



Deployment Guide

Plesk Automation 11.5

Contents

Getting Started	3
Infrastructure Configuration	4
Network Configuration	5
Installing Plesk Automation	7
Upgrading Plesk Automation	9
Deploying Plesk Automation in Odin Cloud Server	10
Deploying Infrastructure	15
Installing a License Key for the Management Node	15
Adding Service Nodes	16
Apache Web Server Nodes	17
IIS Web Server Nodes	19
Postfix Mail Server Nodes	21
SmarterMail Mail Server Nodes	23
External Mail Server Nodes	25
Webmail Server Nodes	26
Database Server Nodes	27
DNS Server Nodes	31
Backup Server Nodes	33
Billing Node	34
Enabling Mail Notifications from Web Hosting Nodes	36
Setting Up LVE in CloudLinux	37
Setting Up CageFS in CloudLinux	38
Installing License Keys for Service Nodes	38
Troubleshooting	40
Installing Plesk Automation	40
Accessing Plesk Automation	40
Adding Service Nodes	40
Using Plesk Automation	42

CHAPTER 1

Getting Started

What Is Odin Plesk Automation?

Odin Plesk Automation (hereafter referred to as Plesk Automation) is a hosting control panel where one central server (*management node*) controls an arbitrary number of other servers that have various roles - web, mail, DNS, and so on. In terms of Plesk Automation, these controlled servers are called *service nodes*. When a customer subscribes to a web hosting plan, Plesk Automation allocates all the necessary resources on service nodes and links these resources to the customer's account. For example, when a customer subscribes to a shared web hosting plan, Plesk Automation creates a webspace on one of the available web server nodes. If the subscription also includes mail services, Plesk Automation creates mailboxes for the customer on one of the mail server nodes.

Plesk Automation Deployment

The process of Plesk Automation deployment consists of two main steps, which are described in this guide:

- 1 [Installing Plesk Automation on the management node](#) (on page 7).
In this step, you install the main Plesk Automation packages on your central server - management node.
- 2 [Deploying attendant multi-server infrastructure](#) (on page 15).
In this step, you build your multi-server infrastructure by adding servers (service nodes) that will provide various hosting services. There are numerous possible configurations: you may use nodes that provide only one type of service (for example, web or mail server only) or employ nodes that combine roles (for example, web and mail server). Even the management node is allowed to provide some types of services. See our recommendations on the [infrastructure](#) (on page 4) and [network](#) (on page 5) configuration in the following sections.

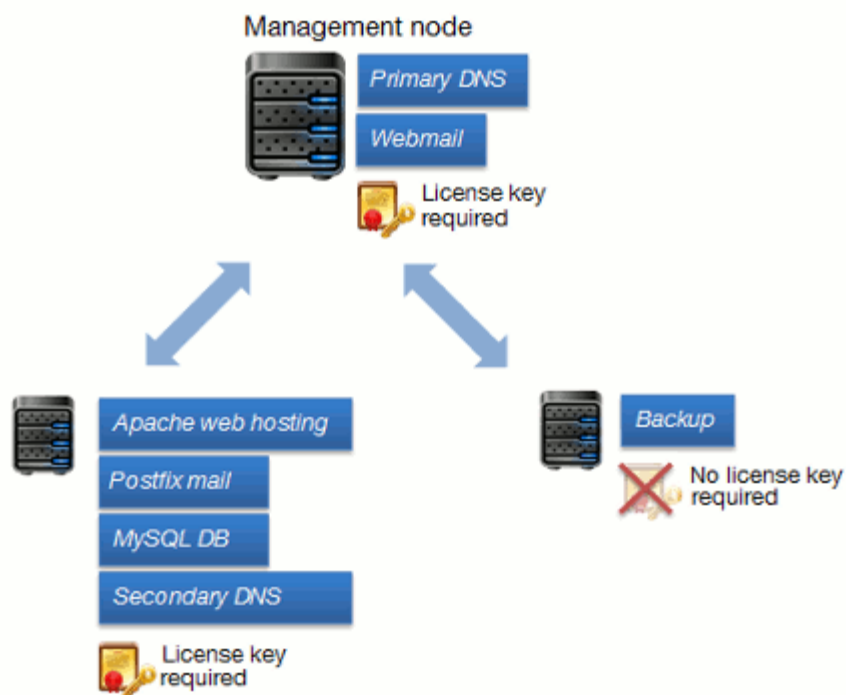
In this chapter:

Infrastructure Configuration.....	4
Network Configuration.....	5

Infrastructure Configuration

The Minimal Infrastructure Configuration

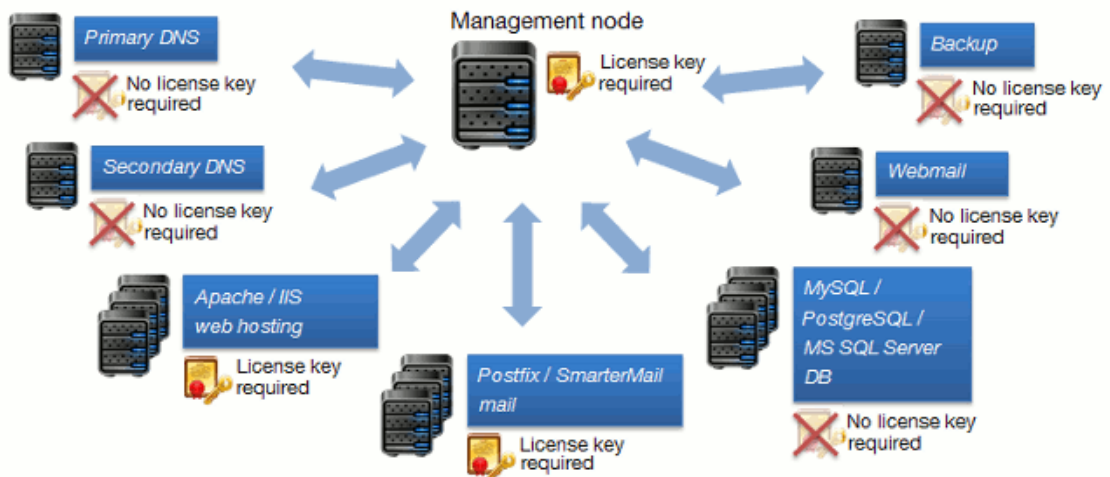
In theory, the majority of hosting services can be provided by the management node (see Hosting Services Provided by the Management Node next in this section). Nevertheless, we strongly recommend that you use a separate node for providing hosting services, even on entry-level environments. Thus, a basic Plesk Automation environment looks like this:



As you grow, consider implementing an optimal configuration as shown below.

The Recommended Infrastructure Configuration

For optimal performance and security, we strongly recommend that you move all services from the management node to separate service nodes. The best practice is to use the management node only for serving the Plesk Automation GUI. The diagram below shows one of the possible Plesk Automation environment configurations. The decision on whether service nodes should provide only one or multiple services is up to you and it should depend on the actual server load.



Hosting Services Provided by the Management Node

The management node provides the following services by default:

- *DNS.*
The node is the master DNS server for all zones created in Plesk Automation. If you want to use a separate server for serving DNS zones, configure it as described in the section [DNS Server Nodes](#) (on page 31), before you start offering hosting services. You can set up a separate DNS server later, but the DNS zones previously created will not be automatically transferred to the new server.
- *Webmail.*
The node provides the webmail service for all mailboxes in Plesk Automation.

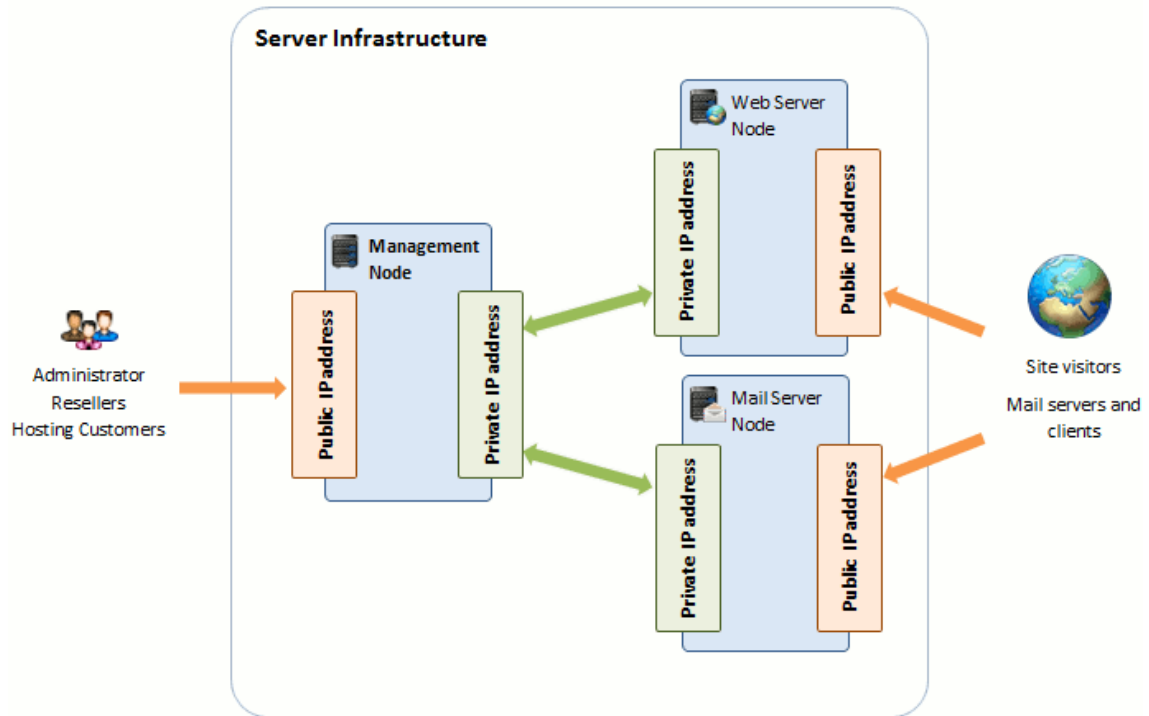
Network Configuration

For security reasons, we recommend that you separate internal and external communications. Thus, it is recommended that the management node and service nodes have separate IP addresses for these purposes:

- One *private IP address* for internal communications between the management and service nodes.

- One or more *public IP addresses* for external communications. The management node will use this IP address for providing the Plesk Automation user interface. Service nodes will use the external address to provide hosting services.

See the diagram below for convenience.



Setting Up Separate Public and Private IP Addresses

Private and public IP addresses of the management node are set during the Plesk Automation installation. See the instructions in [Installing Plesk Automation](#) (on page 7).

Private and public IP addresses of a service node are set when adding the node to Plesk Automation. The corresponding sections of [Adding Service Nodes](#) (on page 16) contain detailed instructions on how to do this.

Note that it is impossible to configure some of the service nodes to communicate with the management node via an internal private IP address, and some others, via an external public IP address. All service nodes should be configured consistently to communicate with the management node either via an internal IP address, or via an external IP address.

CHAPTER 2

Installing Plesk Automation

Plesk Automation installation implies the installation of all Plesk Automation components on a central server - management node. The server must meet the following requirements.

Management Node Requirements

OS	RHEL 6.4, 6.5, or 6.6 (x86-64) * CentOS 6.4, 6.5, or 6.6 (x86-64) * * Plesk Automation does not support kernels with the <i>grsecurity</i> components.
CPU	2-core (3 GHz or higher recommended)
RAM	4 GB minimum
Disk space	<p>Minimal:</p> <p>At least 10 GB free. Disk partitioning should be as follows:</p> <ul style="list-style-type: none"> • / - 5120 MB • /usr/local - 2048 MB * • /var - the rest of the space (3072 MB) ** <p>Recommended:</p> <p>At least 150 GB free. Disk partitioning should be as follows:</p> <ul style="list-style-type: none"> • / - 10 GB or more • /usr/local - 120 GB or more * • /var - the rest of the space (20 GB) ** <p>* The /usr/local directory, among other things, is used to store unpacked installation files of APS apps installed by hosting customers. Ensure that /usr/local has enough disk space, if you expect your customers to install various APS apps.</p> <p>** If you want to host customer websites on your management node, /var should have additional free disk space.</p>
Open TCP ports (Plesk Automation-specific)	8880: HTTP access to Plesk Automation 8443: HTTPS access to Plesk Automation 80, 8352, 8440: Connections between the Administration Panel and service nodes 12443, 10001: The Hosting Panel web server 8354, 8356, 8360, 8362, 8364, 8412, 8490, 8532: Various purposes

Installing Plesk Automation

The Plesk Automation installation is fully automated and performed by the single script file `ppa_installer`. To install Plesk Automation on your server:

- 1 Log in to your server as root.
- 2 Download the Plesk Automation installation script from the Odin website.

```
# wget
http://download.automation.odin.com/ppa/11.5/ppa\_installer
```

3 Allow script execution.

```
# chmod +x ppa_installer
```

4 Run the script with the following options.

```
# ./ppa_installer --password <password> --admin_email <email>
--ip <public_ip> --communication_ip <private_ip>
```

where

- <password> - the Plesk Automation administrator's password.
- <email> - your e-mail address.
- <public_ip>, <private_ip> - public/private IP addresses that must be used for external/internal communications. See the details in Network Configuration (on page 5). If you have only one IP address on the server, omit this option.

Important: If you want to set the language of the Administration Panel other than English, use the `--set_default_lang` option. The following languages are supported: `en_US`, `de_DE`, `fr_FR`, `es_ES`, `ru_RU`, `zh_TW`, `it_IT`, `ja_JP`, `nl_NL`, `zh_CN`.

After the installation of all Plesk Automation components is completed, you can log in to Plesk Automation (as described below) and proceed to the [deployment of your attendant infrastructure](#) (on page 15).

Important: After the installation, Plesk Automation creates the special firewall chain PPA-SN-Rules-INPUT used for communication with service nodes. Do not change it, otherwise, you will not be able to add service nodes to Plesk Automation.

Logging In to Plesk Automation

To log in to Plesk Automation, type the following address in your browser:

https://<PPA_IP_address>:8443

where

- <PPA_IP_address> - the IP address of your management node, or its host name.

When Plesk Automation prompts to enter the administrator's credentials, use the `admin` user name and the password you specified during the Plesk Automation installation.

CHAPTER 3

Upgrading Plesk Automation

Prerequisites

If your service nodes are running CentOS 5.8 or earlier, RHEL 5.8 or earlier: Before upgrading Plesk Automation, upgrade the operating system on the nodes to version 5.9 or later.

Before upgrading Plesk Automation to version 11.5, obtain a new license key for the management node. You will need to install it after the upgrade. The main license keys for management nodes in Plesk Automation 11.1 are not compatible with Plesk Automation 11.5. To purchase a new license key, contact your Odin sales representative or visit <http://www.odin.com/products/plesk-automation/how-to-buy/>.

Known Issues

Mail accounts created in Plesk Automation 11.1, which contain upper and lower case letters, will not work after upgrading to Plesk Automation 11.5. However, such mail accounts, if created after an upgrade, will operate properly.

Steps for Upgrading

To upgrade your installation of Odin Plesk Automation to the latest version, download an upgrade script to the management node and run it by issuing the following commands:

```
wget http://download.automation.odin.com/ppa/11.5/ppa\_upgrade
chmod +x ppa_upgrade
./ppa_upgrade --upgrade
```

Note: The branding themes in Plesk Automation 11.1 and Plesk Automation 11.5 are incompatible. After upgrading to Plesk Automation 11.5, you should re-apply your branding customizations.

Learn more about how to do this:

- In the Operations Guide: http://download.automation.odin.com/ppa/11.5/docs/en-US/online/ppa_operations_guide/72401.htm.
- In the Branding Guide: http://download.automation.odin.com/ppa/11.5/docs/en-US/online/ppa_branding_guide/index.htm.

If you are using Plesk Automation with WHMCS, you also need to upgrade the WHMCS integration module as described in the WHMCS Integration Guide at http://download.automation.odin.com/ppa/11.5/docs/en-US/online/ppa_whmcs_integration_guide/71617.htm.

CHAPTER 4

Deploying Plesk Automation in Odin Cloud Server

This chapter explains how to deploy Plesk Automation in Odin Cloud Server 6.05 or later by means of a special script. The script creates virtual machines in Odin Cloud Server, deploys a management node and service nodes. During deployment, the script uses parameters that you specify in a configuration file.

To deploy Plesk Automation in Odin Cloud Server, follow these steps.

- *Step 1. Create a configuration file:*

1. Log in to the Odin Cloud Server server.

2. Create a text file:

```
# touch <configuration file name>
```

3. Add the following lines there.

```
[ppa]
vm-id: <ID of a virtual machine>
ip: <public IP address>/<network mask>
ip-gw: <IP address of a gateway>
;communication-ip: <private IP address>/<network mask>
os-template: <OS template>
root-password: <administrator's password>
hostname: <host name>
nameserver: <name server's IP address>
diskspace: 150G
ram: 8G
admin-email: <administrator's email address>
;swap: 4G ; this is an optional setting

[sn1]
vm-id: <ID of a virtual machine>
ip: <public IP address>/<network mask>
ip-gw: <IP address of a gateway>
;communication-ip: <private IP address>/<network mask>
os-template: <OS template>
root-password: <administrator's password>
hostname: <host name>
nameserver: <name server's IP address>
diskspace: 10G
ram: 2G
role: <role name>
;role-params:
; <setting 1 = value>
; <setting 2 = value>
;swap: 4G ; this is an optional setting
```

In these lines:

The section starting with [ppa] contains a list of parameters for deployment of a management node.

The sections starting with [sn1], [sn2], [sn3], and so on, contain lists of parameters for deployment of service nodes.

<ID of a virtual machine> is a numerical identifier of a virtual machine that will be created in Odin Cloud Server.

<public IP address> is an external IP address of the management node.

<private IP address> is an internal IP address that the management node uses to communicate with the service nodes. This is an optional parameter.

<IP address of a gateway> is an IP address of the gateway used in your network.

<OS template> is the operating system that you want to install in a container. It can take either of the following values: `centos-6-x86_64` or `redhat-el6-x86_64`.

<administrator's password> is the password that the Odin Plesk Automation administrator will use to connect as root to the container via SSH and to log in to Odin Plesk Automation as the user admin. You will be able to change that password after deployment is finished.

<role name> is the role of a service node. A service node can serve a single purpose, for example, run only Apache Web server, or several purposes, for example, a node can run Apache Web Server, DNS service, and mail server based on Postfix. Role names are self-explanatory:

- PPA_APACHE
- PPA_APACHE_DNS
- PPA_APACHE_MYSQL
- PPA_APACHE_POSTFIX
- PPA_APACHE_POSTFIX_DNS
- PPA_APACHE_POSTFIX_MYSQL
- PPA_APACHE_POSTFIX_MYSQL_POSTGRESOL
- PPA_APACHE_POSTGRESOL
- PPA_BACKUP
- Billing
- PPA_DNS
- PPA_MYSQL
- PPA_POSTFIX
- PPA_POSTFIX_DNS
- PPA_POSTGRESOL
- PPA_WEBMAIL

For certain roles, you need to specify additional parameters below the `role-params` line of the configuration file:

- PPA_MYSQL:
 `ppa_mysql.admin_login = <value>`
 `ppa_mysql.admin_password = <value>`
- PPA_POSTGRESOL
 `ppa_pgsql.admin_login = <value>`
 `ppa_pgsql.admin_password = <value>`
- PPA_APACHE_MYSQL
 `ppa_mysql.admin_login = <value>`

- ppa_mysql.admin_password = <value>
- PPA_APACHE_POSTGRESOL
ppa_pgsql.admin_login = <value>
ppa_pgsql.admin_password = <value>
- PPA_APACHE_POSTFIX_MYSQL
ppa_mysql.admin_login = <value>
ppa_mysql.admin_password = <value>
- PPA_APACHE_POSTFIX_MYSQL_POSTGRESOL
ppa_mysql.admin_login = <value>
ppa_mysql.admin_password = <value>
ppa_pgsql.admin_login = <value>
ppa_pgsql.admin_password = <value>
- PPA_BACKUP
ppa.backup.ftpuser = <value>
ppa.backup.ftpuserpassword = <value>
- Billing
billing.ui.host = <the public IP address of the billing node without a network mask>

ppa.ui.ip = <the public IP address of the management node without a network mask>

Note: You can also use the configuration file at <http://download.automation.odin.com/ppa/11.5/pcs.config.ini.sample> as a basis for your own file.

4. Correct the contents of the configuration file to adjust all necessary values as needed. Replace the items in angle brackets <...> with the proper values. When listing role settings for service nodes in lines such as <setting 1 = value>, be sure to precede such lines with at least one white space. A semicolon (;) means the beginning of a comment. Be sure to remove semicolons preceding the options that you want to use.

▪ ***Step 2. Obtain and run the deployment script***

1. Download the script from the Odin website.

```
# wget  
http://download.automation.odin.com/ppa/11.5/ppa\_deployer
```

2. Allow script execution.

```
# chmod +x ppa_deployer
```

3. Run the script with the following options.

```
# ./ppa_deployer --config=<configuration file name>
```

Step 3. Obtain and install license keys Once the deployment is finished, do the following:

1. Log in to Plesk Automation at <https://<Plesk Automation IP address>:8443>. Use the `admin` username and the password you specified in the configuration file.
2. Obtain and install license keys as described in the section *Installing a License Key for the Management Node* (on page 15).

▪ ***Step 4. Check tasks in the task manager***

Once you have finished with installing license keys, check the Task Manager (in Operations > Tasks) to ensure that there are no failed tasks. If there are any tasks that failed because of a missing license key, restart them.

CHAPTER 5

Deploying Infrastructure

After the Plesk Automation installation is finished, you can proceed to deploying your infrastructure, which includes the following:

- 1 *Install the main license key for the management node.*
Before proceeding to service nodes registration, you should obtain and install a license key that is necessary for the operation of the management node. Learn how to do this in the section *Installing a License Key for the Management Node* (on page 15).
- 2 *Add service nodes to Plesk Automation.*
To allow Plesk Automation to set up new hosting accounts on a server, you should register it in the Administration Panel and specify a role for your server: web, mail, DNS, and so on. Learn more about adding service nodes in the section *Adding Service Nodes* (on page 16). Note that depending on the licensing scheme you choose, you might also need to install separate license keys for service nodes.

In this chapter:

Installing a License Key for the Management Node.....	15
Adding Service Nodes.....	16
Installing License Keys for Service Nodes.....	38

Installing a License Key for the Management Node

Plesk Automation is shipped without a trial license key. To fully use Plesk Automation, you need to obtain the necessary license keys from Odin or its partners and install them after you have finished installing Plesk Automation and adding service nodes.

There are two licensing schemes - one is licensing by the total number of hosted websites, and another, by the number of service nodes. The steps for installing license keys vary depending on the licensing scheme you choose.

If your license key governs the total number of websites, then you only need to install the key on the management node.

If you use licensing per service nodes, then you should use the following steps:

- 1 Install the main license key on the Plesk Automation management node.

- 2 Obtain and install additional license keys for each web and mail service node, except for the nodes that act as *dedicated database or DNS servers* (service nodes with the DNS or MySQL roles). There are three essential types of additional license keys:
 - An unlimited license key for Plesk for Linux-based dedicated hardware servers. These keys should be used with all Linux-based web server or mail nodes.
 - An unlimited license key for Plesk for Microsoft Windows-based dedicated hardware servers. These keys should be used with IIS web server and SmarterMail mail service nodes.
 - A license key for Odin Premium Antivirus. These keys should be used when you want to use antivirus on mail service nodes. Without a license key, antivirus will not check mail for viruses and malware.
- ***To install the main license key for the management node:***
1. Obtain the license key. To do this, go to <http://www.odin.com/products/plesk-automation/how-to-buy/>.
 2. Install the key in Administration Panel > License & Security > License Manager > Main License tab > Install / Update.

Note: If you use licensing per service nodes, you need to obtain and install additional license keys for them. For information about how to do it, refer to the section Installing License Keys for Service Nodes (on page 38).

Adding Service Nodes

This section describes how to add service nodes that provide only one type of service: Apache web server, Postfix mail server, MySQL database server, MS SQL server, and so on. There are also a number of service nodes with mixed roles which can simultaneously provide two or three services: For example, Apache web server and Postfix mail server. Such combinations are not described in this section. The process of adding such nodes to the system is absolutely similar to the one for nodes with a single-service role.

Important: If the process of adding a node fails, follow the guidelines described in the chapter Troubleshooting Plesk Automation Deployment (on page 40).

Next in this section:

Apache Web Server Nodes	17
IIS Web Server Nodes.....	19
Postfix Mail Server Nodes	21
SmarterMail Mail Server Nodes	23
External Mail Server Nodes	25
Webmail Server Nodes	26
Database Server Nodes.....	27
DNS Server Nodes	31
Backup Server Nodes.....	33
Billing Node	34
Enabling Mail Notifications from Web Hosting Nodes.....	36
Setting Up LVE in CloudLinux	37
Setting Up CageFS in CloudLinux	38

Apache Web Server Nodes

An Apache web server node is a web server (Linux-based) that delivers websites to Internet users with the help of Apache HTTP server. When you subscribe customers to a service plan that includes Apache-based web hosting services, Plesk Automation allocates disk space and creates customer websites on one of the nodes with the Apache web server role.

When you assign the Apache web server role to a node, the system automatically installs the following components to that node: Apache, PHP, and ProFTPD.

Server Requirements

Before adding an Apache web server node to the environment, make sure that the server meets the following requirements.

OS	RHEL 5.9, 6.4 (32-bit and 64-bit versions) CentOS 5.9, 6.4 (32-bit and 64-bit versions) CloudLinux 6 (32-bit and 64-bit versions)
CPU	2 GHz minimum, 3.2 GHz recommended
RAM	1 GB minimum
Disk space	At least 10 GB free
Open TCP ports	80, 443: HTTP, HTTPS 8352-8999: Communication between a service node and Plesk Automation panels 22: Communication through SSH 20, 21, 60000-65000: FTP connections

Important: You must disable SELinux on a service node before adding it to the environment. Enabling SELinux after deployment will disrupt the operation of Plesk Automation. To learn how to disable SELinux, please refer to the manuals provided for the OS installed on the node.

Adding a Node

▪ *To register an Apache web server node in Plesk Automation:*

- 1 Add a web server node to the system by starting the Add New Node wizard in Administration Panel > Infrastructure > Service Nodes. The wizard will ask you to provide the following information:
 - The service node role: Apache web server.
 - A node host name or an IP address and a root password.
 - If your node has more than one IP address, you should specify:
 - Backnet IP address - this address will be used for internal communications with the management node.
 - Shared IP address - this address will be used for external communications (shared hosting). See Network Configuration (on page 5) for details.

Important: If you want the added node to provide services on dedicated IP addresses, you should create and assign it an IP pool. This must be done after you add this node to Plesk Automation. Learn more in the Operations Guide, Configuring IP Pools.

- 2 Normally, when the installation is complete, the node is marked as Ready to provide its services. If this does not happen, resolve the issue and mark it manually on the node properties page (Infrastructure > Service Nodes).
- 3 Assign a license key to the node as described in the section Installing License Keys for Service Nodes (on page 38).

Enabling Support for a Large Number of Websites

In the default Plesk Automation configuration, it is not possible to host more than 1000 sites on an Apache service node. If you want to host more sites, do the following:

- 1 Log in over SSH to the Apache service node.
- 2 In the `/etc/init.d/httpd` file, add `ulimit -n 999999` to the start function.
- 3 In the `/etc/security/limits.conf` file, add `nofile 999999`.
- 4 Restart Apache by issuing the command `service httpd restart`.

Automatically Assigned Attributes

When registering an Apache web server node, the system automatically assigns the Apache provisioning attribute to the node.

Enabling Support for the Passive FTP Mode

If you want to switch on the passive mode for the FTP service, do the following:

- 1 Log in over SSH to the Apache service node.
- 2 Add the line `PassivePorts 60000 65000` to the `/etc/proftpd.conf` file.
- 3 Restart the ProFTPD service by issuing the command `service proftpd restart`.

- 4 Configure the firewall to accept connections to these ports.

IIS Web Server Nodes

An IIS web server node is a Windows-based web server that delivers websites to Internet users with the help of the Microsoft Internet Information Services (IIS) software. When you subscribe customers to a service plan that includes the IIS website hosting services, Plesk Automation allocates disk space and creates customer websites on one of the IIS web server nodes.

When you assign the IIS web server role to a node, the system automatically installs PHP on it. Note that it is impossible to install additional PHP handlers on IIS nodes.

Important notes:

You must install IIS on the server before adding it to Plesk Automation.

Plesk Automation does not support dedicated IPv6 addresses on IIS-based subscriptions.

Server Requirements

Before adding an IIS web server node to the environment, make sure that the server meets the following requirements.

OS	Windows 2008 SP1 (32-bit or 64-bit systems)* Windows 2008 R2 (64-bit)* Windows 2012 (64-bit)* Windows 2012 R2 (64-bit)* <i>* with installed IIS</i>
CPU	3.2 GHz or higher
RAM	2 GB minimum
Disk space	At least 10 GB free.
Open TCP ports	80, 443: HTTP, HTTPS 8352-8999: Communication between a service node and Plesk Automation panels 135, 137-139, 445, 51619

Prerequisites on Windows 2012 R2

Before adding a service node running Windows 2012 R2, you need to log in to the node and issue the following commands in the console:

```

netsh advfirewall firewall add rule name="WinRM in"
protocol=TCP dir=in profile=any localport=5985 remoteip=any
localip=any action=allow
netsh advfirewall firewall add rule name="POA in"
protocol=TCP dir=in profile=any localport=8352 remoteip=any
localip=any action=allow
netsh advfirewall firewall add rule name="POA in 2"
protocol=TCP dir=in profile=any localport=8354 remoteip=any
localip=any action=allow
netsh firewall add portopening TCP 5985 WinRM enable SUBNET
netsh firewall add portopening TCP 8352 POA enable SUBNET
netsh firewall add portopening TCP 8354 POA2 enable SUBNET
sc config winrm start= auto
sc start winrm
%windir%\system32\timeout /t 5
cmd /c winrm put winrm/config/service @{AllowUnencrypted =
"true"}
%windir%\system32\timeout /t 2
cmd /c winrm put winrm/config/service/Auth @{Basic = "true"}
%windir%\system32\timeout /t 2
cmd /c winrm create
winrm/config/Listener?Address=*&Transport=http @{Port="5985"}

```

Adding a Node

- *To register an IIS web server node in Plesk Automation:*
 - 1 Add a web server node to Plesk Automation by starting the Add New Node wizard in Administration Panel > Infrastructure > Service Nodes. The wizard will ask you to provide the following information:
 - The service node role: IIS web server.
 - A node host name or an IP address and system administrator's credentials.
 - If your node has more than one IP address, you should specify:
 - Backnet IP address - this address will be used for internal communications with the management node.
 - Shared IP address - this address will be used for external communications (shared hosting). See Network Configuration (on page 5) for details.

Important: If you want the added node to provide services on dedicated IP addresses, you should create and assign it an IP pool. This must be done after you add this node to Plesk Automation. Learn more in the Operations Guide, Configuring IP Pools.
 - 2 Normally, when the installation is complete, the node is marked as Ready to provide its services. If this does not happen, resolve the issue and mark it manually on the node properties page (Infrastructure > Service Nodes).
 - 3 Assign a license key to the node as described in the section Installing License Keys for Service Nodes (on page 38).

Automatically Assigned Attributes

When registering an IIS web server node, the system automatically assigns the IIS provisioning attribute to the node.

Enabling ColdFusion Support

- 1 Obtain a ColdFusion 10 distribution package and start installation on the service node.
- 2 When the installation wizard prompts to select a webserver and the website for ColdFusion, select IIS as the webserver and Defaults Web Site as the website.
- 3 At the end of installation, log in to the ColdFusion Administrator and configure the ColdFusion server as required.
- 4 Register ColdFusion 10 by issuing the following command:

```
c:\Program Files
(x86)\Parallels\Plesk\admin\bin>defpackagemng.exe --set-
params --type=coldfusion --package=coldfusion10 --
values="<?xml version="1.0" encoding="UTF-
8"?><parameters><parameter name="login"
value="admin"/><parameter name="password"
value="setup"/></parameters>"
```

Note: Replace the username and password values with those you specified during the installation.

- 5 Update the list of installed packages: In Server Administration Panel, go to Service Nodes > IIS node, and click Refresh under User-installed packages.
- 6 Monitor the corresponding task in Task Manager and make sure it completes successfully.

Postfix Mail Server Nodes

A Postfix mail server node is a server (Linux-based) that uses the Postfix mail transfer agent for mail delivery. When you subscribe a customer to a plan that includes mail hosting service, the system creates customer's mailboxes on one of the Postfix mail server nodes.

When you assign the Postfix mail server role to a node, the system automatically installs the Postfix software to that server.

Server Requirements

Before adding a mail server node to the environment, make sure that the server meets the following requirements.

OS	RHEL 5.9, 6.4 (32-bit or 64-bit) CentOS 5.9, 6.4 (32-bit or 64-bit) CloudLinux 6 (32-bit or 64-bit)
CPU	2 GHz minimum, 3.2 GHz recommended
RAM	1 GB minimum
Disk space	At least 1 GB free
Open TCP ports	SMTP and POP3: TCP ports 25, 110 Mail submission: TCP port 587 IMAP: TCP port 143 Secure POP: TCP port 995 Secure SMTP: TCP port 465 Secure IMAP: TCP port 993 Communication between a service node and Plesk Automation panels: TCP ports 8352-8999 Communication through SSH: TCP port 22

Important: You must disable SELinux on a service node before adding it to the environment. Enabling SELinux after deployment will disrupt the operation of Plesk Automation. To learn how to disable SELinux, please refer to the manuals provided for the OS installed on the node.

Adding a Node

▪ *To register a mail server node in Plesk Automation:*

- 1 Add a mail server node to Plesk Automation by starting the Add New Node wizard in Administration Panel > Infrastructure > Service Nodes. The wizard will ask you to provide the following information:
 - The service node role: Mail server.
 - A node host name or an IP address and a root password.
 - If your node has more than one IP address, you should specify:
 - Backnet IP address - this address will be used for internal communications with the management node.
 - Shared IP address - this address will be used for external communications (shared hosting). See Network Configuration (on page 5) for details.

Important: If you want the added node to provide services on dedicated IP addresses, you should create and assign it an IP pool. This must be done after you add this node to Plesk Automation. Learn more in the Operations Guide, Configuring IP Pools.

- 2 Normally, when the installation is complete, the node is marked as Ready to provide its services. If this does not happen, resolve the issue and mark it manually on the node properties page (Infrastructure > Service Nodes).
- 3 Assign a license key to the node as described in the section Installing License Keys for Service Nodes (on page 38).

Automatically Assigned Attributes

When registering a Postfix mail server node, the system automatically assigns the Postfix provisioning attribute to the node.

SmarterMail Mail Server Nodes

A SmarterMail mail server node is a server (Windows-based) that uses the SmarterMail software for mail delivery. When you subscribe a customer to a plan that includes SmarterMail mail hosting service, the system creates customer's mailboxes on one of the SmarterMail mail server nodes.

Important: Unlike other roles, Plesk Automation does not automatically install SmarterMail on a node when registering it in the system. You should manually install SmarterMail on the node and configure it before adding it to Plesk Automation.

Server Requirements

Before adding a mail server node to the environment, make sure that the server meets the following requirements.

OS	Windows 2008 SP1 (32-bit or 64-bit)* Windows 2008 R2 (64-bit)* Windows 2012 (64-bit)* Windows 2012 R2 (64-bit)* <i>* with installed SmarterMail 10</i>
CPU	3.2 GHz or higher
RAM	2 GB minimum
Disk space	At least 10 GB free
Open TCP ports	25, 110: SMTP, POP3 143: IMAP 995: Secure POP 465: Secure SMTP 993: Secure IMAP 8352-8999: Communication between a service node and Plesk Automation panels

Before adding a SmarterMail node to Plesk Automation, enable the "Remote Desktop" rule in Windows firewall on that SmarterMail node.

Configuring the SmarterMail Installation

▪ *To configure SmarterMail:*

1. Configure the firewall on the SmarterMail service node: open the ports listed in the table above.
2. Visit the SmarterMail web interface. It should be available at a URL similar to <http://<ip address>:9998/>.
3. Log in as administrator. The default username and password are both admin.
4. Go to Settings > Defaults > Domain Defaults.
5. On the Limits tab, set the resource usage limits in accordance with your service plans in Plesk Automation. For example, if your service plans in Plesk Automation, called plan_1 and plan_2, offer 10 and 20 domain aliases respectively, you need to increase the SmarterMail's limit on "Domain Aliases" to at least 20 items.

Adding a Node

▪ *To register a SmarterMail mail server node in Plesk Automation:*

1. Add a mail server node to Plesk Automation by starting the Add New Node wizard in Administration Panel > Infrastructure > Service Nodes. The wizard will ask you to provide the following information:
 - The service node role: SmarterMail mail server.
 - A node host name or an IP address and a root password.
 - If your node has more than one IP address, you should specify:
 - Backnet IP address - this address will be used for internal communications with the management node.
 - Shared IP address - this address will be used for external communications (shared hosting). See Network Configuration (on page 5) for details.

Important: If you want the added node to provide services on dedicated IP addresses, you should create and assign it an IP pool. This must be done after you add this node to Plesk Automation. Learn more in the Operations Guide, Configuring IP Pools.

2. Normally, when the installation is complete, the node is marked as Ready to provide its services. If this does not happen, resolve the issue and mark it manually on the node properties page (Infrastructure > Service Nodes).
3. After the server appears in the list of nodes, register the SmarterMail API URL in the system (Plesk Automation will use it for communication with the mail server):
 1. Go to Infrastructure > Hosted Applications > Remote SmarterMail Connector > Settings.

2. Adjust SmarterMail API connection settings (API URL and SmarterMail administrator credentials). If you use several SmarterMail nodes, be sure to use the same administrator's username and password for each node.
4. Assign a license key to the node as described in the section Installing License Keys for Service Nodes (on page 38).

Automatically Assigned Attributes

When registering a SmarterMail mail server node, the system automatically assigns the SmarterMail provisioning attribute to the node.

External Mail Server Nodes

Sometimes, you may need to use an MTA which is not supported by standard Plesk Automation node roles or to attach an already existing mail server to Plesk Automation. In both cases you should use the external mail server role for the attached node.

Note that you can attach both Linux and Windows mail servers.

APS Connector

Plesk Automation communicates with such nodes by means of special APS applications (so-called *connectors*). These apps enable Plesk Automation to remotely control services on the nodes.

Before adding an external mail server to Plesk Automation, you should develop the required APS connector or obtain it from third-party developers. Learn how to create your own APS connector in Operations Guide, Appendix B. Creating an APS Connector for External Mail Servers.

Adding a Node

▪ *To register an external mail server node in Plesk Automation:*

1. Prepare or obtain the APS connector app. The APS apps are distributed in the form of ZIP files, for example, `MyAPSMail-0.1.zip`.
2. Register the connector in Plesk Automation by running the command:

```
/usr/local/ppa/bin/apsmail --import MyAPSMail-0.1.zip --name <MailServerName>
```

where `<MailServerName>` is the name you want to set for the external mail server in Plesk Automation.

3. Add an external mail server node to Plesk Automation by starting the Add New Node wizard in Administration Panel > Infrastructure > Service Nodes. The wizard will ask you to provide the following information:
 - The service node role: Depending on the operating system of the attached node, specify either External Mail server (Linux) or External Mail server (Windows).
 - A node host name or an IP address and administrator credentials.

- 4 Assign the attribute with the name you specified on the step 2 as `<MailServerName>` to the node. This should be done in Infrastructure > Service Nodes > select the node > General > Attributes.
 - 5 Mark the node as Ready to provide in Infrastructure > Service Nodes > select the node.
 - 6 Assign a license key to the node as described in the section Installing License Keys for Service Nodes (on page 38).
- ***To provide mail service using the external mail server:***
1. Create a new Mail Service resource type and specify the external mail server as an activation parameter.
 2. Add the resource to a service template.
 3. Create subscriptions with external mail hosting based on the service template.

Webmail Server Nodes

A webmail server node is a Linux server that provides webmail services with the Horde and Roundcube software. When a customer creates a mailbox, the system registers it in the preferred webmail software (defined by the service template) on the node.

By default, if there is no webmail server node in the system, the webmail services are provided by the management node. Adding the webmail node to your environment allows you to decrease the load on the management node.

Important:

1. A webmail server does not require a license key.
2. There can be only one webmail server node in the system.
3. After you add a webmail server node, already existing webmail accounts will be transferred to that node. Note that specific webmail content of these accounts (calendar items, custom skins, and so on) will not be transferred.

When you assign the webmail server role to a node, the system automatically installs the following components to that node: Apache, Horde, and Roundcube.

Server Requirements

Before adding a webmail server node, make sure that the server meets the following requirements.

OS	RHEL 5.9, 6.4 (32-bit or 64-bit) CentOS 5.9, 6.4 (32-bit or 64-bit) CloudLinux 6 (32-bit or 64-bit)
CPU	2 GHz minimum, 3.2 GHz recommended
RAM	1 GB minimum
Disk space	At least 10 GB free
Open TCP ports	Communication between a service node and Plesk Automation panels: TCP ports 8352-8999 Communication through SSH: TCP port 22 Access to webmail: TCP port 80

Important: You must disable SELinux on a service node before adding it to the environment. Enabling SELinux after deployment will result in your Plesk Automation installation malfunctioning. To learn how to disable SELinux, please refer to the manuals provided for the OS installed on the node.

Adding a Node

▪ *To register a webmail server node in Plesk Automation:*

- 1 Add a mail server node to Plesk Automation by starting the Add New Node wizard in Administration Panel > Infrastructure > Service Nodes. The wizard will ask you to provide the following information:
 - The service node role: Webmail server.
 - A node host name or an IP address and a root password.
 - If your node has more than one IP address, you should specify:
 - Backnet IP address - this address will be used for internal communications with the management node.
 - Shared IP address - this address will be used for external communications (shared hosting). See Network Configuration (on page 5) for details.
- 2 Normally, when the installation is complete, the node is marked as Ready to provide its services. If this does not happen, resolve the issue and mark it manually on the node properties page (Infrastructure > Service Nodes).

Automatically Assigned Attributes

As there can be only one webmail server node in the system, Plesk Automation does not assign any attributes to it.

Database Server Nodes

Database server nodes are servers that provide access to a number of databases. There are two main scenarios of registering a database server in the system:

- *Adding a new database server.*

If you have a clean server which you want to use as a database server in Plesk Automation, you can add it in the same way as for other service nodes choosing one of the database server roles.

Notes:

1. You do not need to install database server software on a node: Plesk Automation installs the software automatically when adding the node.
2. Microsoft SQL Server 2008 R2 Express Edition is installed on the nodes with the MS SQL Server 2008 database server role. Learn about limitations of this version at <http://msdn.microsoft.com/en-us/library/cc645993%28v=SQL.100%29.aspx>.
3. Microsoft SQL Server 2012 is installed on the nodes with the MS SQL Server 2012 database server role.
4. Before adding the MS SQL Server 2008 database server node, ensure that .NET Framework 3.5 SP1 and Windows Installer 4.5 are installed on the server.

- *Registering an existing database server.*

If you already have a working database server, you can register it in the system. In this case, Plesk Automation will use the database components that already exist on the server. In this way you can register MySQL, PostgreSQL, and Microsoft SQL Server-based servers.

Learn how to perform these operations next in this section.

Important: Database servers *do not* require a license key. You can register any number of database servers in the system without any limitations.

Adding a New Database Server Node

Before registering a new database server node, make sure that it meets the following requirements.

OS	<p><i>MySQL and PostgreSQL:</i> RHEL 5.10, 6.4 (32-bit or 64-bit) CentOS 5.10, 6.4 (32-bit or 64-bit) CloudLinux 6 (32-bit or 64-bit)</p> <p><i>MS SQL Server 2008:</i> Windows 2008 SP1 (32-bit or 64-bit)* Windows 2008 R2 (64-bit)* * - with installed .NET Framework 3.5 SP1 and Windows Installer 4.5</p> <p><i>MS SQL Server 2012:</i> Windows 2008 R2 (64-bit) SP1 Windows 2012 (64-bit) Windows 2012 R2 (64-bit)</p>
CPU	<p><i>MySQL and PostgreSQL:</i> 2 GHz or higher</p> <p><i>MS SQL Server:</i> 3.2 GHz or higher</p>
RAM	<p><i>MySQL and PostgreSQL:</i> 1 GB</p> <p><i>MS SQL Server:</i> 2 GB</p>
Disk space	At least 10 GB free
Open TCP ports	<p>Communication between a service node and Plesk Automation panels: TCP ports 8352-8999</p> <p>MySQL: TCP port 3306</p> <p>PostgreSQL: TCP port 5432</p>

▪ ***To register a new database server node in Plesk Automation:***

- 1 Add a database server node to Plesk Automation by starting the Add New Node wizard in Administration Panel > Infrastructure > Service Nodes. The wizard will ask you to provide the following information:
 - The service node role: MySQL database server, PostgreSQL database server, MS SQL Server 2008 database server, or MS SQL Server 2012 database server.
 - A node host name or an IP address and a root password.
 - Database server administrator's credentials.
- 2 Normally, when the installation is complete, the node is marked as Ready to provide its services. If this does not happen, resolve the issue and mark it manually on the node properties page (Infrastructure > Service Nodes).

Once the registration is completed, the node will be added to the list of service nodes in Infrastructure > Service Nodes and in Infrastructure > Database Servers.

When registering a database server node, the system automatically assigns the MySQL, PostgreSQL, or Microsoft SQL provisioning attribute to the node.

Registering an Existing Database Server

Supported database servers	MySQL 4.1, 5.0, 5.1, 5.5 PostgreSQL 7.4 – 8.4 Microsoft SQL Server 2000, 2005, 2008, 2008 R2, 2012
----------------------------	--

▪ *To register an existing database server in Plesk Automation:*

- 1 Start the Add Database Server wizard in Administration Panel > Infrastructure > Database Servers.
- 2 Provide the following information to the wizard:
 - A server host name or an IP address and a port number.
 - A database server type: MySQL, PostgreSQL, or Microsoft SQL Server.

Important: To be able to register Microsoft SQL Server-based database servers, you should have at least one IIS web server node registered in Plesk Automation.

- Database server administrator's credentials. Do not use "root" as the username.

When registering an existing database server, the system does not add it to the list of available service nodes and does not automatically assign any provisioning attributes to this server. This server will be shown only in the list in Infrastructure > Database Servers.

Note that these database servers cannot be configured for automatic service provisioning. To use such a server for providing database services, you should assign its IP address to the corresponding MySQL database or PostgreSQL database resource type of a certain service template. This should be done in Products > Service Templates > select a template > Resources tab > select the MySQL database, PostgreSQL, or Microsoft SQL database resource type > Activation Parameters > Edit.

Integrating the myLittleAdmin Tool for Microsoft SQL Server Management

To enable your Windows hosting users to manage databases with a web-based tool called myLittleAdmin, you need to set up an IIS-based webspace on which myLittleAdmin will be deployed. That deployed instance will be used for serving all Windows-based hosting subscriptions. So, you will need to perform the following steps only once:

1. Create an IIS-based webspace with enabled ASP.NET support.
2. Obtain a distribution package from <http://mylittleadmin.com/en/download.aspx>.
3. Upload the package into the `/httpdocs` directory of the webspace and extract its contents.
4. Create a virtual directory linked to the directory with the extracted package, for example, `mssqladmin`.

Now myLittleAdmin can be accessed via http://<webspace_name>/mssqladmin.

5. Configure a connection to MS SQL Server as described in *Installation Guide.pdf*, which is available in the root directory of the extracted package.
6. On the management node, issue the following command in the console:

```
/usr/local/psa/bin/custombutton -c -place domain -text 'MS SQL ADMIN' -public true -url 'http://<webspace_name>/mssqladmin'
```

After that a button with the name 'MS SQL ADMIN' will appear in Hosting Panel > Websites tab, and will lead to http://<webspace_name>/mssqladmin.

DNS Server Nodes

By default, DNS services are provided by the *management node*. It acts as a master DNS server for all zones registered in the system. Setup of DNS zones for newly added domains is automated: When a customer adds a new domain in the Hosting Panel, Plesk Automation automatically generates its zone file and registers it in the name server's database. You can view a list of domains registered in the system in Services > DNS Zones.

The functions of a master DNS server can be delegated to any node with the DNS role. You can also add slave DNS server nodes (slave servers periodically load zone data from the master server) or even more master DNS server nodes. In the latter case, Plesk Automation will create and update the same zone files on all master servers. Note that the DNS service does not require any provisioning attributes - the DNS service is an essential part of any service plan (service template) and is represented as a DNS resource type in the system. Learn more about how to work with DNS servers and the DNS resource in the Plesk Automation: Operations Guide, section DNS.

When you assign the DNS role to a node, the system automatically installs the BIND DNS server to that node.

Important: DNS servers *do not* require a license key. You can register any number of DNS servers in the system without any limitations.

Server Requirements

Before adding a DNS node to the environment, make sure that the server meets the following requirements.

OS	RHEL 5.9, 6.4 (32-bit or 64-bit) CentOS 5.9, 6.4 (32-bit or 64-bit) CloudLinux 6 (32-bit or 64-bit)
CPU	1 GHz or higher
RAM	1 GB minimum
Disk space	At least 1 GB free
Open TCP ports	DNS service: UDP port 53 Communication between a service node and Plesk Automation panels: TCP ports 8352-8999 Communication through SSH: TCP port 22

Important: You must disable SELinux on a service node before adding it to the environment. Enabling SELinux after deployment will result in your Plesk Automation installation malfunctioning. To learn how to disable SELinux, please refer to the manuals provided for the OS installed on the node.

Adding a Node

▪ *To register a DNS server node in Plesk Automation:*

- 1 Add a DNS server node to the system by starting the Add New Node wizard in Administration Panel > Infrastructure > Service Nodes. The wizard will ask you to provide the following information:
 - The service node role: DNS server.
 - A node host name or an IP address and a root password.
 - If your node has more than one IP address, you should specify:
 - Backnet IP address - this address will be used for internal communications with the management node.
 - Shared IP address - this address will be used for external communications. See Network Configuration (on page 5) for details.
- 2 Normally, when the installation is complete, the node is marked as Ready to provide its services. If this does not happen, resolve the issue and mark it manually on the node properties page (Infrastructure > Service Nodes).
- 3 Set this node as a master or slave name server in the DNS resource type properties located at the Products > Resources > DNS > Activation Parameters tab. In addition, you can set the SOA record template parameters: refresh and retry intervals, expiration period, and minimum TTL. The template settings are applied to the SOA record of all zones but can be overridden for a specific zone. Learn how to do this in the Plesk Automation: Operations Guide, section Managing DNS Zones.

Note: You can set up to three name servers in the DNS resource type properties. The first name server is always master (by default, this is the management node).

Backup Server Nodes

In Plesk Automation, administrators and resellers are not provided with a centralized means of backing up and restoring data of their customers. Only users logged in to the Hosting Panel can back up and restore data belonging to their accounts.

Plesk Automation can save backup files only on an external FTP server - a backup server node.

Important:

1. If there are no backup server nodes registered in Plesk Automation, the backup and restore functions cannot be used, and the corresponding buttons are not available to users in the Hosting Panel.
2. Backup server nodes *do not* require a license key.

Server Requirements

Before adding a backup server node to the environment, make sure that the server meets the following requirements.

OS	CentOS 5.9, 6.4 or later (32-bit or 64-bit) CloudLinux 6 (32-bit or 64-bit)
CPU	2 GHz minimum, 3.2 GHz recommended
RAM	1 GB minimum
Disk space	At least 10 GB free. You will need more space for storing customers' backups.
Open TCP ports	Communication between a service node and Plesk Automation panels: TCP ports 8352-8999 Communication through SSH: TCP port 22 FTP: TCP ports 20, 21, 60000-65000

Important: You must disable SELinux on a service node before adding it to the environment. Enabling SELinux after deployment will result in your Plesk Automation installation malfunctioning. To learn how to disable SELinux, please refer to the manuals provided for the OS installed on the node.

Adding a Node

▪ ***To register a backup server node in Plesk Automation:***

- 1 Add a server by starting the Add New Node wizard in Administration Panel > Infrastructure > Service Nodes.
- 2 Provide the wizard with the following information:
 - The service node role: Backup server.
 - A node host name or an IP address and a root password.

- If your node has more than one IP address, you should specify what IP address will be used for management purposes (communication with the management node) and what IP address will be used for shared hosting. *It is a good practice to use separate IP addresses for these purposes.*
- 3 Once the installation of the necessary packages is finished, log in to the backup node via SSH and add the line

```
PassivePorts 60000 65000
```

to the `/etc/proftpd.conf` file

Once you add the backup server node, users will be able to back up the data related to their accounts and websites in the Hosting Panel.

Billing Node

A Billing node is a server (Linux-based) that uses the Plesk Automation Billing software and provides the business support system, such as ordering, billing, account management, invoicing, and other services, including the online store.

Server Requirements

Before adding a Billing node to the environment, make sure that the server meets the following requirements.

OS	CentOS 6.5 (x86-64) or later RHEL 6.5 (x86-64) or later
CPU	2 cores (3 GHz or higher recommended)
RAM	4 GB minimum
Disk space	30 GB free or more (8 GB swap) Disk partitioning should be as follows: <ul style="list-style-type: none"> • <code>/usr/local</code> – 10 GB or more * • <code>/var</code> – 10GB or more ** • <code>/root</code> – 200 MB or more *** • <code>/tmp</code> – 200 MB or more *** <p>* The <code>/usr/local</code> directory, among other things, is used to store logs of Plesk Automation Billing</p> <p>** The <code>/var</code> directory, among other things, is used to store Plesk Automation Billing database</p> <p>*** The <code>/root</code> and <code>/tmp</code> directories are used to store installation packages</p>
Open TCP ports	8352-8999: Communication between a service node and Plesk Automation panels 5221: Connection between Plesk Automation Billing and Plesk Automation 8443: HTTPS access to Plesk Automation Billing 443: HTTPS access to Online Store
Supported virtualization	Odin Cloud Server 6.0 Virtuozzo Containers for Linux 4.7

Important: You must disable SELinux on a service node before adding it to the environment. Enabling SELinux after deployment will result in your Plesk Automation installation malfunctioning. To learn how to disable SELinux, please refer to the manuals provided for the OS installed on the node.

Adding a Node

▪ *To register a Billing node in Plesk Automation:*

- 1 Add a Billing node to Plesk Automation by starting the Add New Node wizard in Administration Panel > Infrastructure > Service Nodes. The wizard will ask you to provide the following information:
 - The service node role: Billing.
 - The Billing node host name or an IP address and a root password.
 - The Billing node public IP address, that may be used to get access to the node from any network.

Important: If your servers are behind the NAT, click Show Extended Parameters and enter the Plesk Automation Management Node's public IP address.

- 2 Plesk Automation places several tasks related to a Billing node registration. Wait until all the tasks are finished. You can check the progress in Operations > Tasks.
- 3 Assign a license key to the Billing node as described in the section Installing License Keys for Service Nodes (on page 38).
- 4 Log out from Plesk Automation.

By default Plesk Automation and Plesk Automation Billing use self-signed SSL certificates for HTTPS connections. If you do not have a valid SSL certificate, then add a security exception to your browser, to switch between Plesk Automation and Plesk Automation Billing in the same browser window:

- Type the Billing node IP address in the browser address bar: <https://<Billing node IP address>:8443>. The browser detects that the connection is untrusted.
- Add the exception. Make sure that the Billing node login page opens. Then log in to Plesk Automation. On the top frame you should see the Billing link that serves to switch between Plesk Automation and Plesk Automation Billing. On Plesk Automation Billing top frame, the Operations link should appear, to switch to Plesk Automation.

However, the security exception does not provide the comprehensive solution of the connection issue. To resolve this issue, you need to create the brand. For details, refer to the Plesk Automation Branding guide.

Enabling Mail Notifications from Web Hosting Nodes

When users schedule tasks under their hosting accounts, they can choose to be notified by email about the task completion. By default, sending of email notices from task scheduler is not configured.

To enable sending of email notices, do the following.

▪ *On Windows-based Web hosting service nodes:*

Issue the following command:

```
"%plesk_bin%\serverconf.exe" --update-mail-message-send-config --host=<mail server's IP address or host name> --port=25 --auth-user=<email address> --auth-password=<mail user's password>
```

where <email address> is the email address of a user registered in the mail sever. It will be used as the notification sender's address.

- *On Linux-based Web hosting service nodes:*

1. Install the msmtplib component by issuing the following command:

```
/usr/local/pem/var/cores/parallels_installer --skip-branch-filter --source http://autoinstall.plesk.com/PPA\_11.5.0/Plesk --select-product-id=plesk --select-release-latest --install-component msmtplib
```

2. Configure msmtplib by issuing the following command:

```
/usr/local/psa/admin/bin/msmtplib --mail-relay <mail server's IP address or host name> --auth-user <email address> --auth-passwd <mail user's password>
```

where <email address> is the email address of a user registered in the mail sever. It will be used as the notification sender's address.

Setting Up LVE in CloudLinux

All webspaces hosted on CloudLinux servers are automatically isolated by means of LVE (Lightweight Virtual Environments). The resource limits for each LVE are configured according to the default settings, which vary among CloudLinux versions.

- *To find out the default settings, issue the following command on the CloudLinux server:*

```
lve limits default
```

- *To configure the default settings for all newly created LVEs:*

1. Log in to the service node with CloudLinux.
2. Issue the command `yum install mod_hostinglimits`.
3. To set up LVE limits, use the `lvectl` utility. For example, to set the maximum CPU usage to 10 percent, maximum I/O to 100 KB/s, maximum memory usage to 512 MB, and maximum physical memory usage to 1 MB, issue the following command:

```
lvectl set default --cpu=10 --io=100 --vmem=512M --pmem=1M
```

To learn more about CloudLinux and the `lvectl` utility, refer to the documentation at <http://docs.cloudlinux.com/>.

- *To configure the limits for a specific LVE:*

1. Log in to the service node with CloudLinux.
2. Find out the FTP user IDs of webspaces:

```
grep `grep SuexecUserGroup
/var/www/vhosts/system/<webpace_name>/conf/httpd.conf | awk
-F '""' '\{print($2)\}'` /etc/passwd | awk -F ':'
'\{print($3)\}'
```

where <webpace_name> is the name of the main domain of the webpace whose LVE settings you want to reconfigure.

3. To set up LVE limits, use the `lvectl` utility. For example, to set up limits for a webpace with system user ID 1, set maximum CPU usage to 10 percent, maximum I/O to 100 KB/s, maximum memory usage to 512 MB, and maximum physical memory usage to 1 MB, issue the following command:

```
lvectl set 10000 --cpu=10 --io=100 --vmem=512M --pmem=1M
```

Setting Up CageFS in CloudLinux

CageFS is a virtualized file system and a set of tools to contain each user in its own "cage", which is similar in purpose to a jailed or chrooted environment.

Note: CageFS does not support `mod_php`; for this reason, some web applications on websites might become inoperable. To learn more about CageFS, refer to <http://docs.cloudlinux.com/index.html?cagefs.html>.

- *To install and enable CageFS for all webspaces:*

Issue the following commands on CloudLinux service nodes:

```
$ yum install cagefs
$ /usr/sbin/cagefsctl --init
$ /usr/sbin/cagefsctl --enable-all
```

After that, all webspaces (existing and new ones) will be caged.

Installing License Keys for Service Nodes

If you use licensing per service nodes, then you should obtain and install additional license keys for each service node, except for those that act as *dedicated database or DNS servers* (service nodes with the DNS or MySQL roles). There are three essential types of additional license keys:

- An unlimited license key for Plesk for Linux-based dedicated hardware servers. These keys should be used with all Linux-based web server or mail nodes.

- An unlimited license key for Plesk for Microsoft Windows-based dedicated hardware servers. These keys should be used with IIS web server and SmarterMail mail service nodes.
- A license key for Odin Premium Antivirus. These keys should be used when you want to use antivirus on mail service nodes. Without a license key, antivirus will not check mail for viruses and malware.

Note: To enable database hosting, license keys for web hosting nodes must support hosting of appropriate databases.

- *To install additional license keys for service nodes:*
 1. Purchase a license key for Plesk for Linux or Windows. You can do this either in the online store (<https://www.plesk.com/plans-pricing/>) or through your infrastructure provider.
 2. Install the license key and assign it to the proper service node in Administration Panel > System > License Manager > Additional Licenses tab > Install / Update.

CHAPTER 6

Troubleshooting

If you are experiencing problems with a certain Plesk Automation deployment step, follow the instructions below to identify and resolve the issue.

In this chapter:

Installing Plesk Automation	40
Accessing Plesk Automation.....	40
Adding Service Nodes.....	40
Using Plesk Automation.....	42

Installing Plesk Automation

Search for errors in the Plesk Automation installation log file
`/usr/local/ppa/log/install.log`.

Accessing Plesk Automation

Search for errors in the access log files located in `/usr/local/ppa/log/`:

- `sso.log`
- `plesk_access.log`

Adding Service Nodes

If Plesk Automation fails to register a service node, we recommend that you:

- 1 Look for the failed tasks in Operations > Tasks. This will allow you to understand in what step Plesk Automation failed to attach the node.
 - 2 Run a special command-line tool called `ppa.sn_test`. This tool performs a number of checks (including firewall configuration, OS version, SSL certificate validity, and so on) that determine whether the node is compatible with Plesk Automation.
- ***To check the compatibility of the node with Plesk Automation:***
 - 1 Log in to your management node as root.
 - 2 Run the check for the node.


```
ppa.sn_test --ip <IP_address>
```

where <IP_address> is the IP address of the node you want to check.

While performing the checks, the tool logs all of its actions and action results. The results are displayed on the screen and also logged to the `/usr/local/ppa/log/check_service_node.log` file. [ERROR] messages in the tool's output mean that a certain check failed and the node cannot be attached to Plesk Automation until the issue is resolved. See an example of the output below.

An Example of the Output

```
[07 May 2013 04:30:28 NOVT][INFO] Service node is not registered in Plesk
Automation
[07 May 2013 04:30:28 NOVT][INFO] Start checking 'Linux' service node with ip
'10.52.53.77', user 'root'
[07 May 2013 04:30:29 NOVT][INFO] Checking the operating system version
running on the service node...
[07 May 2013 04:30:29 NOVT][INFO] [OK]
[07 May 2013 04:30:29 NOVT][INFO] Checking whether the node's host name is
properly defined...
[07 May 2013 04:30:29 NOVT][INFO] [OK]
[07 May 2013 04:30:29 NOVT][INFO] Checking whether the system time is
synchronized between the service node and the management node...
[07 May 2013 04:30:29 NOVT][INFO] [OK]
[07 May 2013 04:30:29 NOVT][INFO] Checking whether SELinux is switched off...
[07 May 2013 04:30:29 NOVT][INFO] [OK]
[07 May 2013 04:30:29 NOVT][INFO] Checking whether the DNS resolve server
names...
[07 May 2013 04:30:30 NOVT][INFO] [OK]
[07 May 2013 04:30:30 NOVT][INFO] Checking whether there is enough disk space
on service node...
[07 May 2013 04:30:30 NOVT][INFO] [OK]
[07 May 2013 04:30:30 NOVT][INFO] Checking connection from service node to
management node...
[07 May 2013 04:30:30 NOVT][INFO] Checking connection from service node to ip
'10.52.166.70', port '80'
[07 May 2013 04:30:30 NOVT][INFO] Checking connection from ip '10.52.53.77',
port '8352' to ip '10.52.166.70', port '8352'
[07 May 2013 04:30:45 NOVT][WARNING] --port 8352 is closed.
[07 May 2013 04:30:45 NOVT][INFO] Checking connection from ip '10.52.53.77',
port '8354' to ip '10.52.166.70', port '8354'
[07 May 2013 04:31:00 NOVT][WARNING] --port 8354 is closed.
[07 May 2013 04:31:01 NOVT][ERROR] Several connections from service node to
management node are failed. Please resolve the issue. The solution is
described in http://kb.parallels.com/en/115202
[07 May 2013 04:31:01 NOVT][INFO] Checking connection from management node to
service node...
[07 May 2013 04:31:01 NOVT][INFO] Checking connection from management node to
ip '10.52.53.77', port '8352'
[07 May 2013 04:31:18 NOVT][WARNING] Unable to connect to port 8352: Timed
out
[07 May 2013 04:31:18 NOVT][INFO] Checking connection from management node to
ip '10.52.53.77', port '8354'
[07 May 2013 04:31:35 NOVT][WARNING] Unable to connect to port 8354: Timed
out
[07 May 2013 04:31:35 NOVT][INFO] Checking connection from management node to
ip '10.52.53.77', port '8443'
[07 May 2013 04:31:37 NOVT][ERROR] Several connections from management node to
service node are failed. Please resolve the issue. The solution is described
in http://kb.parallels.com/en/115202
[07 May 2013 04:31:37 NOVT][INFO] Checking whether a valid SSL certificate is
installed...
[07 May 2013 04:31:37 NOVT][INFO] --retrieving the SSL certificate...
[07 May 2013 04:31:37 NOVT][INFO] --validating the SSL certificate...
[07 May 2013 04:31:37 NOVT][INFO] [OK]
```

```
[07 May 2013 04:31:37 NOVT][INFO] Checking that iptables is installed...
[07 May 2013 04:31:37 NOVT][INFO] [OK]
[07 May 2013 04:31:37 NOVT][INFO] Checking that yum is installed...
[07 May 2013 04:31:38 NOVT][INFO] [OK]
[07 May 2013 04:31:38 NOVT][INFO] Checking whether the yum repositories (base
and updates) are configured...
[07 May 2013 04:31:38 NOVT][INFO] [OK]
[07 May 2013 04:31:38 NOVT][INFO] Checking that yum can install required
packages...
[07 May 2013 04:31:40 NOVT][ERROR] Unable to find the required packages in yum
repositories. Please make sure that yum is configured to use the proper
operating system repositories (base and updates). To learn how to configure
yum, refer to the following article: http://kb.parallels.com/en/115963
[07 May 2013 04:31:40 NOVT][CRITICAL] This node FAILED to meet some of the
Plesk Automation requirements. Please correct all the errors and run the tool
again
[07 May 2013 04:31:40 NOVT][ERROR] Following errors were detected:
[07 May 2013 04:31:40 NOVT][ERROR] - Several connections from service node to
management node are failed. Please resolve the issue. The solution is
described in http://kb.parallels.com/en/115202
[07 May 2013 04:31:40 NOVT][ERROR] - Several connections from management node
to service node are failed. Please resolve the issue. The solution is
described in http://kb.parallels.com/en/115202
[07 May 2013 04:31:40 NOVT][ERROR] - Unable to find the required packages in
yum repositories. Please make sure that yum is configured to use the proper
operating system repositories (base and updates). To learn how to configure
yum, refer to the following article: http://kb.parallels.com/en/115963
```

Using Plesk Automation

Search for errors in the Plesk Automation system logs located in `/usr/local/ppa/log/`:

- `poa.log`, `poa-ui.log`, and `poa.debug.log` for the Administration Panel
- `plesk.log` for the Hosting Panel
- `mail.log` for mail services
- `sitebuilder.log` for Presence Builder

In some cases, you may need to restart the Administration or Hosting panels. You can do this with the following commands:

- *The Administration Panel:*
`/etc/init.d/ppa start|stop|restart`
- *The Hosting Panel:*
`/etc/init.d/sw-cp-server start|stop|restart`

In some cases, you may need to restart services provided by Linux nodes. You can do this with the following commands (executed on a certain node):

- *Apache HTTP server:*
`service httpd start|stop|restart`
- *Postfix mail server:*
`service postfix start|stop|restart`
- *MySQL server:*

```
service mysqld start|stop|restart
```

- *PostgreSQL server:*

```
service postgresql start|stop|restart
```

- *Bind DNS server:*

```
service named start|stop|restart
```

- *Plesk Automation agent:*

```
service ppa_agent start|stop|restart
```