD). An addition to the CIU tool that enables you to configure, order, and download temporary upgrades for your processors. It is used to temporarily increase CPs, IFLs, zAAPs, and ICFs concurrently and non-disruptively. The increased capacity is billed on a 24-hour basis.

On/Off CoD. See On/Off Capacity on Demand.

P

PassTicket. A dynamically generated, random, one-time-use, password substitute in RACF secured

sign-on that a workstation or other client can use to sign on to the host rather than sending a RACF password across the network.

performance index (PI). A measure of the performance of a system, based on metrics such as transaction rates or response times.

PI. See performance index.

policy. A set of rules that controls the provisioning of additional capacity.

provisioning. The process of configuring servers, software, networks, and storage resources.

provisioning condition. See time condition, workload condition.

provisioning criteria. A set of parameters that indicates the target performance index range that is expected of a service class period and the length of time it can go out of range before intervention is required. See also provisioning PI, deprovisioning PI, performance index.

provisioning PI. The maximum of the performance index range for a service class period, at or beyond which the Provisioning Manager considers the service class period to be negatively affected.

provisioning scope. The amount of resources that can be additionally activated for a policy. See also maximum provisioning scope.

R

Resource Measurement Facility (RMF). A feature of z/OS that measures selected areas of system activity and presents the data collected in the format of printed reports, System Management Facility (SMF) records, or display reports.

RMF. See Resource Measurement Facility.

rule. Links a provisioning scope to time conditions and can also link it to workload conditions.

S

SAF. See System Authorization Facility.

System Authorization Facility (SAF). An MVS interface with which programs can communicate with an external security manager, such as RACF.

service class. A group of work items which have the same performance goals, resource requirements, or business importance. For workload management a service goal and optionally a resource group are assigned to a service class.

service class period.   A division of time during which a transaction can execute.

specialty processor.   See zAAP, zIIP.

start time.   The start of a time condition, at which point the Provisioning Manager starts to activate additional capacity if one of the workloads associated with the time condition is negatively affected. See also deadline, end time.

sysplex.   A set of z/OS systems that communicate with each other through certain multisystem hardware components and software services.

T

temporary capacity.   An option available on certain IBM Machines that can be enabled for each applicable TC Eligible Machine that you indicate on a Supplement. IBM can also see TC as "IBM eServer™ On/Off Capacity on Demand," "On/Off Capacity on Demand," or "On/Off CoD."

time condition.   A specification of time periods during which temporary capacity can be activated or deactivated for a rule.

time period.   A section of a time condition. The time periods are delimited by the start time, deadline, and end time.

W

WLM.   See Workload Management.

workload condition.   A definition of work that is eligible to cause activation of additional capacity and the conditions under which activation occurs.

Workload Management (WLM).   A component of z/OS that enables multiple workloads to run at the same time within one z/OS image or across multiple images.

Z

zAAP.   z9® Application Assist Processor. A specialized processing unit that provides an economical Java execution environment for customers who want the traditional quality of service and integration advantages of the z platform.

zIIP.   z9 Integrated Information Processor. A specialty engine designed to improve resource optimization and lower the cost of eligible workloads, enhancing the role of the mainframe as the data hub of the enterprise.

Accessibility

Publications for this product are offered in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when using PDF files, you may view the information through the z/OS Internet Library website or the z/OS Information Center. If you continue to experience problems, send an email to mhvrcfs@us.ibm.com or write to:

IBM Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Building 707
2455 South Road
Poughkeepsie, NY 12601-5400
U.S.A.

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in z/OS enable users to:

- Use assistive technologies such as screen readers and screen magnifier software
- Operate specific or equivalent features using only the keyboard
- Customize display attributes such as color, contrast, and font size

Using assistive technologies

Assistive technology products, such as screen readers, function with the user interfaces found in z/OS. Consult the assistive technology documentation for specific information when using such products to access z/OS interfaces.

Keyboard navigation of the user interface

Users can access z/OS user interfaces using TSO/E or ISPF. Refer to *z/OS TSO/E Primer*, *z/OS TSO/E User's Guide*, and *z/OS ISPF User's Guide Vol I* for information about accessing TSO/E and ISPF interfaces. These guides describe how to use TSO/E and ISPF, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

z/OS information

z/OS information is accessible using screen readers with the BookServer or Library Server versions of z/OS books in the Internet library at:

http://www.ibm.com/systems/z/os/zos/bkserv/

Notices

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

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

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

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

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

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

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

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

Site Counsel
IBM Corporation
2455 South Road
Poughkeepsie, NY 12601-5400
USA

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

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

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

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

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

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.

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

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or

imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Policy for unsupported hardware

Various z/OS elements, such as DFSMS, HCD, JES2, JES3, and MVS, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml .

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft, Windows, Windows NT, Windows Vista, Windows 7 and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

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

Index

Special characters

A

B

C

IBM®

Product Number: 5694-A01

Printed in USA

Spine information:

z/OS

z/OS V1R13.0 MVS Capacity Provisioning User's Guide

Version 1,
Release 13

SC33-8299-05

IBM