

z/OS



MVS Capacity Provisioning User's Guide

Version 1 Release 11

z/OS



MVS Capacity Provisioning User's Guide

Version 1 Release 11

Note

Before using this information and the product it supports, be sure to read the general information under "Notices" on page 133.

This edition applies to Version 1 Release 11 of z/OS (5694-A01) and to all subsequent releases and modifications until otherwise indicated in new editions.

This edition replaces SC33-8299-02.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address below.

IBM welcomes your comments. A form for readers' comments may be provided at the back of this publication, or you may address your comments to the following address:

IBM Research & Development GmbH
Department 3248
Schoenaicher Strasse 220
D-71032 Boeblingen
Federal Republic of Germany

FAX (Germany): 07031+16-3456
FAX (Other Countries): (+49)+7031-16-3456

Internet e-mail: s390id@de.ibm.com
World Wide Web: <http://www.ibm.com/servers/eserver/zseries/zos/webqs.html>

If you would like a reply, be sure to include your name, address, telephone number, or FAX number.

Make sure to include the following in your comment or note:

- Title and order number of this book
- Page number or topic related to your comment

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 2008, 2009.

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

Contents

Figures v

Tables vii

About this document ix

Who should use this document ix

Where to find more information ix

Other Referenced Documents ix

The Capacity Provisioning Web Page x

How to read syntax diagrams x

 Symbols x

 Syntax items x

 Syntax examples xi

Summary of Changes xiii

Part 1. Getting started. 1

Chapter 1. Introducing z/OS Capacity Provisioning 3

What Capacity Provisioning can do for you 3

Considerations for configuring capacity 4

What are the components of Capacity Provisioning? 4

 The Capacity Provisioning Manager 4

 The Capacity Provisioning Control Center 4

 Capacity Provisioning sample data sets and files 5

Prerequisites 5

 System z hardware requirements 5

 z/OS software requirements 6

 Supported LPAR and z/OS Environments and Restrictions 6

Workstation requirements 7

Chapter 2. Capacity Provisioning basics 9

Overview 9

 Capacity Provisioning Domain 10

 Capacity Provisioning Policy 10

 Capacity Provisioning Manager 11

 Capacity Provisioning Control Center 12

Capacity Provisioning in detail 12

 Capacity Provisioning Domain 12

 Capacity Provisioning Policy 13

 Capacity Provisioning Manager 23

 Capacity Provisioning Control Center 29

Naming conventions 30

Chapter 3. Setting up a Capacity Provisioning domain. 33

Planning the domain set up 33

 Choosing names 33

 Defining the runtime environment 34

 Collecting information about prerequisites 36

Preparing the Provisioning Manager 37

 Defining the runtime data sets 37

 Adapting the Provisioning Manager parameters 38

 Creating the started task procedure 41

 Providing APF authorization 42

 Securing the runtime system 42

 Securing the observed systems 46

 Setting up Automatic Restart Manager 47

 Preparing the connection to the CIM server 47

 Preparing the connection to the Provisioning Manager 48

 Defining the connection to the hardware 48

 Tuning measures and workload classification for Capacity Provisioning 49

Installing the Control Center 50

 Installing the CIM Client 50

 Installing the Control Center using the installation wizard 50

Part 2. Operating Capacity Provisioning 53

Chapter 4. Using the Capacity Provisioning Control Center 55

The Control Center window layout 55

 The tree view 56

 The details view 57

 The information view 59

 The menu bar 60

Starting the Control Center 61

Stopping the Control Center 62

Accessing the Provisioning Manager 62

 Defining connections 62

 Working with the Provisioning Manager 63

Working with Domain Configurations 65

 Creating a domain configuration 65

 Installing and activating a domain configuration 68

Working with provisioning policies 68

 Creating a provisioning policy 69

 Installing and activating a provisioning policy 82

 Displaying the policy timeline 82

Chapter 5. Controlling the Provisioning Manager 85

Starting the Provisioning Manager 85

 Syntax 85

 Parameters 85

Provisioning Manager commands 86

Stopping the Provisioning Manager 86

Answering operator messages 87

Chapter 6. Working with reports 89

The domain report 89

The policy report 90

The domain configuration report 92

The workload report	95
The activity report	96
The trace report	97
The log report	97
Managing reports	98

Chapter 7. Considerations for defining policies and domains 99

Choosing service class periods	99
Choosing provisioning criteria	99

Part 3. Reference 101

Chapter 8. Provisioning Manager command reference 103

Introduction	103
Commands	104
ACTIVATE LOG	104
ACTIVATE RESOURCE	105
DEACTIVATE LOG	107
DEACTIVATE RESOURCE	108
DISABLE CONFIGURATION	109
DISABLE POLICY	109
DUMP MANAGER	110
ENABLE CONFIGURATION	111
ENABLE POLICY	111
LIST CONFIGURATION	112
LIST POLICY	113
REPORT ACTIVITY	113

REPORT CONFIGURATION	114
REPORT DOMAIN	114
REPORT LOG	115
REPORT POLICY	116
REPORT TRACE	116
REPORT WORKLOAD	117
RESET CONFIGURATION	117
RESET POLICY	118
RESET TRACE	118
SET DOMAIN	119
SET TRACE	120
STOP MANAGER	122
WRITE LOG	123

Part 4. Appendixes 125

Accessibility 127

Using assistive technologies	127
Keyboard navigation of the user interface	127
z/OS information	127

Capacity Provisioning Terms. 129

Notices 133

Policy for unsupported hardware.	134
Trademarks	136

Index 137

Figures

1. Capacity Provisioning domain	10	13. Domain configuration system definition screen	66
2. Capacity Provisioning policy structure	14	14. Domain configuration CPC definition screen	67
3. Time condition semantics	18	15. Provisioning policy screen	69
4. Provisioning criteria semantics	22	16. Logical processor scope screen	70
5. Control Center installation wizard: Initial installation	51	17. Maximum provisioning scope screen	72
6. Layout of the Graphical User Interface	55	18. Provisioning rule screen	73
7. Details view showing the details of a workload condition.	58	19. Provisioning condition screen	74
8. Messages	59	20. Time condition screen	75
9. Connection report	60	21. Workload condition screen	77
10. Workspace screen	62	22. Importance filters screen	78
11. Provisioning Manager screen.	63	23. Included service class screen	79
12. Login screen	64	24. Excluded service class screen.	81
		25. Select timeline to display screen.	82
		26. Policy timeline screen	83

Tables

1. Syntax examples	xi	9. Naming restrictions	30
2. Support Element (SE) or Hardware Management Console (HMC) requirement by Capacity Provisioning configuration.	5	10. Name information for a new domain	34
3. Provisioning scope - example	15	11. Provisioning Manager runtime environment	36
4. Logical processor scope - example	15	12. Prerequisites information	36
5. Provisioning criteria.	20	13. Provisioning Manager data sets	37
6. Time condition states	25	14. Additional control parameters	40
7. Processing modes	26	15. Control commands.	104
8. Processing modes - requirements and functions supported	27	16. Status commands	104
		17. Debug commands	104

About this document

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

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, 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, refer to *z/OS Information Roadmap*.

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

Other Referenced Documents

Softcopy Title	Title	Order Number
<i>z/OS Security Server RACF Security Administrator's Guide</i>	<i>z/OS Security Server RACF Security Administrator's Guide</i>	SA22-7683
<i>z/OS Security Server RACF Security Callable Services</i>	<i>z/OS Security Server RACF Security Callable Services</i>	SA22-7691
<i>z/OS RMF Report Analysis</i>	<i>z/OS RMF Report Analysis</i>	SC33-7991

Softcopy Title	Title	Order Number
<i>z/OS UNIX System Services Programming Tools</i>	<i>z/OS UNIX System Services Programming Tools</i>	SA22-7805
<i>z/OS UNIX System Services Planning</i>	<i>z/OS UNIX System Services Planning</i>	GA22-7800
<i>z/OS UNIX System Services Parallel Environment: Operation and Use</i>	<i>z/OS UNIX System Services Parallel Environment: Operation and Use</i>	SA22-7810
<i>PR/SM Planning Guide</i>	<i>PR/SM Planning Guide</i>	GA22-7236
<i>Support Element Operations Guide</i>	<i>Support Element Operations Guide</i>	SC28-6802
<i>System z Application Programming Interfaces</i>	<i>System z Application Programming Interfaces</i>	SB10-7030

The Capacity Provisioning Web Page

For the latest information, see the Capacity Provisioning web page at:
<http://www.ibm.com/servers/eserver/zseries/zos/wlm/cp>

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.

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


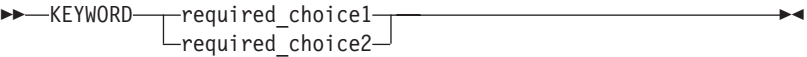

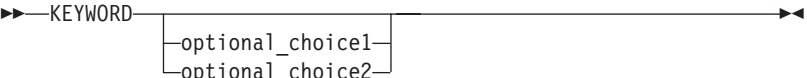
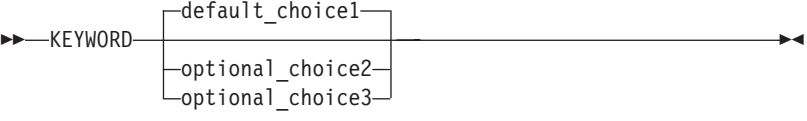



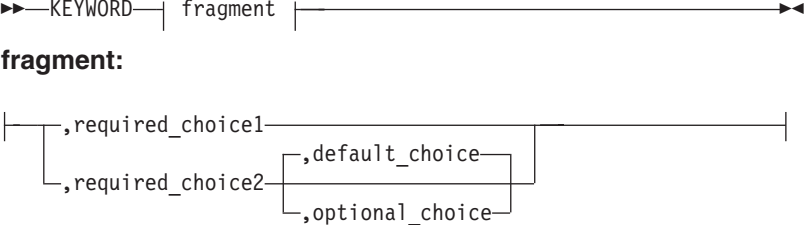
Item	Syntax example
Required item.	
Required items appear on the main path of the horizontal line. You must specify these items.	
Required choice.	
A required choice (two or more items) appears in a vertical stack on the main path of the horizontal line. You must choose one of the items in the stack.	
Optional item.	
Optional items appear below the main path of the horizontal line.	
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.	
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.	
Variable.	
Variables appear in lowercase italics. They represent names or values.	

Table 1. Syntax examples (continued)

Item	Syntax example
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.	
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.	 <p>fragment:</p> <pre> ----- -----,required_choice1----- -----,required_choice2----- -----,default_choice----- -----,optional_choice----- </pre>

Summary of Changes

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 may 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 BCPII-based 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 further information, refer to "REPORT LOG" on page 115.

Part 1. Getting started

This part gives an overview of Capacity Provisioning 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 remains a relatively static task as long as the workloads that need to be considered are sufficiently stable. However, in many environments workloads may fluctuate considerably over time. As the total workload or the mixture of workloads varies it may become increasingly difficult to guarantee service levels. z/OS[®] Workload Management (WLM) allows incoming work to be classified with a performance goal and a priority that reflects the business priority of that work. WLM will try to accommodate the goals of all the work in the system. However, even with an ideal WLM service definition, it may 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 may be compromised first, based on the assigned importance level. Discretionary work will be displaced first, followed by low importance work.

At some point, however, this may not be acceptable, either because the displaced work is relevant from a business perspective, or because it interacts with resources that are required by the more important work. In these cases the processing capacity should be increased to accommodate the increased workload. This may result in a permanent capacity increase for planned growth or a temporary capacity increase for seasonal or unpredictable peak periods. IBM[®] System z provides the capability of quickly and non-disruptively configuring additional processor capacity that is built directly into System z servers — IBM Capacity Upgrade on Demand (CUoD) for a permanent increase of processing capability, and IBM On/Off Capacity on Demand (On/Off CoD) for a temporary capacity increase.

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, by additional processors, or by a combination of both.

What Capacity Provisioning can do for you

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

To accommodate changes of the physical capacity, the configuration of logical processors may need to be changed as well. You can allow Capacity Provisioning to configure logical processors online or offline whenever such resources would block a change to the hardware capacity.

When you use Capacity Provisioning you can select different levels of automation to provide you with an appropriate level of control. For further information on these processing modes, refer to page 26.

For example, it is possible to:

- 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 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 further details, refer to *System z10 Enterprise Class Capacity on Demand User's Guide*, SC28-6871. See your IBM sale representative for further information.

There may be additional fees for non-IBM software. In addition, some non-IBM software packages may require new license keys in order 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) - the server program
- Capacity Provisioning Control Center (Control Center) - the workstation code
- Sample data sets and files

Capacity Provisioning configuration entities, such as policies and domain configurations, are defined using the Control Center on a workstation. Observation of workloads and the interaction with the servers defined to Capacity Provisioning is performed by the Provisioning Manager on the z/OS host.

The following sections briefly describe the components 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. The systems to be observed are defined in a domain configuration file. Details of additional capacity and the rules for its allocation are held in a policy file. These two files are created and maintained using the Control Center.

The Capacity Provisioning Control Center

The Control Center, installed on a workstation, is the graphical user interface to Capacity Provisioning. Through this interface administrators work with provisioning policies and domain configurations, and can transfer these to the Provisioning Manager.

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

Capacity Provisioning sample data sets and files

The Capacity Provisioning component includes several samples to 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 33.
- The Control Center contains sample domain configurations and policies. These samples are used throughout this book 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 exploited with fewer requirements.

System z hardware requirements

- One or more z10 servers.
 - If temporary capacity is to be controlled by the Provisioning Manager running in confirmation or autonomic mode, or if provisioning actions are to be performed through Provisioning Manager commands, temporary capacity must be available. This requires the On/Off CoD enablement (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. For this communication two types of communication are supported:
 - **SNMP.** A TCP/IP based communication that requires a network connection from the z/OS system where the Provisioning Manager runs to the Support Element or the Hardware Management Console (HMC). For further information refer to *System z Application Programming Interfaces*.
- Note:** If you use SNMP communication, support elements (SE) and the Hardware Management Console (when used) must be at driver level D73G, or higher.
- **BCPii.** A z/OS built-in communication that does not require a network connection. If you use BCPii, refer to *z/OS MVS Programming: Callable Services for High-Level Languages*, or to the appropriate Preventive Service Planning (PSP) bucket for further information.
 - If more than one processor complex is to be controlled, an HMC is required. The available options are listed in Table 2.

Table 2. Support Element (SE) or Hardware Management Console (HMC) requirement by 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) requirement by 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 may use an equivalent product.
- Your z/OS security product must support creating 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 allow for great flexibility. Capacity Provisioning supports a broad range of configurations but certain configurations are not supported or are restricted. This chapter summarizes the restrictions that apply to Capacity Provisioning in z/OS Release 11.

- Observed systems must be running z/OS Release 9 or higher. Other operating systems, or the Coupling Facility Control Code (CFCC), may be active in other LPARs.
- Observed systems running as guests under z/VM® are not supported. You are also recommended not to use a z/OS system running as a z/VM guest to run the Provisioning Manager.
- An observed system may run in a *shared* or *dedicated* LPAR. An LPAR with *dedicated* processors, however, can only generate demand 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, no additional demand will be recognized. If the LPAR is *dedicated* no demand for additional special purpose processors will be recognized.
- Demand for additional physical processors – as opposed to increased capacity level – for shared CP, zAAP, or zIIP processors can only be recognized 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 may have general purpose CPs, zAAPs and zIIPs configured.
- The additional physical capacity provided through Capacity Provisioning will be distributed through PR/SM™ and the operating systems. In general the additional capacity will be 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.

- It is recommended not to 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 should not use "initial capping" (hard capping).

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 later
- Screen resolution 1024x768 or higher
- If the Control Center is used to connect to the Provisioning Manager (recommended) a TCP/IP connection to the z/OS system hosting the Provisioning Manager

Chapter 2. Capacity Provisioning basics

A knowledge of the concepts of Capacity Provisioning and the terms used in these concepts is assumed in the remainder of this book. This chapter is intended to clarify these terms and to give the background to the concepts. To set the scene, this is the environment in which Capacity Provisioning operates:

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 which can run on one or more of these CPCs and which 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 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 will trigger intervention, the resources which can be activated, and the time periods during which the rule can be applied.

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

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

These concepts are expanded below in the overview section. The domain is described on page 10, policies on page 10, the Provisioning Manager on page 11 and the Control Center on page 12.

More information on key points follows in “Capacity Provisioning in detail” on page 12. The final section of this chapter is “Naming conventions” on page 30.

Overview

This information describes:

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

Capacity Provisioning Domain

The domain consists of:

- Observed systems which can trigger provisioning (described on page “Observed systems” on page 12), and where the number of logical processors can be changed, or
- Central Processor Complexes (CPCs) on which the configuration can be changed (described on page “CPCs” on page 12).

As Capacity Provisioning is capable of maintaining the configuration of more than one domain for different purposes, each domain should be identified by a unique name.

An example of a domain is:

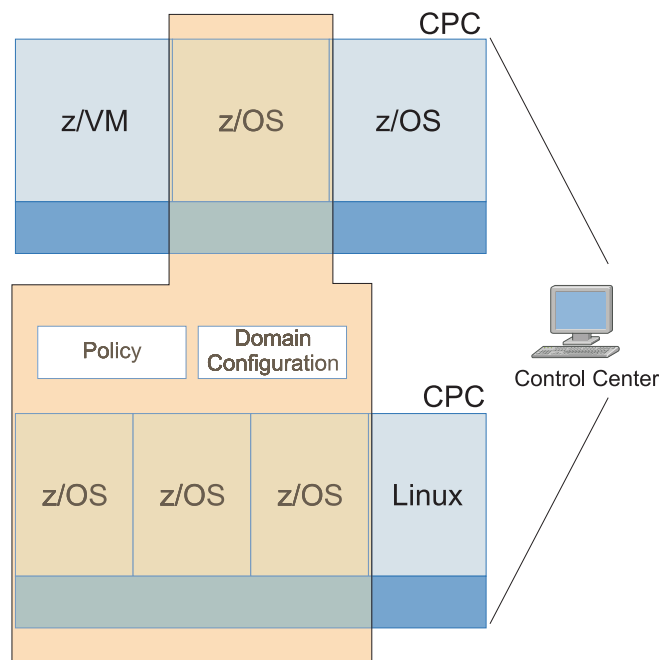


Figure 1. Capacity Provisioning domain

Figure 1 shows an example domain configuration with two CPCs to be managed and four systems to be observed. This shows that Capacity Provisioning can be performed for one or more CPCs. If a sysplex consists of multiple systems then all observed systems of this sysplex must belong to the same Capacity Provisioning domain. It is not supported that one CPC belongs to multiple domains. Each system in the domain configuration is identified by its z/OS system name and by the name of the sysplex it belongs to. 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 any point in time. The policy defines:

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

Each policy has a maximum provisioning scope which defines the total amount of resources that may be activated. This includes:

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

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

In the policy you can optionally specify a logical processor scope, which defines the z/OS systems where the number of logical processors can be changed. For each system you can either specify the maximum number of processors that may be online, 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 (provisioning scope) to the capacity that can be activated, time periods (time conditions) when activation is possible, and triggers (workload conditions) that can cause activation.

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

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

For more information on rules, refer to “Rules” on page 17. For more information on conditions, refer to “Provisioning conditions” on page 17.

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 held in a domain configuration. The Provisioning Manager must be able to access these CPCs from every host system it can run 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: In the rest of this book a HMC is assumed unless otherwise indicated, but the term HMC can be replaced throughout by SE if your system uses this.

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

Domain configurations are held in a domain configuration repository, and policies in a policy repository. As these repositories may contain more than one domain configuration or policy each configuration or policy must be given a unique name

to identify it. At any given time only one configuration and one policy can be active in the domain. Refer to “Defining the runtime data sets” on page 37 for details of the repository files.

The Provisioning Manager can operate in any one of four processing modes with varying powers of autonomy. These modes are described in detail on page 26.

Temporary capacity activated by the Provisioning Manager is referred to as being resources owned by the Provisioning Manager. Resources that are activated manually, either using Provisioning Manager commands or using the interfaces available at the HMC, are not managed by the Provisioning Manager.

Capacity Provisioning Control Center

The Control Center is a program which runs under Windows. It holds information in a workspace directory. You can prepare domain configurations and policies in the workspace and can then transmit these directly from the Control Center to the Provisioning Manager if a communication channel for this is set up. When this 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 details of the Control Center refer to page 29, and for the workspace refer to page 29.

Capacity Provisioning in detail

This information provides more details about Capacity Provisioning.

Capacity Provisioning Domain

The CPCs to be managed and the systems to be observed are specified in a domain configuration. You can create and edit a domain configuration using the Control Center (refer to page 29). If you want to activate the domain configuration you must install it into 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 running on a system or to manage the number of processors of that system the Provisioning Manager must be connected to that system. The information is provided by a CIM server on the system. The domain configuration includes attributes for each system which describe how to connect to the 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 using the Provisioning Manager commands `ENABLE CONFIGURATION` and `DISABLE CONFIGURATION` described on pages 111 and 109.

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 ClassCapacity on Demand User's Guide*. The Provisioning Manager can only activate

the residual capacity in this record within limits which were defined during the order process of the record. It is possible that some CPCs in a domain may not have temporary capacity. In this case the Provisioning Manager can still report resource shortages on these CPCs.

The provisioning domain contains a set of logical partitions (LPARs). These can be parts of a stand-alone system (a monoplex) or can be parts 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, and if it is running in a sysplex this name is further qualified by the name of the sysplex. A system can only be observed and considered for capacity changes 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 SE of that processor complex. For each CPC there is an *enabled* attribute which specifies whether the CPC is to be considered for temporary capacity changes. If it is enabled the Provisioning Manager is allowed to perform changes to the temporary capacity of that CPC. If it is disabled only manual capacity changes using Provisioning Manager commands are allowed. You can switch the *enabled* attribute on or off at runtime, in the same way as for systems, by using the Provisioning Manager commands `ENABLE CONFIGURATION` and `DISABLE CONFIGURATION` described on pages 111 and 109.

The temporary capacity that can be activated on a CPC can be described by multiple capacity records, identified by unique record IDs. Only one of these records can be in use 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 may leave the Provisioning Manager to find it.

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 using the Control Center. When the policy is complete you should 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 on page 14 shows the basic structure of a policy:

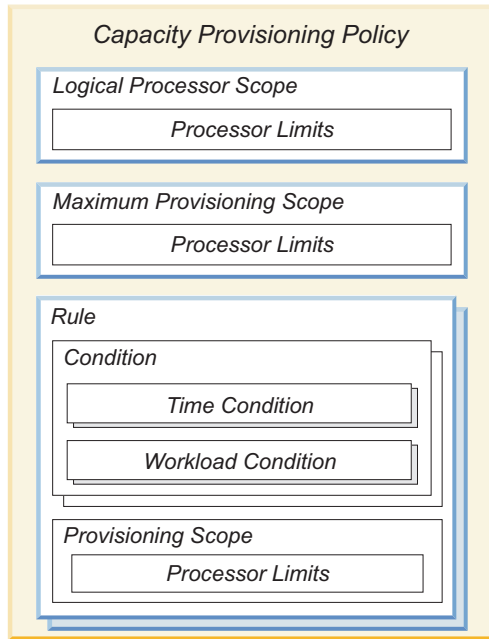


Figure 2. Capacity Provisioning policy structure

The policy contains:

A logical processor scope

defines the systems where Capacity Provisioning should manage the number of logical processors and which processor limits apply for those systems.

A maximum provisioning scope

limits the amount of additional resources that may be activated on behalf of the contained rules.

A set of provisioning rules

A rule contains provisioning conditions and a provisioning scope limiting the additional capacity that may 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 you should identify rules, provisioning conditions, time conditions and workload conditions by names which should be unique within the policy. 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 which reference these policy elements.

Maximum Provisioning Scope

Table 3 on page 15 shows an example of a provisioning scope in which limits are defined for two CPCs named CPC0 and CPC1. The first definition specifies that on

CPC0 200 MSUs and four additional zIIPs may be activated, but no zAAPs. The second definition specifies that on CPC1 a maximum of 300 MSUs, two zIIPs and three zAAPs may be activated.

Table 3. Provisioning scope - example

CPC	Maximum MSUs	Maximum zAAP Processors	Maximum zIIP Processors
CPC0	200	0	4
CPC1	300	3	2

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

For example, suppose you want to allow one additional zAAP to be activated when an online service class suffers, and one or two additional zAAPs when a batch service class suffers, but you do not want to have more than two additional zAAPs active at the same time. To model this scenario you should 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 for an online application at the same time, one of the requests will be unfulfilled (either the batch service class will only be allocated one additional zAAP or the online service class will be allocated no additional zAAPs) so that in total there will never be more than two additional zAAPs active at the same time.

Logical Processor Scope

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

Table 4. Logical processor scope - example

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** A 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 allowed to be active for the system. The system needs to be defined to allow for this amount 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 allowed to be active for the system. The system needs to be defined to allow for this amount 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 allowed to be active for the system. The system needs to be defined to allow for this amount of processors. Alternatively, an asterisk (*) stands for as many logical processors as allowed by the z/OS and LPAR configuration.

Action

Specifies the action to be taken by the Provisioning Manager whenever the need for more or less processors is detected. You can choose between following actions:

- Message on runtime system. The Provisioning Manager issues a message on the system on which the Provisioning Manager runs. If this message appears, you should 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 appears, you should perform the activation and deactivation on the affected system yourself.

For configuring additional logical processors online/offline, your system needs to have offline logical processors. These can be processors that you varied offline or that are defined as reserved processors in the definition of 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 the system is running with shared processors.

Capacity Provisioning takes logical processors online if the number of logical processors puts a limit to the consumption of physical capacity. This can be the case when only logical processors need to be configured online/offline or when the action is performed in combination with a physical activation. Logical processors are configured offline in case the number of logical processors of a system prevents a change in the physical capacity of the CPC on which the system is running. In this case the deactivation of physical resources is postponed until the configuring the logical processors offline is performed. 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 performing activation or deactivation of physical capacity at the CPC.

Rules

A rule can be associated with a particular service class, so that in the provisioning scope you can limit the additional capacity which 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 will then only be activated within periods specified by the time conditions, and when at least one of the associated service classes is suffering. Rules should be defined for all applications to which additional temporary capacity may be allocated.

A rule can be enabled or disabled. Only enabled rules are considered by the Provisioning Manager. You can specify in the policy 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` described on pages 111 and 109. In this way you can specify different scenarios in the policy and activate only those 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 rule. For example, a workload condition could be defined for a service class SC1 associated with month-end jobs, and time conditions could 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 may 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 then you should 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 relevant at any time, or you can temporarily disable part of the policy, for example, if a maintenance period overlaps with a time condition.

Time conditions

A time condition is defined by the following parameters:

Name	This uniquely identifies the time condition within the policy. The name is used in Provisioning Manager reports which reference the time condition.
Start time	The time at which the Provisioning Manager can start to activate additional capacity if one of the associated workloads suffers.
Deadline	The latest time when activation of additional capacity is allowed. Additional capacity which 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.

Figure 3 describes two time conditions and shows how the Provisioning Manager interprets them. On the left you can 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 can 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, so additionally provisioned capacity can remain active for a longer period but cannot be increased after the deadline.

Name	Start Time	Deadline	End Time
TC1	03.15.2008 08:00:00	03.18.2008 10:00:00	03.19.2008 10:00:00
TC2	10.28.2008 08:00:00	10.28.2008 16:00:00	10.30.2008 11:59:00

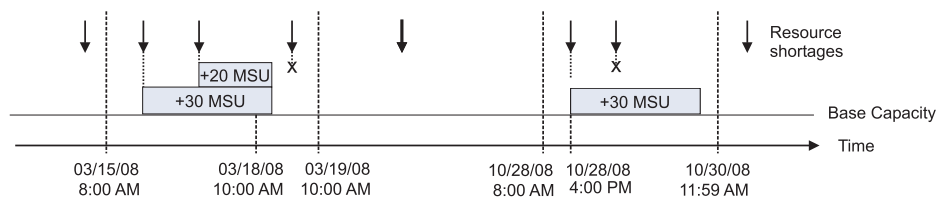


Figure 3. Time condition semantics

Workload conditions

If time conditions are defined in a rule, but no workload conditions, the Provisioning Manager performs scheduled activation and deactivation of additional capacity. At the start of these time conditions the maximum additional resources allowed in the provisioning scope will be activated. The deadline has no effect in this case, but at the end of the time condition the activated resources will be deactivated.

Specification of business critical work eligible for provisioning is based on the WLM service class model. In this model work is assigned to service classes which are associated with goals, such as a response time that should be met when the work is processed. A service class can be allowed up to eight defined periods of operation with specified durations and importance. A different goal can be specified for each period. If a period expires before the work is finished, the work will continue in the next defined period. Parcelling out the work in this manner allows a better distribution of resources, as a high resource usage in one section of the work only impacts the periods during which that section is running and not the entire duration of the work. See *z/OS MVS Planning: Workload Management* for information on WLM service classes.

The importance of service classes is used to resolve resource contention. Service class periods with a higher importance will be allocated resources first, and service class periods with a lower importance will get whatever is left.

Service classes are defined in WLM for the entire sysplex, so every service class is available on every system in the sysplex. Different service classes may be business critical on different systems, depending on the work that is running on each system.

A workload condition allows business critical service class periods to be specified. Each workload condition is given a name to uniquely identify it within the policy and to be used in Provisioning Manager reports. The workload condition has the following parameters:

- **Sysplex** The sysplex in which the workload can run. If you specify '*' for this parameter the workload condition applies to all sysplexes observed by the Provisioning Manager.
- **System** The z/OS system the workload condition applies to. If you specify '*' for this parameter the workload condition applies to all systems observed on the specified sysplex.
- **Importance filters** These allocate service class periods by importance level to sets of provisioning criteria (refer to page 20). The Provisioning Manager will check for resource shortages for all service class periods with an importance level equal to or higher than the specified value. Separate provisioning criteria can be defined for each importance level. Specification of importance filters is optional.
- **Included Service Classes** These identify sets of service class periods by name. For these periods the Provisioning Manager will check for resource shortages. Separate provisioning criteria can be defined for each service class period. Specification of included service classes is optional.
- **Excluded Service Classes Filter** These identify sets of service class periods by name that are not to be considered by the Provisioning Manager. Specification of excluded service classes is optional.

The importance filters allow eligible service class periods to be specified by their importance. If this method is not appropriate to identify business critical service class periods you can specify additional eligible service class periods by name as included service classes. Specifying excluded service class periods allows you to exclude ineligible service class periods which would otherwise be included. At least one importance filter or included service class period must be defined for the workload condition to take effect.

The Provisioning Manager determines the set of eligible service class periods as follows:

1. Service class periods that fulfill the importance filters on the specified system in the specified sysplex are chosen first.
2. This set is then extended to include the periods that match the included service class filters.
3. Service class periods that match the excluded service class filter are then removed from the set.
4. The Provisioning Manager will check for resource shortages 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.

As all work running in an eligible service class period can trigger provisioning, you should verify that 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 suffering from 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. PI thresholds must be defined in the provisioning policy as provisioning criteria associated with importance filters or included service classes.

The PI 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 over-fulfills the goal. A PI higher than 1.0 indicates that the goal is not fulfilled. In practice a PI greater than 1.0 may 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. This 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 should react if a PI is above tolerance is also installation dependant, so 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 beyond which the Provisioning Manager considers the service class period to be suffering.
Duration in min	The length of time during which the performance index must exceed the target PI before the Provisioning Manager intervenes. Note that in practice the actual duration can be longer than the specified duration, for example if the performance monitor sampling interval is not aligned with the specified duration.
Deprovisioning PI	The value of the performance index below which the Provisioning Manager considers the service class period no longer suffering. The deprovisioning PI must be lower than the provisioning PI.
Duration in min	The length of time during which the performance index must be less than the deprovisioning PI before the Provisioning Manager considers that the service class period is no longer suffering.

Table 5. Provisioning criteria (continued)

Provisioning criteria	Explanation
PI Scope	<p>This indicates whether the provisioning PI and deprovisioning PI values refer to the sysplex PI or the system PI of the service class period. The sysplex PI is the PI of the service class period within the sysplex. The system PI is the performance index of the service class period on each system in the sysplex. This is also referred to as the local performance index (local PI). The default and recommended setting is "System". A sysplex PI should only be considered if all systems joining the sysplex are defined to the provisioning domain. If PI scope "Sysplex" was chosen, in addition to monitoring the sysplex PI, the Provisioning Manager monitors the system PI. Thereby, on sysplexes distributed across several CPCs, the Provisioning Manager only provisions resources for systems running on CPCs that are actually suffering.</p> <p>Note: Some system monitoring products may only display the sysplex PI. If you use z/OS RMF the local PI can be found in the RMF Monitor III Data Portal SYSINFO report, in the RMF Monitor III as metric 0x8D1020, or in the RMF WLMGL report if the SYSTEMS option is in effect or if only data from a single system is provided.</p>

Provisioning PI and provisioning PI duration are used by the Provisioning Manager to detect if observed service class periods need 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 a workload condition is specified including service class ONLINE. 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 4 on page 22, the Provisioning Manager would detect three instances where the provisioning PI criteria are fulfilled. At the first two instances the Provisioning Manager will activate additional capacity. The third instance is ignored as it occurs after the deadline. The Provisioning Manager would also detect an instance when the deprovisioning PI criteria are fulfilled. The Provisioning Manager then decides service class ONLINE no longer needs additional capacity and starts to deactivate this.

```

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

```

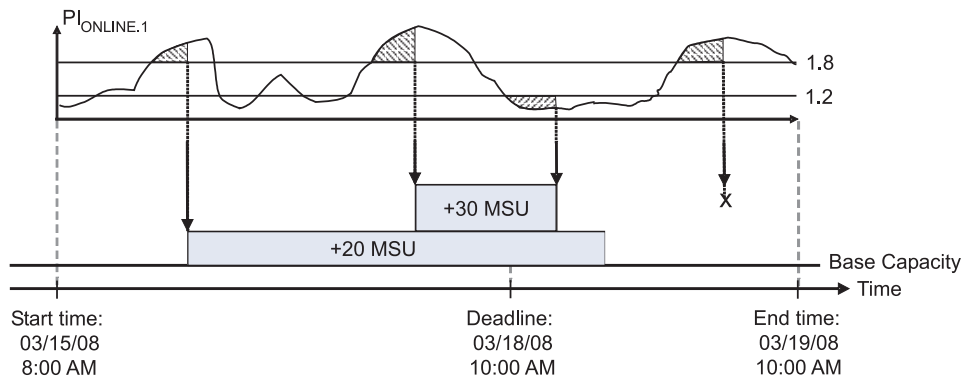


Figure 4. Provisioning criteria semantics

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 (refer to Provisioning criteria) indicating when service class periods matching the importance filter are considered to be suffering.

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 will be applied to them. To define different provisioning criteria only for service class periods of importance value 1, you can 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 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 may 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 may specify '*' to include all service policies matching the other criteria.

Service Class

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

Period

The limiting period of the service class that is 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 less periods than this number all periods will be considered. In an excluded service class filter, this period and all periods with a higher period number are excluded from provisioning.

The filters also include Provisioning Criteria PI values (refer to page 20) which determine if service class periods matching the service class filter are considered to be suffering. Provisioning criteria are used only with included service classes.

Capacity Provisioning Manager

The Provisioning Manager program resides in SYS1.SIEALNKE and in the file system under /usr/lpp/cpo. It must be invoked 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 are created 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/offline

To monitor and control resources a connection to the HMC must be established. You have the following two options:

- An SNMP protocol. To use this, a network path to the console must be available. Refer to "Defining the connection to the hardware" on page 48 for details.
- An internal connection. To use this, the BCPii component of z/OS must be set up and configured. Refer to "Defining the connection to the SEs for BCPii" on page 49 for details.

The processing mode of the Provisioning Manager (refer to Processing modes) is controlled by operator commands. The processing actions available are described in "Processing of configuration online/offline" on page 28. Refer to "Provisioning Manager commands" on page 86 for the method of entering these commands, and to Chapter 8, "Provisioning Manager command reference," on page 103 for the actual commands.

To ensure availability you can install and set up the Provisioning Manager on more than one system. You are recommended to run the Provisioning Manager on a system which is included in the domain. There should be no more than one instance of the Provisioning Manager active at any time. To handle 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 define a restart policy. 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 defined in the active domain configuration. Any CPCs defined in the domain configuration which are not listed as available by the HMC are marked as "not correlated". The Provisioning Manager regularly checks for additional CPCs, and when these are found it checks if they can be correlated to CPCs defined in the domain configuration.

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

Temporary capacity on a CPC in an enabled state can be automatically activated or deactivated by the Provisioning Manager. In a disabled state it can only be activated or deactivated manually 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. This requires a network connection to the observed system to be available, and all required services on this system must be configured and running. These include the CIM server itself and the providers for the workload metrics. If RMF supplies the CIM providers then 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 defined in the domain configuration. Performance information relating to the CPC, the LPAR, and the WLM service classes is then retrieved for the workload defined in the policy. As 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 may cause disruption. Such changes can be 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 may result in some history no longer being valid, and if resources are currently activated by the Provisioning Manager these may be deactivated.

The actual state information about the domain configuration and the observed systems and managed CPCs can be reported by the Provisioning Manager in the domain configuration report. For more information about this report refer to page 92. The enabled state of the system and the CPC domain configuration elements may be changed using Provisioning Manager commands. For details of these commands refer to "ENABLE CONFIGURATION" on page 111 and "DISABLE CONFIGURATION" on page 109.

Processing policy time conditions

One of the parameters of a time condition of a policy is a start time, which defines when the activation of temporary resources may start. The provisioning condition containing the time condition may 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 it is necessary. This calculated time is referred to as the observation start time.

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

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 observation of any system 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 are defined which require systems to be observed if possible. Systems that are referenced by associated workload conditions may 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 policy is enabled but the. 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 may 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. No changes to the activation level of the managed CPCs may be performed 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 may not activate additional temporary resources but may 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. No changes to the activation level of the managed CPCs may be performed by the Provisioning Manager based on the provisioning condition that contains the time condition.

Table 6. Time condition states (continued)

Time condition state	Meaning
Inactive	The current time is after the end time of the condition. No changes to the activation level of the managed CPCs may be performed 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 refer to page 90. The enabled/disabled states of the rule and provisioning condition policy elements may be changed using Provisioning Manager commands. For details of these commands refer to "ENABLE POLICY" on page 111 and "DISABLE POLICY" on page 109. The state of the active policy itself depends on the processing mode of the Provisioning Manager, as described on page 26. The policy is disabled in manual mode and enabled in all other processing modes.

Processing modes

The Provisioning Manager must collect a different amount 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 will not perform any activation or deactivation by itself. You may 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. These contain details of the maximum resources allowed by the policy which can be provisioned to help the current workload situation. In this mode, as in manual mode, the Provisioning Manager does not perform any activation or deactivation by itself. Note: In this mode the Provisioning Manager does not check whether the CPC on which the workload is running can permit the activation. It may report a need for additional resources for CPCs that do not in fact have any temporary resources that can be activated by the Provisioning Manager.

Table 7. Processing modes (continued)

Mode	Explanation
Confirmation	<p>In this mode you are informed through console messages of proposed changes to the capacity settings of the CPCs, 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.</p> <p>If you accept the proposal the Provisioning Manager performs the action and continues processing based on the new activation level.</p> <p>If you deny the proposal the Provisioning Manager will 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 may propose the same or other actions according to the new situation.</p> <p>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 cancelled. If any new requirement has arisen a new proposal will be issued.</p> <p>If you need more information to answer the proposal you may 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.</p>
Autonomic	<p>In this mode the Provisioning Manager autonomically adjusts the capacity settings of the CPCs as required, from 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.</p>

You can switch between these processing modes while the Provisioning Manager is running. Information about activation level changes that have been 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 which 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 using the Provisioning Manager SET DOMAIN command. Refer to page 119 for details of this command. The current processing mode is reported by the Provisioning Manager in the domain report, described on page 89.

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 and policy definitions required.	No	Yes	Yes	Yes
RMF DDS and CIM server required.	No	Yes	Yes	Yes

Table 8. Processing modes - requirements and functions supported (continued)

Requirement/Function	Manual	Analysis	Confirmation	Autonomic
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 recommendations or actions.	No	Recommendations through console messages.	Console messages (WTOR) that may be accepted, rejected, or ignored.	Actions are implemented immediately.
On/Off Capacity on Demand record required to be installed.	No	No	Yes	Yes

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. Refer to Logical Processor Scope for further information.

Processing of configuration online/offline

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

Schedule based provisioning actions are defined by provisioning conditions that do not have any workload condition. All available associated resources are activated at the start of the time condition. 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, may 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 of the observed systems. If the workload suffers because of 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 containing 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 of these changes 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. Blocking means that the Provisioning Manager does not consider it for further changes after any activation or deactivation of temporary capacity has been performed until this 'blocking' time has elapsed.

Temporary resources will not be 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 rules in the provisioning policy become inactive. This 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 which 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 refer to page 96.

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

You are recommended to leave management of the record describing the temporary capacity to the Provisioning Manager, but if necessary you can manually activate and deactivate temporary resources contained in this record. If you manually activate resources these will not be managed by the Provisioning Manager and you must deactivate them manually when needed. If you manually deactivate resources that have been activated by the Provisioning Manager this 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 to capacity provisioning. Through this interface you can work with provisioning policies and domain configurations. If there is a connection to the Provisioning Manager you can then 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 55.

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 director 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 directory **ProvisioningPolicies**, domain configurations in **DomainConfigurations**, and the connection definitions for the Provisioning Manager in **Connections** directory.

You may have several workspace directories, for example a separate one for each provisioning domain, but you can only work on one workspace at a time. During

the startup of the Control Center you are prompted to select a workspace. If you want to switch to a different workspace, just 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, where the new workspace shall be placed. If the directory does not exist, it will be created. Under the specified directory a subdirectory with the name Workspace and its three subdirectories are created. These directories contain sample files which you may use as models to copy into your own definition files. You are strongly advised not to use these samples themselves because service updates to the Control Center can replace the sample files.

The Control Center time zone

Policies contain time conditions which define time periods during which additional capacity can be activated. You may choose what time zone the Control Center will use to display the times contained in the time conditions. The default display time zone is GMT. When you switch the Control Center to a different time zone all times in the time conditions in all policies will be converted.

Independent of the displayed time zone, times in policies are always stored in UTC.

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 this 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 will be altered if necessary.

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

Named elements within a provisioning policy or a domain configuration, and elements referencing external entities such as an operating 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 character within the ASCII range which includes the characters on either side of the hyphen 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, #, \$, %, @, _

Table 9. Naming restrictions (continued)

Name	Minimum length	Maximum length	Initial character	Subsequent characters
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

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.

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

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

Planning the domain set up

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 which you can use to set up a new domain. These samples contain default values for element names. If you are satisfied with these defaults you need not change these values to 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 34 includes space for you to record the names you choose. The following paragraphs describe the element names, their default values and their meaning.

Every domain is identified by a domain name. If you use multiple domains each name should be unique. For further information about the rules for a valid domain name refer to "Naming conventions" on page 30.

The Provisioning Manager runs as a started task, using an entry set up for this purpose in the started task procedure data set used in your installation (normally SYS1.PROCLIB). A sample started task procedure, CPOSERV, is delivered in SYS1.SAMPLIB. This, or an equivalent, can be copied 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 user is assigned to the started task. This user must be defined and must be authorized for all resources accessed by the Provisioning Manager. The Provisioning Manager user requires a password and should have a home directory assigned.

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

Provisioning policies and domain configurations are defined 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 only needs to query the Provisioning Manager then the user should be a member of the Provisioning Manager query security group.
- If the user is allowed to modify the run time behavior of the Provisioning Manager then the user should also be a member of the Provisioning Manager control security group.

The Provisioning Manager and the Control Center communicate using the CIM protocol. The CIM server user will be needed to set up security definitions for this.

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

Table 10. Name information for a new domain

Name	Default	Your value
Domain name	DOMAIN1	
Started task procedure name	CPOSERV	
Runtime data set high-level qualifier	CPO	
Provisioning Manager user	CPOSRV	
Control Center user ¹	CPCCUSR	
Provisioning Manager query security group	CPOQUERY	
Provisioning Manager control security group	CPOCTRL	
CIM server user	CFZADM	
<p>Notes:</p> <ol style="list-style-type: none"> 1. The Control Center user can be any z/OS user 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). 2. The Provisioning Manager user must be set up with a password. To allow for the generation of passtickets it cannot be defined as a NOPASSWORD user. 		

Defining the runtime environment

Once you have defined your names you should define the environment for the Provisioning Manager. To start with you should identify the primary z/OS system on which you will run the Provisioning Manager, and you are recommended to select alternative systems on which a backup of the Provisioning Manager can run in the case that 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 36 and all paths listed in Table 12 on page 36 must be identical on the two systems. The term "runtime systems" in the following refers to all systems on which the Provisioning Manager may run, but note that only one instance of the Provisioning Manager can be running at any one time.

Note: All runtime systems should be on the same z/OS level. If the Provisioning Manager may restart on a system running with a previous z/OS release, configuration or status data may not be readable by the Provisioning Manager and the program terminates processing.

You can use z/OS Automatic Restart Manager (ARM) to restart the Provisioning Manager in the event of failure. If you do, you need to define the ARM restart policy, element name and element type. If you do not use ARM you may use any automation product which 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 need to define your communication protocol. Both protocols need to be 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 will serve the Provisioning Manager must be identified. Note that to manage multiple CPCs you require an HMC. The term HMC is used to mean HMC or SE, unless otherwise noted. The address defined 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 to communicate with the SEs of the CPCs without requiring a network connection from the runtime system to the HMC. Instead, some security definitions on your runtime systems have to be done.

For both protocols, you need the name of the community through which the Provisioning Manager can access the hardware console. It is possible to use the default community name ("public") but it is recommended 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 just needs to be defined at the HMC. Using BCPii requires the community name to be set up at each CPC managed by Capacity Provisioning and all CPCs on which the Provisioning Manager may run..

For service information the Provisioning Manager may write trace and log data. As this is temporary data it is usually written to the /tmp directory on the runtime system. If you want this data to be written to another location you may 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 may be deleted after it is sent to IBM. You should not delete the data while the Provisioning Manager is still running.

You should 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 of these where applicable. You are recommended to record here any values you change for your domain.

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	
HMC address	-	
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 following:

- The installation directory for the Java™ product
- The installation directory for the CIM server
- The location of the CIM Java client
- The location of the System Authorization Facility (SAF) libraries
- The location of the SAF Java library for secured signon function

Table 12 contains a list of all these prerequisite components and products and their default locations. You are recommended to 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, V5 (5655-N98), or V6 (5655-R31)	/usr/lpp/java/J5.0	
CIM server	/usr/lpp/wbem	
CIM Java client	/usr/lpp/wbem/jclient/ sb1imCIMClient.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 may also be one of the observed systems. On the runtime system you should:

- 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 have defined alternative runtime systems and these share the same resources, for example a common RACF database, the definitions only have to be done once.

On the observed systems you must define the security to allow the Provisioning Manager user to connect to the system and to query the information for its 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 you should adjust the examples accordingly. For further information about the different values and their defaults refer to “Planning the domain set up” on page 33.

Defining the runtime data sets

The Provisioning Manager stores permanent and temporary data in data sets. You only need to define these data sets once for a 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	<i>prefix</i> .RESTART	<i>prefix</i> .POLICIES	<i>prefix</i> .DOMCFG	<i>prefix</i> .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 34. For example, with the default values, the restart data set name would be CPO.DOMAIN1.RESTART.

After you have created the data sets, copy two sample files from the Capacity Provisioning installation file system into the data sets for the Provisioning Manager parameters. These are the files `env` and `parm` from directory `/usr/lpp/cpo/samples`. Copy these as members `ENV` and `PARM`, respectively.

Capacity Provisioning provides a sample job for defining these data sets and copying the files. The sample job is available as member `CPOMKDSN` in library `SYS1.SAMPLIB`. Note that this job will delete any existing data sets with the same names as those to be defined.

Adapting the Provisioning Manager parameters

Some parameters of the Provisioning Manager may need to be adapted to your environment. These parameters are held in 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/J5.0/bin` and `usr/lpp/java/J5.0/bin/classic`,

and the Capacity Provisioning installation path `/usr/lpp/cpo/lib`.

CLASSPATH

This entry must contain:

the Capacity Provisioning JAR files, and `hwmcaapi.jar` from the installation directory `/usr/lpp/cpo/classes`,

the SAF JAR file `/usr/include/java_classes/IRRRacf.jar`,

and the CIM Java client `/usr/lpp/wbem/jclient/sblimCIMClient.jar`.

For example:

```
LIBPATH=/usr/lib:/usr/lpp/java/J5.0/bin:usr/lpp/java/J5.0/bin/classic:...
      /usr/lpp/cpo/lib
CLASSPATH=/usr/lpp/cpo/classes/cpom.jar:...
      /usr/lpp/cpo/classes/cpocommon.jar:...
      /usr/lpp/cpo/classes/hwmcaapi.jar:...
      /usr/include/java_classes/IRRRacf.jar:...
      /usr/lpp/wbem/jclient/sblimCIMClient.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 may be included starting 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 the temporary capacity of these, and to activate and deactivate the temporary capacity, if required. You must specify access information for the HMC. The primary information is the protocol. It is specified using the configuration key `Topology.Address`. The value can be either `SNMP` for the SNMP protocol, or `INTERNAL` for `BCPii`. For `BCPii` the information would look like the following:

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

If the protocol is `SNMP`, you also need to specify the protocol. Additionally, you need to specify the host name or IP address of the HMC, and the community name under which all operations are performed. The HMC host address is specified using the configuration key `Topology.Address`. The community name is specified 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 if it is given any value other than "Yes", the Provisioning Manager will not be registered with `ARM`. The value is not case-sensitive.

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

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

Trace and Log data

If you have chosen other directories than the defaults for the trace and log data you must set configuration keys `Trace.Path` and `Log.Path` accordingly. The directories must already 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. It is recommended that you only specify a value if you have a need to override the default.

Table 14. Additional control parameters

Key	Default value	Description
Planner.BlockingTime	15	Number of minutes the provisioning Manager will wait after detection of the CPC capacity before any new capacity change action is initiated. This time allows the workload to be redistributed after a capacity change. If a faster provisioning or deprovisioning is warranted the value may be lowered. The recommended range is a value between 5 and 15 minutes.
Planner.ProvisioningRejectTime	120	Number of minutes a CPC is not considered for Provisioning Manager actions after a provisioning request 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 in confirmation mode has been rejected.
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	Minimum percentage of physical utilization of shared CPs that is required before considering additional general purpose capacity. In some environments severe processor contention can already occur 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	Minimum percentage of physical utilization of shared zAAPs that is required before considering additional zAAP capacity. In some environments severe processor contention can already occur at lower levels of processor utilization. In such environments you can specify a lower percentage value, such as 90.
Analyzer.Threshold. Decision001TotalSharedPhysicalUtilZiip	95	Minimum percentage of physical utilization of shared zIIPs that is required before considering additional zIIP capacity. In some environments severe processor contention can already occur at lower levels of processor utilization. In such environments you can specify a lower percentage value, such as 90.

Creating the started task procedure

You can create the started task procedure by copying the member CPOSERV from data set SYS1.SAMPLIB to the started task procedure data set. This 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 you should change the following values to those you have chosen:

HLQ the high-level qualifier of the runtime data sets
DOMAIN the name of the domain
CPODIR the home directory of the Provisioning Manager user
OUTCLS a suitable output class
RGNSIZE a region size allowed by the server

The sample procedure supplied is:

```

//*****
//* Licensed Materials - Property of IBM
//* 5694-A01
//* Copyright IBM Corp. 2007, 2008
//* Status = HPV7750
//*****
//CPOSERV PROC PMODE='*',
//          POLICY='*'
//* This section of variables may require customization
//HLQ      SET HLQ=CPO           HLQ of runtime data sets
//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=256M      server region size
//*
```

Providing APF authorization

For this, 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 this is overridden by a SYSLIB statement in PROGxx. In addition, the default IEASYSxx value LNKAUTH=LNKLST must 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. The code must be authorized for this; 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 you must 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
- libcpocket.so
- libcpostream.so
- libcpoii.so

The Java library is in /usr/lpp/java/J5.0/bin/classic, and is named libjvm.so. If you have copied the Java SDK code you must ensure that this has APF authorization the same as the Provisioning Manager libraries.

Securing the runtime system

You should set up security on the runtime system and on the observed systems. As an observed system can also be a runtime system you may have to perform both definitions on these. 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 signon function
- Define access for the Control Center user
- Define access to the hardware

The following examples assume your external security manager is RACF. If you have installed a different external security manager you should 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 has been defined for both users.

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 using RACF:

```
RDEFINE STARTED CPOSRV.* 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 UPDATE access to this. If you make changes to the default ARM element type, ARM element name or Provisioning Manager user you must replace the values SYSCPM, SYSCPO or CPOSRV in the following with the values you have chosen. 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. These include:

- Membership of 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) AUTH(USE) GROUP(CPOQUERY)
CONNECT (CPOSRV) AUTH(USE) GROUP(CPOCTRL)

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

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 Java client /usr/lpp/wbem/jclient/sblimCIMClient.jar
- Read access to the SAF library /usr/include/java_classes/IRRacf.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 you must set the "other" read, write, and execute access permissions of the directories and files accordingly, using the UNIX command `chmod`, for example:

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

These permissions will 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 signon function on the runtime system

Communication between the runtime system and the observed systems requires authentication and authorization. This is implemented using the secured signon function, which generates PassTickets when the Provisioning Manager logs on to an observed system. The log on 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 signon 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 signon function you can encrypt the secured signon application keys. If it is not you can mask the secured signon 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 ID(CPOSRV) ACCESS(READ) CLASS(FACILITY)
SETROPTS RACLIST(FACILITY) REFRESH
```

For more information about configuring RACF to use PassTicket services, refer to *z/OS Security Server RACF Security Administrator's Guide*.

Defining security for the hardware access

This step is only required if your communication to the hardware console is based on BCPii. If you are using this communication, you need to have the Common Event Adapter (CEA) running in full function mode and you need to authorize the Provisioning Manager user to some Common Event Adapter (CEA) services and to the CPCs that need to be managed. How to set CEA into full function mode is described 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*

A sample definition would look like the following:

```
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
```

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

- READ access to profile HWI.APPLNAME.HWISERV in the FACILITY class
- CONTROL access to profile HWI.TARGET.net id.name in the FACILITY class. The net id and name represent the SNA name of the CPC as defined at the SE. The APPLDATA of the security definition need to contain the community name for the Provisioning Manager as defined in Table 11 on page 36. A profile is needed for every CPC that is to be managed by Capacity Provisioning and all CPCs on which the Provisioning Manager may 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 SE. A profile is needed for every CPC that is to be managed by Capacity Provisioning.

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('public') 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, refer to *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.

It is recommended that the control center users are defined 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 have been set up as described in *z/OS Common Information Model User's Guide*.

The Control Center user needs 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 this create profile BPX.SRV.** in the SURROGAT class. The CIM server user requires at least READ 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 this user UPDATE access to the CIMSERV profile:

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

```
RDEFINE SURROGAT BPX.SRV.** UACC(NONE)
PERMIT BPX.SRV.** CLASS(SURROGAT) ACCESS(READ) ID(CFZADM)
SETROPTS GENERIC(SURROGAT) REFRESH
```

If instead the Control Center user is authorized to alter the processing characteristics of the Provisioning Manager, add this user to both Provisioning Manager security groups, CPOQUERY and CPOCTRL, and grant this user UPDATE access to the CIMSERV profile:

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

```
PERMIT CIMSERV CLASS(WBEM) ID(CPCCUSR) ACCESS(UPDATE)
SETROPTS CLASSACT(WBEM) RACLIST(WBEM) REFRESH
```

```
RDEF SURROGAT BPX.SRV.** UACC(NONE)
PERMIT BPX.SRV.** CLASS(SURROGAT) ACCESS(READ) ID(CFZADM)
SETROPTS GENERIC(SURROGAT) REFRESH
```

Securing the observed systems

When a system is observed the Provisioning Manager connects to the CIM server on that system and retrieves configuration information and performance information about the workload. To enable this communication, establish a connection in the name of the Provisioning Manager user and authorized by 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 signon function
- Authorize the Provisioning Manager user to access the CIM server

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

Defining the secured signon function on the observed systems

This must be set up on the observed systems as on the runtime system (described in "Defining the secured signon function on the runtime system" on page 44). 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 assumes that the CIM server user is already defined.

- Create the profile CIMSERV in the WBEM class. The Provisioning Manager user needs at least READ access to this profile, and the CIM server user at least CONTROL access.

```
PERMIT CIMSERV CLASS(WBEM) ID(CPOSRV) ACCESS(READ)
SETROPTS RACLIST(WBEM) REFRESH
```

- If the CIM server is configured to require surrogate definitions for all users, define the CIM server user as a surrogate of the Provisioning Manager user. To do this, create profile BPX.SRV.CPOSRV in the SURROGAT class. The CIM server user requires at least READ access to this profile.

```
RDEFINE SURROGAT BPX.SRV.CPOSRV
PERMIT BPX.SRV.CPOSRV CLASS(SURROGAT) ACCESS(READ) ID(CFZADM)
SETROPTS RACLIST(SURROGAT) REFRESH
```

For further information, refer to *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 to exploit 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 should normally be restarted with the policy and processing mode that were in use the last time it ran, together with any modifications to the policy that were triggered by console commands. To achieve this the policy name and the processing mode on the restart command should be specified as '*'.
To achieve this the policy name and the processing mode on the restart command should be specified as '*'.
- The Provisioning Manager may be restarted on another system of the sysplex, provided that this system has access to the runtimedata sets and the required file systems used by the previous system.

An example setup is supplied in member CPOARMP0 of SYS1.SAMPLIB. For more information on ARM refer to *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. You can establish connections through the server using either the HTTP protocol or the HTTPS protocol, provided that the CIM server is configured to support the chosen protocol. For details on how to configure the CIM server refer to the *z/OS Common Information Model User's Guide*. For the HTTPS protocol you should 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 port of 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) you must edit the file you copied (for example 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 control flag manually:

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

5. Verify that a link to the Capacity Provisioning CIM provider library has been 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, you need to 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 from the Provisioning Manager to the hardware, ensure that there is a network connection between the runtime system and the HMC, that any firewall between these will permit access, and that the HMC is configured for remote API operations. The first step is to define the community name that you have chosen in your configuration of the Provisioning Manager (see Table 11 on page 36). Note that the address and network mask of the community name must be defined so that all runtime systems can use this community name. The community name must be authorized for read and write operations. The next step is to allow external programs remote operation using the API. In case you have firewalls installed between the HMC and the network that your runtime systems belong to, you need to allow communication for SNMP (port 161) and on port 3161 from the runtime system to the HMC.

For further information about the configuration of an HMC for API programs, refer to *System z Application Programming Interfaces*.

Defining the connection to the SEs for BCPii

For the BCPii communication, you need to define the community name that you have chosen in your configuration of the Provisioning Manager (see Table 11 on page 36). Note that the address and the network mask of the community name should specify the loopback device 127.0.0.1, 255.255.255.255, respectively. The community name must be authorized for read and write operations. The next step is to allow external programs remote operation using the API. You need to perform the definitions on the SE of each CPC that should be managed by the Provisioning Manager and all CPCs on which the Provisioning Manager may run. For further information about the configuration of an SE for API programs, refer to *System z Application Programming Interfaces*.

Tuning measures and workload classification for Capacity Provisioning

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

You are recommended either to classify the Provisioning Manager and the supporting subsystems into SYSSTC, or to give these an aggressive single period velocity goal at an importance level that is higher than the work that will be 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 (GPMSEVE)
- 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 impact 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 will increase resource consumption by the server:

- A large number of observed systems
- A large number of 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. On systems configured with zAAPs they will be utilized automatically and no additional definitions are required.

Installing the Control Center

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 a CIM client Java archive file (jar) on the workstation. The location of the CIM Java client in the host file system is given in the prerequisites information in Table 12 on page 36. Download the `sblimCIMClient.jar` file in binary mode from the host to your workstation, and make a note of its location on the workstation as this will later be required by the installation wizard. If you use the defaults you can download the file using FTP as follows:

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

Installing the Control Center using the installation wizard

The first step is to download the installation wizard to the workstation from the host. You can then 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/cpccsetup.exe` in binary mode to a temporary directory on your workstation, for example:

```
cd "C:\Documents and Settings\Administrator\Local Settings\Temp"
ftp <host>
ftp> cd /usr/lpp/cpo/pws
ftp> binary
ftp> get cpccsetup.exe
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 `cpccsetup.exe`, for example

```
cd "C:\Documents and Settings\Administrator\Local Settings\Temp"  
cpcsetup
```

The installation will begin with the following panel:

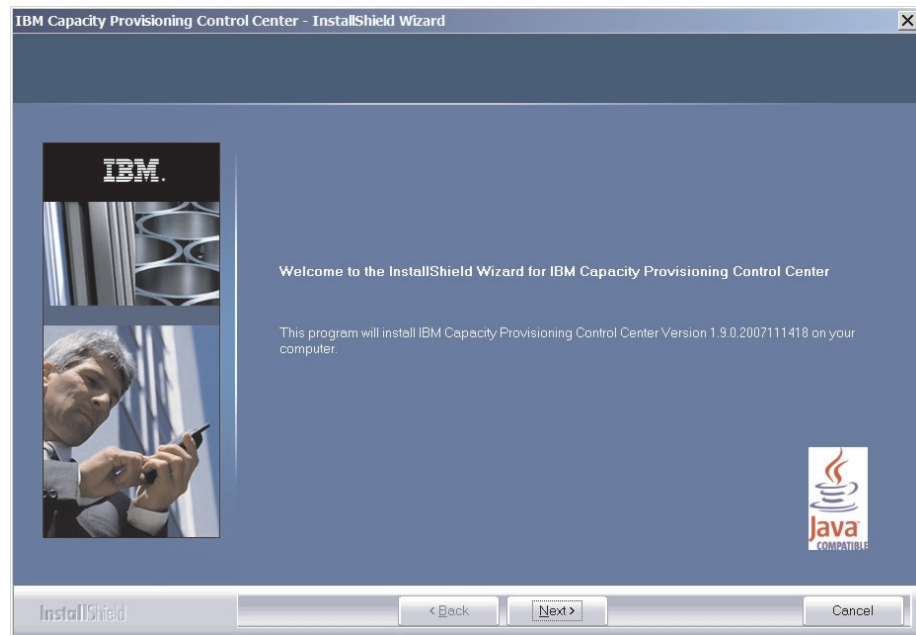


Figure 5. Control Center installation wizard: Initial installation

Follow the steps specified by the installation wizard. You will be asked where to place the Capacity Provisioning workspace (refer to “Workspace” on page 29), and in which directory you have put the `sb1imCIMClient.jar` file.

After the installation is finished you may delete `cpcsetup.exe`.

Updating an existing Control Center installation

Updates will be 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. Service, such as a PTF, will be flagged with a `++HOLD...SYSTEM REASON(DOWNLD)` action to indicate that a new version of the Control Center is available. SMP/E will report the `++HOLD` requirements when the service is received. Apply the service in SMP/E and then download the updated `/usr/lpp/cpo/pws/cpcsetup.exe` binary to a temporary directory on your workstation, as described in “Retrieving the Control Center Installation Package” on page 50.

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. Refer to “Stopping the Control Center” on page 62 for details. Start the update by executing the file `cpcsetup.exe`, as described in “Starting the initial installation” on page 50.

Start the update installation by executing the file `cpcsetup.exe` to reinstall the application with the settings you selected during the first installation. The user settings and the workspace will not be changed. The new version of the Control Center will be installed to the directories you chose in the initial installation.

Repairing an existing Control Center installation: If the same version of the install program is launched again on a system where the Control Center is installed the installation wizard Welcome screen gives you the option to 'Repair or remove the program'. The repair option will reinstall the application with the settings you selected during the first installation. The user settings and the workspace will not be changed. Select **Repair** on the panel. The Control Center will be reinstalled to the directories you chose in the initial installation.

To move the Control Center to a different location, select **Remove** on the panel instead. The program will be removed from your workstation. You should choose the option to keep the Control Center workspace, which contains the connection definitions, the domain configurations and the provisioning policies. You can then install the Control Center in the new location, as described in "Starting the initial installation" on page 50, and can enter the location of the old workspace to use the existing definitions. See the note under Uninstalling the Control Center for more considerations.

Uninstalling the Control Center

If you no longer require the Control Center on a workstation you can use the "Add or Remove Programs" option on the Windows control panel to remove the IBM Capacity Provisioning Control Center program. The installation wizard tracks the installation and any updates and maintains a corresponding uninstall action.

Stop the Control Center before starting the uninstall. Refer to "Stopping the Control Center" on page 62 for details. The Control Center code will be removed from your workstation. You have the option to remove the Control Center workspace as well, 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 will not be removed and must be deleted manually.

Part 2. Operating Capacity Provisioning

This part describes the use of Provisioning Management.

Chapter 4. Using the Capacity Provisioning Control Center

The Control Center is the graphical user interface to 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, and can also use it to transfer these to the Provisioning Manager or query the status, for example to see which policy is active. The Control Center provides the following functionality:

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

Provisioning Policies

Manage provisioning policies, defining how much additional capacity can be activated on each CPC

The Control Center window layout

The Control Center is a graphical user interface, with a screen layout as shown:

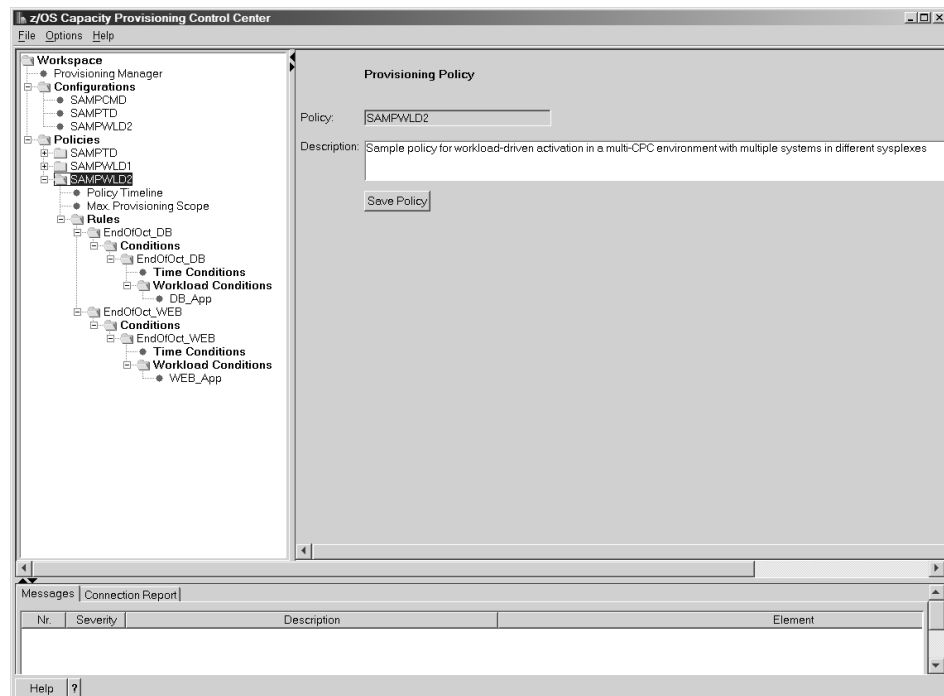


Figure 6. Layout of the Graphical User Interface




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 view on the left, the details view on the right and the information view at the bottom.

- The **tree view** 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 view

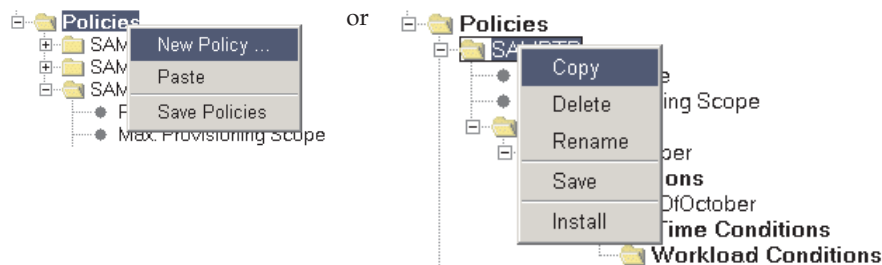
The tree view shows the structure of the Capacity Provisioning workspace. It contains the **Provisioning Manager** specification, the **Configurations** folder and the **Policies** folder. The **Configurations** folder contains one entry for each defined configuration. The **Policies** folder is structured 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 may be **Time Conditions**, **Workload Conditions** or both.

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

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 context menu for the selected object if possible, for example:



If this menu exists the object is also selected and the details are displayed in the **Details view**.

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

The context commands are:

Command Action

New... Creates a new object and prompts for a name.

This command can create a child object in any folder which has a name in **bold** type in the tree view (except the **Workspace** folder).

The **New** command is available on the folders **Configurations**, **Policies**, **Rules**, **Conditions** and **Workload Conditions**.

Command	Action
Copy	<p>Copies an object to the Control Center clipboard. The object can then be pasted at another corresponding position. Only one object can be stored in the clipboard; a second copy command overwrites the previous one.</p> <p>The Copy command is available for a selected configuration, policy, rule, condition or workload condition.</p>
Paste	<p>Pastes a copied object in the selected folder if the type of the copied object allows this. For example, a rule can only be pasted in a Rules folder. The object remains in the clipboard, so it can be pasted more than once. If an object with the name of the copied object already exists in the selected policy, the name of the pasted object is altered by the Control Center to make it unique.</p> <p>The Paste command is available in the folders Configurations, Policies, Rules, Conditions and Workload Conditions. Rules and conditions can only be pasted into the same policy.</p>
Delete	<p>Deletes an object from the workspace. Policies and configurations are deleted immediately. Policy elements are deleted when the policy is saved.</p> <p>The Delete command is available for a selected configuration, policy, rule, condition or workload condition.</p>
Rename	<p>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 the rename.</p> <p>The Rename command is available for a selected configuration, policy, rule, condition and workload condition.</p>
Save...	<p>Saves the selected object or object group in the workspace.</p> <p>Save commands are available in the Provisioning Manager and in the Configurations and Policies folders, and for selected configurations and policies.</p>
Install	<p>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 (refer to “Adapting the Provisioning Manager parameters” on page 38). Domain configurations are installed in the domain configuration repository and policies in the policy repository (refer to “Defining the runtime data sets” on page 37).</p> <p>The Install command is available for a selected configuration or policy.</p>

The details view

The details view shows the properties of the capacity provisioning object which is selected in the tree view. This view also shows related elements for some objects.

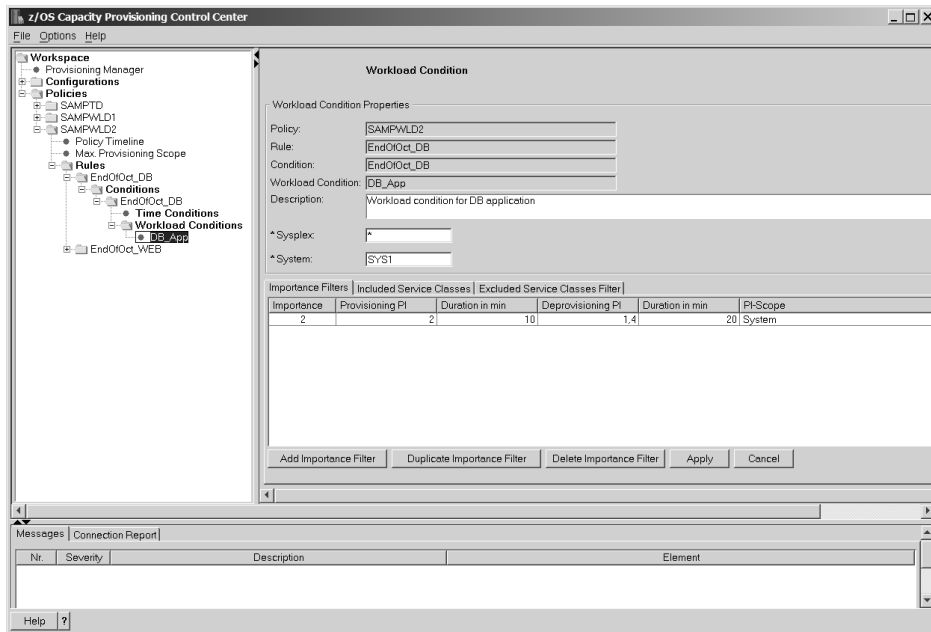


Figure 7. Details view showing the details of a workload condition.

The properties displayed in the upper part of the panel are dependant on the type of object selected. Figure 7 shows the properties of a **Workload Condition**. For most objects you can add a textual description for your reference.

The lower part of the panel may show a table containing additional elements of the displayed object which are not shown in the tree view. On some panels the lower part contains tabs which you may click on 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 table contents, and checks for errors. If you select a different tab or a different node in the tree Apply is executed automatically.
Cancel	Rejects any changes which 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 The methods of doing this are:

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 on the cell. The cursor is placed at the left of the cell, and as soon as you start to type the background color of the cell changes. If you double-click on 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 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 related to the selected object in the tree. If the object belongs to a provisioning policy, messages relating to the complete policy are shown. The list will be refreshed when the **Apply** action is executed or when a different object is selected in the tree.

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





Nr.	Severity	Description	Element
1		CPD9852E A Processor Limit has to be specified.	Policy "NEW"/Maximum Provisioning Scope
2		CPD9852E A Condition has to be specified.	Policy "NEW"/Rule "NEW"
3		CPD9849E CFC Name value is mandatory.	Policy "NEW"/Rule "NEW"/Provisioning Scope/Processor Limit #1
4		CPD9840W A MSU, zAAP, or zIIP limit greater than zero should be def...	Policy "NEW"/Rule "NEW"/Provisioning Scope/Processor Limit #1

Figure 8. 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 on the **Clear Connection Report** button.

The columns in this report show:

Time The time the message was generated

Severity The type of message. This can be:

Symbol **Meaning**



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



For warning messages. These messages are issued in situations that may prevent successful completion. You should check if the situation is OK or if you need to take corrective action.



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

An example connection report is:

Time	Severity	Description	Host Address
21.11.2007 18:31:21	⊗	CPO8053E No connection established to the defined host address	http://2.2.2.5388
21.11.2007 18:31:21	⊗	CPO8031E Unable to connect to CIM server.	http://2.2.2.5388

Figure 9. Connection report

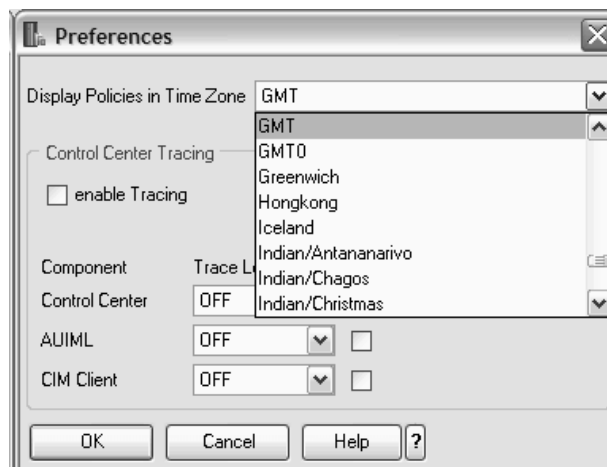
The menu bar

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

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

- 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 workspace.
- Save Configurations** Saves all domain configurations in the workspace.
- Save Policies** Saves all provisioning policies in the workspace.
- Save All** Saves all the above in the workspace.
- Refresh Workspace** Reloads all connection definitions, domain configurations and policies. Before the reload you are asked if you want to save your changes as these will otherwise be overwritten.
- Exit** Closes the Control Center. You will be prompted to save any changes before you exit.

The **Options** menu contains the **Preferences** dialog:



Here you may set the time zone and the trace settings for the Control Center:

Display Policies in Time Zone

The time zone specified here determines the offset with which times are displayed and entered in the **Time Conditions** panel. It affects the display of all policies. Click on 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.

Control Center Tracing

If you are advised by IBM service representatives to enable tracing for the Control Center, check the box **enable Tracing** and fill in the other details as advised. For normal operation the **enable Tracing** box should not be checked.

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

Welcome

This shows an introduction to the Control Center.

About Capacity Provisioning Control Center

This shows the version of the installed Control Center. This information will be required if you send a problem report.

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 client which interfaces between the Control Center and the Provisioning Manager

Starting the Control Center

To start the Control Center click on the IBM Capacity Provisioning Control Center on your desktop or in the IBM Capacity Provisioning program group. When the Control Center starts you will be asked which directory contains your workspace. The default is the directory you last used. (When you start the Control Center for the first time the default is the directory which was specified during installation.) You may have several workspace directories, for example one for each provisioning domain, but you can only work in 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. If the directory does not exist it will be created.

You also have the opportunity at this point to specify the time zone for which policies will be displayed.

The initial screen displayed is:

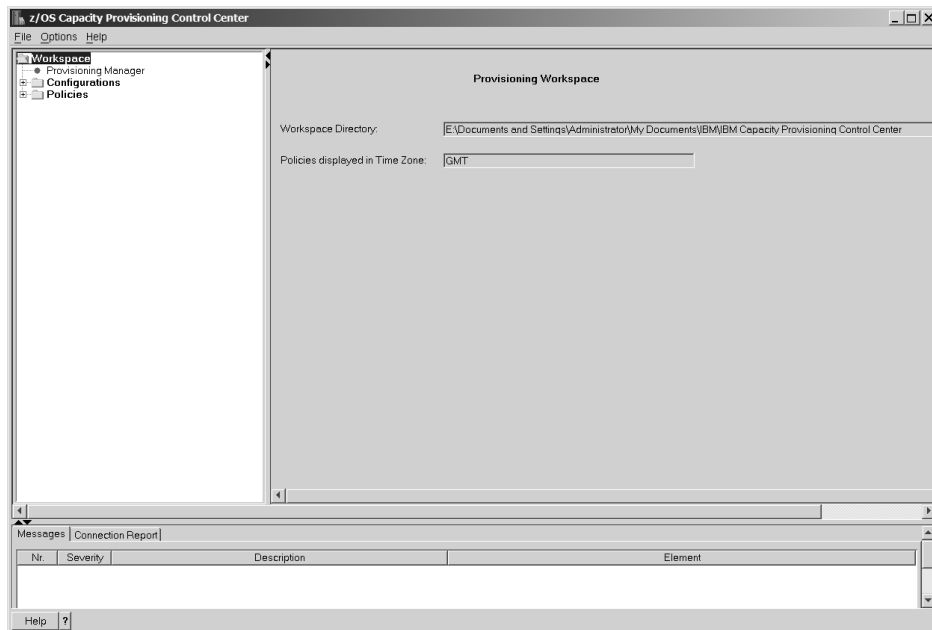


Figure 10. Workspace screen

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 monitors the domain and performs activation and deactivation requests for temporary capacity, based on your active policy and domain configuration. 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.

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 on **Provisioning Manager** in the tree view.
2. Click the **Add Connection** button. A new entry in the Connections table is created.
3. Click on the field in the **Host Address** column and type either the host name or the IP address of the system where the Provisioning Manager is running.
4. To change the default protocol select the arrow in the **Protocol** column. You may choose either HTTP or HTTPS protocol.

5. To change the default port click on 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** button to save the connection definitions in the workspace.

Here is an example showing a system with three host connections defined:

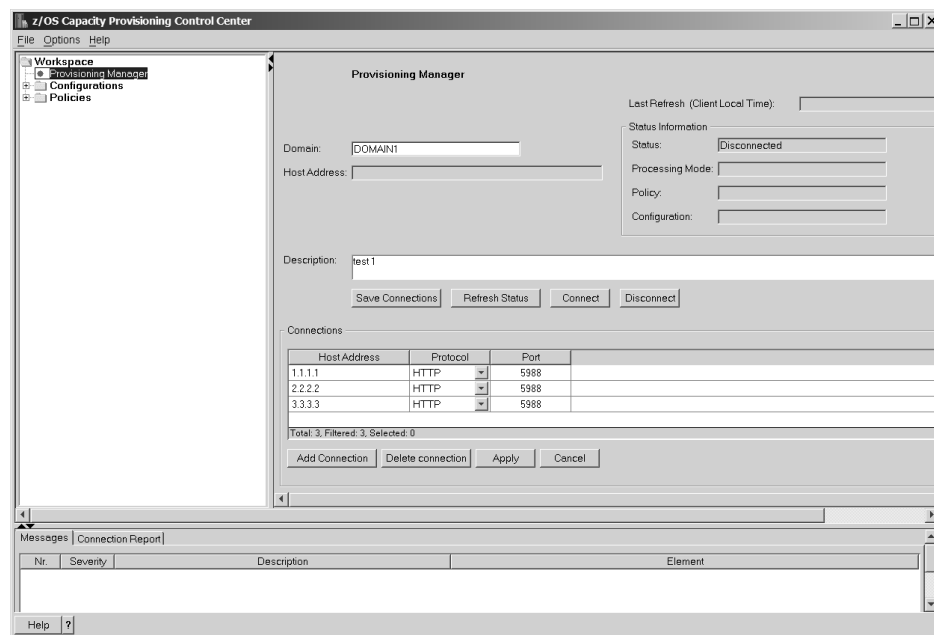


Figure 11. Provisioning Manager screen

It is possible to create more than one connection definition. This is necessary if the Provisioning Manager can be started on more than one system. Only one connection can be active at any time.

Working with the Provisioning Manager

To connect to the Provisioning Manager on a domain you must be a member of the Provisioning Manager query security group (refer to page 39), and if you want to install policies or domain configurations you must also be a member of the Provisioning Manager control security group. The steps to take to make a connection are:

1. Enter the name of the domain in the **Domain** field on the Provisioning Manager screen. This should be the name you used in Table 10 on page 34.
2. Click on the connection you want to use in the Connections table.
3. Click the **Connect** button. A panel asking for the login information is shown:

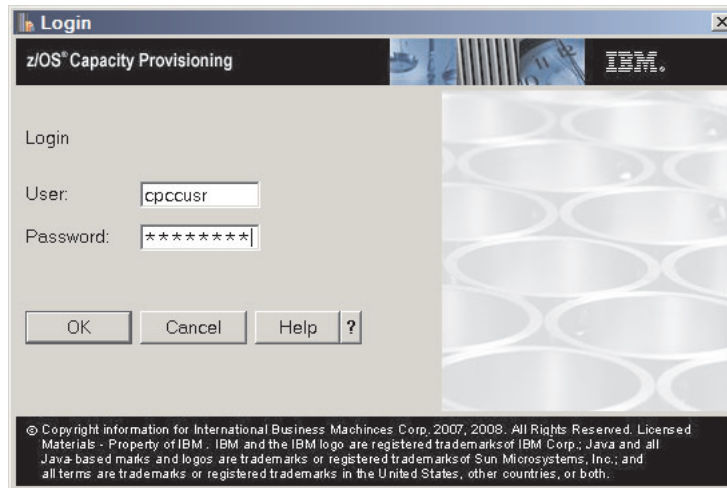


Figure 12. Login screen

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 defined in the Connections table and tries to connect to it using the specified protocol and port. If you are unable to connect you can try an alternative connection using another entry in the Connections table. If no connection can be established check the **Connection Report** in the information view for the cause. refer to page 59 for details.

The status of the connection between the Control Center and the Provisioning Manager is shown in the **Status Information** area of the Provisioning Manager screen. The **Status** field can display:

- 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.
- Started** The connection is established and the Provisioning Manager is running.
- Not active** The connection is established but the Provisioning Manager is not running.

When the status is **Started** you can install policies and domain configurations into the repositories of the domain, and further information is displayed in the other fields of the **Status Information**. The information in each field is:

Processing mode

The mode in which the Provisioning Manager is operating. The following modes are supported:

- Manual** The Provisioning Manager will not perform any activation or deactivation requests on its own.
- Analysis** The Provisioning Manager observes the systems and provides you with information about required additional resources.

Confirmation The Provisioning Manager proposes changes to the capacity settings of the CPCs and asks for confirmation.

Autonomic The Provisioning Manager analyzes the workload situation on the observed systems and autonomically adjusts the capacity settings of the CPCs as required.

For further information about these modes, refer to “Processing modes” on page 26.

Policy The name of the active policy used by the Provisioning Manager

Configuration

The name of the active domain configuration used by the Provisioning Manager

Note: The Provisioning Manager status information is not refreshed automatically. To update the status information click the **Refresh Status** button. The **Last Refresh** field will be updated to show the date and time the information was last gathered.

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

Switching to another domain

If you want to work on a different provisioning domain you should enter its name in the **Domain** field and press the **ENTER** key. If you are still connected to the Provisioning Manager of the current domain you will be asked if you want to switch to the new domain now. Selecting **YES** will close the existing connection.

The next time you start the Control Center the last domain worked on will be the new default.

Working with Domain Configurations

A domain configuration describes the managed CPCs and the observed systems in a domain. The Control Center is used to define domain configurations, and can also be used to install them. An installed domain configuration can be activated for the domain by the Provisioning Manager command SET DOMAIN described on page 119.

This section describes:

- How to create a new domain configuration
- How to define the set of CPCs where the Provisioning Manager may 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, which can be monitored by the Provisioning Manager, and a set of CPCs, which can be activated or deactivated. To create a domain configuration follow these steps:

1. Right-click on the **Configurations** folder in the tree view 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 will be

altered by the Control Center to make it unique. For information on valid names refer to “Naming conventions” on page 30. Note that characters must be entered in upper case.

4. Click **OK**. The new configuration is displayed. Since further steps are needed to complete the domain configuration there will be prompts in the **Messages** panel at the bottom of the screen to indicate the next steps you should take.
5. In the **Description** field you may enter a description of this configuration for your reference. To leave the description field using keystrokes type Ctrl + TAB.

The next steps are to define the observed systems and the controlled CPCs.

Defining the systems

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

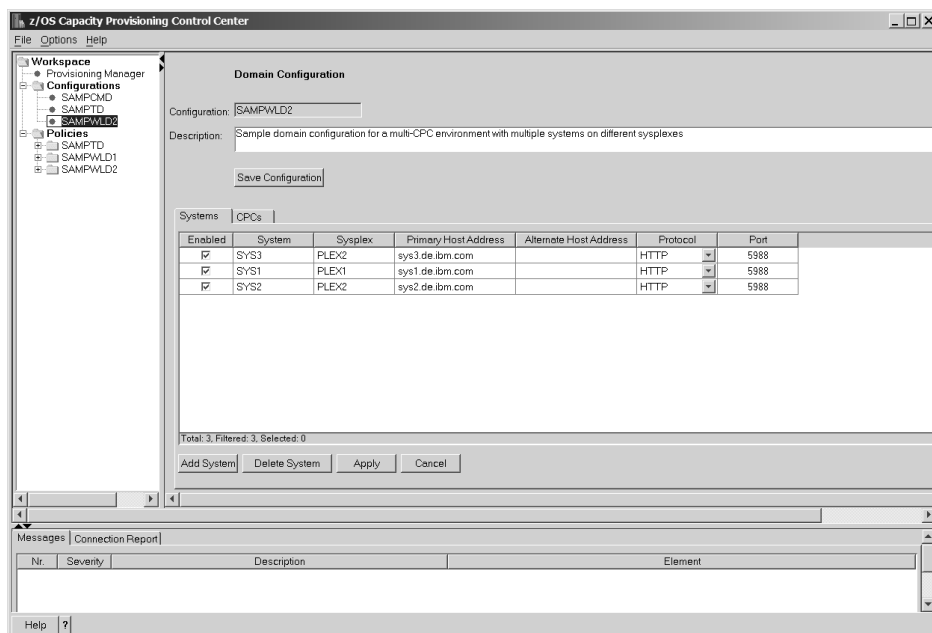


Figure 13. Domain configuration system definition screen

To define the systems perform the following steps:

1. Click the **Systems** tab in the details view of the domain configuration.
2. Click the **Add System** button. This creates a new entry in the systems table.
3. Click on the field in the **System** column and type the name of the z/OS system.
4. Click on the field in the **Sysplex** column and type the name of the sysplex to which this z/OS system belongs.
5. Click on the field in the **Primary Host Address** column and type either the host name or the IP address of this system.
6. If this system has an alternate address, to be used if the primary address is not working, click on the field in the **Alternate Host Address** column and 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 running on the z/OS system is not correct click on the arrow in the **Protocol** column and choose the protocol

to use. To open the protocol combo box 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 on the field in the **Port** column and type the number of the port the CIM server is listening to.
9. Systems are enabled by default. If you want to disable the system click the checkbox in the **Enabled** column to clear it. You can also enable or disable systems at runtime by using the Provisioning Manager commands “ENABLE CONFIGURATION” on page 111 and “DISABLE CONFIGURATION” on page 109.
10. Click the **Apply** button. The Control Center then checks the specifications for errors. If any errors are found they will be reported in the **Messages** section 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 from **Add System**.

Defining the CPCs

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

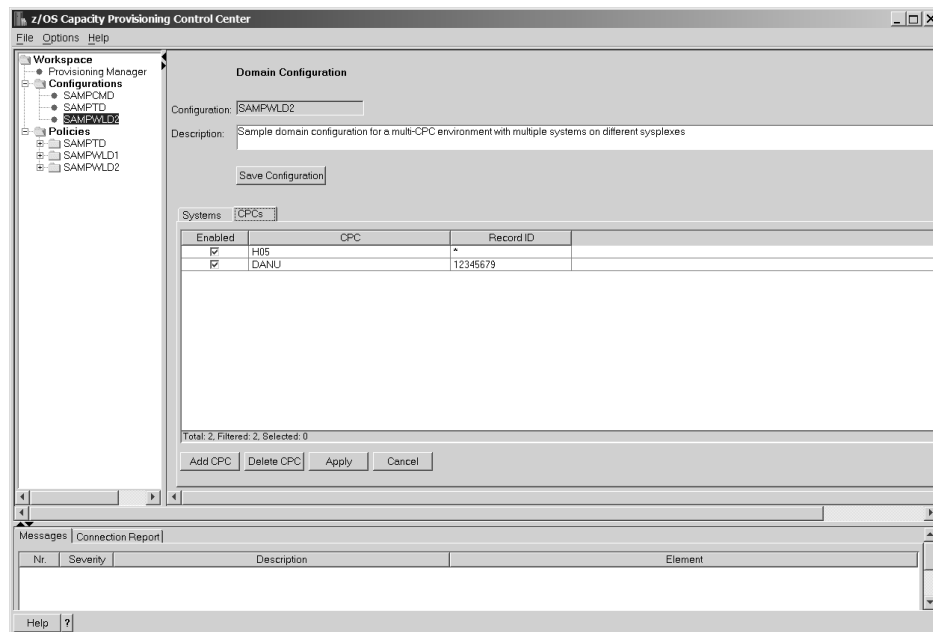


Figure 14. Domain configuration CPC definition screen

To define the CPCs perform the following steps:

1. Click the **CPCs** tab in the details view of the domain configuration.
2. Click the **Add CPC** button. This creates a new entry in the CPCs table.
3. Click on 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.
4. If you want the Provisioning Manager to use a specific On/Off CoD record, click on the field **Record ID** column and enter the identifier of the record describing 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 then find the record. Note that if you specify an asterisk (*) and you have multiple On/Off CoD records, the Provisioning Manager will select an arbitrary one.

5. CPCs are enabled by default. To disable the CPC click the checkbox in the **Enabled** column to clear it. You can also enable or disable CPCs at runtime using the Provisioning Manager commands "ENABLE CONFIGURATION" on page 111 and "DISABLE CONFIGURATION" on page 109.
6. Click the **Apply** button. The Control Center then checks the specifications for errors. If any errors are found they will be 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 from **Add CPC**.

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

Installing and activating a domain configuration

If you want to activate the domain configuration when it is complete and error free you must install it into the domain configuration repository of the Provisioning Manager. To install a domain configuration using the Control Center do the following:

1. Click on **Provisioning Manager** in the tree view and check that the Status field shows **Started**.
2. If it is not connected click the **Connect** button and check that the status changes to **Started**.
3. Right-click on the name of the domain configuration in the tree view.
4. Select **Install**.

To activate a domain configuration do the following:

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 further information refer to "SET DOMAIN" on page 119.

Working with provisioning policies

A provisioning policy is used by the Provisioning Manager to determine when and under which conditions additional capacity may be activated and deactivated. You can define provisioning policies using the Control Center. A completed provisioning policy can be installed and activated for the domain using the Provisioning Manager command "ENABLE POLICY" on page 111. This chapter describes:

- 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 which define the time periods in which additional capacity can be activated and the work which can trigger the activation of this capacity. It also contains a logical processor scope, which defines the z/OS systems where the number of logical processors can be changed and a maximum provisioning scope which places restrictions on the resources which can be activated.

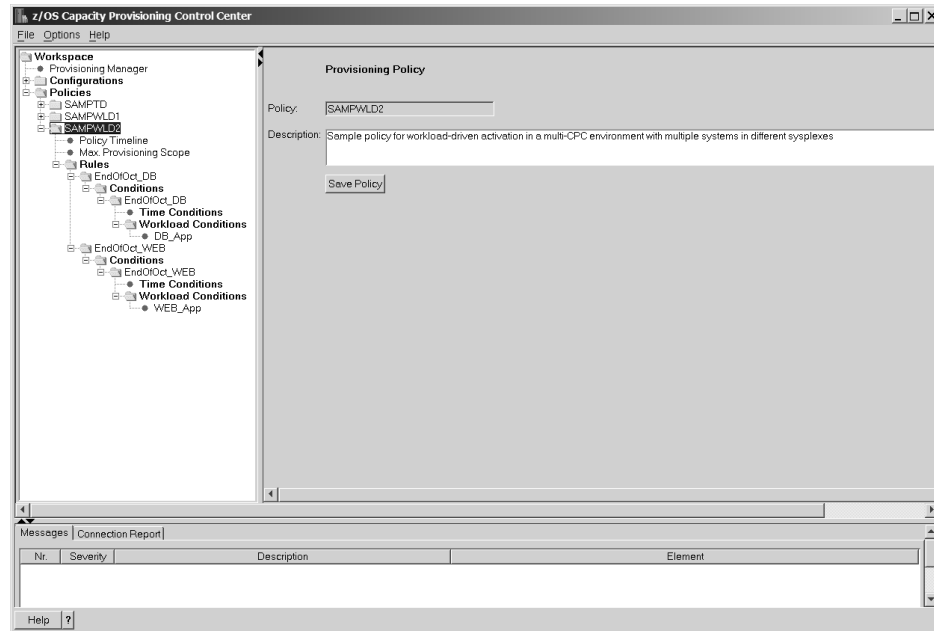


Figure 15. Provisioning policy screen

To create a provisioning policy do the following:

1. Right-click on the **Policies** folder in the tree view of the Control Center.
2. Select **New Policy...**
3. Enter a name for the new policy. If a policy with this name already exists in the workspace the name of the new policy will be altered by the Control Center to make it unique. For information on valid names refer to “Naming conventions” on page 30. Note that characters must be entered in upper case.
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. Since further steps are needed to complete the policy there will be prompts in the **Messages** panel at the bottom of the screen to indicate the next steps you should take.
5. In the **Description** field you may 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, which defines the z/OS systems where the number of logical processors can be changed. For each system you can either specify the maximum number of processors that may be online or specify that the limit of the LPAR definition applies. Regardless of

whether the logical processors were configured online by the Provisioning Manager or not, the Provisioning Manager may not configure additional processors online, when this limit is reached.

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

The following resources are controlled by the Logical Processor Scope:

- The number of Central Processors (CPs)
- The number of Application Assist Processors (zAAPs)
- The number of 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. Figure 16 shows the Logical Processor Scope panel:

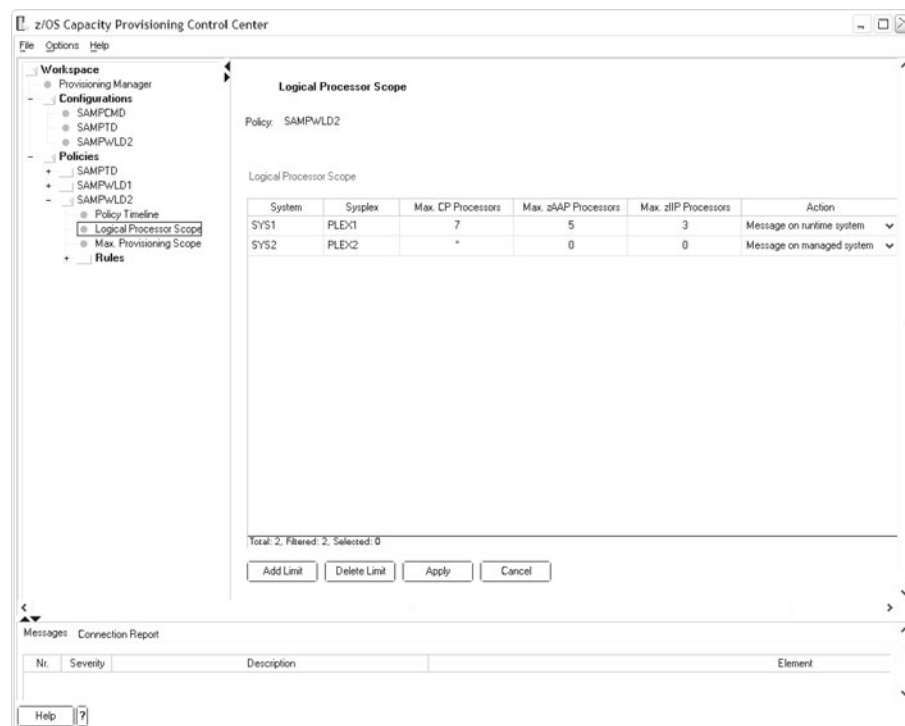


Figure 16. Logical processor scope screen

To define the Logical Processor Scope for your provisioning policy do the following:

1. In the tree view click on '+' to the left of the name of the policy for which you want to specify the logical processor scope.
2. Click on 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 in the Logical Processor Scope table is created. This entry contains the default values for the additional limit.

4. Click on the field in the **System** column and type the name of the z/OS system. For information on valid names, refer to “Naming conventions” on page 30.
5. Click on the field in the **Sysplex** column and type the name of the sysplex to which this z/OS system belongs.
6. If you want to specify a limit for the number of logical CP processors, click on the field in the **Max. CP Processors** column and type the maximum number of processors that may be online. An asterisk (“*”) designates a specification of as many logical processors as allowed by the z/OS and LPAR configuration.
7. If you want to specify a limit for the number of logical zAAP processors, click on the field in the **Max. zAAP Processors** column and type the maximum number of processors that may be online. An asterisk (“*”) designates a specification of as many logical processors as allowed by the z/OS and LPAR configuration.
8. If you want to specify a limit for the number of zIIP processors, click on the field in the **Max. zIIP Processors** column and type the maximum number of processors that may be online. An asterisk (“*”) designates a specification of as many logical processors as allowed by the z/OS and LPAR configuration.
9. Per default the Provisioning Manager sends messages to the system where the Provisioning Manager runs. To change this, select the arrow in the **Action** column. You may choose to 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 which defines the maximum number of additional resources that, at any point in time, may be activated on behalf of all contained rules. Only resources which are activated through a Capacity Provisioning policy are counted to this limit. Resources which are activated manually, either using Provisioning Manager commands or using the interfaces available at the HMC, are not managed by the Provisioning Manager.

The resources controlled by the Maximum Provisioning Scope are:

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

The Maximum Provisioning Scope limits how much additional capacity can be activated for each CPC. You cannot define two different limits for any one CPC in the same Maximum Provisioning Scope.

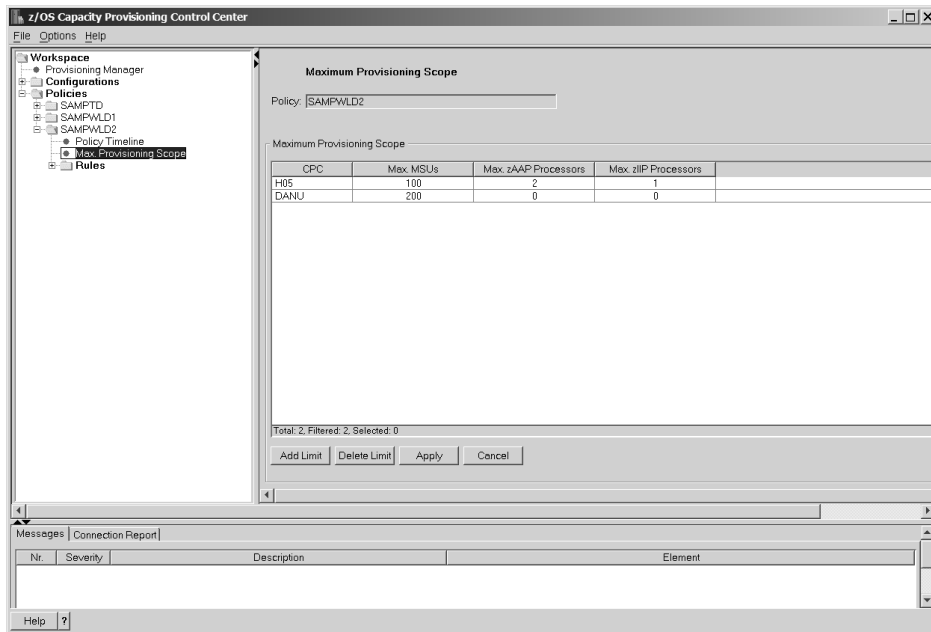


Figure 17. Maximum provisioning scope screen

To define the Maximum Provisioning Scope for your provisioning policy do the following:

1. In the tree view click on the '+' to the left of the name of the policy for which want to specify the maximum provisioning scope.
2. Click on **Max. Provisioning Scope**. The Maximum Provisioning Scope panel is shown in the details view of the Control Center.
3. Click the **Add Limit** button to define a provisioning limit for a processor complex. A new entry in the Maximum Provisioning Scope table is created.
4. Click on 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. If you want to allow the Provisioning Manager to activate additional general purpose capacity click on the field in the **Max. MSUs** column and type the maximum amount of MSUs to be activated.
6. If you want to allow the Provisioning Manager to activate additional zAAP processors click on the field in the **Max. zAAP Processors** column and type the maximum number of processors to be activated.
7. If you want to allow the Provisioning Manager to activate additional zIIP processors click on the field in the **Max. zIIP Processors** column and type the maximum number of processors to be activated.
8. Click the **Apply** button. The Control Center checks that the specifications are error free.

Note: At least one processor limit must be specified, and each limit must define at least one type of capacity.

9. If you want to add a provisioning limit for another processor complex repeat the steps from **Add Limit**.

Creating provisioning rules

A provisioning rule contains a provisioning scope and provisioning conditions. The provisioning scope restricts the capacity that may 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 do the following:

1. Right-click on **Rules** in the tree view of the policy.
2. Select **New Rule...**
3. Enter the name of the new rule. If a rule with this name already exists in the policy the name of the new rule will be altered by the Control Center to make it unique. For information on valid names refer to “Naming conventions” on page 30.
4. Click **OK**. The new rule is created and a **Conditions** folder is created under it in the tree view.
5. In the **Description** field you may 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** checkbox to clear it. If the rule is disabled the Provisioning Manager will 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 111 and “DISABLE POLICY” on page 109.

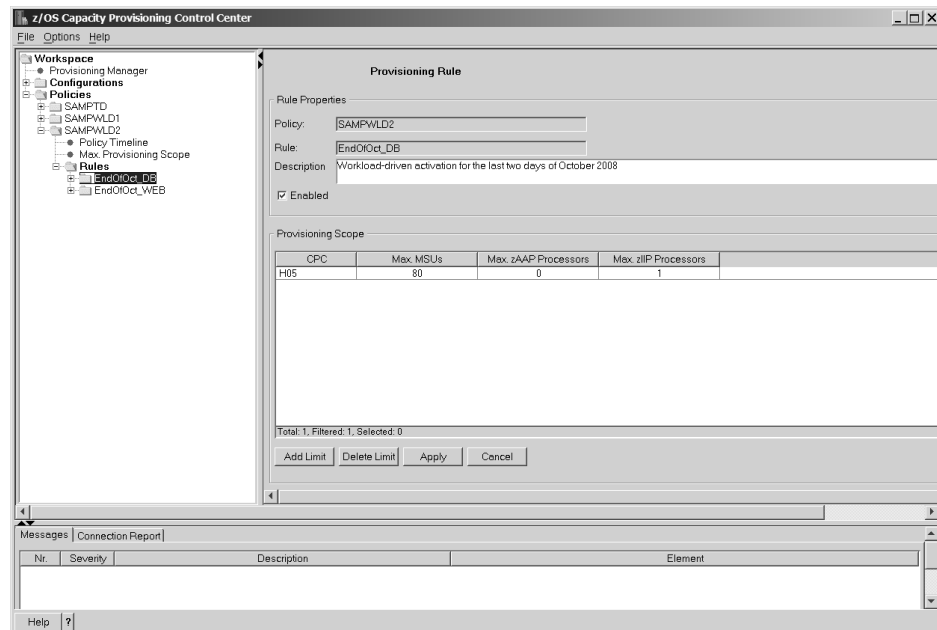


Figure 18. Provisioning rule screen

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 may be activated through 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 should be defined in the maximum provisioning scope. If they are not additional capacity will not be 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 cause activation of additional capacity and the conditions under which that work can trigger the activation of additional capacity.

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

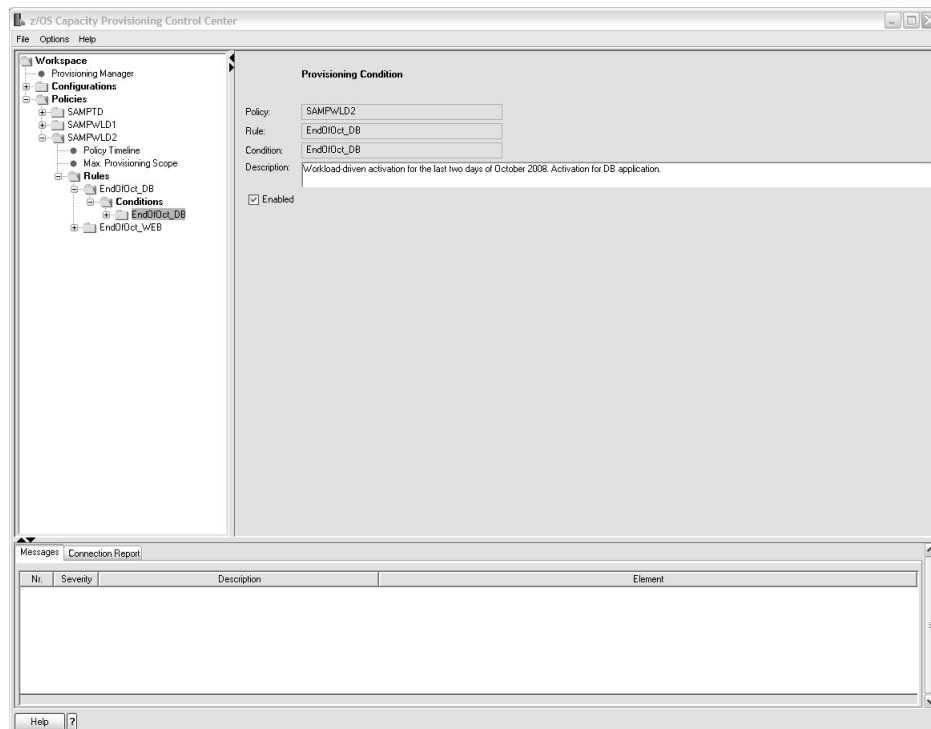


Figure 19. Provisioning condition screen

To specify a provisioning condition do the following:

1. In the tree view click on the '+' 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 will be altered by the Control Center to make it unique. For information on valid names refer to “Naming conventions” on page 30.
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 view.
6. Conditions are enabled by default. If you want to disable the condition click the **Enabled** checkbox to clear it. If the condition is disabled, or the enclosing rule is disabled, the Provisioning Manager will not consider it for triggering activation or deactivation of additional resources. You can also enable or disable conditions at runtime by using the Provisioning Manager commands “ENABLE POLICY” on page 111 and “DISABLE POLICY” on page 109.
7. In the **Description** field you may 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 a period 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 using the time zone displayed in the field **Policy displayed in Time Zone**. The time zone can be changed using the **Options** menu as described in “The menu bar” on page 60. A change to this affects the display of all policies. The actual date and time values are stored in the workspace as Coordinated Universal Time (UTC).

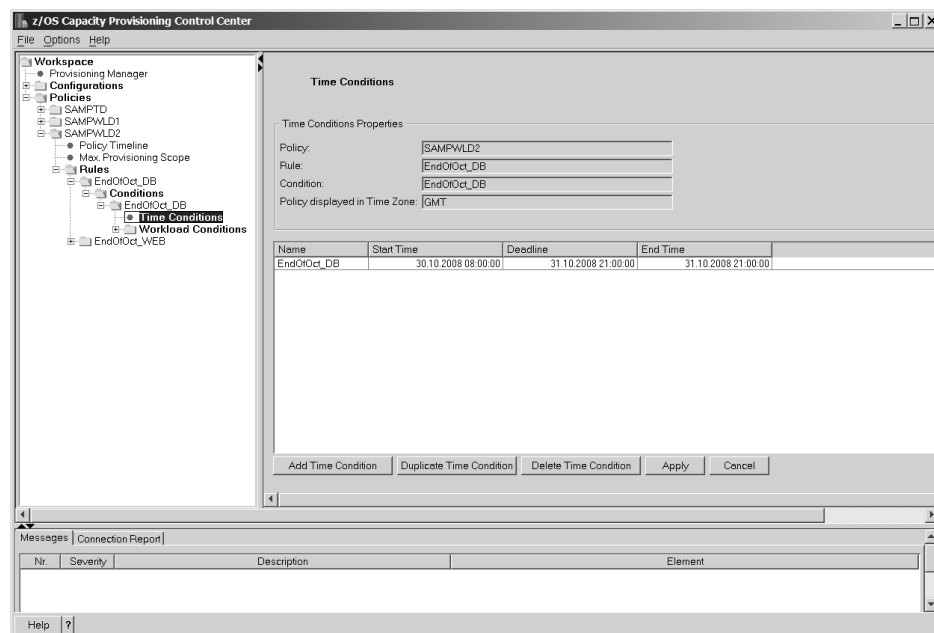


Figure 20. Time condition screen

To specify a time condition do the following:

1. In the tree view click on the '+' to the left of the name of the condition to which you want to add a time condition.
2. Click on **Time Conditions**.
3. Click the **Add Time Condition** button. A new row is added to the table where you can specify the new time condition.
4. Click on the field in the **Name** column and type a name for the new time condition. If a condition with this name already exists in the policy the name of the new time condition will be altered by the Control Center to make it unique. For information on valid names refer to "Naming conventions" on page 30.
5. Click on the field in the **Start Time** column and enter the time for the provisioning period to begin.
6. Click on the field in the **Deadline** column and enter the latest time when activation of additional capacity is allowed. This must be after the **start time**.
7. Click on the field in the **End Time** column and enter the time for the Provisioning Manager to start deactivating the additional capacity. This must be on or after the **deadline**.
8. Click the **Apply** button. The Control Center then checks the specifications for errors. If any errors are found they will be reported in the **Messages** panel at the bottom of the screen.

You now have the option of defining 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, as restricted by the provisioning scope, will be activated. At the end time of the time condition any activated capacity will be deactivated.

Creating a workload condition: A workload condition defines work that is eligible to cause activation of additional capacity, and the conditions under which that work can trigger activation. The specification of eligible work follows the workload model of the z/OS Workload Manager (WLM).

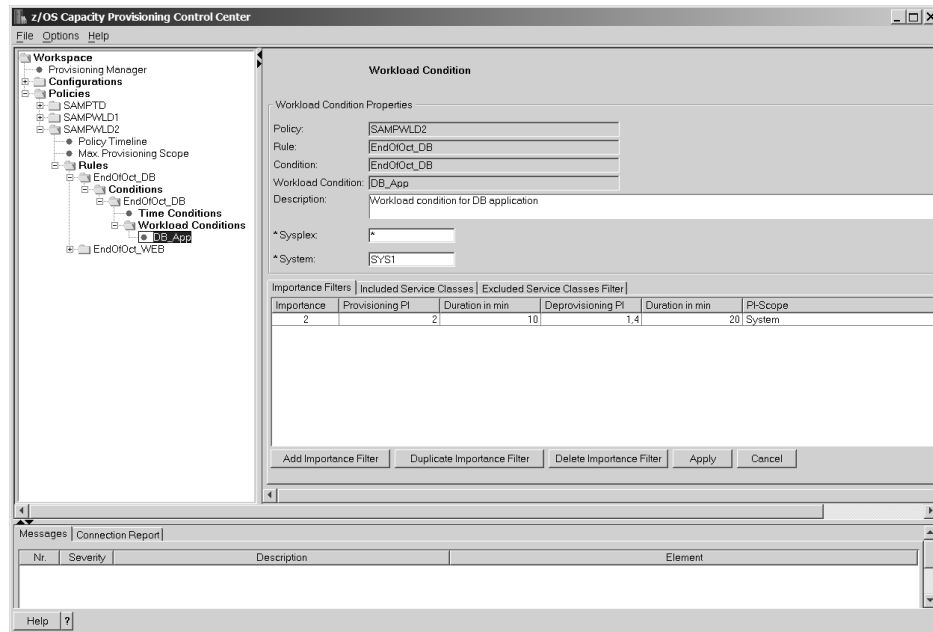


Figure 21. Workload condition screen

To create a workload condition do the following:

1. In the tree view right-click on **Workload Conditions**.
2. Select **New Workload Condition...**
3. Enter the name of the new workload condition. If a condition with this name already exists in the provisioning policy the name of the new workload condition will be altered by the Control Center to make it unique. For information on valid names refer to “Naming conventions” on page 30.
4. Click **OK**. The new workload condition is displayed. Since further steps are needed to complete the workload condition there will be prompts in the **Messages** panel at the bottom of the screen to indicate the next steps you should take.
5. In the **Description** field you may 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 will be 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 will be 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 will be 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 can be used to identify potentially critical service class periods. For details refer to “Workload conditions” on page 18. The tabs are:

Importance Filters

This allows you 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

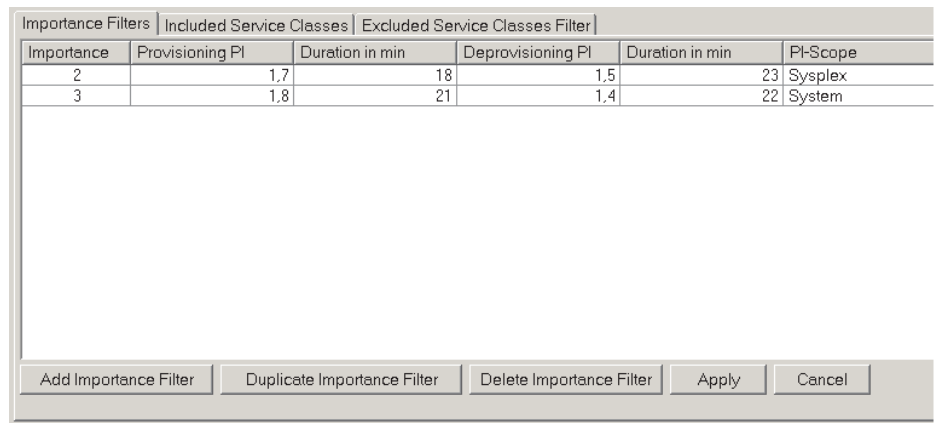
This allows you to specify service classes to be monitored in addition to any identified by importance filters, and the triggers for these.

Excluded Service Classes filter

This allows you 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 equal or higher than the specified value will be monitored by the Provisioning Manager for resource shortages. For each specified importance level additional provisioning criteria must be defined.



Importance	Provisioning PI	Duration in min	Deprovisioning PI	Duration in min	PI-Scope
2	1.7	18	1.5	23	Sysplex
3	1.8	21	1.4	22	System

Figure 22. Importance filters screen

To specify an importance filter do the following:

1. In the tree view of the Control Center click on 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 in the Importance Filters table is created containing the default values for an importance filter. All fields of an importance filter are required. If any of the defaults are not suitable correct them as follows:
 - Click on the field in the **Importance** column to change it. Service class periods with the specified importance level or higher will be observed.
 - Click on the field in the **Provisioning PI** column to change it. If the performance index of a service class period is equal or higher than the specified value the Provisioning Manager considers the service class period to be suffering.

- Click on the field in the first **Duration in min** column to change it. This is the duration in minutes a service class period has to exceed the provisioning PI before the Provisioning Manager considers the service class period to be suffering.
 - Click on the field in the **Deprovisioning PI** column to change it. If the performance index of a service class period is lower than the specified value it is not considered to be suffering. The deprovisioning PI must be at least 0.2 less than the provisioning PI limit, and must be not less than 1.1.
 - Click on the field in the second **Duration in min** column to change it. This is the duration in minutes the PI of the selected service classes must be lower than the specified deprovisioning PI for it to be considered no longer suffering. It must have a value between 5 and 1440 minutes.
 - Click on the field in the **PI-Scope** column to change it. This indicates which PI the other criteria apply to. The possible values are **System** and **Sysplex**. The default is **System**.
4. If you want to add an additional importance filter proceed from the step **Add Importance Filter**.
 5. Click the **Apply** button. The Control Center then checks the specifications for errors. If any errors are found they will be reported in the **Messages** section at the bottom of the screen.

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

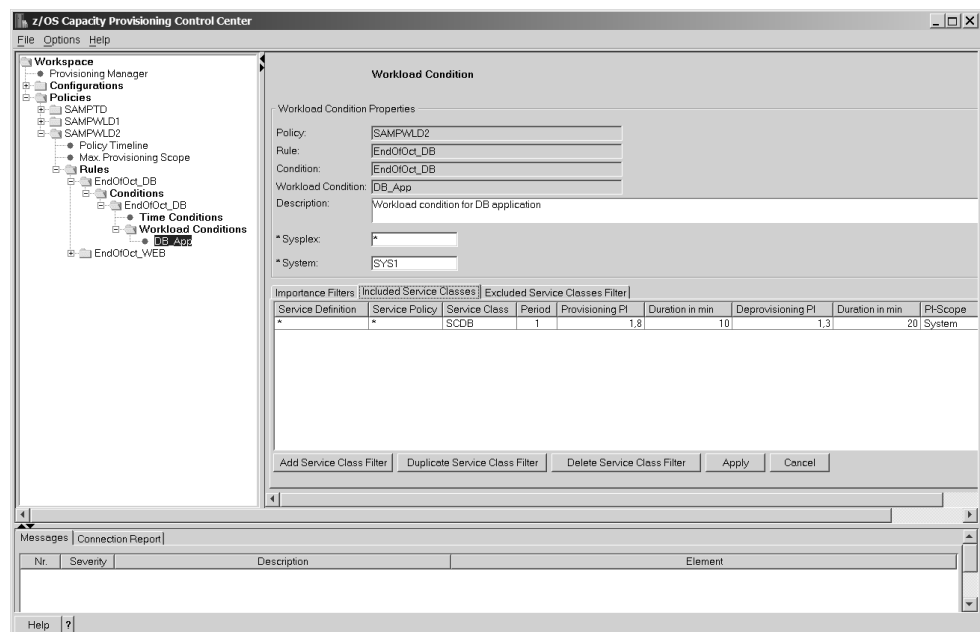


Figure 23. Included service class screen

To add a service class on the **Included Service Classes** panel do the following:

1. Click the **Included Service Classes** tab.

2. Click the **Add Service Class Filter** button. A new entry in the included service classes table is created containing the default values for the additional provisioning criteria. All fields of a service class filter are required.
 - Click on the field in the **Service Definition** column and specify the name of the WLM service definition. To specify all service definitions insert an asterisk (*).
 - Click on the field in the **Service Policy** column and specify the name of the WLM service policy. To specify all service policies insert an asterisk (*).
 - Click on the field in the **Service Class** column and 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:

- Click on the field in the **Period** column and specify the number of the highest period of the service class that should be considered. All periods with a period number lower than or equal to this are considered.
 - Click on the field in the **Provisioning PI** column and insert a value between 1.3 and 10. If the performance index of a service class period is equal to or higher than this value the Provisioning Manager considers the service class period to be suffering.
 - Click on the field in the first **Duration in min** column to change it. This is the duration in minutes a service class period has to exceed the provisioning PI for the Provisioning Manager to consider it to be suffering.
 - Click on the field in the **Deprovisioning PI** column and insert a value between 1.1 and 9.8. If the performance index of a service class period is equal to or lower than the specified value the Provisioning Manager considers the service class period not to be suffering.
 - Click on the field in the second **Duration in min** column to change it. This is the duration in minutes a service class period has to be lower than the provisioning PI for the Provisioning Manager to consider it to be no longer suffering.
 - Click on the field in the **PI-Scope** column to change it. This 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 an additional service class proceed from the step **Add Service Class Filter**.
 4. Click the **Apply** button. The Control Center then checks the specifications for errors. If any errors are found they will be 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. It is used to exclude selected service classes which would otherwise be included by an importance filter. The service classes listed on the **Excluded Service Classes Filter** panel cannot trigger provisioning even if they match the importance filters or the included service classes criteria.

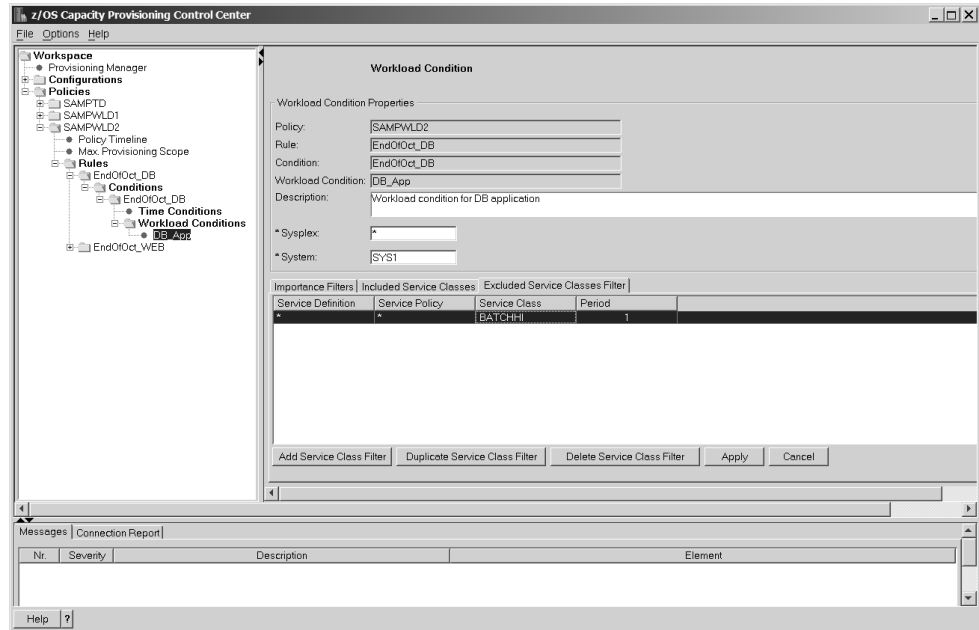


Figure 24. Excluded service class screen

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

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

- Click on the field in the **Period** column and specify the number of the maximum period of the service class which shall not be considered for provisioning. All periods with a number equal to or higher than this are not considered.
3. If you want to exclude additional service classes repeat from the step **Add Service Class Filter**.
 4. Click the **Apply** button. The Control Center then checks the specifications for errors. If any errors are found they will be reported in the **Messages** panel at the bottom of the screen.

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

Installing and activating a provisioning policy

If you want to activate the provisioning policy when it is complete and error free you must install it into the provisioning policy repository of the domain. To install a provisioning policy using the Control Center do the following:

1. Click on **Provisioning Manager** in the tree view and check that the Status field shows **Connected**.
2. If it is not connected click the **Connect** button and check that the status changes to **Connected**.
3. Right-click on the name of the provisioning policy in the tree view.
4. Select **Install**.

To activate a provisioning policy do the following:

1. Log on to the host where the Provisioning Manager is running.
2. Issue the following Provisioning Manager command:

```
SET DOMAIN POL=policy_name
```

For further information refer to “SET DOMAIN” on page 119.

Displaying the policy timeline

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

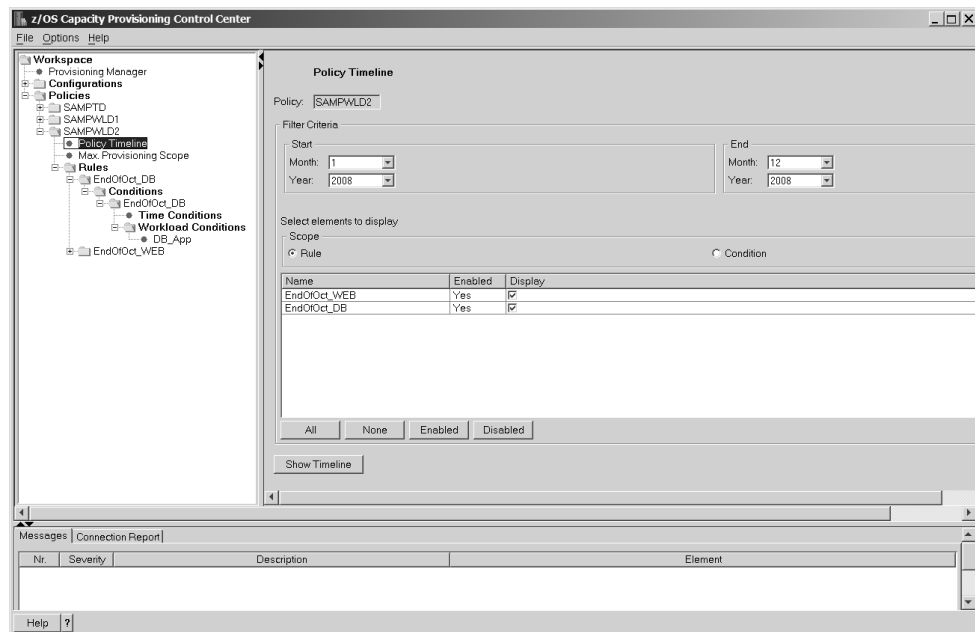


Figure 25. Select timeline to display screen

The procedure for displaying the timeline of a policy is as follows:

1. Select the start and end dates to choose the time period for which you want to see the possible activations. The only years available are those for which time conditions exist in the selected policy.
2. Click on one of the radio buttons to select elements to display from the rules of the policy or from the conditions of the policy.

3. 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 deselect groups of entries:

All All rules or conditions are to be displayed.

None All rules or conditions are deselected and none are displayed.

Enabled All enabled rules or conditions are to be displayed.

Disabled All disabled rules or conditions are to be displayed.

4. When you have selected the rules or conditions that you want to include click the **Show Timeline** button.

A window opens showing the selected time period and the included time conditions of the selected rules or conditions. An example of this is:

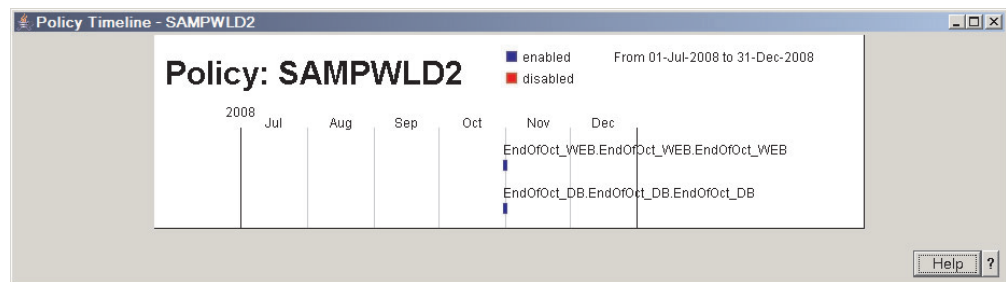


Figure 26. Policy timeline screen

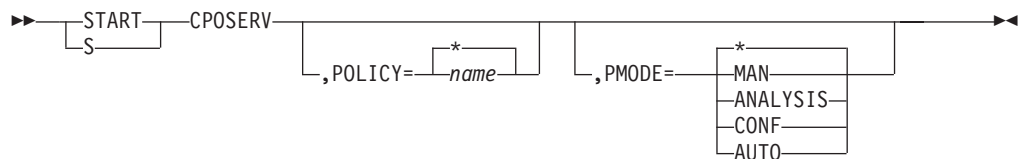
Chapter 5. Controlling the Provisioning Manager

The Provisioning Manager is the server component in a Capacity Provisioning domain which 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 can use the MVS start command to start the program.

Syntax



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 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 policy that was last active in the provisioning domain will be used and no policy will be retrieved from the policy repository. `POLICY=*` is the default of this parameter.

PMODE=*mode*

specifies the initial processing mode of 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

If the Provisioning Manager cannot activate the processing mode it will stop immediately.

You can specify an asterisk (*) instead of a processing mode. In this case the processing mode that was last active in the provisioning domain will be used. `PMODE=*` is the default of this parameter.

If you start the Provisioning Manager for the first time without specifying start parameters it will start 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, containing no CPCs and no systems.

For further information on how to activate a new policy, a new domain configuration or a new processing mode refer to "SET DOMAIN" on page 119.

Provisioning Manager commands

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

The syntax to issue Provisioning Manager commands is:

```
➤—MODIFY—CPOSERV—,—APPL=Provisioning Manager command—➤
   └──┬──┘
```

For information about the Provisioning Manager commands refer to Chapter 8, "Provisioning Manager command reference," on page 103.

Stopping the Provisioning Manager

Two commands can be used to end Provisioning Manager processing:

- The Provisioning Manager stop manager command. For details refer to page 122.
- The MVS STOP command. This is equivalent to the Provisioning Manager command stop manager mode=normal. The format of the MVS command is:

```
➤—STOP—CPOSERV—➤
   └──┬──┘
```

After the Provisioning Manager has been requested to stop 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 can continue to manage resources from the point where it was stopped. This allows for short breaks, for example in case you need to transfer the Provisioning Manager to another system. If you expect a longer interruption to processing you are recommended to 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 necessary 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 will assume that no additional capacity is needed on behalf of workload conditions.

Temporary capacity that has been activated by the Provisioning Manager is not automatically deactivated when the Provisioning Manager stops. If temporary resources must be deactivated you should do this manually before issuing the stop

command. To find out which temporary resources are currently active you can issue a report configuration command (refer to page 114). After the Provisioning Manager has stopped, temporary resources can only be deactivated 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 if there is any need to activate or deactivate temporary resources. The Provisioning Manager proposes a change in the activation level and issues a message asking 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 will not be considered again for this type of action (activation or deactivation) for a period of a few hours.

Until you respond the Provisioning Manager continues to check the policy and the workload to see if the proposed action is still necessary. If the action is no longer necessary then the outstanding message is cancelled. If another action is proposed instead a new message is issued. While the Provisioning Manager is waiting for the answer you may use report commands to help you decide on the response.

In some situations there may 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 will be cancelled.

Chapter 6. Working with reports

You can request various reports of 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 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 `MM/DD/YYYY HH:MM:SS`), for example:

```
CP01008I 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. The following sections 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 the information will be truncated or missing. In this case you should direct the report to a file to get the complete information.

The domain report

To create a domain report issue a `REPORT DOMAIN` command. Refer to page 114 for the syntax of this command. The report contains information about the current setup of the domain managed by the Provisioning Manager. This information is (in the following order):

- 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 as you have 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 as you have 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, the domain configuration and the policy may have occurred in a previous run of the Provisioning Manager and may 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. Refer to page 116 for the syntax of this command. The report contains information about the active policy and its status. Indentation is used in this report to group related items together, similar to the list below. The information reported is:

- The name of the active policy, and its enabled/disabled status. A policy is disabled if the Provisioning Manager is running in processing mode MANUAL. 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. One line is displayed for each entry. This contains the CPC name and the maximum resources which can be activated by all provisioning rules.
- The provisioning rules contained in the policy. The information displayed about each rule is:
 - 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. This contains the CPC name and the resources 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 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 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 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. For each time condition the following information is given:
 - The time condition name and status. The status is one of the following:
 - 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, refer to page 17.

Since time conditions cannot be enabled or disabled, the status reflects the enabled/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 condition. These times are reported in UTC.

An example of a policy report follows:

```
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 MSUs, 3 zAAPs, 3 zIIPs
Rule SampleRule is enabled (default enabled)
Provisioning scope:
  Limit for CPC SAMPCPC is 30 MSUs, 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
```

The domain configuration report

To create a domain configuration report issue a REPORT CONFIGURATION command. Refer to page 114 for the syntax of this command. 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 together, similar to the list below. The information reported is:

- The name of the active domain configuration and its enabled/disabled status. A domain configuration is disabled if the Provisioning Manger is running in processing mode MANUAL. In all other processing modes the domain configuration is enabled.
- Information about the CPCs defined in the domain configuration. For each CPC this contains:
 - The name of the CPC, its record ID, its current enabled/disabled status and the default status defined in the domain configuration when it was activated.
 - Runtime information about the CPC:
 - The status of the CPC at the SE or HMC. This status will be:

not correlated

The CPC has not yet been detected by the SE or HMC. It cannot be used to activate temporary capacity.

correlated

The CPC has been detected by the SE or HMC but detailed information about it is not yet available to the Provisioning Manager. It cannot be used at present to activate temporary capacity.

matched

The CPC has been detected by the SE or HMC and detailed information about it is available. Temporary capacity may be activated on it if a valid record exists.

- The CPC hardware type and model. If the CPC is not supported for capacity management this 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 MSUs, number of zAAPs and number of zIIPs.
 - The permanent model and capacity in MSUs.
 - If the record ID in the domain configuration is defined as "*", the record ID used by the Provisioning Manager for managing temporary capacity is displayed.
 - If a usable record was detected:
 - The record ID used by the Provisioning Manager for managing temporary capacity.
 - The remaining capacity: either the number of processors available which 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: how many resources are currently active for the record. The resources are displayed in MSUs followed by the number of additional processors, the number of increases in the capacity settings, 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. This can be, for example, the record has expired or the configuration of the CPC does not allow commands to perform the temporary capacity change.
- Information about the systems in the domain configuration. For each system this contains:
 - The operating system name, the name of the sysplex it belongs to, its enabled/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 the system is disabled. If the domain configuration is enabled and the system is enabled and if both host addresses are defined the system may be not observed. This 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 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 has been suspended after successfully establishing a connection. The Provisioning Manager tries to reestablish the connection.

unavailable

The connection to the system has been broken. The Provisioning Manager will try 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 this is reported as follows:
 - A note indicating the information is unavailable
 - A message indicating which initialization step has not yet finished or could not finish successfully. If the step could not finish successfully a corresponding message was sent to the console at the first time of this occurrence. This message is one of the following:

The system is not identified

The name of the system and/or the name of the sysplex has not yet been retrieved.

The system is not correlated

The Provisioning Manager has not yet detected if the name of the system and the name of the sysplex this system belongs to match the names in the domain configuration. Both names are reported in the message.

The operating system version 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 on which 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 if the CPC the system is running on is defined in the domain configuration.

The information for retrieving metric values is not available

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 successfully be initialized there may be other conditions which prevent further processing. If so the condition that is not fulfilled is reported. This condition will be one of the following:

The system is not the defined system

The name of the system and/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 system version 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 MSUs, 2 ZAAPs, and 3 zIIPs
Permanent model is 704 with 281 MSUs
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. Refer to page 117 for the syntax of this command. The report contains information about the currently observed workload. The information reported is:

- The number of systems on which workload may be observed.
- For each system that is observed:
 - The name of the operating 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 observed on the system:
 - The service class period name and number, 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 performance index last measured 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 can occur when the workload

running in the observed service class has been displaced. To show how long the performance index has been at this level the line also contains the last time when 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) this lists the service class periods that are suffering. Furthermore, the detailed workload report lists the types of temporary resources needed for a service class that is suffering, or, optionally the reason why an additional temporary resource is not needed.

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 outnumbered amount of physical CPs
```

The activity report

To create an activity report issue a REPORT ACTIVITY command. Refer to page 113 for the syntax of this command. The report contains information about the activation and deactivation of temporary resources 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 display is truncated the oldest data is not displayed. Note that activation and deactivation are processed asynchronously by the CPC. The activity report does not show whether the commands completed successfully.

The information reported is:

- A summary line showing the time period reported and the number of activities performed by the Provisioning Manager.
- For each of these activities the details follow:
 - 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 suffering: the operating system and the sysplex it belongs to.
 - The service class period that was suffering: the active WLM service definition and policy name and the service class name and number.

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. Refer to page 116 for the syntax of this command. The report contains information about the current trace level settings and trace file settings:

- A header "Trace level settings", followed by:
 - The value for the default level
 - The values for each individual trace component
- A header "Trace file settings", followed by:
 - The prefix of the trace file name. The full filename is constructed from this by appending a dot (.) and the sequence number of the trace, starting from 0 (zero). For example the first trace file could be /tmp/cpotrace_20080127134147469.log.0.
 - The maximum size and number of trace files. When the size limit is reached a new file is started. When the maximum number is reached the sequence numbers begins again at 0 and the old files are reused.

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. Refer to page 115 for the syntax of this command. The report contains information about the current log and log file settings:

- A header line showing the configured destination for log files
- A line for each log stating whether writing data for this log is currently active

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 only reports the status information currently in memory, and does not keep a history. If you require a history you must organize this yourself by regularly requesting the reports you are interested in. You should specify a unique file name for each report as the Provisioning Manager overwrites the content of a file if it already exists.

Chapter 7. Considerations for defining policies and domains

This chapter lists some points you should consider when 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 only considers a provisioning action 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.

As an example, an important business application may consist of multiple service classes that are defined as importance 2 and 3 in the WLM service definition. Somewhat simplified, the goal attainment of those service classes primarily depends on other work that may be classified as importance 1, SYSSTC or SYSTEM. When system resources such as processing capacity become constrained WLM will attempt to help the most important work first and assign less resources to other work. In this example resources will be taken from the service class periods of importance 3 first, and these in turn will show a higher (worse) PI.

It is best practice in WLM not to define too many service class periods as active at any point in time. The reason for this is to have a substantial service measurement in any period, so that WLM has sufficient sample data to go on. This 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. Furthermore, the number of transaction endings should be high enough to allow RMF to compute a performance index. At least one transaction ending per RMF MINTIME, and preferably more, are required.

You can only specify service class periods with importance 1 to 5. SYSTEM, SYSSTC, SYSSTC1 to SYSSTC5 and DISCRETIONARY work cannot trigger a provisioning action and will be ignored, if included. You are also recommended not to include any service classes associated with a resource group capacity maximum. If a service class is capped, Capacity Provisioning will avoid provisioning on behalf of it if possible.

You cannot use service class periods that are for transactions using WLM execution delay monitoring services; these are CICS and IMS transaction service class periods. You can use service classes that the servers are managed to, though.

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 the goal for the service class period is defined such that the goal is still achievable at times of peak demand – without additional capacity being active – then 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 would activate additional capacity when the PI of the respective service class period is consistently above the limit. The duration should be viewed relative to the RMF MINTIME, the default of which is 100 seconds. In general the duration should be greater than 3 minutes, to avoid a short term disturbance causing a provisioning action. It may 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 for some time to allow WLM to re-adjust. Such events are, for example, the activation of a new WLM service definition or policy, or a capacity change of the observed CPC.

Part 3. Reference

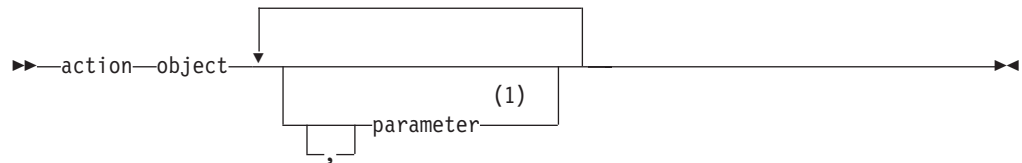
This part contains the Provisioning Manager command reference.

Chapter 8. Provisioning Manager command reference

This chapter describes the Provisioning Manager commands and their syntax. For information on how to pass commands to the Provisioning Manager, refer to page 86.

Introduction

The Provisioning Manager command syntax is based on the z/OS command syntax shown in the following diagram:



Notes:

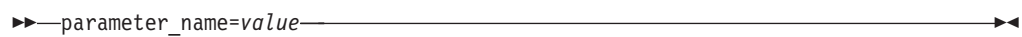
1 Parameters may be required, optional or nonexistent, depending on the specific action and object.

Refer to "How to read syntax diagrams" on page x for help in reading these diagrams.

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 form:

```
/* comment */
```

Parameters have the following form:



You may specify the parameters in any order. A value can be any sequence of characters. If special characters are needed, for example spaces or commas, the parameter value must be enclosed in single quotes (*'value'*). Within these single quotes any character is allowed. To specify an apostrophe (') within the parameter value, it must be enclosed in single quotes, 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 may be case-sensitive if they are not keywords. In this case the value must be enclosed in quotes.

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 (actions and objects) are listed below, together with a short form of the command (which may be used to save typing - note that the short forms are not abbreviations), and the page on which each command is described.

Table 15. Control commands

Command	Short form	Page
ACTIVATE RESOURCE	a r	105
DEACTIVATE RESOURCE	i r	108
DISABLE CONFIGURATION	d c	109
DISABLE POLICY	d p	109
ENABLE CONFIGURATION	e c	111
ENABLE POLICY	e p	111
RESET CONFIGURATION	t c	117
RESET POLICY	t p	118
SET DOMAIN	s d	119
STOP MANAGER	p m	122

Table 16. Status commands

Command	Short form	Page
LIST CONFIGURATION	l c	112
LIST POLICY	l p	113
REPORT ACTIVITY	r a	113
REPORT CONFIGURATION	r c	114
REPORT DOMAIN	r d	114
REPORT LOG	r l	115
REPORT POLICY	r p	116
REPORT TRACE	r t	116
REPORT WORKLOAD	r w	117

Table 17. Debug commands

Command	Short form	Page
ACTIVATE LOG	a l	104
DEACTIVATE LOG	i l	107
DUMP MANAGER	none	110
SET TRACE	s t	120
RESET TRACE	t t	118
WRITE LOG	w l	123

Commands

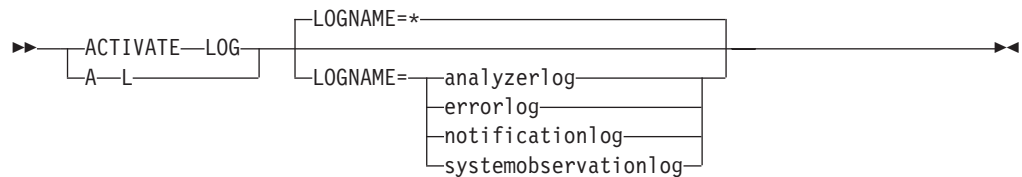
ACTIVATE LOG

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 then 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 33. You must ensure that there is sufficient space in the active location.

The data is written until the log is deactivated (see “DEACTIVATE LOG” on page 107) or the Provisioning Manager terminates. When the Provisioning Manager is started for the first time all logs have their default state. The default state for the error log is activated. For all other logs it is deactivated.

Note: This command should only be used if so instructed by IBM service personnel.

Syntax



Parameters

The command has the following parameter:

LOGNAME=*name*

The type of data to be recorded. This may be:

analyzerlog

workload analysis decisions.

errorlog

unexpected errors detected during processing.

notificationlog

communications with the Provisioning Manager.

systemobservationlog

monitored metrics from the observed systems.

You may also specify LOGNAME=* to indicate that writing should be activated for all logs. This 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 should be:

```
CP01031I Logging successfully activated for log NotificationLog
```

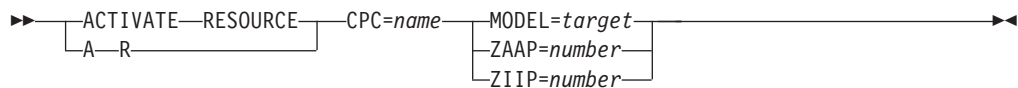
ACTIVATE RESOURCE

Use the ACTIVATE RESOURCE command to manually activate temporary resources of a CPC in the provisioning domain. The temporary resources can only be activated for the On/Off CoD record identified in the domain configuration.

Note: When a number is supplied as a parameter this 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 (has more capacity) and that the target record allows the requested change. The resources are not managed by the Provisioning Manager, and in particular they will not be deactivated automatically.

Syntax



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 at 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 MSUs than the current model. In addition the On/Off CoD record managed by the Provisioning Manager must allow for the capacity 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 should be:

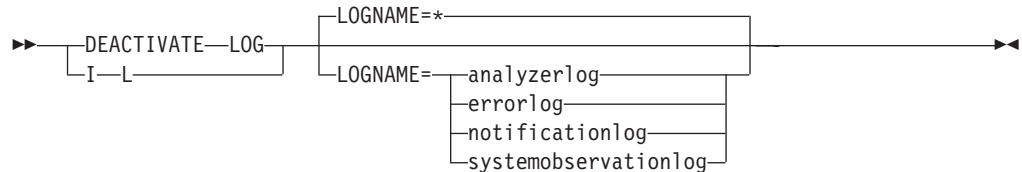
```
CP01026I Activation level change to 1 zAAPs successfully initiated for CPC G14
```

DEACTIVATE LOG

Use the DEACTIVATE LOG command to stop recording log data to a file. The log data will continue 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 33.

Note: This command should only be used if so instructed by IBM service personnel.

Syntax



Parameters

The command has the following parameter:

LOGNAME=*name*

The type of data to stop recording. This may be:

analyzerlog

contains workload analysis decisions.

errorlog

contains unexpected errors detected during processing.

notificationlog

contains communications with the Provisioning Manager.

systemobservationlog

contains monitored metrics from the observed systems.

You may also specify LOGNAME=* to indicate that writing should be deactivated for all logs. This is the default if you omit the LOGNAME parameter. *name* is not case-sensitive.

Example

To stop recording monitored metrics from 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 should be of the form:

```
CP01031I Logging successfully deactivated for log NotificationLog
CP02030I Log information written to file
        /tmp/cpoNotificationLog_20071024131732469.log
```

DEACTIVATE RESOURCE

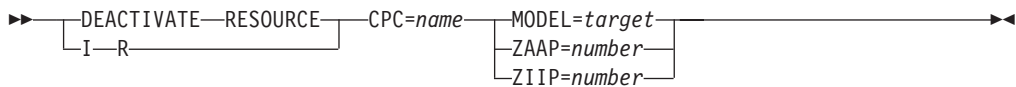
Use the DEACTIVATE RESOURCE command to manually deactivate temporary resources of a CPC in the provisioning domain. The temporary resources can only be deactivated for the On/Off CoD record identified in the domain configuration.

You should use this command to deactivate resources that you activated manually, for example by using the activate resource command (refer to page 105).

Note: When a number is supplied as a parameter this is the total number of resources that you want to have active, not the number of resources that you want to remove from the already active resources.

Before performing the deactivation, the Provisioning Manager checks that the specified resource level is below the currently active resources within the managed record.

Syntax



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 at the CPC that is managed by the Provisioning Manager.

MODEL=*target*

the model capacity identifier that you want to have active on the CPC. The target model must have less general purpose capacity in terms of MSUs than the current model. In addition, the On/Off CoD record managed by the Provisioning Manager must 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 should be:

CP01028I 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 will be listed as disabled in the domain configuration report.

Syntax

```
►►—DISABLE—CONFIGURATION—R=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 which includes the system which you want to disable. A sysplex with this name must be in the active domain configuration.

SYS=*name*

specifies the name of the system which you want to disable. A system with this name must exist in the specified sysplex in 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 should be:

```
CP01012I 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 there are already temporary resources activated through any affected time conditions these resources will be deactivated.

If the command completes successfully the selected rule or provisioning condition will be 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 lower case characters, then your console may require that the name is enclosed in single quotes.

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 lower case characters, then your console may require that the name is enclosed in single quotes.

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 should be:

```
CP01003I Rule CP160106R 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 will be created in the home directory of the Provisioning Manager user.

Note: This command should only be used if so instructed 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 to be taken. 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 take a snap dump issue the following command:

```
MODIFY CPOSERV,APPL=DUMP MANAGER TYPE=HEAP
```

The response on the console should be:

```
CP01088I 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 may get 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 then the selected CPC or system will be listed as enabled in the domain configuration report.

Syntax

```
➔—ENABLE—CONFIGURATION—CPC=name—SYS=name—PLEX=name—SYS=name—➔
```

The diagram shows the syntax of the ENABLE CONFIGURATION command. It starts with a right-pointing arrow, followed by the text "ENABLE CONFIGURATION". Below "ENABLE" is a bracketed "E-C". To the right of "CONFIGURATION" is a bracketed "CPC=*name*". Further right is a bracketed "PLEX=*name*—SYS=*name*". The command ends with another right-pointing arrow.

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 which 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 should be:

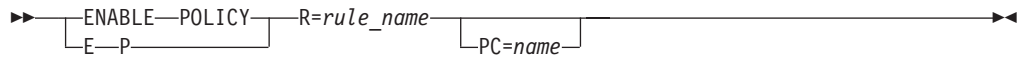
```
CP01011I CPC G14 in current configuration successfully enabled
```

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 may be activated.

If the command is successful the selected rule or provisioning condition will be listed as enabled in the policy report.

Syntax



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 lower case characters, then your console may require that the name is enclosed in single quotes.

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 lower case characters, then your console may require that the name is enclosed in single quotes.

Example

To enable rule CP160106R issue the following command:

```
MODIFY CPOSERV,APPL=ENABLE POLICY R=CP160106R
```

or:

```
F CPOSERV,APPL=E P R=CP160106R
```

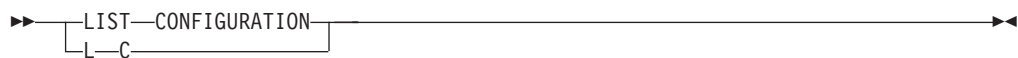
The response on the console should be:

```
CP01001I Rule CP160106R successfully enabled
```

LIST CONFIGURATION

Use the LIST CONFIGURATION command to list the entries in the domain configuration repository of the domain.

Syntax



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 should be something like:

```
CP01049I 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



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 should be something like:

```
CP01048I Policy list generated at 01/17/2006 02:38:39  
BERLINP
```

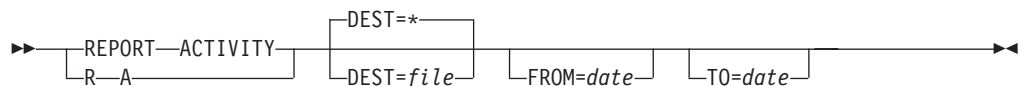
REPORT ACTIVITY

Use the REPORT ACTIVITY command to display the activation and deactivation operations which 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 the information in the report refer to page 96.

Note: Manual activations and deactivations are not recorded by the Provisioning Manager in the activity log.

Syntax



Parameters

The command has the following parameters:

DEST

specifies the destination of the activity report. The following destinations are supported:

* (the default) specifies the report is to be written to the console issuing the command.

file specifies a file where the information is to be stored. If the name includes lower case characters this parameter must be enclosed in single quotes ('). 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

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 done 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 should be before the end date of the report specified using the TO parameter.

The format to specify the start date is mm/dd/yyyy, where mm is the month, dd is the day of the month and yyyy is the year. For example April, 20th 2006 should be specified as 4/20/2006.

TO=*date*

specifies the end date of the report. All activations and deactivations done before the end of that day are reported. If the end date is omitted the current day is used. The end date of the report should be after the start date of the report specified using the FROM parameter.

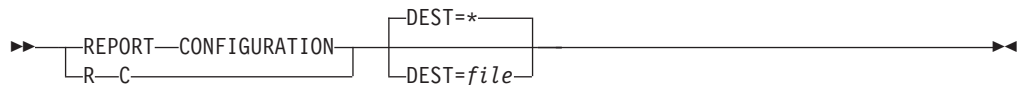
The format to specify the end date is the same as that for the start date above.

REPORT CONFIGURATION

Use the REPORT CONFIGURATION command to display the active domain configuration.

For the information in the report refer to page 92.

Syntax



Parameters

The command has the following parameter:

DEST

specifies the destination of the domain configuration report. The following destinations are supported:

* (the default) specifies the report is to be written to the console issuing the command.

file specifies a file where the information is to be stored. If the name includes lower case characters this parameter must be enclosed in single quotes ('). 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 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 the information in the report refer to page 89.

Syntax



Parameters

The command has the following parameter:

DEST

(the default) specifies the destination of the domain report. The following destinations are supported:

* (the default) specifies the report is to be written to the console issuing the command.

file specifies a file where the information is to be stored. If the name includes lower case characters this parameter must be enclosed in single quotes ('). 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 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 the information in the report refer to page 97.

Syntax



Parameters

The command has the following parameter:

DEST

(the default) specifies the destination of the log report. The following destinations are supported:

* (the default) specifies the report is to be written to the console issuing the command.

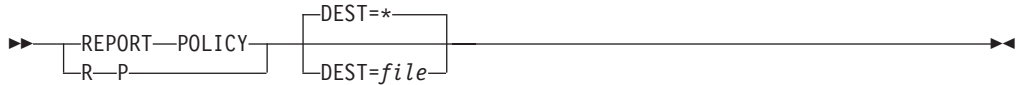
file specifies a file where the information is to be stored. If the name includes lower case characters this parameter must be enclosed in single quotes ('). The file must be in the hierarchical file system. You can specify either an absolute path or a relative path to the file. If this is not absolute the path is relative to the home directory of the user 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 the information in the report refer to page 90.

Syntax



Parameters

The command has the following parameter:

DEST

specifies the destination of the policy report. The following destinations are supported:

* (the default) specifies the report is to be written to the console issuing the command.

file specifies a file where the information is to be stored. If the name includes lower case characters this parameter must be enclosed in single quotes ('). 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 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 the information in the report refer to page 97.

Syntax



Parameters

The command has the following parameter:

DEST

specifies the destination of the trace report. The following destinations are supported:

* (the default) specifies the report is to be written to the console issuing the command.

file specifies a file where the information is to be stored. If the name includes lower case characters this parameter must be enclosed in single quotes ('). 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 running the Provisioning Manager. You must ensure that there is

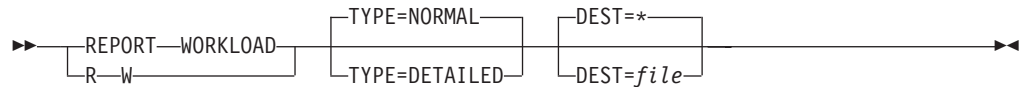
sufficient space in the selected location. The Provisioning Manager user must be authorized to write to this location.

REPORT WORKLOAD

Use the REPORT WORKLOAD command to display the WLM service class periods that are currently monitored on the observed systems.

For further information in the report refer to page 95.

Syntax



Parameters

The command has the following parameters:

DEST

specifies the destination of the workload report. The following destinations are supported:

* (the default) specifies the report is to be written to the console issuing the command.

file specifies a file where the information is to be stored. If the name includes lower case characters this parameter must be enclosed in single quotes ('). 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 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=NORMAL

TYPE=DETAILED

Specifies the type of report to display. The following types are supported:

TYPE=NORMAL

Displays a short workload report

TYPE=DETAILED

Displays a workload report including a list of WLM service class periods that are suffering. For each service class period the report lists which type of temporary resource is needed, or, why an additional temporary resource is not needed.

RESET CONFIGURATION

Use the RESET CONFIGURATION command to undo all configuration changes which have been issued since the domain configuration was activated.

Syntax



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 should be:

```
CP01019I 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 should be:

```
CP01018I 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 by the product.

Note: This command should only be used if so instructed 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 should be:

```
CP01070I The trace configuration has been reset
```

SET DOMAIN

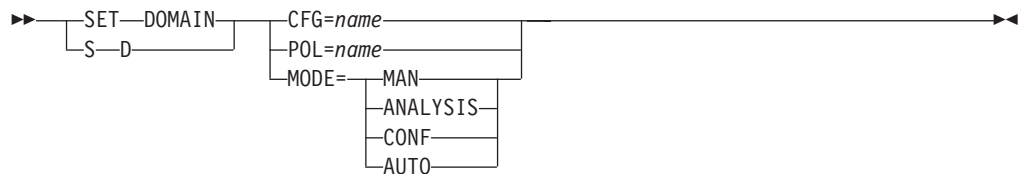
Use the SET DOMAIN command to change the global processing information of the domain. This information includes the active provisioning policy, the active domain configuration and the active processing mode.

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 may be deactivated.

Syntax

Set domain command syntax



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 activating the domain configuration 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 activating the policy, 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 should be:

```
CP01041I 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 should be:

```
CP01020I Policy successfully changed to BERLINP
```

To set the processing mode to autonomic issue the following command:

```
MODIFY CPOSERV,APPL=SET MODE=AUTO
```

or:

```
F CPOSERV,APPL=S D MODE=AUTO
```

The response on the console should be:

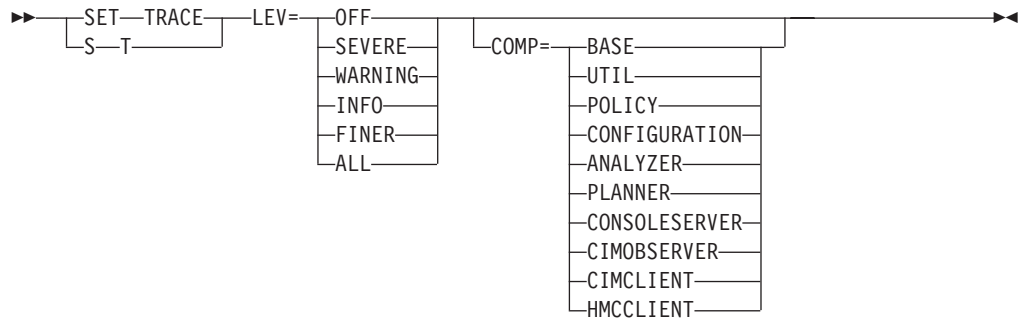
```
CP01009I Processing mode successfully changed to AUTO
```

SET TRACE

Use the SET TRACE command to change the tracing parameters of the Provisioning Manager. You may 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 should only be used if so instructed by IBM service personnel.

Syntax



Parameters

The parameter names and trace values are not case-sensitive. This command has the following parameters:

LEV

the 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 within the Provisioning Manager for which you want to alter the trace level. The supported component names are:

BASE the 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 relevant to planning

CONSOLESERVER
command processing

CIMOBSERVER
processing CIM requests

CIMCLIENT
the CIM client API

HMCCLIENT
the HMC or SE client API

If COMP is not specified the default 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=SET TRACE LEV=ALL
```

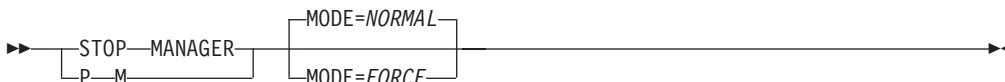
The response on the console should be:

```
CP01060I 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 has been requested to stop it does not accept any other commands. The state of resources does not change. Any active resources remain active.

Syntax



Parameters

The command has the following parameter:

MODE

the 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, or

FORCE

to stop processing immediately. If the Provisioning Manager is registered with ARM the process may get restarted.

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 should be:

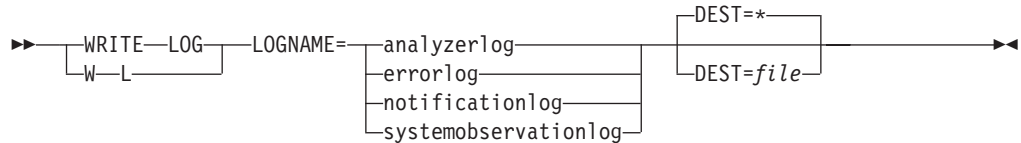
```
CP01007I Stop command for the Provisioning Manager accepted
```

WRITE LOG

Use the WRITE LOG command to save the current data for a specific log to a file.

Note: This command should only be used if so instructed by IBM service personnel.

Syntax



Parameters

The command has the following parameters:

LOGNAME=name

The type of data to be recorded. This may be:

analyzerlog

workload analysis decisions.

errorlog

unexpected errors 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:

***** (the default) specifies the report is to be written to the standard log file in the log path that has been specified during your set-up. 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 lower case characters this parameter must be enclosed in single quotes ('). 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 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 for the specified log has been activated.

Example

To write the notification log to file n1.log issue the following command:

```
MODIFY CPOSERV,APPL=WRITE LOG LOGNAME=NotificationLog DEST='n1.log'
```

or:

```
F CPOSERV,APPL=W L LOGNAME=NotificationLog DEST='n1.log'
```

The response on the console should be:

```
CP01040I Log NotificationLog successfully written to file nl.log
```

Part 4. Appendixes

Accessibility

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/Library Server versions of z/OS books in the Internet library at:

<http://www.ibm.com/systems/z/os/zos/bkserv/>

Capacity Provisioning Terms

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/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 which provides a graphical user interface to Capacity Provisioning. Through this interface administrators can work with provisioning policies and domain configurations, and can transfer these to the Provisioning Manager.

Capacity Upgrade on Demand (CUoD). The capability to permanently activate 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 to add 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). In RACE, a table containing 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 you 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 activated in the time condition before the deadline can remain 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 suffering.

domain configuration. The definition of the CPCs to be managed and the systems to be observed by 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 management of 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 assigning importance levels to sets of provisioning criteria.

Integrated Information Processor. See zIIP

Intelligent Resource Director (IRD). A z/OS facility designed to give your installation an enhanced ability to dynamically move resources to your 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 amount of logical processors that can be configured online for the systems in the provisioning domain.

M

maximum provisioning scope. The total amount of resources which can be additionally activated for a domain. See also provisioning scope.

monoplex. A sysplex consisting 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. In RACF secured sign-on, a dynamically generated, random, one-time-use, password substitute 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 controlling 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 indicating the target performance index range expected of a service class period and the lengths of time it may 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 suffering.

provisioning scope. The amount of resources which 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. A provisioning rule links a provisioning scope to time conditions and may 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 you assign a service goal and optionally a resource group 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 can start to activate additional capacity if one of the workloads associated with the time condition is suffering. 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 may be enabled for each applicable TC Eligible Machine that you indicate on a Supplement. IBM may also refer to 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 may 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 provides the ability to run multiple workloads 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 the 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.

Notices

This information was developed for products and services offered in the USA.

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
USA

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

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

Notices

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

IBM Corporation
Mail Station P300
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.

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. 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 IBM's application programming interfaces.

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

The following terms are trademarks for the IBM Corporation in the United States and/or other countries:

- CICS[®]
- CICSplex[®]
- DB2[®]
- Distributed Relational Database Architecture[™]
- DRDA[®]
- IBM
- IMS[™]
- MVS
- POWER[®]
- PR/SM
- RACF
- Resource Measurement Facility
- RMF
- SAA[®]
- System z
- VTAM[®]
- z/OS
- z/VM
- z9[®]
- z10
- zSeries[®]

Intel[®] and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

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

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

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

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

Index

Special characters

/pws 50
/tmp 35, 43
/u/cposrv 44
/usr/include/java_classes/
 IRRRacf.jar 36, 43
/usr/lib 36, 38
/usr/lpp/cpo 23, 38, 42, 43
/usr/lpp/java 36, 38, 42, 43
/usr/lpp/wbem 36, 38, 43
/var 43

A

about capacity provisioning control
 center 61
access
 ARM 42, 43
 automatic restart manager 42, 43
 hardware 42
accessibility 127
accessing the provisioning manager 62
action
 connect 59
 disconnect 59
 exit 60
 install 68, 82
 new condition 74
 new configuration 60, 65
 new policy 60, 69
 new rule 73
 new workload condition 77
 refresh status 59
 refresh workspace 60
 save all 60
 save configurations 60
 save connections 60
 save policies 60
 welcome 61
activate log command 104
activate resource command 105
activating a domain configuration 68
activating a provisioning policy 82
activation 14, 24, 28, 75, 76, 86, 87, 96,
 113
 manual 29
 temporary resource 13
activation level 25, 27, 28
 target 96
activation time 90
activation using provisioning manager
 command 29
active and disabled, time condition
 state 25
active and enabled, time condition
 state 25
active domain configuration 89, 92, 119
active processing mode 89, 119
active provisioning policy 90, 119
activity report 29, 96

adapting the provisioning manager
 parameters 38
add button 58
add connection button 62
add CPC button 67
add importance filter button 78
add limit button 72
add or remove programs
 Windows control panel 52
add service class filter button 80, 81
add system button 66
add time condition button 76
additional capacity 14, 17, 18, 21, 69, 71,
 86
address
 alternate host 66
 alternate IP 66
address, HMC 36
administrator 50
all button 83
allow action 87
altered name 30, 65, 69, 73, 75, 77
alternate host address 66
alternate IP address 66
alternative runtime system 36
alternative system 34
analysis processing mode 24, 26, 64, 85
answering operator messages 87
APAR 51
APAR level 61
APF authorization 37, 42
application assist processor 11, 71
apply button 58, 63, 67, 68, 72, 76, 81
applying an update for the control
 center 51
ARM 24, 34, 39, 47
 definition 129
ARM access 42, 43
ARM element name 36
ARM element type 36
ARM policy 39
ARM restart 36
ARM.ElementName 39
ARM.ElementType 39
ARM.Register 39
AT-TLS configuration 47
authorization
 APF 37
automatic restart manager 24, 34, 39, 47
 definition 129
automatic restart manager access 42, 43
automatic restart manager policy 39
automation product 24
autonomic processing mode 24, 27, 65,
 85
availability 23

B

background color, cell 58
base control program 4

base control program (*continued*)
 definition 129
BCP 4
 definition 129
BCPii
 communication 5
blocking 29
bottleneck 20
BPX.SRV.** 46
BPX.SRV.CPOSRV 47
button
 add connection 62
 add CPC 67
 add importance filter 78
 add limit 72
 add service class filter 80, 81
 add system 66
 add time condition 76
 all 83
 apply 63, 67, 68, 72, 76, 81
 clear connection report 59
 condition 82
 connect 63, 68, 82
 disabled 83
 disconnect 65
 enabled 83
 none 83
 refresh status 65
 rule 82
 save connections 63
 save policy 81
 show timeline 83
button, add 58
button, apply 58
button, cancel 58
button, delete 58

C

cancel button 58
capacity 10
 additional 17, 18, 69
 definition 131
 processing 20
 remaining 92
 residual 13
 temporary 12, 13, 17, 24, 39
capacity maximum 6
 resource group 99
capacity provisioning component 51
capacity provisioning control center 4,
 12, 29, 55
 definition 129
capacity provisioning domain 9, 10, 12
capacity provisioning installation
 directory 43, 50
capacity provisioning installation
 path 38
capacity provisioning jar files 38
capacity provisioning manager 4, 11, 23
capacity provisioning policy 9, 10, 13, 15

- capacity provisioning program group 61
- capacity provisioning workload
 - classification 49
- capacity provisioning workspace 51, 56
- capacity record 12, 13
- capacity shortage 17
- Capacity Upgrade on Demand 3
 - definition 129
- capped service class 99
- capping 6
- CDT
 - definition 129
- cell, background color 58
- central processor complex 9, 10
 - definition 129
- CFCC 6
 - definition 129
- CFG 119
- change directory 61
- change interval 24
- change workspace 30
- checkbox
 - enabled 75
- chmod
 - UNIX command 44
- choosing service class periods 99
- CIM 33, 34, 47
 - definition 129
- CIM client 50
- CIM client version 61
- CIM Java client 36, 38, 43, 50
- CIM Java client location 36
- CIM port 67
- CIM protocol 66
- CIM provider library link 48
- CIM provider properties file 48
- CIM server 12, 23, 24, 34, 36, 46, 47, 49, 50, 59
- CIM server installation directory 36
- CiM server port 47
- CIM server port 12
- CIM server provider directory 48
- CIM server user 34, 46, 47
- CIM.ModifyGroup 39
- CIM.ReadGroup 39
- CIMSERV 46, 47
- CIU
 - definition 129
- class descriptor table
 - definition 129
- CLASSPATH 38
- clear connection report button 59
- clipboard 57
- clipboard, control center 57
- command
 - activate log 104
 - activate resource 105
 - context 56
 - deactivate log 107
 - deactivate resource 108
 - disable configuration 12, 13, 24, 67, 68, 109
 - disable policy 17, 26, 75, 109
 - dump manager 110
 - enable configuration 12, 13, 24, 67, 68, 111
 - enable policy 17, 26, 68, 73, 75, 111
- command (*continued*)
 - list configuration 112
 - list policy 113
 - MVS modify 86
 - MVS start 85
 - MVS stop 86
 - operator 23
 - provisioning manager 24, 86
 - report activity 96, 113
 - report configuration 87, 92, 114
 - report domain 89, 114
 - report log 97, 115
 - report policy 90, 116
 - report trace 97, 116
 - report workload 95, 117
 - reset configuration 117
 - reset policy 118
 - reset trace 118
 - set domain 27, 65, 68, 82, 86, 119
 - set trace 120
 - stop manager 86, 122
 - syntax diagrams x
 - write log 123
- command syntax 103
- command, copy 57
- command, delete 57
- command, install 57
- command, paste 57
- command, rename 57
- command, save 57
- commandnew 56
- common information model 12
- common interface module
 - definition 129
- communication channel 12
- community
 - HMC 35
- community name 35, 39
- community name, SNMP 36
- component
 - capacity provisioning 51
- condition
 - provisioning 11, 17, 25, 28, 90
 - time 11, 14, 17, 18, 21, 23, 25, 30, 56, 74, 75, 91
 - workload 11, 14, 17, 18, 19, 20, 21, 23, 25, 28, 56, 74, 76, 77, 86, 90
- condition button 82
- conditions folder 73
- configuration 56, 65
- configuration information 38, 46
 - provisioning manager 38
- configuration parameters 37
- configurations folder 56
- confirmation processing mode 24, 27, 65, 85, 87
- connect action 59
- connect button 63, 68, 82
- connect to the provisioning manager 63
- connecting status 64
- connection 29, 63
 - define 62
 - provisioning manager 48
- connection report 60, 64
- connection report panel 59
- connection status 93
- connections directory 29
- connections table 62, 63
- console 89
 - MVS 85
- console messages 26, 27, 87
- contention
 - resource 18
- context command 56
- context menu 56
- control center 4, 7, 9, 12, 13, 23, 29, 33, 35, 47, 49, 50, 55, 60, 62, 65, 66, 67, 73, 75, 81, 82
 - applying an update 51
 - definition 129
 - installation wizard 50
 - installing 50
 - service 51
 - starting 61
 - stopping 62
 - time zone 30
 - tracing 61
 - uninstalling 52
 - updating 51
 - user 39, 42
 - version 61
 - window layout 55
- control center commands authorization
 - security groups 39
- control center installation package
 - retrieving 50
- control center user
 - security 45
- control center, clipboard 57
- control center, user 34
- control center, workstation 36
- control security group
 - provisioning manager 34, 39, 43, 45, 63
- control security group, provisioning manager 34
- controlling the provisioning manager 85
- coordinated universal time 25, 30, 75, 90, 91, 96
- copy command 57
- correlated CPCs 24
- coupling facility
 - definition 129
- coupling facility control code 6
- CPC 9, 10, 11, 12, 15, 24, 25, 29, 31, 39, 65, 71, 74, 85, 90, 92, 96, 100, 106, 108, 109, 111
 - definition 129
 - managed 24, 65
- CPC hardware type 92
- CPC model 92
 - current 92
 - permanent 92
- CPC record ID 31
- CPC status 92
- cpcsetup.exe 50, 51
- CPCs panel 67
- CPCs tab 67
- CPCs table 67
- CPO.DOMAIN1.RESTART 38
- creating a domain configuration 65
- creating a provisioning policy 69
- creating provisioning rule 73
- creating the started task procedure 41

- criteria
 - provisioning 19, 20
- CUoD 3
 - definition 129
- current CPC model 92
- cursor 58
- customer initiated upgrade
 - definition 129

D

- data set
 - provisioning manager parameters 38
 - runtime 41
- data set, restart 37
- data sets
 - high-level qualifier 34
 - provisioning manager 34, 43
 - runtime 37
- date format 75
- DD 91, 95
- DDS 24
- deactivate log command 107
- deactivate resource command 108
- deactivation 24, 28, 29, 86, 87, 96, 113
 - manual 29
 - temporary resource 13
- deactivation using provisioning manager
 - command 29
- deadline 17, 18, 21, 25, 28, 76, 91
 - definition 129
- dedicated LPAR 6
- default directory 61
- default domain configuration 86
- default policy 85
- default processing mode 85
- default time zone 30
- default trace level 120
- define a domain configuration 99
- define a policy 99
- define connection 62
- define the provisioning scope for a rule 74
- define the runtime data sets 37
- define the runtime environment 34
- delete button 58
- delete command 57
- deny action 87
- deprovisioning
 - definition 130
- deprovisioning performance index
 - limit 91, 95
- deprovisioning performance index limit
 - duration 91, 95
- deprovisioning PI 20, 21, 79, 80
 - definition 129
- desktop 61
- details view 55, 56, 57, 67
- dialog 56
 - preferences 60
- directory
 - CIM server provider 48
 - connections 29
 - default 61
 - domainconfigurations 29
 - provisioningpolicies 29
 - workspace 12, 29, 61

- disability 127
- disable configuration command 12, 13, 24, 67, 68, 109
- disable policy command 17, 26, 75, 109
- disable provisioning condition 110
- disable rule 110
- disabled button 83
- disconnect action 59
- disconnect button 65
- disconnected status 64
- DISCRETIONARY 99
- display policies in time zone 60
- distributed data server 24
- DL 91, 95
- domain 9, 10, 11, 12, 13, 21, 24, 30, 33, 37, 38, 41, 63, 82, 85, 89, 119
- domain configuration 9, 10, 11, 12, 13, 23, 24, 29, 31, 55, 57, 59, 60, 62, 65, 67, 111, 117, 119
 - activating 68
 - active 89, 92, 119
 - creating 65
 - default 86
 - define 99
 - definition 129
 - installing 68
 - processing 24
- domain configuration file 4
- domain configuration report 24, 92
- domain configuration repository 11, 12, 37, 57, 68, 119
- domain configuration system definition
 - screen 66
- domain name 33, 34
- domain report 27, 89
- domain switching 65
- domainconfigurations directory 29
- drained and disabled, time condition
 - state 25
- drained and enabled, time condition
 - state 25
- driver level 5, 61
- dump
 - heap 110
 - Java 110
 - Java system 110
- dump manager command 110
- duration
 - provisioning 86
 - provisioning PI 25
- duration in min 20, 79, 80

E

- edit table cell 58
- element name, ARM 36
- element type, ARM 36
- eligible service class 20
- enable configuration command 12, 13, 24, 67, 68, 111
- enable policy command 17, 26, 68, 73, 75, 111
- enable provisioning condition 112
- enable rule 112
- enabled attribute 12, 13
- enabled button 83
- enabled checkbox 75

- enabled status 93
- end date 82
- end time 18, 25, 28, 76, 91
 - definition 129
- error message 59
- errors 59
- excluded service class 19, 91
- excluded service class period 22
- excluded service class screen 80
- excluded service classes filter 80
- excluded service classes filter tab 78
- excluded service classes tab 81
- exit action 60

F

- FACILITY class 43, 44
- file menu 60
- file system
 - installation 38
 - log data 35
 - trace data 35
- filter
 - excluded service classes 80
 - importance 19, 20, 22, 78, 90
 - included service class 20, 79
 - service class 22
 - service class period 22
- folder
 - conditions 73
 - configurations 56
 - policies 56, 69
 - rules 56, 69
 - workload conditions 75
- FORCE mode 122
- FTP 50

G

- general purpose capacity 71
- general purpose processor 5, 11
- GMT
 - time zone 30
- goal 18, 20, 99
 - velocity 49
- goal attainment 99
- graphical user interface 4, 9, 29, 55
- GUI 29, 55

H

- hardware
 - security 45
- hardware access 42
- hardware console 11
- hardware console protocol 36
- hardware elements 9
- hardware management console 5, 11, 23, 24, 29, 39, 87
 - definition 130
- hardware requirements 5
- hardware type
 - CPC 92
- heap dump 110
- help menu 61
- high-level qualifier 38

- high-level qualifier *(continued)*
 - runtime data set 41
- high-level qualifier, runtime data set 34
- history 24
 - report 98
- HMC 5, 6, 11, 23, 24, 29, 34, 39, 87
 - community 35
 - definition 130
 - driver level 5
 - host name 35, 39
 - TCP/IP address 35, 39
- HMC, address 36
- home directory
 - provisioning manager user 41, 44
- host 50, 51, 64, 82
 - z/OS 51
- host address 12, 59, 62, 93
 - alternate 66
- host name 66
 - HMC 35, 39
- host system 11
- HTTP protocol 47, 62
- HTTPS protocol 47, 50, 62

I

- I 90
- IBM capacity provisioning program
 - group 61
- IBM security server 6
- importance 18, 22, 78, 90
- importance filter 19, 20, 22, 78, 90
 - definition 130
- importance filters screen 78
- importance filters tab 78
- importance filters table 78
- importance level 19
- inactive, time condition state 26
- included service class 19, 20, 91
- included service class filter 20, 79
- included service class period 22
- included service class screen 79
- included service classes tab 78, 79
- included service classes table 80
- information message 59
- information view 55, 59, 64
- initial installation 50
- initial policy 85
- initial processing mode 27, 85
- install action 68, 82
- install command 57
- installation directory
 - capacity provisioning 43, 50
 - CIM server 36
 - Java 36, 43
- installation file system 38
- installation package
 - control center 50
- installation path
 - capacity provisioning 38
 - Java 38
- installation wizard 50, 52
- installation wizard panel 51
- installation wizard welcome screen 52
- installing a domain configuration 68
- installing a provisioning policy 82
- installing the control center 50

- integrated information processor 11
- integrated information processors 71
- intelligent resource director 20, 28
 - definition 130
- IP address 66
 - alternate 66
- IRD 20, 28
 - definition 130
- IRR.RTICKETSERV 44

J

- jar file
 - SAF 38
 - system authorization facility 38
- jar file, SAF 36
- jar file, system authorization facility 36
- jar files
 - capacity provisioning 38
- Java 2 technology edition SDK for
 - z/OS 36
- Java client
 - CIM 38, 43, 50
- Java client, CIM 36
- Java dump 110
- Java installation directory 36, 43
- Java installation path 38
- Java library 42
- Java SDK code 42
- Java system dump 110

K

- keyboard 127

L

- last refresh field 65
- LIBPATH 38
- libraries
 - provisioning manager 42
- library
 - Java 42
 - SAF 43
 - secured signon function 36
 - system authorization facility 43
- library location
 - SAF 36
 - system authorization facility 36
- library path
 - SAF 38
 - system authorization facility 38
- library, SAF 36
- library, system authorization facility 36
- link list 42
- list configuration command 112
- list policy command 113
- local performance index 21
- local PI 21
- location
 - CIM Java client 36
 - SAF libraries 36
 - system authorization facility
 - libraries 36
- location, log data 36
- location, trace data 36

- log data 39, 43
- log data file system 35
- log data location 36
- log report 97
- logical partition 13
- logical processor 6, 28
 - definition 130
 - limits 15
 - scope 15
- logical processor scope 15, 90
- login 63
- LPAR 6, 10, 13, 24, 28

M

- main window 55
- managed CPC 24, 65
- managing reports 98
- manual activation 29
- manual change 13, 29
- manual deactivation 29
- manual processing mode 26, 64, 85
- maximum provisioning scope 11, 14, 56, 69, 71, 90
 - definition 130
- maximum provisioning scope screen 71
- menu
 - file 60
 - help 61
 - options 60
- menu bar 55, 60
- message description 59
- message severity 59
- message, error 59
- message, information 59
- message, warning 59
- messages 59, 67
 - console 87
 - operator 87
- messages panel 59, 66, 68, 69, 76, 77, 80, 81
- messages, console 26, 27
- Microsoft Windows 7
- mode
 - processing 89, 119
- MODE 119
- model
 - CPC 92
 - permanent CPC 92
 - WLM service class 77
 - workload management service
 - class 77
- modify command 86
- monoplex 13
 - definition 130
- MSU 15, 71, 72, 92, 106
- MVS
 - console 85
 - modify command 86
 - start command 85
 - stop command 86

N

- name
 - altered 30, 65, 69, 73, 75, 77

- name, domain 34
- name, started task procedure 34
- naming conventions 30
- network 6, 24
- new command 56
- new condition action 74
- new configuration action 60, 65
- new policy action 60, 69
- new rule action 73
- new workload condition action 77
- none button 83
- NORMAL mode 122
- not active status 64
- Notices 133

O

- observation start time 25
- observation status 93
- observed system 6, 10, 11, 12, 13, 23, 24, 28, 37, 42, 44, 46, 49, 65
 - securing 46
- observed systems 10
- observing and disabled, time condition state 25
- observing and enabled, time condition state 25
- offline processors 6
- OMVS 43, 45, 46
- OMVS segment 42
- On/Off Capacity on Demand 3
 - definition 130
- On/Off CoD 3, 5
 - definition 130
- On/Off CoD record 5, 29, 68, 87, 92, 105
- operating system 93, 95, 96
 - z/OS 9
- operations
 - tables 58
- operator command 23
- operator messages 87
- options menu 60
- output class 41
- overview 9

P

- panel 55
 - connection report 59
 - CPCs 67
 - messages 59, 66, 68, 69, 76, 77, 80, 81
 - systems 66
 - workload condition 77
- parameters
 - provisioning manager 38
- parameters data set 38
- parameters, provisioning manager 37
- passticket 6, 44, 46
 - definition 130
- paste command 57
- PD 90, 91, 95
- peak demand 99
- pending, time condition state 25
- percentile goals 99
- performance index 20, 28, 95, 99
 - definition 130

- performance index (*continued*)
 - scope 91
- performance index, local 21
- performance information 46
- period 22, 80
 - service class 18, 19, 20, 21, 22, 81, 96, 99
- permanent CPC model 92
- PI 20, 28, 95, 99
 - definition 130
 - provisioning criteria 22, 23
- PI scope 21, 79, 80
- PI, local 21
- PI, sysplex 21
- PI, system 21
- PL 90, 91, 95
- PLEX 109, 111
- POL 119
- policies folder 56, 69
- policy 9, 10, 11, 12, 13, 17, 19, 24, 26, 28, 30, 49, 56, 57, 59, 62, 65, 96, 118, 119
 - active 90, 119
 - ARM 39
 - automatic restart manager 39
 - capacity provisioning 15
 - default 85
 - define 99
 - definition 130
 - initial 85
 - provisioning 29
 - WLM 91, 94, 100
 - workload management 91, 94, 100
- policy file 4
- policy report 26, 90
- policy repository 11, 13, 37, 57, 82, 119
- policy time condition 25
- policy timeline 69, 82
- policy timeline screen 83
- port 63, 93
 - CIM 67
 - CIM server 12, 47
- portal, RMF monitor III data 21
- PR/SM 6, 28
- preferences dialog 60
- preparing the connection to the
 - provisioning manager 48
- preparing the provisioning manager 37
- prerequisite 5, 36, 37, 50
- primary host address 66
- primary runtime system 36
- primary system 34
- processing activations and deactivations 28
- processing capacity 20
- processing mode 12, 23, 26, 64, 89, 119
 - active 119
 - analysis 24, 64, 85
 - autonomic 24, 65, 85
 - confirmation 24, 65, 85, 87
 - default 85
 - initial 27, 85
 - manual 26, 64, 85
- processing mode, analysis 26
- processing mode, autonomic 27
- processing mode, confirmation 27
- processing mode, manual 26
- processing policy time conditions 25

- processing the domain configuration 24
- processing weight 28
- processor
 - application assist 11
 - general purpose 5, 11
 - integrated information 11
 - logical 28
 - specialty 3
- processor complex 67, 72
- processor pool 6
- processor resource 20
- program controlled flag 48
- program group
 - IBM capacity provisioning 61
- properties file
 - CIM provider 48
- protocol 12, 93
 - CIM 66
 - HTTP 12, 47, 62
 - HTTPS 12, 47, 50, 62
 - simple network management 34
 - SNMP 23
- protocol, hardware console 36
- provisioning
 - definition 130
- provisioning condition 6, 11, 14, 17, 25, 28, 30, 73, 74, 90
 - definition 130
 - disable 110
 - enable 112
- provisioning condition screen 74
- provisioning criteria 19, 20
 - definition 130
- provisioning criteria PI 22, 23
- provisioning domain 9, 12, 13, 21, 89
- provisioning duration 86, 100
- provisioning manager 4, 6, 7, 9, 11, 12, 17, 18, 19, 20, 21, 23, 24, 25, 26, 33, 34, 35, 37, 39, 45, 47, 49, 55, 57, 65, 66, 68, 82, 87
 - accessing 62
 - configuration information 38
 - controlling 85
 - starting 85
 - status 29
- provisioning manager command 24, 86
 - activation using 29
 - deactivation using 29
- provisioning manager configuration information 38
- provisioning manager connection 48
- provisioning manager control security group 34, 39, 43, 45, 63
- provisioning manager data sets 34, 43
- provisioning manager libraries 42
- provisioning manager parameters 37, 38
- provisioning manager parameters data set 38
- provisioning manager query security group 34, 39, 43, 45, 63
- provisioning manager runtime environment data 38
- provisioning manager screen 63
- provisioning manager specification 56
- provisioning manager user 33, 34, 35, 37, 42, 44, 46, 47
 - home directory 41, 44

- provisioning manager user security 43
- provisioning performance index
 - limit 90, 91, 95
- provisioning performance index limit
 - duration 90, 91, 95
- provisioning PI 20, 21, 78, 80
 - definition 130
- provisioning PI duration 21, 25
- provisioning policy 10, 13, 26, 28, 29, 30, 49, 55, 68, 118
 - activating 82
 - active 90
 - creating 69
 - installing 82
 - screen 69
- provisioning rule 11, 14, 30, 69, 90
 - creating 73
- provisioning rule screen 73
- provisioning scope 11, 14, 17, 18, 73, 90
 - define for a rule 74
 - definition 130
- provisioning policies directory 29
- PTF 51
- PTKTDATA 44

Q

- query security group
 - provisioning manager 34, 39, 43, 45, 63
- query security group, provisioning manager 34

R

- R_GenSec 6
- RACF 6, 42, 44, 47
- reaction time 100
- receiving an update 51
- record
 - capacity 12, 13
 - On/Off CoD 5, 68, 87, 92, 105
- record ID 68
- refresh status action 59
- refresh status button 65
- refresh workspace action 60
- region size 41
- Release 9
 - z/OS 6
- remaining capacity 92
- rename command 57
- repair or remove the program 52
- report 17, 19
 - activity 29, 96
 - connection 60, 64
 - domain 27, 89
 - domain configuration 24, 92
 - log 97
 - managing 98
 - policy 26, 90
 - trace 97
 - workload 95
- report activity command 96, 113
- report configuration command 87, 92, 114
- report domain command 89, 114
- report history 98
- report log command 97, 115
- report policy command 90, 116
- report trace command 97, 116
- report workload command 95, 117
- repository
 - domain configuration 11, 12, 68, 119
 - policy 11, 13, 82, 119
- repository, domain configuration 37, 57
- repository, policy 37, 57
- reserved processors 6
- reset configuration command 117
- reset policy command 118
- reset trace command 118
- residual capacity 13
- resource access control facility 6
- resource consumption 49
- resource contention 18
- resource definition 23
- resource demand 20, 21
- resource group 6
- resource group capacity maximum 99
- resource measurement facility 6, 21, 24, 49, 99
 - definition 130
- resource shortage 13, 18, 19
- response time 18, 20, 99
- restart 24, 34, 37, 47, 86
- restart data set 37
- retrieving the control center installation
 - package 50
- RMF 6, 24, 49, 99
 - definition 130
- RMF MINTIME 24, 50, 99, 100
- RMF monitor III data portal 21
- RMF WLMGL 21
- RMF, z/OS 21
- row 58
- rule 9, 15, 17
 - define the provisioning scope 74
 - definition 130
 - disable 110
 - enable 112
 - provisioning 11, 69, 90
 - provisioning condition for 74
- rule button 82
- rules folder 56, 69
- runtime data set
 - high-level qualifier 41
- runtime data set high-level qualifier 34
- runtime data sets 37
 - define 37
- runtime environment 34
- runtime environment data
 - provisioning manager 38
- runtime information 34
- runtime paths 34
- runtime system 37, 44, 49
 - securing 42
- runtime system, alternative 36
- runtime system, primary 36
- runtimedata sets 47

S

- S 91, 95
- SAF 6

- SAF (*continued*)
 - definition 130
- SAF jar file 36, 38
- SAF libraries location 36
- SAF library 36, 43
- SAF library path 38
- samples 4, 5, 33, 38
- save all action 60
- save command 57
- save configurations action 60
- save connections action 60
- save connections button 63
- save policies action 60
- save policy button 81
- schedule 18, 28, 76
- scope
 - logical processor 15
 - maximum provisioning 14
 - provisioning 11, 14, 17, 18, 90
- scope for the performance index 91, 95
- scope, PI 21
- screen
 - domain configuration system
 - definition 66
 - excluded service class 80
 - importance filters 78
 - included service class 79
 - maximum provisioning scope 71
 - policy timeline 83
 - provisioning condition 74
 - provisioning manager 63
 - provisioning policy 69
 - provisioning rule 73
 - select timeline to display 82
 - time condition 75
 - workload condition 76
 - workplace 62
- SDK for z/OS, Java 2 technology
 - edition 36
- SE 5, 6, 11, 13, 34, 67, 72
- secured signon function 42, 44, 46
- secured signon function library 36
- securing observed system 46
- securing the runtime system 42
- security 37
 - control center user 45
 - hardware access 45
 - provisioning manager user 43
- security definition 33
- security group
 - control 63
 - provisioning manager control 34, 39, 43
 - provisioning manager query 34, 39, 43
 - query 63
- security group, provisioning manager
 - control 34
- security group, provisioning manager
 - query 34
- security groups for control center
 - commands authorization 39
- security server
 - IBM 6
- select table row 58
- select timeline to display screen 82

- server
 - CIM 12, 23, 24, 34, 46, 47, 50
- server, CIM 36, 59
- service
 - control center 51
- service class 6, 17, 21, 22, 96, 99
 - capped 99
 - definition 130
 - eligible 20
 - excluded 19, 91
 - included 19, 20, 91
 - WLM 17, 18, 24, 80, 81, 91
 - workload management 81, 91
- service class filter 22
- service class model
 - WLM 11, 18, 77
 - workload management 77
- service class period 18, 19, 20, 21, 22, 81, 96, 99
 - definition 131
 - WLM 91, 95
 - workload management 91, 95
- service class period filter 22
- service class periods
 - choosing 99
- service definition 22
 - WLM 20, 21, 80, 81, 91, 94, 96, 99, 100
 - workload management 81, 91, 94, 96, 99, 100
- service definition, WLM 22
- service element 11
- service information 90
- service policy 22
 - WLM 19, 80, 81
 - workload management 81
- set domain command 27, 65, 68, 82, 86, 119
- set trace command 120
- setting up a capacity provisioning domain 33
- severity
 - message 59
- shared LPAR 6
- shortcut keys 127
- show timeline button 83
- simple network management protocol 34
- SMP/E 51
- SNMP 6, 34
 - communication 5
- SNMP community name 36
- SNMP protocol 23
- software elements 9
- software requirements 6
- specialty processor 3
 - definition 131
- SSL certificates 47
- start command
 - MVS 85
- start date 82
- start time 17, 25, 28, 76, 91
 - definition 131
- started status 64
- started task 33, 37, 42, 49, 85
- started task procedure 23
 - creating 41

- started task procedure name 34
- starting the control center 61
- starting the initial installation 50
- starting the provisioning manager 85
- state information 24
- status
 - connecting 64
 - disconnected 64
 - not active 64
 - started 64
- status field 64
- status information 64
- stop command 86
- stop manager command 86, 122
- stopping the control center 62
- support element 5, 34, 67, 72
- SURROGAT class 46, 47
- switching domain 65
- syntax
 - z/OS command 103
- syntax diagrams
 - how to read x
- SYS 109, 111
- SYS1.PROCLIB 41
- SYS1.SAMPLIB 33, 38, 41, 47
- SYS1.SIEALNKE 23, 42
- sysplex 10, 13, 17, 19, 31, 47, 66, 77, 80, 90, 93, 95, 96, 109, 111
 - definition 131
- sysplex PI 21
- SYSSTC 49, 99
- system 31, 66, 80, 90, 95, 96, 109, 111
 - alternative 34
 - observed 28
 - primary 34
 - z/OS 19, 77
- SYSTEM 99
- system authorization facility 6
 - definition 130
- system authorization facility jar file 36, 38
- system authorization facility libraries
 - location 36
- system authorization facility library 36, 43
- system authorization facility library path 38
- system PI 21
- System z10 3, 4, 5
- systems panel 66
- systems tab 66
- systems table 66

T

- tab
 - CPCs 67
 - excluded service classes 81
 - excluded service classes filter 78
 - importance filters 78
 - included service classes 78, 79
 - systems 66
- table cell, edit 58
- table operations 58
- table row, select 58
- tabs 58
- target activation level 96

- TCP/IP 5, 7, 49
- TCP/IP address
 - HMC 35, 39
- temporary capacity 3, 12, 13, 17, 24, 39, 68, 86
 - definition 131
- temporary resource 25, 28, 86
- temporary resource activation 13
- temporary resource deactivation 13
- time condition 11, 14, 17, 18, 21, 23, 25, 30, 56, 74, 75, 91
 - definition 131
- time condition screen 75
- time condition state, active and disabled 25
- time condition state, active and enabled 25
- time condition state, drained and disabled 25
- time condition state, drained and enabled 25
- time condition state, inactive 26
- time condition state, observing and disabled 25
- time condition state, observing and enabled 25
- time condition state, pending 25
- time condition status 91
- time format 75
- time period 11, 18
 - definition 131
- time zone 25, 60, 75
 - control center 30
 - default 30
 - GMT 30
- timeline
 - policy 82
- Topology.Address 39
- Topology.Community 39
- trace 50
 - trace data 39, 43
 - trace data file system 35
 - trace data location 36
 - trace file 97
 - trace level 97, 120
 - default 120
 - trace report 97
 - trace settings 61
 - Trace.Path 39
 - tree 56
 - tree view 55, 56, 62

U

- uninstalling the control center 52
- UNIX command chmod 44
- update
 - applying 51
 - receiving 51
- updating an existing control center installation 51
- user
 - CIM server 34, 46, 47
 - control center 39, 42, 45
 - provisioning manager 33, 35, 37, 41, 42, 44, 46, 47
 - user, CIM server 34

- user, control center 34
- user, provisioning manager 34
- user, z/OS 34
- UTC 25, 30, 75, 90, 91, 96

V

- velocity 20
- velocity goal 49
- version
 - control center 61

W

- warning message 59
- warnings 59
- WBEM class 47
- welcome action 61
- welcome screen
 - installation wizard 52
- window layout
 - control center 55
- Windows 12, 50, 55
- Windows control panel
 - add or remove programs 52
- WLM 3, 20, 28, 49, 76, 99, 100
 - definition 131
 - policy 24, 91, 94, 100
 - service class 17, 18, 24, 80, 81, 91
 - service class model 11, 18, 77
 - service class period 91, 95
 - service definition 20, 21, 24, 80, 81, 91, 94, 96, 99, 100
 - service policy 19, 80, 81
 - workload model 14, 76
- WLM, service class 31
- WLM, service definition 22, 30
- WLM, service policy 31
- work velocity 20
- working with domain configurations 65
- working with provisioning policies 68
- workload 24, 46
- workload classification for capacity provisioning 49
- workload condition 9, 11, 14, 17, 18, 19, 20, 21, 23, 25, 28, 30, 56, 74, 76, 77, 86, 90
 - definition 131
- workload condition panel 77
- workload condition screen 76
- workload conditions folder 75
- workload management 3, 28, 49, 99, 100
 - definition 131
- workload management policy 91, 94, 100
- workload management service class 81, 91
- workload management service class model 77
- workload management service class period 91, 95
- workload management service definition 81, 91, 94, 96, 99, 100
- workload management service policy 81
- workload manager 76
 - z/OS 14

- workload model
 - WLM 14, 76
- workload report 95
- workload target 28
- workplace screen 62
- workspace 29, 56, 57, 65
 - capacity provisioning 51
 - change 30
- workspace directory 12, 29, 61
- workstation 4, 35, 50, 51, 52, 55
 - requirements 7
- workstation, control center 36
- write log command 123

Z

- z/OS 9, 13
 - command syntax 103
 - host 51
 - operating system 9
 - Release 9 6
 - system 19, 23, 24, 33, 34, 65, 66, 77
 - workload manager 14
- z/OS, RMF 21
- z/OS, user 34
- z/VM 6
- zAAP 3, 5, 6, 11, 15, 71, 72, 92, 96, 106, 108
 - definition 131
- zAAP-eligible 50
- zIIP 3, 5, 6, 11, 15, 71, 72, 92, 96, 106, 108
 - definition 131

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

z/OS
MVS Capacity Provisioning
User's Guide
Version 1 Release 11

Publication No. SC33-8299-03

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

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

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

Comments:

Thank you for your support.

Submit your comments using one of these channels:

- Send your comments to the address on the reverse side of this form.
- Send a fax to the following number: FAX (Germany): 07031+16-3456
FAX (Other Countries): (+49)+7031+16-3456
- Send your comments via e-mail to: s390id@de.ibm.com

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

Name

Address

Company or Organization

Phone No.

E-mail address



Fold and Tape

Please do not staple

Fold and Tape



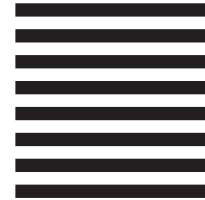
NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

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

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Research & Development GmbH
Department 3248
Schoenaicher Strasse 220
D-71032 Boeblingen
Federal Republic of Germany



Fold and Tape

Please do not staple

Fold and Tape



Program Number: 5694-A01

Printed in USA

SC33-8299-03



Spine information:



z/OS

z/OS V1R11.0 MVS Capacity Provisioning User's Guide

Version 1
Release 11

SC33-8299-03