



DNS Manager

4PSA DNS Manager 3.7.0

Client's User Guide

For more information about 4PSA DNS Manager, check:
<http://www.4psa.com>
Copyrights 2002-2010 Rack-Soft, Inc.

Client's User Guide

Manual Version 65511.56 at 2010/04/19 18:10:20

For suggestions regarding this manual contact:

docs@4psa.com

All rights reserved

Distribution of this work or derivative of this work is prohibited unless prior written permission is obtained from the copyright holder.

4PSA is a Registered Trademark of Rack-Soft, Inc.

Plesk is a Registered Trademark of Parallels, Inc.

Linux is a Registered Trademark of Linus Torvalds.

RedHat is a Registered Trademark of Red Hat Software, Inc.

FreeBSD is a Registered Trademark of FreeBSD, Inc.

All other trademarks and copyrights are property of their respective owners.

Table of Contents

Preface	5
Who Should Read This Guide	5
Chapter 1. About 4PSA DNS Manager 3.7.0	6
Where to Use 4PSA DNS Manager	6
4PSA DNS Manager 3.7.0 Features	6
Chapter 2. Logging in to 4PSA DNS Manager	9
Editing Account Information	9
Chapter 3. Managing DNS zones	11
Creating a New DNS zone	12
Adding a Single DNS Zone Name	13
Adding Multiple DNS Zones with Complete DNS Records	15
Editing a DNS Zone Configuration	16
Enabling/Disabling the Zone	17
Setting SOA Parameters	17
Checking the Nameservers	19
Managing DNS Records	19
Adding DNS Records	30
Editing DNS Records	30
Removing DNS Records	30
Global Operations on DNS Zones	30
Glue Records	32
SPF Rules	33
Removing DNS Zones	34
Managing DNS Zones Remote Update Locations	35
Creating a New Remote Update Location	37
Editing a Remote Update Location Settings	38
Removing a Remote Update Location	38
Remote Logs	38
Backing Up DNS Records	39
Backing Up DNS Zones	39
Backing Up a DNS Zone	39
Transfer IP Addresses	40

Managing Round Robin Polls	40
Editing Round Robin Polls	40
Adding Round Robin Polls	41
Chapter 4. The Settings Configuration	43
Available Options	43
Managing DNS Templates	44
Creating a New DNS Template	45
Managing a Template's DNS Records	45
Managing a Template's IPs	55
Editing DNS Templates	55
Removing DNS Templates	56
Setting Interface Preferences	56
Configuring SOA settings	56
Managing Custom Buttons	58
Adding Custom Buttons	59
Editing Custom Buttons	60
Removing Custom Buttons	60
XML export	60
XML import	61
Chapter 5. Remote Update Location Configuration	62
1. 4PSA DNS Manager as a Secondary Server	62
2. 4PSA DNS Manager as a Primary Server	64
Appendix A. Supported Dump File examples	66

Preface

Who Should Read This Guide

This Client's Guide must be read by the 4PSA DNS Manager clients.



Chapter 1

About 4PSA DNS Manager 3.7.0

4PSA DNS Manager 3.7.0 is a server-level application that allows users to manage DNS zones. With 4PSA DNS Manager you can create and manage DNS zones and DNS Records, backup DNS zones, manage DNS templates, gather DNS information from remote servers, etc. Thanks to its advanced features, 4PSA DNS Manager is the ideal tool for automatic DNS management. 4PSA DNS Manager can load DNS zone names from remote servers, regardless of the control panel or operating system that runs on these servers.

Where to Use 4PSA DNS Manager

Unlike other DNS management applications, 4PSA DNS Manager offers superior automation features and a friendly client level interface. Clients who use hosting services will find 4PSA DNS Manager to be a very easy to use solution. Most DNS applications are frustrating; it is a known fact that even some administrators do not fully understand all DNS functions. With 4PSA DNS Manager these problems have become history.

Below you can find several utilization scenarios:

- Centralize DNS information from multiple servers. You will be able to offer two name servers no matter how many hosting servers you have and what platform or control panel is used on these. The centralization process is automatic and you do not have to add DNS zone information to the 4PSA DNS Manager server. Interface scripts for Plesk, Cpanel, Ensim, DirectAdmin, InterWorx Control Panel, Helm and Cobalt are included.
- Offer DNS redundancy. 4PSA DNS Manager can act as a secondary DNS server, gathering zone names from all the participant servers and automatically updating DNS zone information.
- Offer DNS hosting. Hosting companies can use your services for DNS redundancy. Because no work is actually required to update the list of DNS zones, DNS hosting becomes a very simple task. Clients will love the nice interface and the zone validation.

4PSA DNS Manager 3.7.0 Features

4PSA DNS Manager 3.7.0 offers the following features:

- Administrator and client management levels
- System designed for automatic DNS hosting
- Client permissions and limits
- Command line creation utilities
- Supports both RFC1912 and timestamp SOA Serial number formats
- SOAP API third party integration
- DNS zone Management:
 - Advanced Reverse DNS zones management
 - Create DNS zones in interface (single zones or from file)
 - Master/Slave zones supported
 - A, AAAA, CNAME, NAPTR, NS, MX, PTR, SRV, TXT Records supported
 - Advanced Record management with owned and wide server level and client level DNS templates support
 - Update DNS zone information from remote servers (can retrieve the list of DNS zones added in any control panel interface)
 - Per server or per client Start of Authority (SOA) Records: refresh time, retry time, expire time, minimum TTL, default TTL
 - Automatic query of reverse DNS

- Supports E 164 zones
- Remote update locations management:
 - Remote zone types / Update interval
 - Remote update statistics
 - Advanced parallelism and QoS settings for maximum performance
- Backup DNS zones in CSV format:
 - Server level backup (backups for all DNS zones on the server)
 - Client level backup (backups for all DNS zones owned by a client)
 - Backups for separate DNS zones
- Runs on RedHat servers. It can be installed on servers running Plesk (the Plesk server will be the centralized DNS server)
- Automatic import scripts for Plesk, Cpanel, Ensim, DirectAdmin, InterWorx Control Panel, Helm and Cobalt are included in the package
- Create and manage client DNS templates
- DNS Server monitoring with administrator alerting
- Email notifications triggered by the actions of clients, administrators or other events
- Custom buttons support (that allow users to link and interact with other systems)
- Users sessions management with advanced options
- Foreign and new .net domain names support
- Skin-able interface
- Language packs capabilities

Chapter 2

Logging in to 4PSA DNS Manager

You can log in to the 4PSA DNS Manager interface at `https://<installation_url>:8550/` using a Client account.

The 4PSA DNS Manager navigation menu is available on the left side of the interface. The navigation menu provides an easy method for you to manage DNS zones and Records, backup DNS Records, and modify settings.

Editing Account Information

In order to modify the account's details, click the  Edit Account Details button available in the Tools area.

Company name – This is the company name

Contact Name – This is used by the 4PSA DNS Manager to identify the client

Login – This is the username used to access his 4PSA DNS Manager account

Password – This is the password used by the client to access his 4PSA DNS Manager account



Note

The **Login** name must be unique on the system.

The **Password** should be 6 to 14 characters long and should not contain quotes, spaces or national alphabet characters. For security reasons, the **Password** cannot be the same as the **Login** name.

Confirm Password – This is required to make sure the correct password is entered

Phone – This is the phone number

Fax – This is the fax number

E-mail – This is the email address, which is used as the default bounce address for the client's domains

Address – This is the client's postal address

City – This is the client's city

Postal/ZIP code – This is the ZIP or postal code

State

Country

Language - The interface language.

The required fields are marked with an asterisk. Click OK to save the changes you have made. Click Cancel, if you want to return to the previous page without saving these changes.

Chapter 3

Managing DNS zones

You can add new DNS zones to the 4PSA DNS Manager system and manage the DNS Records for a zone. In order to perform these tasks, click the [DNS zones](#) link available in the navigation menu.

In this area, the following details are available:

S – This column displays the status of the DNS zone:  enabled or  disabled

T – This column displays the type of the corresponding DNS zones. This can be  Master or  Slave.

DNS zone name – The name of the DNS zone.

First name server – The hostname of the first name server registered on this DNS zone.



Note

The first name server of slave zones is not displayed.

Created – The date when the zone was created on the system.

The information can be sorted by type, DNS zone name, and creation date by clicking the table header links.

When you are searching for specific DNS Zone, you can use one or more of the available filters:

Show {name} and include [] records also, where:

{name} - Use the available text box to specify the name of the DNS Zones you are looking for.

[] - Select this check box if you want the search to be performed through the Value field from the DNS records.

[Search](#) - By clicking this link, all the DNS Zones matching the chosen search criteria will be displayed.

[Show all](#) - After the DNS Zones list was filtered, you may click this link to discard the filter and display all the DNS Zones.



Note

If you want to hide/reveal the search options, click the  [Toggle search](#) link.

Other operations can be performed by using the following action links:

[Show columns](#) - You can filter the columns displayed in the table by clicking this link.

[Group operations](#) – Choose the desired zones from the list by selecting their corresponding check boxes and click this link to make group changes to all the selected DNS zones. For more information, see [this](#) section.

Creating a New DNS zone



In order to add a new DNS zone, click the  Add DNS zones button in the DNS zones page. You can add a single DNS zone or multiple DNS zones with complete DNS Records.



Note

You must have the necessary permissions to add and manage DNS zones. These permissions are set up by the administrator.



Note

4PSA DNS Manager also accepts **internationalized domain names (IDN)** - Internet domain names that contain non-ASCII characters.

Adding a Single DNS Zone Name

In order to add a single DNS zone name, you must enter all the information required in the Add DNS zone name area.

DNS zone name – Enter a valid DNS zone name that is unique in the system. You can add a Forward zone, a Reverse zone or an E.164 zone. The name must be unique in the system. Here are some typical examples:

- For forward zones, one must use the following format: <lower level domain(s)>.<top level domain>. For instance:
 - racksoft.com
 - wikipedia.org
 - amazon.co.uk
- For reverse zones, one must use the following format: <lower level domain(s)>.IN-ADDR.ARPA. For instance:
 - 2.85.64.IN-ADDR.ARPA
 - 4.3.2.1.IN-ADDR.ARPA
- For E.164 zone, one must use the following format <lower level domain(s)>.E164.ARPA. For instance:
 - 2.2.3.E164.ARPA
 - 1.1.1.E164.ARPA



Note

For reverse zones, 4PSA DNS Manager accepts the following zone Name types:

- Class A (/8) - 1.IN-ADDR.ARPA
- Class B (/16) - 2.1.IN-ADDR.ARPA
- Class C(/24) - 3.2.1.IN-ADDR.ARPA
- zone Names with a mask lower than 24 (having a numeric value higher than 24) - 192/26.1.2.3.IN-ADDR.ARPA that covers IPs between 3.2.1.192 and 3.2.1.255; or 4.3.2.1.IN-ADDR.ARPA for a complete /32 delegation.

DNS zone template – You can use the DNS zone templates available or can choose not to use any template at all.

Template IP – This field is available when a DNS zone template is selected. All occurrences of [ip] in the template will be replaced with this IP

DNS zone type – The type of the DNS zone: master or slave.



Note

A slave zone will acquire its zone data only after receiving the notification from the respective master zone, or after it is manually reloaded on the server. 4PSA DNS Manager does not reload slave zones due to the extra overhead involved on busy environments, therefore is recommended to setup notifications on master zones.

- When the chosen type is master, the Allow DNS zone transfer option becomes available and the Slave DNS servers IP addresses option is disabled.
- When the chosen type is slave, the Transfer DNS zone from master servers option is enforced and the Master DNS servers IP addresses option becomes available.

Two more options are available, but they depend on the DNS zone type. When the chosen type is master, the following check boxes can be enabled:

Forward zone - When this option is enabled, this is considered to be a regular zone.

Reverse zone – When this option is enabled, this is considered to be a zone used for reverse DNS lookup (i.e. a zone in the *in-addr.arpa* domain).

E.164 zone - When this option is enabled, this is considered to be an E.164 zone used for mapping telephone numbers into DNS (i.e. a zone in the *e164.arpa* domain).

Allow DNS zone transfer – When this option is enabled, allowed slave servers will be able to retrieve the zone information from the master server (in this case the 4PSA DNS Manager system).

Slave DNS servers IP addresses – When the Allow DNS zone transfer option is enabled, you can enter in this text box the IP addresses of the slave DNS servers. Click the plus/minus icons to add/remove fields for the slave IP addresses. The DNS zone will be transferred only to these IP addresses.

When the chosen type of the DNS zone is slave, the following options **MUST** BE enabled:

Transfer DNS zone from master servers – The DNS zone information will be transferred from the master DNS servers with the IP addresses set in the field below.

Master DNS servers IP addresses – Use this text box to specify the IP addresses of the master DNS servers.

The required fields are marked with an asterisk. Click OK to create the new DNS zone. Click Cancel, if you want to return to the previous page without creating the DNS zone.

Adding Multiple DNS Zones with Complete DNS Records

In order to add multiple DNS zones with complete DNS Records, click the  Add DNS zone button, then click the  Full zones from file button available in the area. The following fields will be displayed:

Select file – Enter the name of the file that contains the DNS zone names or click the Browse ... button to locate the desired file.



Note

The uploaded file MUST be in dump format (identical to the file generated by backing up DNS zones in 4PSA DNS Manager). For more information on the dump file format, please read the [Supported Dump File examples](#) appendix.



Note

A slave zone will acquire its zone data only after receiving the notification from the respective master zone, or after it is manually reloaded on the server. 4PSA DNS Manager does not reload slave zones due to the extra overhead involved on busy environments, therefore is recommended to setup notifications on master zones.

Two more options are available, but they depend on the DNS zone type. When the chosen type is master, the following fields can be enabled:

Allow DNS zone transfer – When this option is enabled, allowed slave servers will be able to retrieve the zone information from the master server (in this case the 4PSA DNS Manager system).

Add the following allow transfer IPs to master zones - The IP addresses specified in this field will be recorded in the allow transfer clauses of the named.conf file for MASTER DNS zones

Add the following master IPs to slave zones - The IP addresses specified in this field will be recorded in the masters clauses of the named.conf file for SLAVE DNS zones

Click OK to create the new DNS zone. Click Cancel, if you want to return to the previous page without creating the DNS zone. This may take some time depending on the size of the file you have specified.

Editing a DNS Zone Configuration

In order to manage a DNS zone, the client must click the chosen DNS zone name and enter the DNS zone management page.



Warning

Records of zones that have been added from a remote location cannot be modified from interface.

For zones added from remote locations, 4PSA DNS Manager displays the following warning message:

This zone is managed by Remote Update and can not be edited in the interface.

In the Actions area, you can switch the zone type from Master to Slave and vice-versa by clicking the  Switch to Master or  Switch to Slave button.

In this page there are several details available about the DNS zone, like zone type, last DNS zone update and Last DNS zone update source, and you can add a transfer IP address.



Note

Pay particular attention to the **Last DNS zone update**. This is the time when the zone was actually updated by the low level program.

To add a Master/Slave DNS server IP address enter the IP address in the corresponding field and click the OK button.

To manage your transfer IPs, click the  Transfer IP addresses button.

In order to create a local backup file of the DNS zone, click the  Backup DNS zone button. The file contains a list of the DNS Records for the chosen domain account.

If you are editing a forward zone and if the client is allowed Round Robin management, the  DNS Round Robin button will be available in the Tools area. Press this button to open the Round Robin polls management page.

Enabling/Disabling the Zone

You can switch the DNS zone between the Enabled and Disabled status:

- If the DNS zone is currently enabled, click the  zone is enabled button to disable it and switch the button to  zone is disabled.
- If the DNS zone is currently disabled, click the  zone is disabled button to enable it and switch the button to  zone is enabled.

Setting SOA Parameters

The SOA (Start of Authority) Record defines global parameters for the DNS zone. There is only one SOA Record allowed in a DNS zone file.

The default SOA parameters values for all the DNS zones that belong to the client account can be modified. The following options can be customized:

Serial - The DNS Zone serial number that must be a natural value between 1 and 4294967295 (a 32 bit unsigned number). The value must increment when any resource record in the zone file is updated. A slave (secondary) DNS server will read the master's DNS SOA record periodically, either when refresh expires or when it receives a NOTIFY and will arithmetically compare the value of the serial number it currently stores with the one received from the master (primary) DNS. If the master's serial value is arithmetically higher than the one currently stored by the slave, then a zone transfer is initiated. If the value is the same or lower, then the zone transfer is not initiated and the slave DNS will not update.



Note

Serial example: 1271668821

This value represents the current date and time (2010-04-19 12:20:21) using the UNIX time stamp.

The serial is generated automatically - Select this check box if you want the serial number to be automatically generated.

Depending on if you enabled this option or not, the serial can behave in three ways:

1. If the check box is selected, then the serial number will be automatically generated.
2. If the check box is selected and the serial number is manually modified, then DNS Manager will use for the first time the modified serial and, after this, it will automatically generate new serial numbers.
3. If the check box is not selected, then the serial will not be automatically generated and the value entered in the Serial text box will be used. This method will force the serial to a certain value and the slave DNS server will never update the zone.

Refresh time – 32 bit time value in seconds. This is the period of time that the secondary name server should wait before checking with the primary server to see whether the data has been modified. Default value: 10800 seconds.



Note

RFC 1912 recommends 1200 to 43200 seconds, if your data is volatile or 43200 (12 hours) if it is not.

Retry time – Signed 32 bit value in seconds. When a secondary name server requests for a zone refresh from the primary server and this fails to respond, the secondary name server waits for the refresh time before attempting another zone refresh after the failed attempt. Default value: 3600 seconds.

Expire time – Signed 32 bit value in seconds. This setting indicates when the zone is no longer authoritative and new interrogation of the root servers is required. It applies to Slaves only. Default value: 604800 seconds.



Note

RFC 1912 recommends 1209600 to 2419200 seconds (2–4 weeks).

Minimum TTL – This value is used as the default TTL for new Records created within the zone. It is also used by other DNS servers to cache negative responses (for example when a Record does not exist). Default value: 86400 seconds.

Default TTL – Signed 32 bit value in seconds. This is the amount of time that zone Records are kept in a remote host cache. It is recommended that this value be set large. A small value will force remote servers to query the DNS server again for unchanged data. Default value: 604800 seconds.

Checking the Nameservers

You can verify the availability of the name servers for a zone by clicking the  Check Name Servers button in the Tools area of the zone's management page. The page will be updated with a new area entitled Check Name Servers which lists all the name servers and displays their availability using the following indicators:

- Not available - The name server is unavailable.
- Timed out - The name server did not answer in due time.
- Available - The name server is available.
- Unknown - The name server could not be found.

Managing DNS Records

In order to manage DNS Records for a DNS zone, click the chosen DNS zone name.



Warning

Records of zones that have been added from a remote location cannot be modified from interface.

For zones added from remote locations, 4PSA DNS Manager displays the following warning message:

This zone is managed by Remote Update and can not be edited in the interface.

The DNS zone management displays the following details:

DNS zone type – This field displays the type of the DNS zone, which can be Master or Slave. It also displays the number of Transfer IPs for Master zones and the number of Master IPs for Slave zones respectively.

Hosts in this zone - Displays the first and last available IP (these parameters depend on the reverse zone ip class).



Note

Hosts in this zone is displayed only for reverse DNS zones.

Last DNS zone update – This field displays the date when the DNS zone was last updated by the user or from the remote update location.

Last DNS zone update source – The source of the last update. The DNS zone can be updated from the interface or from a remote update location. If the zone was update from a remote location and you have the permission to manage remote update locations, the  icon is displayed. Click this icon to access the configuration page of the respective remote update location.

You can add new DNS Records, view and delete existing Records.



Note

To be able to manage DNS Records, you must have the appropriate permissions enabled.



Warning

Records can be modified only for zones added from the 4PSA DNS Manager control panel.

In the list of existing DNS Records, the following details are available:

S - Indicates whether the record is enabled or disabled.

- The  icon indicates that the record is enabled. Click it to disable the corresponding record.
- The  icon indicates that the record is disabled. Click it to enable the corresponding record.
- The  icon indicates that the record has been temporarily disabled by Round Robin who hasn't been able to access it.



Warning

The records status can be modified only for zones added from the 4PSA DNS Manager control panel.

P - Indicates whether there are any Round Robin polls monitoring the record.

- The  icon indicates there are Round Robin polls set up for the corresponding record. Clicking it will open the Round Robin polls management page for the record.
- The  icon indicates there are no Round Robin polls set up for the corresponding record.



Warning

This column is available only for forward zones added from the 4PSA DNS Manager control panel.

Host – This field displays the host name or IP address of every DNS Record

Record type – This is the type of the DNS Record. Based on the DNS zone type it can be:

- For Forward DNS zones
 - IP Address (A) - Maps a hostname to a 32-bit IPv4 address. Type A rules have the following format:
`hostname. IN A XXX.XXX.XXX.XXX`
where:
 - `XXX.XXX.XXX.XXX` is the IP address for the hostname.
 - `hostname.` is the zone name or one of its subdomains.For example:
`domain.com. IN A 1.2.3.4`
`subdomain.domain.com. IN A 1.2.3.4`
For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.
 - AAAA Record (AAAA) - Maps a hostname to a 128-bit IPv6 address. AAAA rules have the following format:

hostname. IN AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA

where:

- AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA is the IPv6 address for the hostname.
- hostname. is the zone name or one of its subdomains.

For example:

domain.com. IN AAAA abcd:1234:ffff:0:12:3:ab1:aa

subdomain.domain.com. IN AAAA abcd:1234:ffff:0:12:3:ab1:aa

For more information about this type of record, go to <http://tools.ietf.org/html/rfc3596>.

- Alias for record (CNAME) - Canonical name record is an alias (or nickname) of one name to another. The A record to which the alias points can be either local or remote - on a foreign name server. This is useful when running multiple services (like an FTP and a webserver) from a single IP address. Each service can then have its own entry in DNS (like ftp.example.com. and www.example.com.). It is also used when running multiple HTTP servers, with different names, on the same physical host. CNAME rules have the following format:

hostname. IN CNAME servername.

where:

- hostname. is the zone name or one of its subdomains
- servername. is a fully qualified domain name (FQDN) either inside or outside the zone.

For example:

ftp.domain.com. IN CNAME inside.domain.com.

ftp1.domain.com IN CNAME outside.zone.com.



Note

Rfc 1034 states: "If a CNAME record is present at a node, no other data should be present; this ensures that the data for a canonical name and its aliases cannot be different."

In order for these requirements to be met in 4PSA DNS Manager, the value specified in the **zone alias name** field of the CNAME record cannot be set for the **DNS zone name** filed in NS, A, AAAA, SRV, CNAME and TXT records or for the **zone email** field in an MX record.

For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.

- **Nameserver (NS)** - Maps a domain name to a list of DNS servers authoritative for that domain. Delegations depend on NS records. NS rules have the following format:

hostname. IN NS servername.

where:

- hostname. is the zone name or one of its subdomains
- servername. is a domain name which specifies an authoritative host for the specified hostname.

For example:

domain.com. IN NS ns1.example.com.

domain.com. IN NS ns2.example.com.



Note

The NS records of \$ORIGIN are displayed in bold characters.

4PSA DNS Manager allows to choose in the interface which is the primary nameserver on a zone (required for some local TLDs). In order to setup an NS record as primary check **Make primary** when you add/edit the desired NS record.



Caution

For BIND to take a DNS zone into consideration, at least one NS record must be defined for \$ORIGIN in the respective zone.

For best practice, it is recommended to have at least two NS records defined for each public domain.

For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.

- **Mail exchanger (MX)** - Maps a domain name to a list of mail exchange servers for that domain. MX rules have the following format:

hostname. IN MX preference servername.

where:

- hostname. is the zone name or one of its subdomains

- preference indicates the hostname's priority. The lower the preference, the higher the priority. This parameter accepts values between 0 and 50.
- servername. is a fully qualified domain name (FQDN) inside the zone

For example:

mail.domain.com. IN MX 10 domain.com.

webmail.domain.com. IN MX 5 domain.com.

For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.

- Text record (TXT) - Allows an administrator to insert arbitrary text into a DNS record. This has been used to implement new functions with DNS support without allocating new record types. For example, this record is used to implement the Sender Policy Framework and DomainKeys specifications. TXT rules have the following format:

hostname. IN TXT "Text information"

where:

- hostname. is the zone name or one of its subdomains
- "Text information" can be any type of string including strings generated by SPF Rules

For example:

domain.com. IN TXT "k=rsa; p=MEwwDQYerwqEWwE"

subdomain.domain.com. IN TXT "this is a test"

For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.

- Service Record (SRV) - Specifies the location of the server(s) for a specific protocol and domain. SRV rules have the following format:

_Service._Protocol.Hostname. IN SRV TTL Priority Weight Port Target

where:

- Service is the symbolic name of the desired service. You can find a list of the available services at <http://www.dns-sd.org/ServiceTypes.html>.
- Protocol is the protocol of the desired service. This is usually TCP or UDP, but 4PSA DNS Manager supports all the protocols listed here <http://www.iana.org/assignments/protocol-numbers>.
- Hostname. is the domain name for which the record is valid.

- TTL is the standard DNS time to live field. If there is no TTL specified for the record, the TTL value for the zone will be employed.
- Priority is the priority of the target host. The lower the value, the higher the priority level.
- Weight indicates a relative weight between records with the same priority.
- Port is the port on which the service is to be found.
- Target is the domain name of the target host.



Note

The Target parameter can not be an alias (CNAME).
When Target is set to . the service is unavailable.

For example:

```
_service._tcp.domain.com. IN SRV 0 1 9 subdomain.domain.com.  
*._tcp.domain.com. IN SRV 0 0 0 . ; no other service is available  
on tcp protocol
```

For more information about this type of record, go to <http://tools.ietf.org/html/rfc2782>.

• For Reverse DNS zones

- Nameserver (NS) - Specifies a host which should be authoritative for the specified class.

For class C reverse zones, 4PSA DNS Manager accepts NS records for \$ORIGIN and supports classless delegation records, as described in RFC 2317, chapter 4.



Note

The NS records of \$ORIGIN are displayed in bold characters.

4PSA DNS Manager allows to choose in the interface which is the primary nameserver on a zone (required for some local TLDs). In order to setup an NS record as primary check **Make primary** when you add/edit the desired NS record.



Caution

For BIND to take a DNS zone into consideration, at least one NS record must be defined for \$ORIGIN in the respective zone.

For best practice, it is recommended to have at least two NS records defined for each public domain.

Class A and B zones support NS records for \$ORIGIN and inferior class zones and do not support classless delegation records.

For class C reverse zones, 4PSA DNS Manager automatically generates CNAME records that correspond to the NS records created for classless delegation records. If the Automatically generate CNAME records for delegated subnets check box is selected, then the CNAME records will be automatically generated. This check box is available only for NS records with a subnet mask lower than 24 (having a numeric value higher than 24). NS rules have the following format:

`ip_part.host_ip_addr.in-addr.arpa. IN NS servername.`

where:

- `host_ip_addr.in-addr.arpa.` is the zone name
- `ip_part` is the IP section that completes the IP address when prepended to `host_ip_addr` (for class A, B and D zones, and for class C \$ORIGIN NS)
- for classless delegation records, `ip_part` is the IP section that completes the IP address when prepended to `host_ip_addr` including the subnet mask
- `servername.` is a domain name which specifies an authoritative host for the specified zone.

For example:

`1.2.3.in-addr.arpa. IN NS ns2.server.com.`

`1.2.3.in-addr.arpa. IN NS ns3.server.com.`

`0/29.1.2.3.in-addr.arpa. IN NS example.com.`

For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.

- Reverse record (PTR) - Maps an IPv4 address to the canonical name for that host. Setting up a PTR record for a hostname in the `in-addr.arpa.` domain that corresponds to an IP address implements reverse DNS lookup for that address. PTR rules have the following format:

`IPaddress IN PTR hostname.`

where:

- `IPaddress` is the IPv4 address in the `IN-ADDR.ARPA.` domain

- `hostname.` is the corresponding location in the domain name space

For example:

`5.1.2.3.in-addr.arpa. IN PTR test.com.`

For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.

- Alias for record (CNAME) - A canonical name record is an alias of one name to another. According to RFC 2317, CNAME records are only supported in C class reverse zones. CNAME rules have the following format:

```
ip_part.network.host_ip_addr.in-addr.arpa.      IN      CNAME
ip_part.host_ip_addr.in-addr.arpa.
```

where:

- `ip_part` is the IP section that completes the IP address when prepended to `host_ip_addr`
- `network` is the subnet mask
- `host_ip_addr.in-addr.arpa.` is the zone name

For example:

`0.1.2.3.in-addr.arpa. IN CNAME 0.0/29.1.2.3.in-addr.arpa.`

`1.1.2.3.in-addr.arpa. IN CNAME 1.0/29.1.2.3.in-addr.arpa.`

...

`7.1.2.3.in-addr.arpa. IN CNAME 7.0/29.1.2.3.in-addr.arpa.`

For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.

- Text record (TXT) - Allows an administrator to insert arbitrary text into a DNS record. This has been used to implement new functions with DNS support without allocating new record types. For example, this record is used to implement the Sender Policy Framework and DomainKeys specifications. TXT rules have the following format:

```
ip_part.host_ip_addr.in-addr.arpa. IN TXT "Text information"
```

where:

- `ip_part` is the IP section that completes the IP address when prepended to `host_ip_addr`
- `host_ip_addr.in-addr.arpa.` is the zone name
- `"Text information"` can be any type of string

For example:

```
4.1.2.3.in-addr.arpa. IN TXT "This is a test"
```

For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.

- For E.164 zones

- Nameserver (NS) - Maps a domain name to a list of DNS servers authoritative for that domain. Delegations depend on NS records. NS rules have the following format:

```
hostname. IN NS servername.
```

where:

- hostname. is the zone name or one of its subdomains
- servername. is a domain name which specifies an authoritative host for the specified hostname.

For example:

```
1.2.e164.arpa. IN NS ns1.example.com.
```

```
1.2.e164.arpa. IN NS ns2.example.com.
```

```
5.1.2.e164.arpa. IN NS ns1.example.com.
```



Note

The NS records of \$ORIGIN are displayed in bold characters.

4PSA DNS Manager allows to choose in the interface which is the primary nameserver on a zone (required for some local TLDs). In order to setup an NS record as primary check **Make primary** when you add/edit the desired NS record.



Caution

For BIND to take a DNS zone into consideration, at least one NS record must be defined for \$ORIGIN in the respective zone.

For best practice, it is recommended to have at least two NS records defined for each public domain.

For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.

- NAPTR record (NAPTR) - Naming Authority Pointers. NAPTR rules have the following format:

order preference services flag regexp replacement

where:

- order indicates the order in which records are to be processed when a query returns multiple NAPTR records
- preference indicates the processing order for multiple records with identical order
- services indicate the resolution protocol and resolution services employed when applying a rewrite according to the regexp or replacement field
- flag is a modifier that affects the next DNS lookup
- regexp is the primary field used for rewrite rules
- replacement is a secondary field used for rewrite rules

For example:

```
1.2.e164.arpa. IN NAPTR 100 10 "u" "sip+E2U" "!^.*$!  
sip:information@foo.se!i" .
```

```
1.2.e164.arpa. IN NAPTR 102 10 "u" "smtp+E2U" "!^.*$!  
mailto:information@foo.se!i" .
```

For more information about this type of record, go to <http://tools.ietf.org/html/rfc3403>.

Value – Depending on the Record type, this field displays an IP address, an alias, a name server, a host name, or a text.

Last update - The date when the record was last modified (from the web based interface, or by updateurl).

M – By clicking the  icon, you can edit the details of the corresponding DNS Record.



Warning

Records can be modified only for zones added from the 4PSA DNS Manager control panel.



Note

For Slave DNS zones you cannot add Records and the current Records are not displayed because the actual DNS Records are transferred from the master server(s)

Adding DNS Records



Warning

Records can be added only for zones added from the 4PSA DNS Manager control panel.

In order to add a DNS Record, you must select the Record type in the New DNS Record area and click  Add DNS Record. Each Record type has its own different setup.

For more information on DNS records, please read the [Managing DNS Records](#) section.

Editing DNS Records

To edit a DNS Record, you must click the  icon corresponding to the respective record. You are able to change the type of the records and all the settings specific to each record type.

For more information on DNS records, please read the [Managing DNS Records](#) section.

Removing DNS Records

To remove a DNS Record, enable the corresponding check box and follow the [Remove Selected](#) link. 4PSA DNS Manager will ask for your confirmation before the Records will be permanently deleted. Multiple Records can be deleted at the same time.



Warning

Records can be deleted only for zones added from the 4PSA DNS Manager control panel.

Global Operations on DNS Zones

You can change records belonging to two or more DNS zones simultaneously. In order to access the Global operations page, select the

respective DNS zones and click the  [Global operations](#) link located above the table.

This displays the Global operations page and, depending on the types of DNS zones you have selected, this page will contain one or more of the following sections: Forward zones, Reverse zones and E.164 zones. Each section contains fields that allow you to specify formulas for the respective type of zone. Each formula is defined by filling in three drop-down lists and two text boxes.

- In the first drop-down list, you must choose the type of records that will be modified. The available options are:
 - NS, A, AAAA, CNAME, MX, TXT and SRV records for forward zones
 - NS, PTR and TXT records for reverse zones
 - NS and NAPTR records for E.164 zones
- In the second drop-down list, you must choose the matching algorithm: The available options are:
 - equals when the value parameter of the records must be identical to the specified value
 - contains when the value parameter of the records must contain the specified value
- In the first text box, you must specify the search criteria.



Note

The * character can be used to match any set of characters.

- In the third drop-down list, you must select the action you would like to perform on the matching records. The available options are:
 - replace with if you would like to modify the matching records
 - drop record if you would like to erase them
- The last text box must contain the new value that will be used to modify the respective records.



Note

This text box is disabled if you selected drop record in the previous drop-down list.



Note

In order to have the domain name automatically completed, you must enter [domain] in the text box.

By pressing the  button, you can add additional rules to a particular section. Use the  buttons to remove formulas.

When you are done, click OK to apply the new values to the respective records.

Glue Records

Name servers in delegations appear listed by name, rather than by IP address. This means that a resolving name server must issue another DNS request to find out the IP address of the server to which it has been referred. Since this can introduce a circular dependency if the nameserver referred to is under the domain that it is authoritative of, it is occasionally necessary for the nameserver providing the delegation to also provide the IP address of the next nameserver. This record is called a glue record.

In practice glue records are used for two purposes:

- To speed up queries - and consequently reduce DNS load - by providing the name and IP addresses (the glue) for all authoritative name servers, both within and external to the domain.
- To break the query deadlock for referrals which return name servers within the domain being queried.



Note

Glue Records can only be defined for forward master DNS zones.



Warning

Glue Records can only be defined for forward master DNS zones introduced/added from the control panel.

In order to create a Glue Record, there must exist a NS and an A record which meet the following requirements:

- The NS record must NOT have a corresponding A record.
- The A record MUST be defined on \$ORIGIN or on a subdomain of \$ORIGIN

The following table displays an example of the records that are required in order to create a Glue Record

Table 3.1. Required Records

Host	Record Type	Value
sub.example.com	NS	ns.sub.example.com
sub.example.com	A	1.2.3.4

In order to create a Glue Record, the administrator must select the desired zone name from the zones list and click the [Blue Records](#) link located above the table.

Table 3.2. XXX Resulting Glue Record

Host	Record Type	Value
ns.sub.domain.com	A	1.2.3.4

SPF Rules

You can add Server Policy Framework (SPF) rules to your DNS zones. SPF allows the owner of an Internet domain to use special format DNS TXT rules to specify which machines are authorized to transmit e-mail for that domain. For this purpose, in the DNS zones page, select the desired zones and click the  [SPF Rules](#) link. In the new page that opens, you can manage the SPF rules.



Warning

SPF Rules can be defined only for zones added from the control panel.

In order to create a SPF for one of the origin's subdomains, in the Host text box, enter the subdomain using the following format subodmain.[domain]. Leaving this field empty, will generate the TXT record for \$ORIGIN. Next, enter the actual rule. Each rule comprises three elements:

1. Use the first drop down box to select a qualifier. The following qualifiers are available:

- "+" Pass
 - "-" Fail
 - "~" SoftFail
 - "?" Neutral
2. Use the second drop down box to select a mechanism or a modifier. The following mechanisms are available:
- all
 - ip4
 - ip6
 - a
 - mx
 - ptr
 - exists
 - include
- And the following modifiers:
- redirect
 - exp
3. Use the text box to enter the target URL.

Use the  button to add rules to the list and the  button to remove rules from the list. When you are done, click OK to apply your changes and return to the DNS zones page. Click Cancel if you wish to return to the DNS zones page without applying your changes.

Removing DNS Zones

To remove one or more DNS Zones from the system, follow these steps:

1. Choose the zones you want to delete by selecting their corresponding check boxes.
2. Click the  [Remove selected](#) link.
3. Review the list. If you want to proceed with the removal, select the Confirm the removal check box and click OK. Otherwise, click Cancel to return to the previous page without deleting anything.



Warning

When a zone managed from a Remote Update location is deleted, it is no longer possible to be imported from that Remote location. The respective zone can be imported only by pressing the **Update now** button.

Managing DNS Zones Remote Update Locations

The remote update locations are files located on remote machines that contain DNS zone information. 4PSA DNS Manager is able to automatically download and retrieve these files using the HTTP, HTTPS and FTP protocol in order to load DNS zone information from remote servers. You can add new locations, view, search, edit and remove existing remote update locations.



Note

To be able to add and manage DNS zone remote update locations, you must have the appropriate permissions enabled.



Note

For more details about remote update locations, including integration with a current infrastructure see section [Remote Update Location Configuration](#) .



In the DNS zones Management page, click the Remote Updates button to manage the remote update locations.



Warning

If the **Remove zones no longer present in update source** setting is activated for the respective client account, the DNS zones that have been updated via a remote update location will be deleted if the file that was retrieved from the remote location NO LONGER CONTAINS the definition for the respective zones. If this option is activated, 4PSA DNS Manager displays the following warning message:

zones that are not found in the source update URL will be removed from the system.



Warning

If the **Lock zones to an update source** setting is activated for the respective client account, a zone will be associated with a single update remote location (the

first update location where the zone description is retrieved from). Any other update location that contains a duplicate description will be ignored. If this option is activated, 4PSA DNS Manager displays the following warning message:

**zones will always be updated from the same URL source for each zone.
The URL priorities will not change the update source for existing zone.**

In the Remote Update Locations page the following information is available:

S – This column displays the status of the remote update location. This can be  enabled or  disabled

Remote location – The URL where the file that contains update information can be found



Note

Remote update locations can be also in IDN format.

Priority – The priority of the zone definitions downloaded from this URL over other (duplicate) zone definitions.



Caution

When a remote location is updated, 4PSA DNS Manager clears the hash for all the owner's remote locations!

Update interval – The time interval between two consecutive retrievals of the remote location

Last updated – The date and time (in month, day, year format) when the last DNS zone update from the corresponding remote location was performed

M – Click this  Modify icon to edit the details of the remote update location



Note

When the client is not allowed by an administrator to edit the DNS zone remote update locations, he can only view the details of these remote locations.

The information can be sorted by the remote update location name, the update interval, and the date of the last update by clicking the corresponding table header links.

To instantly update the DNS zone information with data from the remote location you have just set up, click the  Update Now button located in the Tools section of the page.

Creating a New Remote Update Location

In order to add a new remote update location to the system, you must enter all the required details:

Remote update location – The URL of the file that contains the update information (HTTP, HTTPS and FTP protocols supported)



Note

4PSA DNS Manager does NOT support the following URL formats:

- ftp://username:password@domain.com
- ftp://username:password@192.168.10.10

Keep minimum [X] minutes between updates – The time interval between two consecutive retrievals of the remote location

Remote URL Priority – The priority of the zone definitions downloaded from this URL over other (duplicate) zone definitions.



Note

If there are two or more update locations, having different priorities, that update the same zone(s), the location that last updates a zone, is called the **Owner location**.

If the **Lock zones to an update source** setting is:

- **disabled** - the zones will be updated by the remote update URL with the highest priority.
- **enabled** - the zones will be updated by the remote update owner location, ignoring the priorities.

Username - HTTP, HTTPS or FTP authentication username.

Password - HTTP, HTTPS or FTP authentication password.

Add the following master IPs to slave zones - The IP addresses specified in this field will be recorded in the masters clauses of the named.conf file for SLAVE DNS zones

Add the following allow transfer IPs to master zones - The IP addresses specified in this field will be recorded in the allow transfer clauses of the named.conf file for MASTER DNS zones

The required fields are marked with an asterisk. Click OK to create the new remote update location.

Editing a Remote Update Location Settings

When allowed by an administrator, you can edit existing remote update locations. In order to modify the settings of an existing remote location, click the corresponding  Modify icon. The details of the chosen remote location can be modified in the new page.

The required fields are marked with an asterisk. Click Ok to save the changes you have made. Follow the [Up Level](#) link, if you want to return to the previous page without saving these changes.

When you are not allowed to change remote update locations, you can only view this information.

Removing a Remote Update Location

In order to delete a remote update location, enable the corresponding check box and follow the [Remove Selected](#) link. 4PSA DNS Manager will ask for your confirmation before the location will be permanently deleted. Multiple locations can be deleted at the same time.

Remote Logs

You are able to view the remote update logs by pressing the  Remote Logs icon in the Remote Update Locations page.

The following information is available:

Date - The date and time when the event occurred.

Level - The type of the event.

Message - An explanatory message regarding the event.

Log Data - Specific information regarding the event.

You can clear the remote update logs by pressing the Clear logs button.

When the logs list is too long, the Search feature may be used to find specific logs:

Write the search criteria in the text box. By clicking the  button or the Search label, the system will display only the logs that match the search criteria.

To display the entire list, press the  button or the Show all label.

Backing Up DNS Records

You can create a CSV file backup of all DNS zones from your account and of a chosen DNS zone.

Backing Up DNS Zones

In order to create a local backup containing complete information for all the DNS zones for your account, click the  Backup DNS zones button available in the Actions area of the DNS zones Management page.

A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file. The file contains a list of the DNS Records for all the domains that belong to your account.

Backing Up a DNS Zone

In order to create a local backup of a chosen DNS zone available on the server, click the chosen DNS zone name available in the list. Next, click the  Backup DNS zone button.

A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file. The file contains a list of the DNS Records for the chosen domain.

Transfer IP Addresses

The Transfer IPs are DNS server IPs that are allowed to transfer (copy) the zone information from the server (master or slave for the zone). These IPs will be recorded in the `named.conf` file in the `acl` (Access Control Lists) clauses.

You can access the zone Transfer page by clicking the  Transfer IP addresses button located in the DNS zones Management page.



Warning

The Transfer IP addresses can be modified only for zones that have been added from the 4PSA DNS Manager control panel.

In this page there are several details available about the DNS zone: DNS zone type and Last DNS zone update

You must specify the required IP addresses in the available text boxes. In order to add more slave IP addresses, the administrator must click the  icon.



Note

Pay particular attention to the **Last DNS zone update**. This is the time when the zone was actually updated by the 4PSA DNS Manager low level program.

Managing Round Robin Polls



Warning

The DNS Round Robin button is available only for forward zones added from the 4PSA DNS Manager control panel.

Editing Round Robin Polls

If you are editing a forward zone and if the client is allowed Round Robin management, the  DNS Round Robin button will be available in the Tools area. If the forward zone is not allowed Round Robin management, the icon will



be grayed out like this  DNS Round Robin. Press this button to open the Round Robin polls management page. This page will list all the polls that have been set up for the DNS zone. The table comprises the following columns:

- S - Indicates the poll's state. Press the icon in this column to switch between the  active and  inactive state.
- Name - Indicates the poll's name. Click on it to edit the poll.
- Monitored records - Indicates the number of monitored records.
- Active records - Indicates how many of the monitored records are active.
- Last update - Indicates the date and time of the most recent update.
- The final column contains a check box that allows you to select one or multiple polls in the list in case you wish to delete them.

Adding Round Robin Polls



If you wish to add a new poll, click the  Add new poll button in the New Round Robin poll area. In the new page that opens, fill in the following information:

- Name - Enter the poll's name
- Tested protocol - Select the protocol you wish to test. The available protocols are HTTP, IMAP, MySQL, PING, POP3, SIP and SMTP.
- Monitoring interval - Enter the number of minutes between two subsequent tests.
- Tested resource - Enter a resource pertaining to the protocol that is to be tested. You can type a particular IP address or hostname, or you can monitor the value set for the selected records. For the later, use the \$RR variable.



Note

\$RR is replaced by one of the entries in the Value column listed for the selected records. You can use expressions such as `http://$RR` or `http://$RR/test.php`.

- Try resource for X seconds - Enter for how long Round Robin will attempt to access the resource before failing.

Then, select the DNS records you wish to add to the poll from the table below. Click the  [Apply changes](#) button to associate the selected records with the new poll.

When you are done, press OK to save your settings and return to the previous page or Cancel to return to the previous page without applying your settings.

Chapter 4

The Settings Configuration

You can manage various settings: DNS templates, DNS settings, and interface preferences. In order to perform these tasks, follow the [Settings](#) link available in the navigation menu.

Available Options

The page is divided in two sections:

1. Options

-  DNS Templates - Manage DNS templates. For more information, please read the [Managing DNS Templates](#) section.
-  Interface Settings - Manage interface settings. For more information, please read the [Interface Settings](#) page.

-  Custom Buttons - Manage custom buttons. For more information, please read the [Managing Custom Buttons](#) section.
-  Application settings - Manage SOA settings. For more information, please read the [Configuring SOA Settings](#) section.

2. Database

-  XML Export - Click this button to export all client's data into XML format.
-  XML Import - Imports an XML file that is a backup of the client's database. For more information, please read the [XML Import](#) section.

Managing DNS Templates

The client can create and manage DNS templates. In the Settings management page click the  DNS templates button to manage your DNS templates. In the DNS templates page you can add new templates, edit and delete owned templates. There are some templates that the client can only view and use in zone creation but he cannot modify them because there are created by administrator.



Note

To be able to create and manage DNS templates, you must have the appropriate permissions enabled. The administrator can enable these permissions.



Note

4PSA DNS Manager also accepts **internationalized domain names (IDN)** - Internet domain names that contain non-ASCII characters.

Creating a New DNS Template

In order to add a DNS template, you must open the Templates management page by clicking the DNS Templates button in the Settings page and follow the steps:

1. Enter a name in the Template name text box.
2. Choose the type of the template by clicking the respective radio box. The available options are:
 - Forward - a template for forward DNS zones
 - Reverse - a template for reverse DNS zones
 - E.164 - a template for E.164 zones
3. Click the OK button. A new page opens allowing you to define DNS records and Template IPs.



Note

If you want the domain name to be automatically replaced by the name of the newly created domain, enter [domain] in the domain name field. In order to have an IP address automatically replaced, use the [ip] tag.

In this area you can also view a list of DNS Records which are included in the template. The following details are available:

Host – This field displays the host name or IP address of every DNS Record

Record type – This is the type of the DNS Record

Value – Depending on the Record type, this field displays an IP address, an alias, a name server, a host name, or a text.

If you have the permission, you can also remove DNS Records from a template. Enable the corresponding check box and follow the [Remove Selected](#) link. 4PSA DNS Manager will ask for your confirmation before the Records will be permanently deleted. Multiple Records can be deleted at the same time.

Managing a Template's DNS Records

To access the Template management section, click the name of the template.

In this area, the administrator can view the list of DNS Records included in the template. The following details are available:

Host – This field displays the host name or IP address of every DNS Record

Record type – This is the type of the DNS Record

Value – Depending on the Record type, this field displays an IP address, an alias, a name server, a host name, or a text.

M – By clicking the  icon, the administrator can edit the details of the corresponding DNS Record.

You can also remove DNS Records from a template. Enable the corresponding check box and follow the [Remove Selected](#) link. 4PSA DNS Manager will ask for your confirmation before the Records will be permanently deleted. Multiple Records can be deleted at the same time.

Adding a DNS record to the template

To add a DNS record to the template, click the  Add DNS records button in the respective Template's management page. The Add new record page opens. You must choose the record type and configure each record accordingly. The following types of DNS records are available:

- For Forward DNS zones
 - IP Address (A) - Maps a hostname to a 32-bit IPv4 address. Type A rules have the following format:

hostname. IN A XXX.XXX.XXX.XXX

where:

- XXX.XXX.XXX.XXX is the IP address for the hostname.
- hostname. is the zone name or one of its subdomains.

For example:

domain.com. IN A 1.2.3.4

subdomain.domain.com. IN A 1.2.3.4

For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.

- AAAA Record (AAAA) - Maps a hostname to a 128-bit IPv6 address. AAAA rules have the following format:

hostname. IN AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA

where:

- AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA is the IPv6 address for the hostname.

- `hostname.` is the zone name or one of its subdomains.

For example:

```
domain.com. IN AAAA abcd:1234:ffff:0:12:3:ab1:aa
```

```
subdomain.domain.com. IN AAAA abcd:1234:ffff:0:12:3:ab1:aa
```

For more information about this type of record, go to <http://tools.ietf.org/html/rfc3596>.

- Alias for record (CNAME) - Canonical name record is an alias (or nickname) of one name to another. The A record to which the alias points can be either local or remote - on a foreign name server. This is useful when running multiple services (like an FTP and a webserver) from a single IP address. Each service can then have its own entry in DNS (like `ftp.example.com.` and `www.example.com.`). It is also used when running multiple HTTP servers, with different names, on the same physical host. CNAME rules have the following format:

```
hostname. IN CNAME servername.
```

where:

- `hostname.` is the zone name or one of its subdomains
- `servername.` is a fully qualified domain name (FQDN) either inside or outside the zone.

For example:

```
ftp.domain.com. IN CNAME inside.domain.com.
```

```
ftp1.domain.com IN CNAME outside.zone.com.
```



Note

Rfc 1034 states: "If a CNAME record is present at a node, no other data should be present; this ensures that the data for a canonical name and its aliases cannot be different."

In order for these requirements to be met in 4PSA DNS Manager, the value specified in the **zone alias name** field of the CNAME record cannot be set for the **DNS zone name** filed in NS, A, AAAA, SRV, CNAME and TXT records or for the **zone email** field in an MX record.

For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.

- **Nameserver (NS)** - Maps a domain name to a list of DNS servers authoritative for that domain. Delegations depend on NS records. NS rules have the following format:

hostname. IN NS servername.

where:

- hostname. is the zone name or one of its subdomains
- servername. is a domain name which specifies an authoritative host for the specified hostname.

For example:

domain.com. IN NS ns1.example.com.

domain.com. IN NS ns2.example.com.



Note

The NS records of \$ORIGIN are displayed in bold characters.

4PSA DNS Manager allows to choose in the interface which is the primary nameserver on a zone (required for some local TLDs). In order to setup an NS record as primary check **Make primary** when you add/edit the desired NS record.



Caution

For BIND to take a DNS zone into consideration, at least one NS record must be defined for \$ORIGIN in the respective zone.

For best practice, it is recommended to have at least two NS records defined for each public domain.

For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.

- **Mail exchanger (MX)** - Maps a domain name to a list of mail exchange servers for that domain. MX rules have the following format:

hostname. IN MX preference servername.

where:

- hostname. is the zone name or one of its subdomains
- preference indicates the hostname's priority. The lower the preference, the higher the priority. This parameter accepts values between 0 and 50.

- `servername.` is a fully qualified domain name (FQDN) inside the zone

For example:

```
mail.domain.com. IN MX 10 domain.com.
```

```
webmail.domain.com. IN MX 5 domain.com.
```

For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.

- Text record (TXT) - Allows an administrator to insert arbitrary text into a DNS record. This has been used to implement new functions with DNS support without allocating new record types. For example, this record is used to implement the Sender Policy Framework and DomainKeys specifications. TXT rules have the following format:

```
hostname. IN TXT "Text information"
```

where:

- `hostname.` is the zone name or one of its subdomains
- "Text information" can be any type of string including strings generated by SPF Rules

For example:

```
domain.com. IN TXT "k=rsa; p=MEwwDQYerwqEWwE"
```

```
subdomain.domain.com. IN TXT "this is a test"
```

For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.

- Service Record (SRV) - Specifies the location of the server(s) for a specific protocol and domain. SRV rules have the following format:

```
_Service._Protocol.Hostname. IN SRV TTL Priority Weight Port Target
```

where:

- Service is the symbolic name of the desired service. You can find a list of the available services at <http://www.dns-sd.org/ServiceTypes.html>.
- Protocol is the protocol of the desired service. This is usually TCP or UDP, but 4PSA DNS Manager supports all the protocols listed here <http://www.iana.org/assignments/protocol-numbers>.
- Hostname. is the domain name for which the record is valid.
- TTL is the standard DNS time to live field. If there is no TTL specified for the record, the TTL value for the zone will be employed.

- Priority is the priority of the target host. The lower the value, the higher the priority level.
- Weight indicates a relative weight between records with the same priority.
- Port is the port on which the service is to be found.
- Target is the domain name of the target host.



Note

The Target parameter can not be an alias (CNAME).
When Target is set to . the service is unavailable.

For example:

```
_service._tcp.domain.com. IN SRV 0 1 9 subdomain.domain.com.  
*._tcp.domain.com. IN SRV 0 0 0 . ; no other service is available  
on tcp protocol
```

For more information about this type of record, go to <http://tools.ietf.org/html/rfc2782>.

- For Reverse DNS zones

- Nameserver (NS) - Specifies a host which should be authoritative for the specified class.

For class C reverse zones, 4PSA DNS Manager accepts NS records for \$ORIGIN and supports classless delegation records, as described in RFC 2317, chapter 4.



Note

The NS records of \$ORIGIN are displayed in bold characters.

4PSA DNS Manager allows to choose in the interface which is the primary nameserver on a zone (required for some local TLDs). In order to setup an NS record as primary check **Make primary** when you add/edit the desired NS record.



Caution

For BIND to take a DNS zone into consideration, at least one NS record must be defined for \$ORIGIN in the respective zone.

For best practice, it is recommended to have at least two NS records defined for each public domain.

Class A and B zones support NS records for \$ORIGIN and inferior class zones and do not support classless delegation records.

For class C reverse zones, 4PSA DNS Manager automatically generates CNAME records that correspond to the NS records created for classless delegation records. If the Automatically generate CNAME records for delegated subnets check box is selected, the CNAME records will be automatically generated. This check box is available only for NS records with a subnet mask lower than 24 (having a numeric value higher than 24). NS rules have the following format:

`ip_part.host_ip_addr.in-addr.arpa. IN NS servername.`

where:

- `host_ip_addr.in-addr.arpa.` is the zone name
- `ip_part` is the IP section that completes the IP address when prepended to `host_ip_addr` (for class A, B and D zones, and for class C \$ORIGIN NS)
- for classless delegation records, `ip_part` is the IP section that completes the IP address when prepended to `host_ip_addr` including the subnet mask
- `servername.` is a domain name which specifies an authoritative host for the specified zone.

For example:

`1.2.3.in-addr.arpa. IN NS ns2.server.com.`

`1.2.3.in-addr.arpa. IN NS ns3.server.com.`

`0/29.1.2.3.in-addr.arpa. IN NS example.com.`

For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.

- Reverse record (PTR) - Maps an IPv4 address to the canonical name for that host. Setting up a PTR record for a hostname in the `in-addr.arpa.` domain that corresponds to an IP address implements reverse DNS lookup for that address. PTR rules have the following format:

`IPaddress IN PTR hostname.`

where:

- `IPaddress` is the IPv4 address in the `IN-ADDR.ARPA.` domain

- `hostname.` is the corresponding location in the domain name space

For example:

`5.1.2.3.in-addr.arpa. IN PTR test.com.`

For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.

- Alias for record (CNAME) - A canonical name record is an alias of one name to another. According to RFC 2317, CNAME records are only supported in C class reverse zones. CNAME rules have the following format:

```
ip_part.network.host_ip_addr.in-addr.arpa.      IN      CNAME
ip_part.host_ip_addr.in-addr.arpa.
```

where:

- `ip_part` is the IP section that completes the IP address when prepended to `host_ip_addr`
- `network` is the subnet mask
- `host_ip_addr.in-addr.arpa.` is the zone name

For example:

`0.1.2.3.in-addr.arpa. IN CNAME 0.0/29.1.2.3.in-addr.arpa.`

`1.1.2.3.in-addr.arpa. IN CNAME 1.0/29.1.2.3.in-addr.arpa.`

...

`7.1.2.3.in-addr.arpa. IN CNAME 7.0/29.1.2.3.in-addr.arpa.`

For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.

- Text record (TXT) - Allows an administrator to insert arbitrary text into a DNS record. This has been used to implement new functions with DNS support without allocating new record types. For example, this record is used to implement the Sender Policy Framework and DomainKeys specifications. TXT rules have the following format:

```
ip_part.host_ip_addr.in-addr.arpa. IN TXT "Text information"
```

where:

- `ip_part` is the IP section that completes the IP address when prepended to `host_ip_addr`
- `host_ip_addr.in-addr.arpa.` is the zone name
- `"Text information"` can be any type of string

For example:

```
4.1.2.3.in-addr.arpa. IN TXT "This is a test"
```

For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.

- For E.164 zones

- Nameserver (NS) - Maps a domain name to a list of DNS servers authoritative for that domain. Delegations depend on NS records. NS rules have the following format:

```
hostname. IN NS servername.
```

where:

- hostname. is the zone name or one of its subdomains
- servername. is a domain name which specifies an authoritative host for the specified hostname.

For example:

```
1.2.e164.arpa. IN NS ns1.example.com.
```

```
1.2.e164.arpa. IN NS ns2.example.com.
```

```
5.1.2.e164.arpa. IN NS ns1.example.com.
```



Note

The NS records of \$ORIGIN are displayed in bold characters.

4PSA DNS Manager allows to choose in the interface which is the primary nameserver on a zone (required for some local TLDs). In order to setup an NS record as primary check **Make primary** when you add/edit the desired NS record.



Caution

For BIND to take a DNS zone into consideration, at least one NS record must be defined for \$ORIGIN in the respective zone.

For best practice, it is recommended to have at least two NS records defined for each public domain.

For more information about this type of record, go to <http://tools.ietf.org/html/rfc1035>.

- NAPTR record (NAPTR) - Naming Authority Pointers. NAPTR rules have the following format:

order preference services flag regexp replacement

where:

- order indicates the order in which records are to be processed when a query returns multiple NAPTR records
- preference indicates the processing order for multiple records with identical order
- services indicate the resolution protocol and resolution services employed when applying a rewrite according to the regexp or replacement field
- flag is a modifier that affects the next DNS lookup
- regexp is the primary field used for rewrite rules
- replacement is a secondary field used for rewrite rules

For example:

```
1.2.e164.arpa. IN NAPTR 100 10 "u" "sip+E2U" "!^.*$!  
sip:information@foo.se!i" .
```

```
1.2.e164.arpa. IN NAPTR 102 10 "u" "smtp+E2U" "!^.*$!  
mailto:information@foo.se!i" .
```

For more information about this type of record, go to <http://tools.ietf.org/html/rfc3403>.

Table 4.1. DNS Template Example

Host	Record Type	Value
[domain].	NS	ns.[domain].
[domain].	A	[IP]
[domain].	MX (10)	mail.[domain].
ftp.[domain].	CNAME	[domain].
mail.[domain].	A	[IP]
ns.[domain].	A	[IP]
webmail.[domain].	A	[IP]

Editing a Template's DNS Record

To edit a DNS Record from a Template, click the icon in the M column from the record's list. In the new page that opens, the DNS record's configuration can be modified. For more information on DNS records, please read the [Adding a DNS Record to the Template](#) section.

Managing a Template's IPs

To access the Template's IP Management page, click the template's name in the templates list and then the  Template IPs button. This page displays the list of the template's IPs and allows you to add new IPs. The following details are available for the existing IPs:

T - The icon in this column shows the type of the IP address. It can be  - master or  - allow transfer. The type of the IP can be changed by pressing the icon in this column.

IP address - The IP address

When the IPs list is too long, the Search feature may be used to find specific IP:

The administrator can write the search criteria in the text box. By clicking the  button or the Search label, the system will display only the IPs that match the search criteria.

To display the entire list, the administrator must press the  button or the Show all label.

To add an IP to the template, you must specify the respective IP in the appropriate field from the Add Template IPs section:

- Add the following master IPs to slave zones - for master IPs assigned to slave zones. Multiple IPs can be added by pressing the  button.
- Add the following allow transfer IPs to master zones - for allow transfer IPs assigned to master zones. Multiple IPs can be added by pressing the  button.

After specifying the IPs, click OK to add the respective IPs to the template.

Editing DNS Templates

To be able to manage DNS templates, you must have the appropriate permissions enabled. You can manage a DNS template by clicking its name. In the DNS templates page, records can be added, edited and deleted.

Removing DNS Templates

When you have the appropriate permissions enabled, you can remove DNS templates. Enable the corresponding check box and follow the [Remove Selected](#) link. 4PSA DNS Manager will ask for your confirmation before the template will be permanently deleted. Multiple templates can be deleted at the same time.

Setting Interface Preferences

4PSA DNS Manager allows you to customize the application's default look and settings from the Interface Preferences page. There you can define the system language, the application's skin and the number of rows in the records list.

There are two possibilities to access this page:

1. Directly from the top frame by clicking the [My interface](#) link.
2. From the Settings management page by clicking the Interface settings icon.

You can customize the following options:

- Rows in table – Use this text box to set the number of rows that will be displayed in the client interface.
- Interface skin – Use this drop down list to choose the skin used in the client account interface.
- System language – Use this drop down list to choose the language used in the client account interface.

The same options can be accessed

Configuring SOA settings

The SOA (Start of Authority) Record defines global parameters for the DNS zone. There is only one SOA Record allowed in a DNS zone file.

The default SOA parameters values for your DNS zones that have no custom

configurations, can be modified by clicking the  Application settings button in the Options section of the page. You can manage the following options:

Remove zones no longer present in update source – When this option is enabled, DNS zones that have been updated via a remote update location will

be deleted when the file that was retrieved from the remote location no longer contains the definition for the zone. This setting helps you keep the 4PSA DNS Manager server perfectly synchronized with the remote update locations.

Lock zones to an update source – When this option is enabled, a zone will be associated with a single update remote location (the first update location where the zone description is retrieved from). Any other update location that contains a duplicate description will be ignored.



Note

The **Remove zones no longer present in update source** and **Lock zones to an update source** options are available only if the administrator has given you the permission to manage them.

Warn if an update from a location fails more than X times - Enter the number of subsequent failed updates 4PSA DNS Manager will attempt before displaying a warning. This parameter is optional. You can enter a numeric value between 1 and 100.

Refresh time – 32 bit time value in seconds. This is the period of time that the secondary name server should wait before checking with the primary server to see whether the data has been modified. Default value: 10800 seconds.



Note

RFC 1912 recommends 1200 to 43200 seconds, if your data is volatile or 43200 (12 hours) if it is not.

Retry time – Signed 32 bit value in seconds. When a secondary name server requests for a zone refresh from the primary server and this fails to respond, the secondary name server waits for the refresh time before attempting another zone refresh after the failed attempt. Default value: 3600 seconds.

Expire time – Signed 32 bit value in seconds. This setting indicates when the zone is no longer authoritative and new interrogation of the root servers is required. It applies to Slaves only. Default value: 604800 seconds.



Note

RFC 1912 recommends 1209600 to 2419200 seconds (2–4 weeks).

Minimum TTL – This value is used as the default TTL for new Records created within the zone. It is also used by other DNS servers to cache negative

responses (for example when a Record does not exist). Default value: 86400 seconds.

Default TTL – Signed 32 bit value in seconds. This is the amount of time that zone Records are kept in a remote host cache. It is recommended that this value be set large. A small value will force remote servers to query the DNS server again for unchanged data. Default value: 604800 seconds.

When you have finished setting up your preferences, click OK to save your settings and return to the previous page.

Click Cancel to return to the previous page without applying your changes.

If you would like to revert your settings to their default values, click the Default SOA button.

Managing Custom Buttons

In order to manage the custom buttons available for your account, click  Custom buttons. On this page you can add new buttons, edit and delete the existing buttons.

In the custom buttons list the following details are available:

- S – The status of the button displayed using an icon:  Enabled or  Disabled.
- A – The availability of the button
- L – The location of the button:  means that the button is displayed in the left panel and  means that the button is placed in the right panel.
- I – The icon associated with the button



Note

If the button is associated with the default icon, 4PSA DNS Manager displays



- Label – This is the label that will be displayed below the button
- URL – This is the URL which will open in a pop-up window when you click the button
- Priority

The information can be sorted by button label, URL, and context help by clicking the table header links.

Adding Custom Buttons



In order to add a new button, click  Add custom button available in the Tools area. In the new page that opens, the following fields are available:

Label – This is the label that will be displayed below the button.

Title – This is the tip that will be displayed when the mouse is positioned on the button's icon.

Location – Use this drop down list to choose where the button will be displayed:

Default image for all skins – When this option is enabled, 4PSA DNS Manager displays a default icon for the button. If you disable this check box, 4PSA DNS Manager displays additional controls that allow you to load custom icons for the button:

- Use the Browse button to locate a graphic file on your computer.
- Enable the check box corresponding to the skin where the icon will be used.
- Enable the All skins check box if you want to use the same icon for all the 4PSA DNS Manager skins installed on the server.
- You can use the   buttons to add icons for different skins at the same time.

Client ID – When this option is selected, the ID of the currently selected client is appended to the URL linked with the button.

E.g.: `http://www.4psa.com/interface.php?client=<cl_id>`

URL – This is the URL which will open in a pop-up window, when you click the button.

Context help – This is the description of the button that will appear in the context help area on mouse-over.

Priority – The value in this text box defines the order in which the custom buttons are displayed in the interface.

Inheritance level – Use this drop down list to specify the visibility of the button:

- 0 – The button is visible only to the client user.

- 1 – The button is visible to multiple users.

Action – Use this drop down list to choose if the URL will be opened in the:

- Current window or
- New window

Click OK to update the button's details. Click Cancel, if you want to return to the previous page without saving the button.

Editing Custom Buttons

In order to edit the existing buttons, click the button label link. You can modify the available fields, as presented in the previous section. Click OK to update the button's details. Click Cancel, if you want to return to the previous page without saving the changes.

Removing Custom Buttons

To remove a custom button, enable the corresponding check box and follow the [Remove Selected](#) link. 4PSA DNS Manager will ask for your confirmation before the buttons will be permanently deleted. Multiple buttons can be deleted at the same time.

XML export

4PSA DNS Manager allows the client to export this account in XML format. This feature can be used for backup or for migration purposes.

A client account will export all of the following:

- Clients' accounts details
- Clients' settings
- Clients' remote locations
- Clients' DNS templates
- Clients' custom buttons
- Clients' interface settings
- Clients' DNS zones



To export the database in XML format, the client must click the XML export button in the Database section of the Server Settings page.

XML import

4PSA DNS Manager allows client to import an XML file that is a backup of the client account.

The details of the logged in client's account will be updated, the zones are updated (or new zones added) and all preferences will be updated.



Note

The existing client's account details will be updated.

From the XML file, new zones are created. The records from existing zones are replaced with the records from the XML file.

zones that do not have any records will not be created.

The zones that are defined on the server will not be deleted if they do not exist in the XML file.



To import a database in XML format, the client must click the XML import button in the Database section of the Server Settings page. Then use the Browse button to locate the backup file.



Chapter 5

Remote Update Location Configuration

4PSA DNS Manager is able to get files containing DNS zones and full DNS Records information from remote servers. In order to be able to retrieve this information, you have to set up a Cron job on the remote server; this Cron job must prepare the list of the DNS zones. Every time 4PSA DNS Manager updates its database with the information from this URL, the Records will be up to date.

Generating a list of DNS zones on a server is a pretty straightforward job.

Let's assume that you have a Plesk server and you want to provide centralized DNS and redundancy for this server. The algorithm can be applied to as many servers as you want, no matter what control panel they have installed.

1. 4PSA DNS Manager as a Secondary Server

The easiest option is to let 4PSA DNS Manager act as a slave DNS server for your multiple Plesk servers which have DNS zones setup as primary.

In order to achieve this, the following requirements have to be met:

1. 4PSA DNS Manager is allowed to obtain DNS zone information from the primary server

2. 4PSA DNS Manager knows the names of the DNS zones which must be obtained from the primary server

In order to satisfy these two basic requirements, you have to configure the DNS server on the Plesk server to allow transfer from the 4PSA DNS Manager IP. Since every DNS zone created on a Plesk server includes an ACL called `common-allow-transfer`, all you have to do is to add the Allow transfer IPs in the [Remote Update Locations](#) page.



Note

Since Plesk uses its database to write the `named.conf` file, the best solution is to insert the IP address of the 4PSA DNS Manager server in the PSA database. This way you can be sure that the `named.conf` file will remain correct. To do this, execute the following commands in the PSA database:

```
MySQL>INSERT INTO misc VALUES  
( 'DNS_Allow_TransferXX', '<Secondary Server IP>' );
```

Where: XX is a unique number (increment it to add more IP addresses), <Secondary Server IP> is the IP of the 4PSA DNS Manager server.

The second step is to let 4PSA DNS Manager obtain the list of the DNS zones from the master server (Plesk server). In order to do this we will install on the Plesk server a program supplied in the 4PSA DNS Manager in the `DNSMANAGER_ROOT_D/remote` directory.

The `plesk_export.sh` is a shell script written by 4PSA for Plesk servers. It writes a file containing the name of all domains that exist on this server. The program accepts the final destination file as argument. All you have to do is to insert this file in cron and make sure that it will write the list of the domains to a directory which can be accessed over the web.

First you will have to configure the script to export slaves zones and master records (edit the script to set the required variables as defined in the script).

For example:

```
sh plesk_export.sh /home/httpd/vhosts/mydomain.com/httpdocs/  
dnslist.txt
```

will dump the list of domains to a file that can be accessed over the web at:

`http://www.mydomain.com/dnslist.txt`



Note

Keep in mind that you must add the `plesk_export.sh` invocation in cron on the Plesk server. This way the `dnslist.txt` file will be updated at regular time intervals and 4PSA DNS Manager will retrieve the latest list of the domains available on the server.

Now you have to setup 4PSA DNS Manager to update the list of the DNS zones from this location. This will be a remote update location in 4PSA DNS Manager. For more information on how to set up remote update locations, view the [Managing DNS zones Remote Update Locations](#) section.

2. 4PSA DNS Manager as a Primary Server

4PSA DNS Manager can act as a primary DNS server while updating the DNS zone information from a remote server. In this case, 4PSA DNS Manager will have to get full DNS zone information from the remote server, not only the DNS zone names like in the previous case. Once again we will have as an example a Plesk server.

In order to generate the full DNS zones information on a Plesk server, we will use a script from the 4PSA DNS Manager in the `DNSMANAGER_ROOT_D/remote` directory.

The `plesk_export.sh` is a shell script written by 4PSA for Plesk servers. It writes a file containing the name of all domains which exist on this server and their full DNS Records. The program accepts the name of the final destination file as argument. All you have to do is to insert this file in cron and make sure that it will write the list of the domains to a directory which can be accessed over the web.

First, you will have to configure the script to export master zones and optionally allow_transfer records (edit the script to set the required variables as defined in the script).

For example:

```
sh plesk_export.sh /home/httpd/vhosts/mydomain.com/httpdocs/zone.txt
```

will dump the list of the domains to a file that can be accessed over the web at:

```
http://www.mydomain.com/zone.txt
```



Note

Keep in mind that you must add the `plesk_export.sh` invocation in cron on the Plesk server. In this way, the `dnslist.txt` file will be updated on regular intervals and 4PSA DNS Manager will retrieve the latest list of the domains available on the server.

Now you have to setup 4PSA DNS Manager to update the list of the DNS zones from this location. This will be a remote update location in 4PSA DNS Manager.

Scripts to perform the same tasks can be written for any control panel. 4PSA will update the list of scripts that must be used on remote servers and will place them in the `DNSMANAGER_ROOT_D/remote` directory.

With current version of 4PSA DNS Manager are shipped update scripts for Plesk, Ensim, InterWorx Control Panel, Helm, Cobalt and older DNS Manager versions.

For other control panels, which use `bind/named` (like Cpanel or Direct Admin), you can use the `bind_export.sh` script. The `bind_export.sh` script is located in the `DNSMANAGER_ROOT_D/remote/bind`. This script generates a dump file for all the zones defined in the `named.conf` file by acquiring the data from the zone files defined on `named.conf`.

Appendix A. Supported Dump File examples

In 4PSA DNS Manager 3.7.0, the file dump format has changed. The major improvements are:

- The zone type is preserved in the dump. Basically it's possible to have both slave and master zones in the same file, so it is no longer needed to have two types of update locations in DNS Manager.
- The SOA parameters can be included in the dump. When these are not included, the client or server global parameters are used.
- It is possible to include allow_transfer and masters parameters, according to the zone type.

Examples of zone dump:

```
domain.ltd.|master {  
    |REFRESH| |108002| || ||  
    |RETRY| |36002| || ||  
    |EXPIRE| |604802| || ||  
    |MIN_TTL| |86402| || ||  
    |DEFAULT_TTL| |86402| || ||  
    |SERIAL| |1271668821| || ||  
    |ALLOW_TRANSFER| |4.3.2.1| || ||  
    |NS| |domain.ltd.| |ns1.domain.ltd.| ||  
    |NS| |aa.domain.ltd.| |ns.domain.ltd.| ||  
    |CNAME| |cname.domain.ltd.| |canonical.name.| ||  
    |CNAME| |somedir.domain.ltd.| |domain.ltd.| ||  
    |CNAME| |ftp| |domain.ltd.| ||  
    |A| |mail.domain.ltd.| |192.168.10.32| ||  
    |AAAA| |sub.domain.ltd.| |2001:db8:85a3:88:8a2e:370:7334:89| ||
```

```

|MX| |zone.domain.ltd.| |email.exchanger| |10| | | | | | |
|TXT| |txt.domain.ltd.| |v=spf1 exists:%{ir}.%{v}.arpa -all | ||
|TXT| |some-text.domain.ltd.| |any text| ||
|TXT| |domain.ltd.| |sometext| ||
|TXT| |private._domainkey.domain.ltd.| |k=rsa; p=MEwwDQYerwqEWwE| ||
|SRV| |_sip._tcp.domain.ltd.| |.| |5| |25| |12345| ||
|SRV| |_sip._tcp.domain.ltd.| |anotherdomain.com.| |10| |20| |5560| ||
|SRV| |_h323._udp.domain.ltd.| |sub.domain.ltd.| |15| |25| |8550| ||
}
testdomain.com.|master {
    |$ORIGIN| |com.| || ||
    |TXT| |testdomain| |v=spf1 a mx ptr mx:mail.testdomain.com ~all| ||
    |NS| || |ns1.test-web| ||
    |NS| || |ns2.test-web| ||
    |A| || |64.85.2.56| ||
}

```

If the zone type is missing, it is assumed to be a master zone definition.

```

domain.ltd.{
    |REFRESH| |108002| || ||
    |RETRY| |36002| || ||
    |EXPIRE| |604802| || ||
    |MIN_TTL| |86402| || ||
    |DEFAULT_TTL| |86402| || ||
    |SERIAL| |1271668821| || ||
    |ALLOW_TRANSFER| |4.3.2.1| || ||
}

```

```

|NS| |domain.ltd.| |ns1.domain.ltd.| || | | | | | |
|NS| |aa.domain.ltd.| |ns.domain.ltd.| ||
|CNAME| |cname.domain.ltd.| |canonical.name.| ||
|CNAME| |somedir.domain.ltd.| |domain.ltd.| ||
|CNAME| |ftp| |domain.ltd.| ||
|A| |mail.domain.ltd.| |192.168.10.32| ||
|AAAA| |sub.domain.ltd.| |2001:db8:85a3:88:8a2e:370:7334:89| ||
|MX| |zone.domain.ltd.| |email.exchanger| |10|
|TXT| |txt.domain.ltd.| |v=spf1 exists:%{ir}:%{v}.arpa -all | ||
|TXT| |some-text.domain.ltd.| |any text| ||
|TXT| |domain.ltd.| |sometext| ||
|TXT| |private._domainkey.domain.ltd.| |k=rsa; p=MEwwDQYerwqEwwE| ||
|SRV| |_sip._tcp.domain.ltd.| |.| |5| |25| |12345| ||
|SRV| |_sip._tcp.domain.ltd.| |anotherdomain.com.| |10| |20| |5560| ||
|SRV| |_h323._udp.domain.ltd.| |sub.domain.ltd.| |15| |25| |8550| ||
}

```

Slave zones are defined as follows:

```

3.2.1.in-addr.arpa.|slave {
    |MASTER| |6.7.8.9| || ||
}

aa.com.|slave {
    |MASTER| |6.7.8.9| || ||
}

```

The rules mentioned above also apply to the reverse DNS zones. Below are explained full DNS zones with /24 /28 and /32 subnet mask.

```

4.3.2.in-addr.arpa.|master {
    |REFRESH| |10800| || ||
    |RETRY| |36000| || ||
    |EXPIRE| |604800| || ||
    |MIN_TTL| |86400| || ||
    |DEFAULT_TTL| |86400| || ||
    |SERIAL| |1271668821| || ||
    |NS| |4.3.2.in-addr.arpa.| |ns1.name.com.| ||
    |NS| |0/25.4.3.2.in-addr.arpa.| |ns.domain.com.| ||
    |PTR| |5.4.3.2.in-addr.arpa.| |zone.name.| ||
    |PTR| |5.4.3.2.in-addr.arpa.| |dom1.com.| ||
    |PTR| |5.4.3.2.in-addr.arpa.| |dom2.com.| ||
    |PTR| |5.4.3.2.in-addr.arpa.| |dom3.com.| ||
    |CNAME| |10.4.3.2.in-addr.arpa.| |10.0/25.4.3.2.in-addr.arpa.| ||
    |TXT| |host.4.3.2.in-addr.arpa.| |value| ||
    |TXT| |4.3.2.in-addr.arpa.| |sometext| ||
}

```

```

4/28.3.2.1.in-addr.arpa.|master {
    |REFRESH| |10800| || ||
    |RETRY| |3600| || ||
    |EXPIRE| |60480| || ||
    |MIN_TTL| |86400| || ||
    |SERIAL| |1271668821| || ||
    |DEFAULT_TTL| |86400| || ||
    |ALLOW_TRANSFER| |7.8.9.10| || ||

```

```

|NS| |4/28.3.2.1.in-addr.arpa.| |aa.com.| ||
|PTR| |6.4/28.3.2.1.in-addr.arpa.| |zone.c.om.| ||
|PTR| |6.4/28.3.2.1.in-addr.arpa.| |dom1.com.| ||
|PTR| |6.4/28.3.2.1.in-addr.arpa.| |dom2.com.| ||
|TXT| |a.4/28.3.2.1.in-addr.arpa.| |text value| ||
|TXT| |4/28.3.2.1.in-addr.arpa.| |sometext| ||
}

```

```

4.3.2.1.in-addr.arpa.|master {
    |REFRESH| |10800| || ||
    |RETRY| |3600| || ||
    |EXPIRE| |60480| || ||
    |MIN_TTL| |86400| || ||
    |SERIAL| |1271668821| || ||
    |DEFAULT_TTL| |86400| || ||
    |ALLOW_TRANSFER| |7.8.9.10| || ||
    |NS| |4.3.2.1.in-addr.arpa.| |aa.com.| ||
    |PTR| |4.3.2.1.in-addr.arpa.| |zone.c.om.| ||
    |TXT| |abc.4.3.2.1.in-addr.arpa.| |sometext| ||
}

```

The "@" character is accepted when defining zones.

```

testdomain.com.|master {
    |NS| |@| |ns.isdomain.com.| ||
    |NS| || |new| ||
    |MX| |@| |mail.testdomain.com.| |10|
    |MX| |test| |mail1.testdomain.com.| |15|
}

```

```

|TXT| |@| |this is not a test| ||
|CNAME| |*.new| |newtest.com.| ||
}

```

The "-" character is also accepted when defining reverse zones.

```

4-28.3.2.1.in-addr.arpa.|master {
    |REFRESH| |10800| || ||
    |RETRY| |3600| || ||
    |EXPIRE| |60480| || ||
    |MIN_TTL| |86400| || ||
    |SERIAL| |1271668821| || ||
    |DEFAULT_TTL| |86400| || ||
    |ALLOW_TRANSFER| |7.8.9.10| || ||
    |NS| |4-28.3.2.1.in-addr.arpa.| |aa.com.| ||
    |PTR| |6.4-28.3.2.1.in-addr.arpa.| |zone.com.| ||
    |PTR| |6.4-28.3.2.1.in-addr.arpa.| |dom1.com.| ||
    |PTR| |6.4-28.3.2.1.in-addr.arpa.| |dom2.com.| ||
    |TXT| |a.4-28.3.2.1.in-addr.arpa.| |text value| ||
    |TXT| |4-28.3.2.1.in-addr.arpa.| |sometext| ||
}

```

If the SOA records are not found in the zone definition, they are inherited from the client, if the client has SOA records defined. If the client has no SOA records defined, the system wide SOA settings defined by the administrator are used.

```

domain.ltd.|master {
    |ALLOW_TRANSFER| |4.3.2.1| || ||
    |NS| |domain.ltd.| |ns1.domain.ltd.| ||
}

```

```

|NS| |aa.domain.ltd.| |ns.domain.ltd.| ||
|CNAME| |cname.domain.ltd.| |canonical.name.| ||
|CNAME| |somedir.domain.ltd.| |domain.ltd.| ||
|CNAME| |ftp| |domain.ltd.| ||
|A| |mail.domain.ltd.| |192.168.10.32| ||
|MX| |zone.domain.ltd.| |email.exchanger| |10|
|TXT| |txt.domain.ltd.| |v=spf1 exists:%{ir}.%{v}.arpa -all | ||
|TXT| |some-text.domain.ltd.| |any text| ||
|TXT| |private._domainkey.domain.ltd.| |k=rsa; p=MEwwDQYerwqEwWE| ||
|TXT| |domain.ltd.| |text value| ||
}

4/28.3.2.1.in-addr.arpa.|master {
    |NS| |4/28.3.2.1.in-addr.arpa.| |aa.com.| ||
    |PTR| |6.4/28.3.2.1.in-addr.arpa.| |zone.com.| ||
    |PTR| |6.4/28.3.2.1.in-addr.arpa.| |dom1.com.| ||
    |PTR| |6.4/28.3.2.1.in-addr.arpa.| |dom2.com.| ||
    |TXT| |a.4/28.3.2.1.in-addr.arpa.| |text value| ||
    |TXT| |4/28.3.2.1.in-addr.arpa.| |sometext| ||
}

```

To mark a primary nameserver, 1 is wrote on last position of the NS record from dump file, as ns2.server.ltd in the example below:

```

domain.ltd.|master{
    |NS| |domain.ltd.| |ns1.server.ltd.| ||
    |NS| |domain.ltd.| |ns2.server.ltd.| |1|
    |CNAME| |cname.domain.ltd.| |canonical.name.| ||

```

```

|CNAME| |somedir.domain.ltd.| |domain.ltd.| ||
|CNAME| |ftp| |domain.ltd.| ||
|A| |mail.domain.ltd.| |192.168.10.32| ||
|MX| |zone.domain.ltd.| |email.exchanger| |10|
|TXT| |txt.domain.ltd.| |v=spf1 exists:%{ir}.%{v}.arpa -all | ||
|TXT| |some-text.domain.ltd.| |any text| ||
|TXT| |domain.ltd.| |text value| ||
}

```

Also the closing bracket may be placed on the same line with an record, as below:

```

domain.ltd.|master{
    |NS| |@| |ns1.server.ltd.| ||
    |NS| |@| |ns2.server.ltd.| |1|
    |A| |mail.domain.ltd.| |192.168.10.32| ||
    |TXT| |domain.ltd.| |text value| ||}

```