SWsoft, Inc.

Virtuozzo Power Panels

VPS Administrator's Guide

ISBN: N/A
SWsoft Inc
13755 Sunrise Valley Drive
Suite 325
Herndon, VA 20171
USA
Tel: +1 (703) 815 5670
Fax: +1 (703) 815 5675

Contents

Table of Figures

CHAPTER 1

Introduction

The Virtuozzo Power Panels (VZPP) functionality provides you as VPS administrator with the ability to manage your VPS(s) with the help of any standard Web browser on any platform. VZPP allows you to manage Virtual Private Servers residing on Hardware Nodes running both the Windows 2003 Server and Linux operating systems. Main principles of the VZPP operation for both operating systems are very similar. However, there are some features peculiar to only Windows 2003 Server or Linux. In case of differences between the two versions, the steps written specifically for the Windows version are marked with the  icon and the steps for the Linux version - with the  icon.

A list of supported browsers is given below:

- Internet Explorer 6.0 and above;
- Mozilla 1.7 and above;
- Firefox 1.0 and above.

Chances are that you will also be able to use other browsers, but Virtuozzo has not been extensively tested with them.

Currently, you are able to manage your VPS in the following ways:

- Start, stop, or restart the VPS;
-  Mount and unmount the VPS in the repair mode;
-  Reinstall the VPS;
- Back up and restore the VPS;
- Change the VPS root/Administrator password;
- Start, stop, or restart certain services inside the VPS;
- View the list of VPS processes and send them signals;
- View the current resources consumption and resources overusage alerts;
- View logs and monitors for the VPS;
- Customize the VZPP interface;
-  Connect to the VPS by means of RDP;
-  Connect to the VPS by SSH,
- etc.

Note: Hereinafter, the root/Administrator denotation is used to identify the main user in the Linux and Windows operating systems, respectively.

In This Chapter

Logging In

To log in to your VPS, use the IP address (or hostname) and TCP port of your VPS proper. Your provider should inform you of the IP address (or hostname) and TCP port to enter in the address line of your browser and of the credentials (user name and password) to use to log in to the VPS.

There are two possible ways to log in to your VPS:

1. Enter VPS administrator credentials: the user name (`root` for a Linux-based VPS and `Administrator` for a VPS run on Windows) and the password your provider has given you.
2. Enter `admin` as the user name and the password of the Plesk `admin` user. This is possible only if the Plesk control panel is installed inside your VPS and your provider has entitled you to do so.

 Your provider may supply you with the credentials of the Plesk `admin` user for you to use the benefits of the Plesk control panel in your VPS management. If you have logged in to your VPS using the VPS IP address and the TCP port of Plesk (by default, it is 8443), and the Plesk control panel is not installed in your VPS, you will be asked to install it after you have logged in to the VPS. To do this, follow any of the links (except for the Virtuozzo link) on the Plesk main menu in the left part of the displayed window. You will be warned with a message saying that Plesk is not installed in your VPS and offering you to install it. To complete the installation you should follow the instructions on the screen. After you have successfully installed the Plesk control panel in your VPS, you can proceed with the normal course of work.

In either case, once you have connected to the VPS, you are recommended to:

1. Change your root/Administrator password at once by following the Change password link in the left pane of the VZPP page.
2. Provide a valid email address on the VZPP configuration page to be able to log in to VZPP if you forget your password. In case you are unable to reach your VPS due to password-related problems, you can follow the Forgot your password? link on the login page, which requests you to enter your user name and the email address provided on the VZPP configuration page. On filling in these fields you will receive a URL at the email address entered informing you how to change your password.

VZPP Interface Overview

The Virtuozzo Power Panels interface has been designed for the VPS administrator to quickly perform all possible tasks through an intuitive navigation system.

All VZPP pages have a *menu* on the left and a *status bar* on top. If VZPP is integrated in the Plesk control panel, the VZPP menu will be replaced with the Plesk menu. The VZPP menu looks like this:

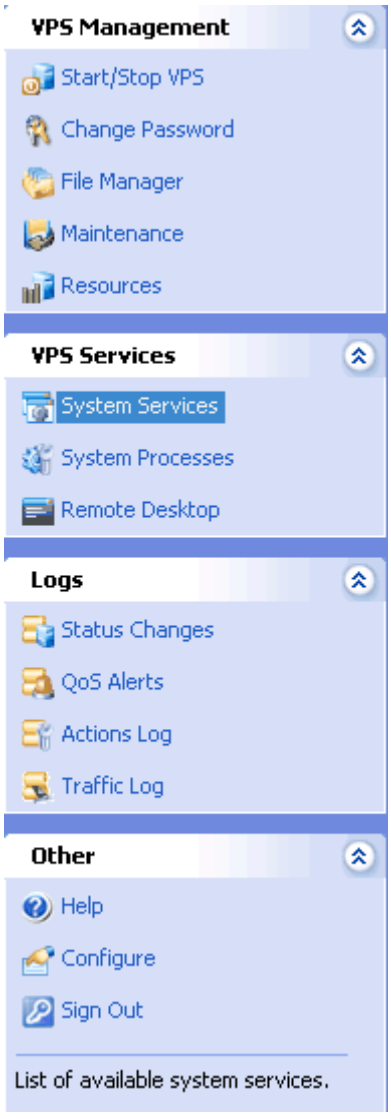


Figure 1: VZPP Menu

It provides links to VZPP pages where you can perform various tasks. To open any of these pages, run the cursor over the link and click it. The link to the page currently open is highlighted. The description of the corresponding page is displayed at the bottom of the menu. All links are gathered into four groups: VPS Management, VPS Services, Logs, and Other, the names of the first three groups being links themselves. When performing a particular task, you may first click the name of the group to open the corresponding dashboard and then choose a task, or you may select the task at once on the menu under the corresponding group.

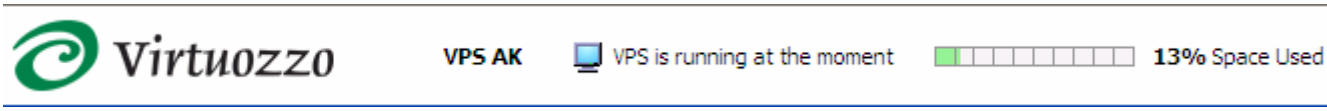
Note: If your VPS resides on the Hardware Node running the Windows 2003 Server operating system, the Firewall, Install Plesk and SSH Connection links on the VZPP menu are unavailable. At the same time, you can make use of the Remote Desktop link.

The links on the menu do the following:

Link	Description
VPS Management	Opens the VPS Management dashboard where you can learn more about various VPS management tasks and perform any of them.
Start/Stop VPS	Opens the page where you can start, stop, or reboot the current VPS.
Change Password	Opens the page for changing the VPS root/administrator password.
File Manager	Opens the File Manager page where you can view a list of files and directories and perform all the essential file operations.
Maintenance	Opens the page where you can manage your VPS backups,  recover the original template files of your VPS if something has gone wrong, or  start your VPS in the so-called repair mode to perform command line checks and fixes.
Resources	Opens the page where you can learn the current consumption of the hardware resources by your VPS.
VPS Services	Opens the Service Management dashboard, which lets you learn more about various service management tasks and perform any of them.
System Services	Opens a list of principal services inside your VPS with the opportunity to start, stop, restart any of them and to control their behavior on the VPS startup.
System Processes	Opens a list of processes running inside your VPS with the opportunity to send various signals to any of them.
Firewall	Opens your firewall current settings.
The Plesk control panel	This link is displayed only if the Plesk application template is installed in the VPS being managed. It opens the Plesk control panel login window.
Install Plesk	Open Install Plesk page that allows you to install the Plesk control panel in the VPS(s).
Confixx control panel	 This link is displayed only if the Confixx application template is installed in the VPS being managed. It opens the Confixx control panel login window.
Remote Desktop	 Opens a Remote Desktop session for connecting to your VPS via RDP.
SSH Connection	 Opens a ssh terminal window for connecting to your VPS via SSH.
Logs	Opens the Logs dashboard where you can learn more about various logs available for your VPS and view any of them.

Status Changes	Opens a list of status changes your VPS has recently undergone.
QoS Alerts	Opens a list of alerts of your VPS overusing any hardware resources or coming close to the usage limits imposed on it.
Actions Log	Opens a list of actions you have recently performed in VZPP with the current VPS.
Traffic Log	Opens the page where you can view your traffic statistics for a specified period in the past.
Help	Opens this help system.
Configure	Opens the page where you can customize the VZPP interface.
Sign out	Following this link logs you out of VZPP.

The status bar on top is presented on the following figure:



It consists of the following elements (from left to right):

1. The Virtuozzo logotype providing a link to the VZPP main page.
2. The ID or the host name of the current VPS.
3. The current state of the VPS.
4. The percent of the available disk space used by the VPS.
5. The SWsoft copyright information.

The area in the lower right corner of any VZPP page not covered by the menu and by the status bar provides the contents proper of the page. It has a *title bar* on top (just below the status bar), an example of which is shown below:

Figure 2: VZPP Title Bar

It consists of the following elements (from left to right and from top to bottom):

1. The icon corresponding to the current VZPP page.
2. The hierarchy of levels superior to the level of the current VZCC page or the links to the pages visited prior to the page you are on. These levels or links are called the route elements. They present links for moving up to any of these levels or pages.
3. The name of the current VZPP page.
4. The screen ID of the current VZPP page. If you are running any trouble with VZPP, mentioning the ID of the problem screen in your support call is likely to facilitate resolving your issue.
5. A link to the Active Tasks page. It opens the page with the list of those tasks related to managing your VPS that you have scheduled by means of VZPP, but that have not yet been completed.

6 A link to refresh the current screen.

7 A link to open the context-sensitive help. The help window opens at the topic related to the current VZPP page, but you will also be able to browse the entire help from this window.

There is an Up Level link/button at the bottom of the page which provides the way up to the the next route element from the current page.

The contents proper of any VZPP page vary depending on the screen ID. The topmost-level page, which is displayed right after logging on to VZPP, provides brief information on the current VPS in the VPS Summary table and links to the three VZPP dashboards (see above).

Notes: 1. In case your VPS is short of any resource, the corresponding warning is displayed with the link to the Resources page for you to check the state of resources consumption by your VPS. 2. In case you have not yet provided your contact e-mail, which is necessary to enable the functionality of restoring the password, a link is provided to the page where you can do it.

The VPS Summary table has the following fields:

Field Name	Description
ID	The ID of the current VPS.
Hostname	The hostname of the current VPS.
Current status	Indicates whether the VPS is running, down, being repaired, or in any other state. The description of all possible VPS statuses is provided in the VPS Statuses section (on page 30).
IP Address(es)	Specifies the IP address(es) of VPS network interfaces. These address(es) are assigned by your provider.
Operating System	Indicates what operating system is running inside your VPS.
Applications Installed	Enumerates additional applications installed in the VPS by your provider. Shown only in case there are any.

You can also download Virtuozzo Power Panels User's Guide at the bottom of the page.

CHAPTER 2

Virtual Private Server Operations

The common VPS operations are accessible in VZPP from the VPS Management dashboard. This dashboard is displayed after you click the VPS Management link on the menu.

The following VPS operations are available either by following the links under the VPS Management group on the menu or through the links on the VPS Management dashboard itself:

- Starting, stopping, or restarting the VPS (the Start/Stop VPS link);
- Working with VPS files and directories (the File Manager link);
- Viewing the current resources consumption (the Resources link);
- Changing the VPS root/administrator password (the Change Password link);
- Backing up and restoring the VPS (the Maintenance link);
-  Reinstalling the original template files into the VPS (the Maintenance link);
-  Mounting and unmounting the VPS in the repair mode (the Maintenance link).

In This Chapter

Starting and Stopping VPS

A Virtual Private Server may be started up, restarted, and shut down like an ordinary computer. The VZPP page that provides access to these functions is available on clicking the Start/Stop VPS link on the VZPP menu.

Depending on the VPS state, only those operations are accessible that comply with its current state. For example, a running VPS cannot be started for obvious reasons, and so on. The following VPS states can be characterized as stable:

Status	Description
Running	The VPS is running; therefore, it may only be restarted or stopped.
Down	The VPS is stopped; therefore, it may only be started.

Repairing	The VPS is being repaired. You cannot perform any action on the VPS until you press the Finish Repair button on the Repair Mode page.

Besides these states, during VPS operations a VPS may be in one of the transitional states: mounting, starting, stopping, etc. When in a transitional state, you cannot perform any action on the VPS until the operation is finished. The description of all possible VPS statuses is provided in the VPS Statuses section (on page 30).

Press the Start VPS, Stop VPS, or Restart VPS button to perform the corresponding action. On pressing one of these buttons, this action is logged.

If you are managing a VPS residing on the Hardware Node with the Linux operating system installed and wish to stop your VPS, bear in mind that there is a two-minute timeout for the VPS shutdown scripts to be executed. If the VPS is not stopped in two minutes, the system forcibly kills all the processes in the Virtual Private Server. The Virtual Private Server will be stopped in any case, even if it is seriously damaged. To avoid waiting for two minutes if you are operating a Virtual Private Server that is known to be corrupt, you may use the Fast Stop VPS button. The option is available only for a Service VPS user (for example, `vzagent0`).

Working With VPS Files and Folders

For a running VPS, you can navigate inside the VPS directory structure, list the VPS files and directories and perform all essential file operations on the File Manager page. This page can be accessed by following the File Manager link on the General tab of the VPS dashboard. Right after following this link, you are presented with a list of drives inside the VPS. Click on a drive (e.g. C:) to see its contents. Whatever the directory you are in, the following information is given on its contents:

Column Name	Description
T	The icon in this column indicates if this is a directory or a file.
Name	The name of the directory or file.
Size	The size of the file.
Modified	The date and time of the last modification of the directory or file.
Permissions	The first symbol in this column indicates if this is a directory (the letter `d`) or not (the minus sign). The following three symbols designate the permissions that the owner of the directory/file has on it, then go another three symbols for the permissions of the users belonging to the group assigned to the directory/file, and the final set of three symbols denotes the permissions of all the rest. The symbols in each of the set express consecutively the following permissions: read, write, and execute. The presence of a letter (correspondingly, `r`, `w`, or `x`) indicates that the permission is given, and the minus sign - that it is absent.
User	The owner of the file/directory.
Group	The users' group that has certain permissions on the file/folder. These permissions are presented by the 5th thru 7th symbols in the Permissions column.
Actions	Hyperlinks for performing certain operations with the directory or file (see below).

Note: If the VPS is being repaired (see page 19), the file manager root directory (`/`) corresponds to the `/repair` directory of the temporary VPS, in other words, it represents the root directory of the problem VPS, not that of the newly-created one.

Apart from viewing a list of files and directories with their essential properties, you are able to perform the following operations:

- Create a new folder in the current directory (see page 14);
- Create a new text file in the current directory (see page 14);
- Edit existing text files (see page 15);
- Upload a file from your local computer to the current VPS directory (see page 15);
- Download a file from the current VPS directory to your local computer (by clicking the diskette icon in the Actions column);
- Copy any number of files or folders to another directory inside the VPS (see page 15);
- Move any number of files or folders to another directory inside the VPS (see page 15);
- Edit the properties of any folder or file (see page 16).
- Remove any number of files or folders by selecting them and following the Remove link.

To perform a certain operation (e.g. copying) on a number of directories or files, tick the corresponding checkboxes. The uppermost checkbox allows you to select all the directories and files at once.

Creating Folder

The page where you can indicate the name of a new folder to be created is accessible by following the Create Folder link on the File Manager page.

Enter the folder name in the Folder Name field and click Submit. The new folder will be created in the current directory (designated above the field).

Creating Text File

The Create File page allows you to create simple text files directly inside the VPS, without having to upload them from your local computer. The page where you can do it is accessible by following the Create File link on the File Manager page.

On the Create File page, you should enter the name of the file to be created in the current directory (this directory is indicated under the page heading) and, optionally, type the text of the file. Click Create when you are finished to create the new file.

Editing Text File

VZPP allows you to edit any text file inside your VPS directly thru the VZPP interface. The Edit File page can be accessed by clicking on the central icon in the Actions column for the corresponding text file on the File Manager page.

This page presents the contents of the file in an editable field. Make your modifications and click Submit to write a new version of the file.

Uploading File To VPS

The current version of VZPP allows you to upload external files to the VPS, one file at a time. The Upload File page is displayed after clicking the Upload File link on the File Manager page.

Click the Browse button, navigate to the local file you wish to upload and double-click it. The path to the file will be displayed in the Specify File field. Another way of indicating the file is to enter this path manually.

When you click Upload, the file that you have specified will be uploaded to the current directory inside the VPS. For your reference, this directory is indicated above the Specify File field.

Copying Files and Folders Inside VPS

The Copy File(s) page, where you can perform the copy operation, gets displayed after you have selected one or more files and/or folders by ticking the corresponding checkboxes on the File Manager page and clicked Copy.

On the Copy File(s) page, click Select and, in the popup window, navigate to the folder where you want to copy the files and/or folders, check the radio button to the left of it, and press Select. The path to the target folder will be displayed in the Destination Path field. Click Copy to begin the copy process.

Moving Files and Folders Inside VPS

The Move File(s) page, where you can perform the move operation, gets displayed after you have selected one or more files and/or folders by ticking the corresponding checkboxes on the File Manager page and clicked Move.

On the Move File(s) page, click Select and, in the popup window, navigate to the folder where you want to move the files and/or folders, check the radio button to the left of it, and press Select. The path to the target folder will be displayed in the Destination Path field. Click Move to begin the move process.

Editing File or Folder Properties

The page where you can view and edit some properties of a certain file or folder is accessible by clicking the leftmost icon in the Actions column for the corresponding file or folder on the File Manager page.

The information is given on the following file or folder general properties, whether editable or not:

Field	Description	Editable?
Name	The name of the file or folder.	Yes.
Path	The path to the file or folder inside the VPS.	No. See Moving Files and Folders Inside VPS for information on how to change the path.
Size	The size of the file. To save the time needed to open the page, a link is given for a folder to calculate its overall size.	No.
Modified	The date and time of the last modification of the file or folder.	No.

 In case of a Linux-based VPS, you can also change such file/folder properties as permissions and ownership.

When you click Submit on the Change Properties page, your changes will be applied to the given file or folder.

Changing VPS Root/Administrator Password

The Change root/Administrator password page is displayed on clicking the Change Password link on the VZPP menu. Only the root/Administrator password for the current VPS can be changed. You should enter a new root/Administrator password for the current VPS into the fields provided and click Change.

Note that VZPP does not check the entered password as to its length and non-conformity to dictionary entries, so choosing a simple password rests entirely at your own risk. It is recommended to use a chaotic set of lowercase (a-z) and uppercase (A-Z) letters, digits (0-9), and punctuation marks as root/administrator password. The following punctuation marks are allowed: ! “ $ % & , ( ) * + - . / ; : < = > ? [\ ] ^ _ { | }. The space character, #, and @ symbols are not allowed. The password should not be less than 5 or more than 14 characters.

Reinstalling VPS

 VPS reinstallation means recovering the original state of a Virtual Private Server in case you have unintentionally modified, replaced, or deleted any file that is part of an application or OS template, and the action has brought about the VPS malfunction. The VPS reinstallation process restores these files as they were at the time when the VPS was created or when other applications were added to the VPS afterwards, if so.

Reinstallation is likely to bring about some irrevocable changes to your VPS, therefore, to be on the safe side, it is recommended to back up your VPS before reinstallation.

The Reinstall VPS introductory page is displayed after clicking on the Reinstall VPS link on the VZPP menu. Click Next> on this page to review the available options and to decide whether you really need to reinstall your VPS and in what way.

Note: If the VPS is running, clicking Next> on the introductory page will first take you to the page where you can stop the VPS, and only then to the page with the reinstallation options. The description of all possible VPS statuses is provided in the VPS Statuses section (on page 30).

Stopping VPS Prior to Reinstallation

The given page of the Reinstall VPS wizard is displayed only if you have selected the Reinstall VPS option for a running VPS. Inasmuch as there is no possibility to reinstall running VPSs, on this page you can stop the VPS before proceeding to the reinstallation proper.

Press Next to stop the VPS you are going to reinstall. This will take you to the page where you can view the reinstallation options and select the appropriate ones.

Selecting Reinstallation Type

The page where you should choose the mode of reinstallation is displayed after you click Next> on the Reinstall VPS introductory page. You shall select one of the two reinstallation options and specify whether to preserve or drop your VPS password database.

When selecting a reinstallation option, bear in mind that there is one thing both options have in common: the original files of the OS and applications templates are restored in the VPS. Pay attention to the fact that any customization changes you have made to these files will be lost during the VPS reinstallation. In case you have not seriously modified any system configuration files, reinstalling the original files is likely to solve many problems.

However, you have probably already filled the VPS with your personal files. If you are sure these files cannot cause problems or you need them in your VPS, select the first option - Preserve the existing VPS content. In this case, your VPS is created anew with all existing files moved to the `/old` directory inside the VPS. You shall be sure there is enough disk space to perform this operation, otherwise, it will fail. Be prepared to move the necessary files from the `/old` directory to the new existing installation manually. If such files are numerous, this may prove a tedious task.

If you think you have nothing to lose at all, select the second option: Drop the existing VPS content. Your VPS will be erased and recreated from the original template(s). Naturally, all your personal files will be lost. That is why, you should select this option only if you have no valuable data in your VPS or if you have a backup of your personal files elsewhere.

Pay attention to the Password Options group. The Preserve the password database option retains the information on the VPS users and groups. Selecting the Drop the password database radio button will purge this information altogether and create only the root account with the password specified in the Set root password and Retype password fields under the radio button. This option may prove useful if your VPS has got a corrupted password database.

When you are done, click Next> to proceed to the Reinstall VPS confirmation page.

Confirming Reinstallation

On the third page of the Reinstall VPS wizard you shall confirm the reinstallation or give it up. The reinstallation option you have chosen at the previous step is displayed for you to have a last chance to revise what you are about to do. Press the Do Reinstall button to begin the reinstallation process.

Do not forget to start the VPS when the operation is complete. To see the current status of the operation, click the Active Tasks link or press the  ,  , or  icon on the title bar. Note that the icons vary according to the interface skin selected.

Repairing VPS

 Repairing a VPS is another way to solve problems with the VPS functioning. In Virtuozzo terminology, the VPS is mounted in the repair mode. This means that a new VPS is temporarily created from scratch with the same network and other parameters as the broken VPS, and the root directory of the broken VPS is mounted as `/repair` into the newly-created VPS. Thereafter, the administrator is supposed to connect to the new VPS via `ssh` or VZPP file manager (see page 13) using the network and login parameters of the broken VPS, go to the `/repair` directory, and perform one of the following actions:

1. Find the personal data that needs to be saved and copy it to a safe location elsewhere. Do not copy your personal data directly into your new VPS, as it will be destroyed once you exit the repair mode. After quitting the repair mode, the broken VPS can be reinstalled and the personal data can further be loaded into it from the place where you have saved them.
2. Identify the source of the problem and manually correct it. This method can be recommended to advanced VPS administrators, as it presupposes some technical expertise. And it is still recommended to save first your personal data in a safe location, just in case something goes wrong.

Note: When working inside the VPS being repaired by means of the VZPP file manager, the file manager root directory (`/`) corresponds to the `/repair` directory of the temporary VPS, in other words, it represents the root directory of the problem VPS, not that of the newly-created one.

The Repair Mode page is accessible through the Repair Mode link on the VZPP menu. Pressing the Run Repair button on this page mounts the VPS in the repair mode. It is not necessary to stop the VPS beforehand; if the VPS is running at the moment of pressing the Run Repair button, it will be first automatically stopped. The description of all possible VPS statuses is provided in the VPS Statuses section (on page 30).

When the page is refreshed after pressing the Run Repair button, click the Details link at the end of the blue line to see if the repair mode has been successfully entered. Once the VPS enters the repair mode, connect to the new VPS via `ssh` or VZPP file manager and do what you deem reasonable inside the VPS. After closing your `ssh` session, press the Repair Mode link on the VZPP menu once again and press the Finish Repair button to exit the repair mode. After the repair mode is exited, the broken VPS is returned to the stopped state, and you may start it to check the repairing effect.

Backing Up and Restoring VPS

Any Virtual Private Server is defined by its operating system files, applications installed, configuration files, and personal information. VZPP allows you to back up all these components. A regular backing up of the existing Virtual Private Servers is essential for any VPS reliability.

The Maintenance page, which allows you to perform backing up and restoring operations, opens after you click the Maintenance link on the main menu or selecting the Maintenance link on the VPS Management dashboard accessible after clicking the VPS Management link on the menu. If you already have backups of the given VPS, it displays a table summarizing the backups.

Note: Apart from dealing with VPS backups, the Maintenance tab gathers links for all those operations that would guarantee the integrity and overall operability of your VPS, such as reinstalling the VPS (the Reinstall VPS link) and mounting the VPS in the Repair Mode (the Repair Mode link).

Column Name	Description
Backed Up	The date and time when the backing up was performed.
Size	The size of the backup.
Type	Denotes if it is a full or incremental backup. An incremental backup stores not all the files and settings of the VPS at the given period of time, but only the changes the VPS has undergone since the last backup.

You can manage your backups on this page in the following ways:

- The New Backup button begins the process of backing up the current state of your VPS, be it running or not. The description of all possible VPS statuses is provided in the VPS Statuses section (on page 30). This option is available only if you have not reached the maximal number of allowed backups for your VPS. If you have, remove one of the backups first (see below for details). VZPP allows you to place the backup of your VPS only onto the Node where your VPS is hosted.
- The Restore VPS button restores the VPS backup currently selected in the table. Only one backup should be selected for this operation. The page opened provides instructions to guide you through the process. The VPS will be restored with all the values overwritten from the backup, including its IP address, password, application set, etc. The changes in the VPS made after the date of this backup will be lost after the VPS has been restored.

  Note: If you are using an IP address of your VPS to connect to it, you may have to reconnect to the VPS with the IP address retrieved from the backup after the VPS is restored.

- The Remove Backups button removes the VPS backup(s) currently selected in the table. Usually this is done to provide extra space for making new VPS backups. Use the checkbox at the upper left corner to select/deselect all the backups at once.
- If you have reached the limit on the number of VPS backups you are allowed to create, you can make use of the Renew Backup button to renew a VPS backup without having to delete any of your existing VPS backups. By default, the oldest backup is renewed. You can also renew another VPS backup by selecting the checkbox opposite the corresponding backup and clicking on the Renew Backup button.
- Clicking on a backup date in the table opens the Backup Details page where you can also restore or remove the corresponding VPS backup.

Backup Details

The Backup Details page available by clicking any backup link on the list of VPS backups provides general information on the corresponding backup and lets you perform a number of actions on the given backup by pressing the corresponding buttons. The information on backups is presented in the following table:

Column Name	Description
Creation Date	The date and time when the backing up was performed.
Backup Size	The size of the backup.
Backup Type	Denotes if it is a full or incremental backup. An incremental backup stores not all the files and settings of the VPS at the given period of time, but only the changes the VPS has undergone since the last backup.
Hostname	The hostname the VPS had at the backup time. If the VPS is restored from this backup, this hostname is also restored and replaces the current one.
IP Address(es)	The IP address(es) the VPS had at the backup time. If the VPS is restored from this backup, these addresses are also restored and replace the current one(s).
Applications Installed	All applications that had been installed in the VPS by the backup time. If the VPS is restored from this backup, these applications are also restored and replace the current one(s). Shown only in case there are any applications in the given VPS backup.

- The Browse Backup link (see page 22) allows you to browse the directory structure of the archived VPS as if it had been already restored and to restore only the needed files and folders.
- The Restore VPS button restores the VPS from the current backup. The changes in the VPS made after the date of this backup will be lost after the VPS has been restored. Mind that you have to confirm restoring the VPS on the Restore Confirmation page to accomplish the process.
- The Remove Backup button removes the current VPS backup. Usually this is done to provide extra space for making new VPS backups.

Browsing Backup Contents

VZPP allows you to browse the directory structure of any VPS backup as if this backup had already been restored and restore only the needed files and folders. The Browse Backup page opens after you follow the Browse Backup link on the Backup Details page (see page 21).

The contents of any directory inside a backup is presented in the table providing the following information:

Column Name	Description
T	The icon in this column indicates if this is a directory or a file.
Name	The name of the directory or file.
Size	The size of the file.
Modified	The date and time of the last modification of the directory or file.

It is worth noting that if you are browsing an incremental backup, the information is shown not only on the files and folders from this backup, but on all the contents of the VPS, should it be restored from this incremental backup. In other words, the backed up VPS is always presented in its integrity and not as a collections of sporadic changes from the incremental backup.

To restore separate files and folders from the backup to the actual VPS, just select them by ticking the corresponding checkboxes in the rightmost column and click the Restore link.

Monitoring VPS Resources

The Resources feature of VZPP allows you to view the current consumption of hardware resources by a Virtual Private Server. On the Resources page you can view the consumption of principal resources - CPU units, system resources, bandwidth, disk space, and disk inodes. This page is displayed on clicking the Resources link on the VZPP menu.

You can learn about the current consumption of the corresponding resource, and about the quota imposed on this resource for the VPS. The percent bars graphically show the current consumption of resources by the VPS.

In the Current VPS template table at the top of the Resources page, you can view the name, description and additional info on the VPS template the given Virtual Private Server is based on. The name and description of the VPS template is unavailable for a Windows-based VPS due to the present limitations of the product.

The resources and the usage data displayed on the Resources page are explained in the following table:

CPU — This is a positive integer number that determines the minimal guaranteed percentage share of the CPU time your Virtual Private Server will receive. For stopped VPSs, this parameter is not available. Load Average for the CPU usage is the average number of active processes for the past 1, 5, and 15 minutes, respectively. Value 0.00 means that the CPU is idle, 1.00 that the CPU is fully used. Value 2.00 denotes that the CPU load exceeds the nominal value by two times.

System	This is a cumulative figure presenting the averaged consumption of a number of critical memory-related parameters by your VPS.
Disk Space	Total amount of disk space allocated to the Virtual Private Server. When the space used by the Virtual Private Server hits the soft limit (or reaches 100% on the percent bar), the VPS can be allowed additional disk space up to the hard limit during the grace period (see below for more details on the grace period). To the left of the percent bar there is a table presenting a more detailed account of the resource usage. It deciphers the percentage figure at the bar and yields the numeric data on the total amount of disk space set for the VPS, the disk space consumed at the moment and the portion of the disk space that rests yet available for the VPS usage.
Disk Inodes	Total number of disk inodes (files, directories, and symbolic links) allocated by the Virtual Private Server. When the number of inodes used by the Virtual Private Server hits the soft limit, the VPS can create additional file entries up to the hard limit during the grace period (see below for the more details on the grace period). To the left of the percent bar there is a table with a more detailed account of the resource usage. It deciphers the percentage figure at the bar and yields the numeric data on the total number of disk inodes set for the VPS, the number of disk inodes consumed at the moment and the share that rests yet available for the VPS usage.
Bandwidth	There may be limitations imposed on the bandwidth for outgoing traffic available for the VPS. This indicator shows what portion of available bandwidth is currently used.

You can view details on the resources consumption by clicking the Extended button.

Note: If any resource has "n/a" in the Current Use field, this means that either this field makes no sense for the given resource (for example, the `quotatime` resource is not used if you are not on the grace period) or your VPS is down, so some information on resources consumption cannot be fetched.

The resources are grouped by their relations to various computer subsystems for you to easier find the information on the resource that interests you. The last three groups of VPS resources - Primary UBC Parameters, Secondary UBC Parameters, and Auxiliary UBC Parameters - are the ones that constitute the averaged value of the System parameter on top of the Resources page.

Note: The Secondary UBC Parameters and Auxiliary UBC Parameters groups are available only for HNs with the Linux operating system installed.

To learn more on the particular resources comprising all the presented groups, see the Extended Resource Consumption Data section (on page 27).

System Resource

The System percent bar on the Resources page reflects the current consumption of the Hardware Node memory-related resources by your Virtual Private Server. These resources can be displayed by clicking the Primary UBC parameters block on the Resources page. The current memory consumption of your VPS may relate to either of the four zones: green, yellow or red. There is also a black zone indicator implemented for Linux-based VPSs.

The System percent bar is marked green if the VPS on the average consumes less than 90% of memory-related resources allowed to it. To view the current consumption of any particular memory-related resource, press the Extended button on the Resources page.

The System percent bar is marked yellow if the VPS consumes between 90% and 100% of the memory-related resources allowed to it. This is an averaged value, so you should find out what particular resource is causing the problem. To view the current consumption of any particular memory-related resource, press the Extended button on the Resources page.

It is up to you to decide whether this situation suits you, but you should bear in mind that additional applications launched inside the VPS might experience shortage of some memory-related resources. Judging by the offending resource, you might determine the reason for its shortage and take the corresponding measures.

The System percent bar is marked red if the VPS is currently consuming 100% or more of the memory-related resources allowed to it. This is a very serious situation, so you should get to know what particular resources are causing the problem as the shown value is average across all the memory-related resources. To view the current consumption of any particular memory-related resource, press the Extended button on the Resources page. Judging by the offending resources, determine the reason for the problem or call for your provider's support.

A VPS is allowed to consume more than 100% of its quota only in extreme situations. If you do not solve the problem in a reasonable time, applications running inside the VPS may be denied some of the resources, so application crashes and other problems are most probable.

 The System percent bar is marked black if the VPS has been denied some memory-related resources due to their overusage. This might have resulted in application crashes or other problems inside the VPS. This is a very serious situation, so you should get to know what particular resources are causing the problem as the shown value is the average across all the memory-related resources. To view the current consumption of any particular memory-related resource, press the Extended button on the Resources page. Judging by the offending resources, determine the reason for the problem or call for your provider's support.

Note: After the situation has been corrected, please wait 4 minutes for the zone color to be reset.

CPU Resource

The CPU percent bar on the Resources page reflects the current consumption of the Hardware Node CPU time by the Virtual Private Server. The percent value is calculated not in proportion to the power of the Hardware Node, but in proportion to the limit on using the Node CPU power by the VPS. Judging by the color of the percent bar, the current CPU consumption of the VPS may relate to either of the three zones: green, yellow, and red.

The CPU percent bar is marked green if the VPS consumes less than 90% of the CPU time allowed to it. This means that you can run more applications inside the VPS without violating the performance of the current ones. If the VPS consumes more than 90% of the allowed CPU time, but for an insignificant time, the color remains green as this situation is not perilous.

The CPU percent bar is marked yellow if the VPS consumes between 90% and 100% of the CPU power allowed to it for a relatively long while. Usually this means that the running processes consume too much CPU power. It is up to you to decide whether this situation suits you, but you should bear in mind that additional applications launched inside the VPS might experience shortage of available CPU power. You may need to consider the possibility of cutting down the number of processes.

The CPU percent bar is marked red if the VPS consumes 100% of the CPU power allowed to it, i.e. all the available CPU power, for a long time. Usually this means that currently there is some CPU-intensive process inside the VPS caused by a temporary task. For example, this may happen if you are compiling a package in the VPS or in similar cases. In this case you should simply wait for this task to complete.

However, if you do not know the reason for the CPU overconsumption, turn to the VZPP System processes page to determine which process(es) are causing the problem and take the corresponding measures. For example, you might want to terminate or kill the offending process. Otherwise, the system performance may continue low for a long while.

Bandwidth Resource

 The Bandwidth percent bar on the Resources page informs you of the bandwidth for outgoing traffic the VPS is currently using related to the bandwidth limit you have imposed on the VPS. There can be no limitations on the bandwidth for in-going traffic, so there's no indicator for it. The value of the bandwidth parameter is not calculated in real time, but averaged for the latest hour.

As far as you cannot exceed the bandwidth limit and there is no danger in approaching this limit, the bandwidth consumption is always in the green zone, unlike other resources consumption. If you do not set any bandwidth limits, the bandwidth parameter is not available.

Disk Space Resource

The Disk Space percent bar on the Resources page and on the status bar of any VZPP window reflects the current consumption of the Hardware Node disk space by the Virtual Private Server. The percent value is calculated not in proportion to the total disk space of the Hardware Node, but in proportion to the soft limit (quota) on using the Node disk space by the VPS.Judging by the color of the percent bar, the current disk space consumption by the VPS may relate to either of the four zones: green, yellow or red.  There is also a black zone indicator for VPSs hosted on a Linux Node.

The Disk Space percent bar is marked green if the VPS consumes less than 90% of disk space allowed to it. This means that the VPS has currently no problem with disk space.

The Disk Space percent bar is marked yellow if the VPS is using between 90% to 95% of the disk space available to it on the Hardware Node. The situation is moderately dangerous. You should consider the possibility of erasing unnecessary data from the VPS, or it may be a problem to upload new data to it.

The Disk Space percent bar is marked red if the disk space consumption value lies within the range from 95% to 100% allowed to the VPS on the Hardware Node. This is a very serious situation, and, depending on the considered parameter, either some process might be killed at any time in the VPS, or the next resource allocation request might be refused to you VPS. Therefore you should erase unnecessary data from the VPS immediately. On a Linux Node, a VPS is allowed to consume more than 100% of its quota only during the grace period (see the `quotatime` parameter in the resources consumption details). If you do not solve the problem during this time, the VPS will be denied some of the disk space and you might lose valuable data. For a VPS running on a Linux Node you can consult `.ssh` directories to rearrange the disk space consumption.

 The Disk Space percent bar is marked black if the VPS has reached the hard limit, and either a resource allocation has been refused or some process has been killed. This might have resulted in a loss of some valuable data or other problems inside the VPS. To discontinue this very serious situation, you should erase unnecessary data from the VPS immediately.

Note: After the situation has been corrected, please wait 4 minutes for the zone color to be reset.

Disk Inodes Resource

 The Disk Inodes percent bar on the Resources page reflects the current consumption of the Hardware Node disk inodes (files, directories, and symbolic links) by the Virtual Private Server. The percent value is calculated not in proportion to the total disk inodes available on the Hardware Node, but in proportion to the soft limit (quota) on using the disk inodes by the VPS. Judging by the color of the percent bar, the current disk inodes consumption by the VPS may relate to either of the four zones: green, yellow, red, or black.

The Disk Inodes percent bar is marked green if the VPS uses less than 90% of disk inodes allowed to it. This means that new files, directories, or symbolic links can so far be fearlessly created inside the VPS.

The Disk Inodes percent bar is marked yellow if the VPS uses between 90% and 100% of the disk inodes available to it on the Hardware Node. You should consider the possibility of erasing unnecessary files/directories/symbolic links from the VPS, or it may be a problem to upload new data to it.

The Disk Inodes percent bar is marked red if the VPS is currently using 100% or more of disk inodes allowed to it on the Hardware Node. This is a very serious situation, so you should erase unnecessary files/directories/symbolic links from the VPS immediately. A VPS is allowed to consume more than 100% of its quota only during the grace period (see the `quotatime` parameter in the resources consumption details). If you do not solve the problem during this time, the VPS will be denied some of the disk inodes and you might lose valuable data.

The Disk Inodes percent bar is marked black if the VPS has been denied some disk inodes due to their overusage. This might have resulted in a loss of some valuable data or other problems inside the VPS. To discontinue this very serious situation, you should erase unnecessary files/directories/symbolic links from the VPS immediately.

Note: After the situation has been corrected, please wait 4 minutes for the zone color to be reset.

Extended Resource Consumption Data

The Extended page (accessible through opening the Resources page first via VZPP menu and then clicking the Extended button on the displayed page) provides an ample description of every resource parameter used by the VPS.

The following resource parameters are available for extended monitoring:

CPU Parameters

Parameter	Description
`cpuunits`	This is a positive integer number that determines the minimal guaranteed share of the CPU time your Virtual Private Server will receive.
`cpulimit`	This is a positive number indicating the CPU time in per cent the corresponding VPS is not allowed to exceed.

Disk Quota

Parameter	Description
`diskinodes`	Total number of disk inodes (files, directories, and symbolic links) allocated by the Virtual Private Server. When the number of inodes used by the Virtual Private Server hits the soft limit, the VPS can create additional file entries up to the hard limit during the grace period.
`diskspace`	Total size of disk space consumed by the Virtual Private Server. When the space used by the Virtual Private Server hits the soft limit, the VPS can allocate additional disk space up to the hard limit during the grace period.
`quotatime`	The grace period for the disk quota overusage defined in seconds. The Virtual Private Server is allowed to temporarily exceed its quota soft limits for no more than the `QUOTATIME` period.
`quotaugidlimit`	Number of user/group IDs allowed for VPS internal disk quota. If set to 0, UID/GID quota will not be enabled.

The resources a Virtual Private Server may allocate are defined by the system resource control parameters, also called user beancounters (UBC). These parameters can be subdivided into the following categories: primary, secondary and auxiliary parameters. The primary parameters are the starting point for defining the relative power of a Virtual Private Server. The secondary parameters are dependent on the primary ones and are calculated from them according to a set of constraints. The auxiliary parameters help improve fault isolation among applications in one and the same Virtual Private Server and the way applications handle errors and consume resources.

Listed below are all the system resource control parameters. The parameters starting with "num" are measured in integers. The parameters ending in "buf" or "size" are measured in bytes. The parameters containing "pages" in their names are measured in 4096-byte pages in the Virtuozzo 32-bit version and in 16384-byte pages in the Virtuozzo 64-bit version for IA-64 processors.

Primary UBC parameters

Parameter	Description
`numproc`	The maximal number of processes the VPS may create.
`numsessions`	The number of simultaneous terminal sessions that can be opened to the VPS.
`vprvmem`	The size of private (or potentially private) memory allocated by the VPS. The memory that is always shared among different applications is not included in this resource parameter.
`numtcpsock`	The number of TCP sockets (PF_INET family, SOCK_STREAM type). This parameter limits the number of TCP connections and, thus, the number of clients the server application can handle in parallel.
`numothersock`	The number of sockets other than TCP ones. Local (UNIX-domain) sockets are used for communications inside the system. UDP sockets are used, for example, for Domain Name Service (DNS) queries. UDP and other sockets may also be used in some very specialized applications (SNMP agents and others).
`vmguarpages`	The memory allocation guarantee, in pages. VPS applications are guaranteed to be able to allocate additional memory so long as the amount of memory accounted as privvmpages (see the auxiliary parameters) does not exceed the configured barrier of the vmguarpages parameter. Above the barrier, additional memory allocation is not guaranteed and may fail in case of overall memory shortage.
`avnumproc`	The average number of processes and threads.

Secondary parameters

Parameter	Description
`kmemsize`	The size of unswappable kernel memory allocated for the internal kernel structures for the processes of a particular VPS.
	Note: For the Virtuozzo 64-bit version for IA-64 processors, it takes 4 (four) times more the size of the kernel memory than that for the Virtuozzo 32-bit version to handle one and the same process.

`tcpsndbuf`	The total size of send buffers for TCP sockets, i.e. the amount of kernel memory allocated for the data sent from an application to a TCP socket, but not acknowledged by the remote side yet.
`tcprcvbuf`	The total size of receive buffers for TCP sockets, i.e. the amount of kernel memory allocated for the data received from the remote side, but not read by the local application yet.
`othersockbuf`	The total size of UNIX-domain socket buffers, UDP, and other datagram protocol send buffers.
`dgramrcvbuf`	The total size of receive buffers of UDP and other datagram protocols.
`oomguarpages`	The out-of-memory guarantee, in pages. Any VPS process will not be killed even in case of heavy memory shortage if the current memory consumption (including both physical memory and swap) does not reach the oomguarpages barrier.

Auxiliary parameters

Parameter	Description
`privvmpages`	The size of private (or potentially private) memory allocated by an application. The memory that is always shared among different applications is not included in this resource parameter.
`lockedpages`	The memory not allowed to be swapped out (locked with the mlock() system call), in pages.
`shmpages`	The total size of shared memory (including IPC, shared anonymous mappings and tmpfs objects) allocated by the processes of a particular VPS, in pages.
`numfile`	The number of files opened by all VPS processes.
`numflock`	The number of file locks created by all VPS processes.
`numpty`	The number of pseudo-terminals, such as an ssh session, the screen or xterm applications, etc.
`numsiginfo`	The number of siginfo structures (essentially, this parameter limits the size of the signal delivery queue).
`dcachesize`	The total size of dentry and inode structures locked in the memory.
`numiptent`	The number of IP packet filtering entries.

The information on the resources is organized into the following table:

Column Name	Description
ID	The name of the QoS parameter.
Current Use	The numerical representation of the resource consumption by the VPS at the moment.
Limit	The limit on the consumption of the given resource by the VPS.

Soft Limit	The limit on the consumption of the given resource by the VPS that once reached or exceeded can lead to grave problems inside the VPS. Depending on the considered parameter, either some process might be killed at any time in the VPS, or the next resource allocation request might be refused to it. However, the VPS is allowed to temporarily exceed its quota soft limit for the Disk Space and Disk Inodes resources without any damage to the VPS processes for the grace period, set in the `quotatime` parameter in the Disk Quota table.
Hard Limit	The limit on the consumption of the given resource by the current VPS that cannot be exceeded in any circumstances.
Units	The units in which the value of the Limit/ Soft Limit and Hard Limit column is measured.
Description	The description of the parameter.

VPS Statuses

At any point of time, any VPS is characterized by a status (or state). There are four stable statuses and a number of transitional statuses that a VPS may have. If the VPS is in one of the stable states, it means that it is likely to continue in this state until its administrator performs a task that would change its status. If the VPS is in one of the transitional states, it means that it is currently passing from one stable state to another. During a transition stage, no operation can be performed on the VPS until the transition is finished.

The stable statuses are:

Status	Description	Possible Actions
`down`	The VPS is stopped and its private area is unmounted.	Starting/repairing/reinstalling
`mounted`	The VPS private area is initialized and ready to work, but the VPS is not running.	Starting
`running`	The VPS private area is mounted and the VPS is running.	Stopping/rebooting/repairing
`repairing`	The VPS is mounted in the repair mode.	Exiting the repair mode.

The transition statuses are:

Status	Description
`creating`	The VPS is being created.
`mounting`	The VPS is being mounted.
`starting`	The VPS is being started.
`stopping`	The VPS is being stopped.
`unmounting`	The VPS is being unmounted.
`destroying`	The VPS is being destroyed.
`starting-repair`	The VPS is entering the repair mode.
`stopping-repair`	The VPS is quitting the repair mode.

`setting`	The VPS parameters are being set.
`migrating`	The VPS is being migrated.
`moving`	The VPS is being moved.
`cloning`	The VPS is being cloned.
`updating`	The VPS is being updated.
`backing-up`	The VPS is being backed up.
`restoring`	The VPS is being restored.

CHAPTER 3

Managing VPS Services and Processes

VZPP allows you to manage services and processes inside VPSs in a number of ways by following the corresponding links on the VPS Services dashboard. You can:

- Open a list of principal services inside your VPS through the System Services link with the opportunity to start, stop, restart any of them and control their autostart option.
- Open a list of processes running inside the VPS by clicking the System Processes link with the opportunity to send various signals to any of the processes.
- Log in to the Plesk control panel via the Plesk Panel link in case the corresponding template is installed in the VPS. If the Plesk template is not installed, the Plesk Panel link is not displayed. Instead you can make use of the Install Plesk link provided in lieu of the Plesk Panel link to install the Plesk control panel in the VPS ( this link is available for a Virtual Private Server running the Linux operating system).
-  Log in to the Confixx control panel by choosing the Confixx control panel link in case the corresponding template is installed in the VPS. If the template is not installed, the Confixx control panel link is not displayed. The feature is available for a Linux-based VPS.
-  Open an `ssh` terminal window with the help the SSH Connection link for connecting to the VPS via SSH. This link is available if you are managing a VPS running the Linux operating system.
-  Open a Remote Desktop terminal window through the Remote Desktop link for connecting to the VPS via RDP (Remote Desktop Protocol). This link is available if you are managing a VPS running Windows 2003 Server.
-  Open the VPS Firewall page through the Firewall link if the VPS you manage runs the Linux OS.

In This Chapter

Managing VPS Services

The process of managing services inside Virtual Private Servers running the Windows operating system and the Linux operating system varies slightly:

- To learn how to manage services in VPSs running the Linux operating system, please see the Managing Services in Linux subsection.
- To learn how to manage services in VPSs running the Windows operating system, please see the Managing Services in Windows subsection.

Managing Services in Linux

 The System Services page is displayed after clicking on the System Services link on the VPS Services dashboard. The page has two tabs: Standard and Xinetd (see page 34).

The Standard tab is used to view all the services you are running on the VPS except for the `xinetd`-dependent services. To see the `xinetd`-dependent services list, click the Xinetd tab. By default, 20 services are shown for each tab, but you may have more services displayed by pressing the appropriate link on top of the table. You may also have the System Services table display only those services that have a particular name or status. On top of the table, press the  icon to display the fields where you can specify the name or the status of the service you wish to view; then click on the Search link.

The Standard page presents a table reflecting the services inside the VPS and providing the following information:

Column Name	Description
Name	The system ID of the service executable file.
Status	Indicates whether the service is running or not. A green arrow means that the service is running; a red cross - that it is stopped.
Autostart	If there is a green tick in this column, this service is started automatically on the VPS startup; if a red cross - it is not.

You can perform the following actions on any service in the table:

- Stop the service by selecting its checkbox and clicking on the Stop button. Only running services are subject to this action.
- Restart the service by selecting its checkbox and clicking Restart. Only running services are subject to this action.
- Start the service by selecting its checkbox and clicking on the Start button. Only stopped services are subject to this action.
- Enable/disable the autostart feature by clicking the name of the service in the Name column and opening the Services Details page, where you can manage the option.

Note: If you have just started the VPS and opened the Services page, not all the services may have had enough time to start. Wait a little and refresh the page to update the state of the services.

Managing xinetd-Dependent Services

The System Services page is displayed after clicking on the System Services link on the VPS Services dashboard. The page has two tabs: Standard (see page 33) and Xinetd.

The Xinetd tab is used to view all the services you are running on this VPS that are dependent on the `xinetd` service. To see the other services, click the Standard tab. By default, 20 services are shown for each tab, but you may have more services displayed by pressing the appropriate link on top of the table. You may also have the System Services table display only those services that have a particular name or status. On top of the table, press the icon to display the fields where you can specify the name or the status of the service you wish to view; then click on the Search link.

The Xinetd page presents a table reflecting the `xinetd`-dependent services inside the VPS and providing the following information:

Column Name	Description
Name	The system ID of the service executable file.
Status	Indicates whether the service is enabled or not. A green arrow means that the service is enabled; a red cross - that it is disabled.
Autostart	If there is a tick in this column, the `xinetd` service is started automatically on the VPS startup, so is the given service; if a cross - it is not.

You can perform the following actions on any service in the table:

- Enable the service by selecting its checkbox and clicking on the Enable button. Only disabled services are subject to this action.
- Disable the service by selecting its checkbox and clicking on the Disable button. Only enabled services are subject to this action.

Viewing Service Details

 The Service Details page opened on clicking the name of the service you have selected on the System Services page provides the principal information on the given service and lets you manage it.

The following information is provided:

- The description of the service;
- Whether the service is running or stopped;
- Whether the service is started automatically on the VPS startup or not.

You may perform the following actions on any such service:

- Stop the service by clicking the Stop Service button. Only running services are subject to this action.
- Restart the service by clicking the Restart Service button. Only running services are subject to this action.
- Start the service by clicking the Start Service button. Only stopped services are subject to this action.
- Enable/disable the autostart feature by clicking the Enable Autostart/ Disable Autostart button, correspondingly.

Viewing xinetd-Dependent Service Details

 The Service Details page opened on clicking the name of the service you have selected on the Xinetd tab of the System Services page provides the principal information on the given service and lets you manage it.

As the service is dependent on the xinetd service, i.e. xinetd is charged with launching the service when necessary, you can only either enable or disable such a service - depending on its current state - by clicking the Enable/Disable Service button, correspondingly. Moreover, the `xinetd` service must be running to perform any such action; otherwise, the operation will result in an error. You cannot manage the autostart feature of `xinetd`-dependent services, as its value is inherited from the `xinetd` service.

Managing Services in Windows

 The System Services page is displayed when clicking on the System Services link on the VZPP main menu. It presents the table reflecting those services inside your VPS that you can manage. The table provides the following information:

Column Name	Description
Name	The name of the service running inside your VPS.
Status	Indicates whether the service is running or not.
Startup Type	Indicates whether: ▪ The service is started automatically on the VPS startup; ▪ The startup type of the service is set to `SERVICE_DISABLED`.

Logon as	Indicates the user account (the `LocalService` account, the `NetworkService` account, etc.) that was used to start the service.

You can perform the following operations on any service in the table:

- Stop the service by selecting its checkbox and clicking on the Stop button. Only running services are subject to this action.
- Restart the service by selecting its checkbox and clicking Restart. Only running services are subject to this action.
- Start the service by selecting its checkbox and clicking on the Start button. Only stopped services are subject to this action.
- Open the Services Details page to enable/disable the autostart feature by clicking on the name of the service in the Name column.

To facilitate working with VPS services, you may have the System Services table display only those services that have a particular name, startup type (automatic, manual, disabled), are in a certain state (running or stopped), or were started by a certain user. On top of the table, press the icon to display the fields where you can specify the parameters your services should meet; then click on the Search link. To view all the services currently running inside your VPS, click on the Show All link to the right of the parameter fields.

Changing Service Startup Type

The Service Management page opened on clicking the name of the service you have selected on the System Services page allows you to change the startup type of your VPS services:

- Make a service automatically start on the VPS startup by selecting the Automatic Startup checkbox and clicking on the Submit button.
- Set a service as "manual" meaning that you should start the service manually before it can be loaded by the operating system and made available for use. To this effect, select the Manual Startup checkbox and click on the Submit button.
- Disable a service by selecting the Startup is Disabled checkbox and clicking on the Submit button.

Note: Changing the default service settings might prevent key services from running correctly. It is especially important to use caution when changing the startup type of services that are configured to start automatically.

Managing VPS Processes

The System Processes page is displayed when clicking on the System Processes link on the VPS Services dashboard. It presents a table reflecting all the running processes inside the VPS. The table provides the following information:

Column Name	Description
PID	The process ID.
%CPU	The percent of the CPU time the process is currently using.
%MEM	The percent of the RAM size the process is currently using.

Command	The command that is used to launch the process.
Nice	The relative priority of the process assigned to it by the user. The negative values mean that the user has manually increased the priority, the positive values - that they have decreased it.
Pri	The absolute priority of the process assigned to it by the process scheduler. On a Linux Node, the range is from 0 (the highest priority) to 39 (the lowest priority). The usual process priority is 30. On a Windows Node, the range can be from 0 (the highest priority) to 31 (the lowest priority). The usual process priority is 8.
RSS	(Resident Segment Size) The size of physical memory the process really uses (in Kilobytes).
Stat	The state of the process. The possible states are: R - runnable, on the run queue; S - sleeping; T - traced or stopped; D - uninterruptable sleep; Z - defunct, "zombie". If two letters are shown, the second letter means the following: W - has no resident pages; < - high-priority process; N - low-priority task; L - has pages locked in memory; s - the process is a session leader; "+" means the process is in the foreground process group of its control terminal.
Time	The total amount of the CPU time the process has used so far.
User	The user the process belongs to.

To have the information in the table refreshed automatically with the current values, click the Enable Auto Refresh button. It is worthy to note that only the table on the current page is refreshed, which takes much less resources in comparison with refreshing the whole VZCC page.

You may select any number of processes by ticking the checkbox(es) against the corresponding process(es) (tick the uppermost checkbox to select all the processes at once) and send them a standard signal. Choose the needed signal on the drop-down menu and press the Send Signal button. The following signals can be sent:

- SIGHUP - is a hang-up signal. It is often used to ask a daemon process to re-read its configuration.
- SIGTERM - sends the termination signal to the process. This is the best way to give the process a chance for an orderly shutdown and proper data saving. As the process might be able to catch this signal and stay alive, you may have to make use of the sigkill or sigint signals.
- SIGCONT - continues the process causing it to resume.
- SIGSTOP - stops (suspends) the process. The process will still be on the task list.
- SIGINT - causes the process to immediately interrupt. The signal is very close to sigkill, the difference being that, unlike sigkill, it can be caught by the process and ignored if the process gets out of hand. In this case you should send sigkill to shut down the process.
- SIGKILL - unconditionally kills the process. Mind that sending sigkill to any process removes any chance for it to do a tidy cleanup and shutdown, which might have unfortunate consequences.

Managing VPS Firewall

A firewall is part of your OS and its security. Its main function is to block or permit traffic between two systems or two parts of a network. A firewall is either a program (or a set of programs) or a computer it runs on. Virtuozzo has a built-in firewall that can be managed through both the Virtuozzo Power Panels and the Virtuozzo Control Center. Along with - and apart from - the VZPP and VZCC web interface a command line is an effective tool to manage a firewall. Here are the basic principles that make a firewall work.

A firewall applies a control *policy* over the firewalled system. There are three policies:

- *accept* the packet: if the packet is accepted, it gains access to the system;
- *drop* the packet: if the policy is to drop the packet, the packet is denied access to the system;
- *reject* the packet: the system does not let the packet in, notifying the sender of the fact;

The policies, along with ports and protocols, are chains' attributes. A *chain* is a list (or a chain) of rules grouped by the criterion of what type of packets they process. There are three packets types:

- *input;*
- o*utput;*
- *forward.*

Therefore we can create three chains - the Input chain, the Output chain and the Forward chain. The Input chain examines the incoming packets. If there is a rule to process a packet, the latter is either let in (accept policy) or not (drop/reject policy). Otherwise, the packet is examined by the next rule. If, finally, there is not any rule to match, the default system policy is applied. The first rule applied to a packet is the first one on the list that forms a chain.

If a packet is created inside the system, it is sent to the Output chain.

Packets that pass through the system, traverse the Forward chain.

When configuring a firewall, you can change a rule's position on the list, delete a rule from the list, create, edit and add rules to the list.

To configure the firewall, click on the Firewall link on the VPS Services dashboard.

Configuring Firewall in Normal Mode

In the normal mode the rules you delete or add are called *access rules*. The VPS access rules are 15 preset groups of standard firewall rules. Each access rule refers to a most widely used service and corresponds to a number of standard firewall rules that ensure the availability of this service. In the normal mode each access rule is dealt with as a single entity. This implies that enabling or disabling an access rule results in enabling or disabling all the standard firewall rules it corresponds to. By default, 6 preset access rules are active:

1. Access to outer world;
2. DNS server;

3 Mail server;

4 POP3 server;

5 SSH server;

6 WEB server.

The remaining 9 access rules that are not enabled by default can be added on the page, which you can access by clicking Add access rule.

To delete a rule, select one of the check boxes on the right of the screen, click Delete over the check boxes, and then OK to confirm. To delete all the rules, select the uppermost check box, click Delete over the check boxes, and then OK to confirm. Note that no access rules can be permanently deleted from the system. A *deleted* rule is, in fact, temporarily disabled and can be enabled back as described on the Adding Access Rule in Normal Mode subsection (on page 39).

To change the mode, click Firewall Setup.

Note: If this page informs you that you cannot manage firewall on this VPS, refer to the Dealing With Misconfigured Firewall subsection.

Dealing With Misconfigured Firewall

If your firewall has not been configured yet, you are most probably having this page now. The page can also appear if you did misconfigure your firewall. The common way to misconfigure a firewall is to add or edit your own specific rules in the advanced mode and then switch to the normal mode without deleting these rules first.

At this point you will have to decide upon one of two basic strategies: to select the normal mode or to select the advanced mode:

- select the normal mode to deny all services except those critical to connecting to the Internet. To select the normal mode, click Switch the firewall back to the normal mode.
- select the advanced mode to create a rule to permit, deny, or monitor the access to or from the system for each service you need. If you are going to separately edit each rule, click Select the advanced firewall mode.

Adding Access Rule in Normal Mode

To open this page, follow the Add Rule link on the Firewall page. Here you have the rules that have not been included into the list of active rules you can see on the Firewall page. To *add* a rule here means actually to *enable* it. To add a rule, select a check box on the opposite and click Submit - or Cancel if you want to restore the firewall settings prior to the last action.

Selecting Mode

If you have only just started using the firewall by clicking the Firewall link on the VPS Services dashboard, the Firewall Setup page is the first one you have displayed.

On the Firewall Setup page, you can choose one of the following modes your firewall operates in:

- The normal mode. If the security strategy you are planning out does not require a complicated system of specific rules and all you are going to do is as simple as providing your system with access to the Internet and the maximum safety, then the best option is the normal mode.Hence, select the normal mode to configure your firewall using the 15 built-in access rules (see page 38) or to fix the firewall rules settings corrupted either in the advanced mode or in the normal mode.
- The advanced firewall mode with default policy Accept, or the advanced firewall mode with default policy Drop. The advanced mode takes more time and experience to configure, but then there is more flexibility and potential in it to make use of.

Besides, the Firewall Setup page can be reached with the Firewall Setup link from both advanced and normal mode pages. If so, the choice is quite the same.The only difference is that in this case the normal mode can also be used as an option to reset to if you want to roll back the changes in the firewall rule(s) settings you have made.

After selecting a mode, click Submit. Click Cancel to return to the previous screen.

Building Input Chain

To build and edit the *Input Chain*, select the Input tab. When you click either Advanced firewall mode with default policy Accept or Advanced firewall mode with default policy Drop, on the page described in the Selecting mode subsection (see page 40), the first chain of rules is the *Input Chain*. The *Input Chain* is a set of rules for the incoming traffic.

Here you can edit, add, delete, enable, disable, filter or change its position in the list of any or all of 9 default rules the input chain consists of. In case you need to come back to the original advanced mode settings, the default rules are:

1. Web server input;
2. SSH server input;
3. Mail server input;
4. POP3 server input;
5. DNS server tcp input;
6. DNS server udp input;
7. All tcp input for hi port allowed;
8. All udp input for hi port allowed;
9. Default system policy.

If, for some reason, you need to have this ruleset back, click Firewall setup and select the Normal firewall mode radio button.

The table below describes the attributes of the rules in the chain:

Name	Description
Name	The name of a specific web service this rule applies to
Policy	One of three policies: Accept, Drop or Reject
Protocol	One of two protocols used for package transmission - Transmission Control Protocol (TCP), defined by IETF RFC793 or User Datagram Protocol (UDP), defined by IETF RFC768
Source Address	The internal address of the packets (e.g.: IPv4 or IPv6 address, the name of a network interface, etc.)
Source Port	The internal port of the packets
Destination Address	The address where the packets are sent to
Destination Port	The port where the packets are sent to
Status	The current status of the rule (Enabled/Disabled)
Move	Moving the rule a level up or a level down from its current position

The default system policy access rule cannot be changed as this rule decides the packet's destiny - to accept or to drop - when the packet has not any other rule to be processed by.

To edit a rule, click its name in the Name column. To add - or replace - a specific rule, click Add Rule in the Tools group. To disable, enable or delete a rule select its check box and then click Disable, Enable or Delete. To move a rule a level up its position, click . To move a rule a level down its position, click . To filter rules by the policy, the protocol, or the current status, click .

You can also switch to the normal mode by clicking Firewall setup and selecting normal mode there.

Building Output Chain

To build and edit the Output Chain, select the Output tab. The output chain regulates the outbound access. The default rules list is the same as in the Input Chain (see page 40), the only difference being the *output*, instead of the *input* characteristic of the rules. The list of rules on this page is this:

1. Web server output;
2. SSH server output;
3. Mail server output;
4. POP3 server output;
5. DNS server tcp output;
6. DNS server udp output;
7. All tcp output allowed;
8. All udp output allowed;

9 Default system policy.

The default system policy access rule cannot be changed as this rule decides the packet's destiny - to accept or to drop - when the packet has not any other rule to be processed by.

If, for some reason, you need to have this ruleset back, click Firewall setup and select the Normal firewall mode radio button.

The attributes of the rules in the chain are described on the Building Input Chain subsection (see page 40).

Here you can edit, add, delete, enable, disable, filter or move in the list any or all of the 9 default rules the output chain consists of. To edit a rule, click its name in the name column.To add a specific rule, click Add Rule in the Tools group. To disable, enable or delete a rule select its check box and then click Disable, Enable or Delete. To move a rule a level up its position, click . To move a rule a level down its position, click . To filter rules by the policy, the protocol, or the current status, click .

You can also switch to the normal mode by clicking Firewall setup and selecting normal mode there.

Building Forward Chain

To build and edit the Forward chain, select the Forward tab. Unlike the Input and Output chains, the only default rule the forward chain has is Default system policy. Conceivably, this one is not to be edited or deleted. Instead, you are free to decide upon any number and kinds of specific rules to create and add to the Forward chain by clicking on the Add Rule link in the Tools group.

After the number of rules in your Forward chain becomes bigger, you may need to sort them out. To do that, click and pick the three possible values from the three drop-down menus: the policy, the port, and the current status of the rule(s). Click to take a rule a level up its current position in the chain, or to relocate it a level down. If two or more rules can be applied to the given packet, the uppermost rule takes priority.

To switch to the normal mode of managing the firewall, click Firewall Setup link in the Tools group.

The default forward chain policy is the policy selected on the Firewall Setup (on page 40) menu.

Adding Rule in Advanced Mode

To get to this page, click Add rule icon on the Input Chain (see page 40), Output Chain (see page 41), or Forward Chain (see page 42) pages. On this page you can elaborate your own specific rule. Below are the basics of the advanced mode rules adding:

- the Name field is marked because this field is an obligatory one;
- Source Address and Netmask, Source Port or Port Range, Destination Address and Netmask and Destination Port or Port Range fields are left to your own discretion, but in case of an error there is a pink stripe over the field that has to be corrected;
- the standard format for Source/Destination Address and Netmask field is 1.2.3.4/255.255.23.4;
- the standard Port range format is 80-123;
- to enable a rule, select the Enable check box;
- if you are creating this rule for future purposes, clear this box;
- to include the rule into one of three chains, select Input, Output, or Forward on the drop-down menu;
- on the The rule's position in the chain drop-down menu you are to decide what priority this rule will have in its chain. There are two options for you to choose between: the bottom and the top of the chain;
- for the changes you have made to become operational, click Submit, to undo the changes and return to the previous page, click Cancel.

Editing Rule in Advanced Mode

The main difference here from the operations described in the Adding Rule in Advanced Mode subsection (on page 43) is that the rules you edit are not those you create as you deem it expedient. If you edit a rule (with the exception of renaming it), the rule changes and works differently from the way it did. Before submitting the new settings make sure they meet your security strategy. Otherwise, click Cancel.

The other detail to be aware of is the possible consequences of changing the initial (default) firewall settings. If you feel your expertise in the security area permits some future development, do not change them at all. Applying the changes you are not completely certain of may decrease your system's security.

Installing Plesk

 The Install Plesk page allows you to install the Plesk control panel in the VPS(s). This page can be accessed by clicking the Install Plesk link on the VZPP menu, which is displayed if the Plesk template is not installed in the VPS.

To install Plesk in a Virtual Private Server, you should press the Install button on the Install Plesk page. Just follow the instructions on the screen to complete the installation. After you have successfully installed the Plesk control panel in the VPS, the Plesk Panel link becomes visible on the VZPP menu. Follow this link to start working in Plesk.

Note: You can't install Plesk unless authorized to do so by your provider. If you have any problems initializing the Plesk control panel auto install, seek your provider's help. Mind though that the Plesk auto install denial may be due to the shortage in your VPS QoS resources. To check if this is the case, you can go to the Viewing QoS Alerts Log page where you'll be informed in the Description column which parameter has caused the auto install failure. You might have to consider the possibility of killing some unnecessary memory-demanding process from the VPS or ask the Node administrator to allocate more resources as needed to run Plesk on your VPS.

Working in Plesk Control Panel

In case the Plesk control panel is installed inside the VPS, the Plesk control panel link becomes visible on the VZPP menu. You can click on this icon to go to the Plesk control panel page.

On this page you can use the Login to Plesk link to start a Plesk control panel session. A new browser window with the Plesk control panel is launched and you are able to get straight down to work there.

To change the Plesk `admin` password, click the Change Password link on the Plesk Control Panel page. Setting a new password from time to time is recommended to assure the maximum security of a VPS.

Logging In to Plesk Control Panel

The Login to Plesk link on the Plesk control panel page offers you to open a pop-up window to start managing the VPS via Plesk.

In this window, you should open the Login to Plesk link to start a Plesk control panel session. A new browser window with the Plesk control panel is launched and you are able to get straight down to work there.

The logging in to Plesk is performed automatically, you do not need to enter the name and password of the admin user since you have already been identified by your VZPP user credentials.

You might wish to change the VZPP user Plesk admin password used to log in to VZPP via Plesk. The Change Plesk Admin Password page allows you to change the current password of the `admin` user, which should be done from time to time to maintain the maximum security of the VPS.

Note: If your Plesk version is lower than 7.0.2, the option of changing the `admin` password is not provided for VZPP.

Changing Plesk Administrator Password

Although logging in to Plesk from VZPP is performed automatically and does not require specifying the credentials of the `admin` user, the Plesk `admin` user name and password may be of use for a VZPP user willing to directly log in to the VPS via Plesk (see page 7). To maintain the maximum security of the VPS, it is recommended to change occasionally the current password of the `admin` user. The Change Plesk Admin Password page opened through the Change Password link on the Plesk Control Panel page allows you to edit the administrator password.

To set a new password, you need to type it into the New admin password field and then retype it in the Retype new admin password field below to ensure you have provided a correct password. The password should be no less than 5 characters and difficult enough to guess to guarantee the privacy of the VPS.

After you have entered a new admin password, press Change to submit the changes made.

Note: If your Plesk version is lower than 7.0.2, the option of changing the `admin` password is not provided for VZPP.

Logging In to Confixx Control Panel

 In case the Confixx control panel is installed inside the VPS, the Confixx control panel icon becomes visible on the VZPP menu. You can click on this icon to go to the Confixx control panel login window.

In this window, you should enter your credentials (login and password) into the corresponding fields and press the Login to Confixx button. You may learn the credentials from your provider. In case the credentials entered are correct, a new browser window with Confixx control panel is launched and you are able to get straight down to work there.

If you select the Save Login data checkbox, you won't have to type your login and password again when you later visit this page - the credentials will be filled in automatically. In this case, the credentials information is stored not on the server, but on the client side (i.e. on the computer where your browser window is launched).

Note: The Confixx control panel with version below 3.0 is not supported.

Using SSH to Connect to VPS

 If you are managing a Hardware Node with the Linux operating system installed, you can use Secure Shell (`ssh`) to remotely connect to the VPS you are operating and work inside its directory tree using standard Linux command line tools. To connect to the VPS by `ssh`, you should make sure that:

1. You are launching VZPP in Internet Explorer 5.0 or above. SSH connection to the VPS is supported by other browsers only if you have a Java Virtual Machine on your computer.
2. The VPS is running. If it is not, start it on the Start/Stop VPS page.

Note: If the VPS you are managing resides on the Hardware Node running Windows 2003 Server, please turn to the Using Remote Desktop Connection to Access VPS section (on page 48) to learn to manage a VPS by means of the Remote Desktop Protocol.

The SSH Client window is opened upon clicking on the SSH Connection icon on the VZPP menu. You are presented with the Login and Password fields where you should enter the relevant information (`Root` or any other user name you might have created for this VPS and this user's password) to be passed to the `ssh` server inside the VPS.

After you have filled in these two fields, press the Login button. If you are doing this for the first time, your browser may display a window like this asking you to install additional components:

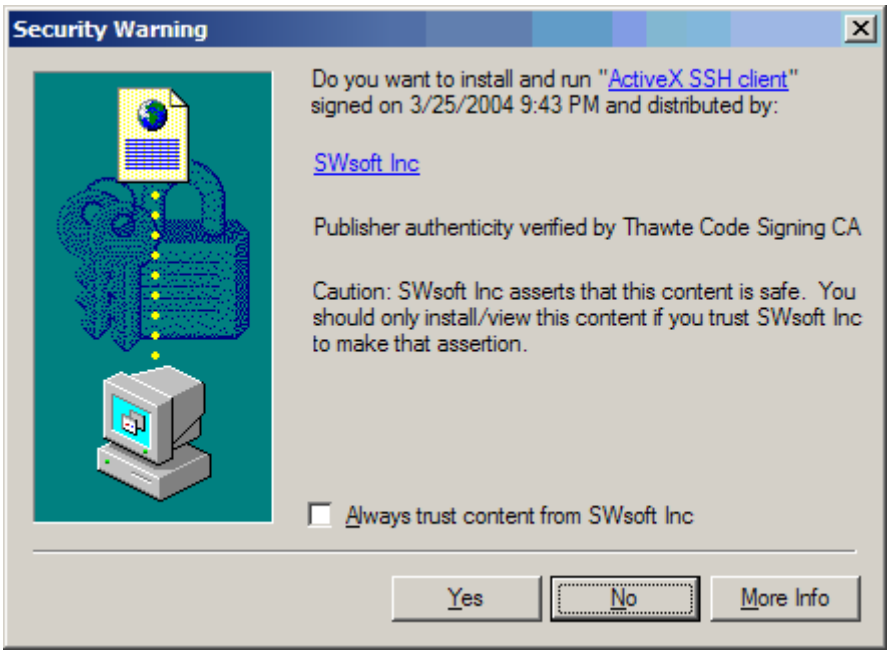


Figure 3: Installing ActiveX SSH Client

Click Yes in this window and wait for the `ssh` terminal window to appear, whereupon you get connected to the VPS and may start sending commands to it via `ssh`.

Using Remote Desktop Connection to Access VPS

For a VPS running Windows 2003 Server, you can use Remote Desktop Connection - a standard Windows application - to connect to the VPS by means of the Remote Desktop Protocol (RDP). The feature is available only for Internet Explorer 5.0 or above. It is not supported by other browsers. To connect to the VPS via RDP, you should make sure that the VPS is running. If it is not, start it.

Note: If you are managing a Linux-based Virtual Private Server, please turn to the Using SSH to Connect to VPS section (on page 46) to learn to manage the VPS by means of Secure Shell.

The Remote Desktop window is opened upon clicking on the Remote Desktop Connection icon on the VZPP menu. You are presented with the Login button that you should press to open the Remote Desktop session. If you are doing this for the first time, your browser may display a window like this asking you to install additional components:

Figure 4: Installing Remote Desktop ActiveX Control

Click Yes in this window and wait for the Remote Desktop terminal window to appear, whereupon you will be presented with the Login and Password fields. After entering the necessary information (`Administrator` or any other user name you might have created for this VPS and this user's password) in the fields provided, press Enter to get connected to the VPS and start sending commands to it via Remote Desktop.

CHAPTER 4

Monitoring Operations and Viewing Logs

VZPP is able to display four kinds of logs maintained for your Virtual Private Server:

- History of VPS Status Changes. This log reflects such changes as starting, stopping, rebooting the VPS, or mounting it in the repair mode. These changes may have been invoked either through VZPP or by other means.
- Quality of Service Alerts. This log reflects those states of your VPS when it hits limits on some hardware resource. To know more about resources, read the Monitoring VPS Resources section (on page 22).
- Actions. This log reflects only those actions related to VPS management that were performed by means of VZPP.
- Traffic Log. This log allows you to display your network traffic statistics for a specified period of time.

You may view all these logs by following the corresponding links from the Logs dashboard accessible by clicking the Event Manager link on the VZPP main menu.

You can also monitor the VPS operations that are either currently under way or have already been completed by viewing:

- Active Tasks. This monitor provides the information on any VPS operation currently under way.
- Task Details. This monitor lets you see details not only on the real-time VPS operations but on the ones already completed as well. It provides information on the Virtuozzo utilities messages during this or that operation performance.

VZPP also provides specific information in case of an operation failure for you to learn the error cause(s).

In This Chapter

Viewing History of VPS Status Changes

The Status Changes page (accessible by clicking the Status Changes link on the Logs dashboard) keeps track of all the changes in the status of the VPS. These changes may happen due to the VPS routine management via VZPP, or due to the operation of some programs. The three-column table presents the time when the VPS status changed, the old status of the VPS, and the status obtained. By default, 20 records are shown, but you may have more records displayed by pressing the appropriate link on top of the table. The description of all possible VPS statuses is provided in the VPS Statuses section (on page 30).

You may have the Status Changes table display only those log records that have a particular date and time. On top of the table, press the icon to display the fields where you can specify the boundaries of the time interval for which you wish to view the log; then click on the Search link.

Viewing Alerts Log

Every time a VPS consumes more of a resource than is specified by the limit on that resource, or is coming close to that limit, an alert is generated and logged. Turn to the Monitoring VPS Resources section to know more about the limits for corresponding resources. You shall pay attention to the problem resource and correct the situation.

The alerts log is shown on the QoS Alerts page available on clicking the QoS Alerts link on the Logs dashboard.

You may have the QoS Alerts table display only those alerts that have a particular date or are generated for a definite resource parameter. On top of the table, press the icon to display the fields where you can specify the boundaries of the time interval or the resource parameter for which you wish to view the log; then click on the Search link.

The QoS Alerts table provides you with the following data:

Time	The date and time when the alert was generated.
Type	The alert sign displays the type of alert for the VPS. See the Monitoring VPS Resources section for more details on the existing alert indicators.
Parameter	The type of the VPS resource that required the consumption value alert.

Note: There are certain correspondencies between the alert zone indicators and the alert signs in the Type column. A green tick stands for the green zone, an orange triangle points to the yellow zone, a red triangle refers to the red zone, and a black cross means that the current resource consumption has entered the black zone. Depending on the parameter under alert, you can learn more about alert zones on the relevant resource type in the CPU Resource, System Resource, Disk Space Resource or Disk Inodes Resource sections of the Monitoring VPS Resources section (on page 22).

Viewing Actions Log

The Actions Log page keeps track of your latest operations performed by means of VZPP. You may consult this page to check the status of any VPS operation recently performed. You can access this page by following the Actions Log link on the Logs dashboard.

By default, 20 records are shown, but you may have more records displayed by pressing the appropriate link on top of the table. You may also have the Actions Log table display only those log records that have a particular date or refer to a specific operation status. On top of the table, press the icon to display the fields where you can specify the boundaries of the time interval and the status of the operation you are interested in; then click on the Search link. You can press the Show All button to check all the operations performed on the VPS.

The actions list is presented as a following table:

Column Name	Description
Started	The date and time when the operation began.
Operation	The name of the operation.
Status	Indicates whether the operation was completed or failed.

Clicking on the Details link next to an operation displays the corresponding success/failure details in a pop-up window.

Viewing Traffic Log

The Traffic Statistics page enables you to view the information on all incoming and outgoing traffic for your Virtual Private Server over a specified time period in the past. This page can be accessed by clicking the Traffic Log link on the VZPP main menu.

To display traffic statistics, you should perform the following operations:

1. In the Show traffic for field, specify the time span for which you wish to see your traffic by selecting the corresponding duration unit on the drop-down menu. Depending on the selected unit, the field to the right of the drop-down menu changes and offers you a list of appropriate values to choose from. The duration units are listed below:
   - `Day`: Click on the calendar and specify the exact date (i.e. day, month, and year) for which you wish to view your network traffic statistics.
   - `Month`: Specify the month and year to display your traffic statistics for.
   - `Year`: Specify the year to display your traffic statistics for.
   - `Period`: Specify the period for which you wish to view your traffic statistics by selecting the start and end dates on the calendar.
2. In the Traffic unit field, specify the unit of measurement your traffic statistics will be displayed in.
3. Click on the Submit button to display your traffic statistics for the specified period.

The results will be presented in the following table:

Column Name	Description
<Period>	Denotes the specified period. The name of this column depends on the duration unit selected in the Period field.
Incoming	The input traffic statistics (in the selected unit of measurement) during the specified period.
Outgoing	The amount of output traffic (in the selected unit of measurement) during the specified period.

The Total row at the bottom of the table summarizes all the incoming and outgoing network traffic for the specified time span.

Viewing Active Tasks

Almost all VZPP pages, except for those containing an error report, allow you to check for any VPS operations currently under way. The Active Tasks window can be accessed by pressing the  icon at the right end of the title bar of a VZPP page. If you are planning to perform any operation on your VPS, it is a good idea to check the Active Tasks window and wait for the tasks to complete, if there are any. The window is refreshed every few seconds.

By default, 20 operations are listed, but you may have more operations displayed by pressing the appropriate link on top of the table. You may also have the Active Tasks table display only those operations that have a particular status. On top of the table, press the  icon to display the field where you can specify the status of the operation you wish to view the information on; then click on the Search link.

The information on the active tasks is presented as a table with the following columns:

Column	Description
Started	The date and time when the operation was started.
Operation	The name of the operation.
Status	Indicates the operation status. At present the only one possible is "In Progress", which means that the operation is under way.

The Details link beside a task leads to the Task Details page, where you can view the details of the operation.

When the operation is successfully completed or fails, the table is closed, and the `No active tasks at the moment` message appears.

Viewing Task Details

The Task Details page provides information on the Virtuozzo utilities messages when performing this or that operation. In other words, these messages would be displayed as if you performed a VPS operation not by means of VZPP, but by means of the command line (for example, over ssh).

You can access this page from the Actions Log page by clicking on the Details link next to the corresponding operation. Another way to access this page is to follow the Details link right after performing the operation, i.e. before going to any other VZPP page.

The task details are presented as a table with the following columns:

Column Name	Description
Time	The time when a certain operation stage began.
Event	The corresponding Virtuozzo utility message.

The table is preceded by a heading informing you of the current status of the operation - In progress, Completed, or Failed.

Viewing Error Details

The Error Details page provides specific information in case of an operation failure. When you are trying to perform an operation on a VZPP page and the operation fails, the corresponding VZPP page is refreshed with a thick red line across the page informing you of the failure and providing the Details link to learn more about this failure.

This page presents a complete response as to why the operation failed. This response might help you understand the reason for the failure.

If an operation fails, and a green line is displayed informing that the operation has been scheduled, it means that the failure occurred after the operation had been scheduled. That is why, it is desirable to always check the status of the scheduled operation by following the Details link at the right end of the green line to make sure that the operation has been successfully completed.

CHAPTER 5

Customizing VZPP Interface

Clicking on the Configure link on the VZPP left menu opens the Virtuozzo Power Panels interface configuration page where you can set a number of parameters related to the VZPP interface. The options provided on the Configure Power Panels page are the following:

Option	Description
Interface Skin	Here you may choose a suitable interface skin for your VZPP interface. The skin affects such elements as the VZPP general layout (framed or non-framed), icons and images, and the color palette.
Status Bar Refresh	This setting affects the refreshing period of the status bar located at the top of any VZPP page (see VZPP Interface Overview (on page 8)). If you select the Smart Update option, the status bar will be refreshed only when you follow VZPP links, but not more than once per 60 seconds. If this option is disabled, it means that the chosen interface skin does not use frames; therefore, it is impossible to reload only part of the page.
Local Time Zone	This setting affects the date and time information found on such VZPP pages as Status Changes, QoS Alerts, Actions Log. Choose the time zone you wish to apply when viewing different kinds of logs.
Interface Language	As VZPP is localized into a number of languages, this drop-down menu lets you choose the default interface language for VZPP. This setting affects the language of both your current VZPP session, and all future sessions if User Default is chosen as the interface language on the VZPP login screen.
Contact email	This field should be filled in with a correct email address to enable the functionality of restoring the password, should the current user forget it. This email address pertains to the current user only; other VZPP users of the given VPS may fill in this field with other addresses. The link for restoring the password is located on the VZPP login page.

After you decide on the suitable configuration and press the Submit button, the settings will be remembered for the current browser only. If you change the browser or move to another computer for working with VZPP, the default settings will be used until you perform a new customization.

CHAPTER 6

Troubleshooting

VZPP is an indispensable means for solving various kinds of problems related to the VPS functioning. It is still more flexible due to its ability to work with not running VPSs. The common groups of problems lending themselves readily to be handled by VZPP boil down to the following:

- Services inaccessibility;
- Elusive problems.

You can also consult the Network Problems section to try to find out why the VPS is inaccessible by network, and the File Problems section.

Note: The problem situations described in this chapter mainly concern Virtual Private Servers with the Linux operating system installed. However, it can be also of great use for those managing the VPSs running Windows 2003 Server.

In This Chapter

Services Inaccessibility

Various tasks you are accustomed to perform by means of your VPS (accessing your web site or sending email and the like) may fail if the corresponding services are inaccessible.

Try consecutively the following three steps to determine the reason for this and do away with it:

1. Check if your VPS is running. To this effect, log in either as a Service VPS user or as your VPS root/Administrator user and look at the status bar to determine if the VPS is running or down. You can also check the status of your VPS on the Service Unavailable screen by clicking the corresponding link provided on this screen. If the VPS is down, click the Start/Stop VPS link on the menu and press the Start VPS button. Wait a little for the VPS and all the services to start.
2.  Go to the Services page (see page 33) and check the status of the service in question. The service must be running for the corresponding functionality to be accessible. For example, `psa` and `mysqld` must be running for the Plesk control panel to handle your requests, `httpd` - for your web site to function properly, `sshd` - for the VPS to be accessible by `ssh`, `sendmail` - for you to be able to send email, `popa3d` - to receive email by the POP3 protocol, etc. You may also try to stop the `iptables` service to see if it solves the problem, because some `iptables` rules might prevent certain network connections.

3 Go to the Resources page (see page 22) to determine if your VPS is short of any resources. If some of the resources are marked in red or black, this is a hazardous situation that should be resolved immediately. For more information on resources, turn to the Resources section of this guide.

If the Plesk control panel is installed inside your VPS and you are working with this panel, the Service Unavailable screen may sometimes be displayed when you are trying to perform this or that Plesk-related operation. This situation is normally handled as described above. However, in case none of the recommended measures works, you may have to reinstall the Plesk control panel into the VPS, as the Plesk installation might be corrupted.

Elusive Problems

Sometimes it is hard to determine the exact reason for a problem. The problem might persist despite any actions undertaken. The most grievous situation of the kind happens when you cannot even start your VPS. Such problems call for going back to an earlier state of the VPS with these problems missing. This change-over is usually effected by means of:

1 Restoring the VPS from a working backup (see page 20);

2 Reinstalling the VPS (see page 17);

Note: It is for you to decide which way suits you most. Generally, these two options are applicable if you can start your VPS to copy the valuable information from it. To assure a safe data saving in the situation where you cannot start the VPS, repairing your VPS is the most advisable problem-solving option.

3 Mounting your VPS in the repair mode and copying the valuable personal data to a secure place outside the VPS. Using the repair mode is covered in the Repairing VPS section (on page 19).

Network Problems

Problem

Your VPS is inaccessible by its hostname or IP address, or you cannot log in as root.

Solution

- If you are using the hostname, try to use the IP address, and vice versa.
- Ping your VPS.
- Ask your provider to create a Service VPS user for you. Log in to the Service VPS which is responsible for managing all your Virtual Private Servers and check the problem VPS hostname and IP address.
- Log in to the Service VPS and change the VPS root/Administrator password.
- Log in to the Service VPS and disable the `iptables` service inside the problem VPS.

File Problems

VZPP is tuned to not allow giant files to be uploaded to VPSs. There is a maximal file size (e.g. 512 Mb, but it may be any other value) allowed to be uploaded to a VPS by means of VZPP. If you need to upload larder files to your VPS, you should contact your service provider.

Index