CLOUD CALLING™

DNS Manager

# 4PSA DNS Manager 4.0.0

# Client's User Guide

For more information about 4PSA DNS Manager, check:
http://www.4psa.com

# Client's User Guide

Manual Version 79252.10 at 2011/04/11 11:37:58

For suggestions regarding this manual contact:

docs@4psa.com

# Table of Contents

# Preface

## Who Should Read This Guide

This User Guide must be read by the 4PSA DNS Manager clients.

Chapter 1

# About 4PSA DNS Manager 4.0.0

4PSA DNS Manager 4.0.0 is a server-level multitenant software automation solution that allows users with a minimum IT experience to manage DNS Zones. With 4PSA DNS Manager, you can create and administer DNS Zones and DNS Records, backup DNS Zones, manage DNS templates, gather DNS information from remote servers, etc. 4PSA DNS Manager can load DNS zone names from remote servers, regardless of the control panel or the operating system that runs on these servers.

Thanks to its advanced features, 4PSA DNS Manager is the ideal tool for automatic DNS management.

## 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.

Here are 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 they use. The centralization process is automatic and you do not have to add DNS Zone information to the 4PSA DNS Manager server.

  The interface scripts for most popular hosting panels like Plesk, Cpanel, Ensim, InterWorx Control Panel and Helm 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 4.0.0 Features

Some of the most important features offered by 4PSA DNS Manager 4.0.0 are:

- Administrator and client management levels.
- System designed for automatic DNS hosting.
- Client permissions and limits.
- Client actions auditing that logs information about DNS zone changes.
- Command line creation utilities.
- Supports both RFC1912 and timestamp SOA Serial number formats.
- System 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.
- E 164 Zones support.
- IPV6 reverse Zones support.

- 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 Red Hat servers. It can be installed on servers running Plesk (the Plesk server will be the centralized DNS server).
- Automatic import scripts for Plesk, Ensim, 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

# Navigation

4PSA DNS Manager provides a multitenant software automation solution, designed to deliver advanced DNS hosting to service providers and businesses. The product's clear and intuitive web based interface is meant to ease the users' experience, reducing the time required to navigate between the wide range of available options.

## The Navigation Panel

4PSA DNS Manager groups all the important features into several categories that can be accessed at any time from the navigation panel, available in the left side of the screen:

- General - This section allows you to access the management options for the DNS Zones, as well as the global server settings and server preferences.
  -  DNS Zones - Clicking this link will open the DNS Zones management page that displays a list with all the Zones currently set up for your

account, while also providing the tools required to backup them and to add new ones, if required.

- Settings - The DNS templates, the general options, the interface preferences or the database settings are some of the options that can be configured from the Server Settings page.

- Options - To terminate your session and disconnect, click the Logout icon.

  In case you are impersonated as one of your client accounts, to return to your administrator context, click the Return to my account icon.

## The Top Frame Controls

When navigating through the web interface, the top frame controls are always available and can be used to log out and to change your interface preferences.


The top frame controls

The three controls are:

- Logged in as: {your_contact_name} - Click this link to edit your contact details or if you want to change your password.
- My interface - If you want to change your interface preferences, click this link and use the controls available in the My Interface Settings page.
- Logout - Click this link to log out from your 4PSA DNS Manager account. The current session will be closed and you will be required to provide your username and password to log in again.

## The Main Frame Controls

On the top right corner of each page displayed in the main frame you can find another set of controls, used primarily for navigation and for opening the help window.

By default, the only control ever present is the Help icon. Anytime, anywhere, when there is something you need more information about, click this link and read the help file.

**Note**

Your browser must allow pop-up windows in order for the help file to be displayed on screen.

Going down in the application structure, you will be able to move up one level and return to the previous page by using the Up level icon.

## Using the Search Functions

All the tables and lists available in 4PSA DNS Manager allow you to search for the desired items. The search functions can be simple or advanced. This section is intended to describe the basic search controls and to provide you an overview of how you can customize the tables layout.


**Note**

To hide/reveal the search options, click the Toggle search link.

These simple controls can be used for searching a specific word:

- Search – Use the text box to specify the words you are looking for. Click the Search link to display only the records that match your search criteria. The table will be updated accordingly.
- Show all – Click the Show all link to display the entire list.

The search criteria is retained until a new search is performed and it is not lost when navigating to other pages.

## The Table Controls

Each table in 4PSA DNS Manager provides several configuration tools designed to offer you a better overview of the available records. Depending on your preferences, you can:

1. Customize the total number of records displayed in each page by clicking the 10, 25 and 100 links available on the right side of the table. The total number of records as well as other details (e.g.: call cost) are shown on the left side.

   In the tables with more than one page of records, you can navigate between pages using the following controls:

   **Note**

   Have in mind though that a larger number of records per page may cause your system to work slower.

2. Customize the table layout by choosing the columns to be displayed. To do so, click the Show columns icon and select (or deselect) the desired columns. This is especially useful for the tables with many columns where you have to scroll in order to see all the information.
3. Sort the table by a certain criterion. To do so, simply click a table header and the entire list will be sorted accordingly. The table header will be highlighted and an arrow will indicate how the list was sorted: ascendingly or descendingly. The sort direction can be changed by another click on the corresponding header.

## How to Remove Table Records

4PSA DNS Manager offers you a straightforward method for removing the unnecessary records from a table. This method implies the following steps:

1. Choose the records you want to delete by selecting their corresponding check boxes available at the end of the table.
2. Click the Remove selected link. A confirmation pop-up window will be displayed.

**Note**

In some situations, another page will be opened and you will be required to review and confirm the removal.

3. Click **Ok** if you want to remove the record(s). If you do not want to proceed, click **Cancel**.

Chapter 3

# Logging In

You can log in to the 4PSA DNS Manager interface using any of the available web browsers. Simply type in the address where the application was installed:

https://<installation_url>:8550/

Chapter 4

# General Account Management

This chapter contains information about how to set up and modify your own contact details.

4PSA DNS Manager allows you to edit the following account details:

- Client Account Information
  - Company name
  - Contact name
  - Login – The username you must provide in order to log in to the 4PSA DNS Manager interface.

    Note

    The **Login** name must be unique in the system.
  - Password – The password you must provide in order to log in to the 4PSA DNS Manager interface.

> **Note**
>
> The **Password** must be between 6 and 14 characters long and can contain the following character types:
>
> - Any of the **26 letters of the Latin alphabet [a-z]**, also included in the American Standard Code for Information Interchange (ASCII). The scripts of non-Latin languages (such as Arabic, Cyrillic, Chinese, Greek, Indian, Korean or Japanese) are illegible.
> - Any combination of the **10 decimals [0-9]**, also included in the ASCII.
> - Special characters like: **!?@#$%\/*()_+={}`~[];:,.|^&**.
>
> For security reasons, the **Password** cannot be the same as the **Login** name.

- Confirm password
- Phone
- Fax
- E-mail – Your email address, which is used as the default bounce address for all his domains.
- Address
- City
- Postal/ZIP code
- State/Province - Use the drop-down list to select your state/province, if his home Country is United States.
- Country
- Language - The language your interface will be displayed in.

Click Ok to save the new contact details. Click Cancel to return to the previous page without modifying anything.

Chapter 5

# Manage the Application

This chapter describes how can the 4PSA DNS Manager interface be customized to meet your layout and interface requirements. These features can be accessed from the  Settings page as follows:

- From the Options section:
  -  Interface settings
  -  Custom buttons

## Manage Interface Preferences

4PSA DNS Manager allows you to customize the application's default look and settings from the Interface Preferences page. Here, you can define the

interface language, the application's skin and the number of rows in the records list.

You can customize the following preferences:

- Interface Preferences
  - Rows in table – Use this text box to set the number of rows that will be displayed in the interface for all the tables and lists. The accepted values range from 1 to 9,999. The default value is 50.
  - Interface skin – Use this drop down list to choose the skin used by your interface.
  - System language – Use this drop down list to choose the language used by your interface.

> **Caution**
>
> 4PSA DNS Manager does not allow you to use language packs that were created for earlier versions of the interface. The following warning message is displayed:
>
> Impossible to switch to preferred interface language *{outdated language}*, because an outdated language pack is installed on the system. Please contact your provider to correct this situation.
>
> Only the system administrator can fix this problem.

## My Interface Settings

4PSA DNS Manager allows you to customize the application's default look from the Interface Preferences page. There you can define the interface language and skin or the number of rows displayed in the tables for the logged in user (client in your case).

The following preferences can be customized according to your needs are the same as the ones described in this section.

# Manage the Custom Buttons

4PSA DNS Manager allows you to customize the functionality of the control panel by adding custom buttons linked to specific URLs.

The Custom Buttons management page allows you to:

- View the list of custom buttons defined at client level.
- Define a new button by clicking the  Add custom button icon available in the Tools section.
- Modify the existing custom buttons' settings.
- Remove unused buttons from the system.

4PSA DNS Manager displays the following information about the available custom buttons:

- S – The button's status:
  -  Enabled
  -  Disabled
- L – The button's location:
  -  shows that the button is displayed in the left panel.
  -  shows that the button is placed in the right panel.
- I – The icon associated with the button.

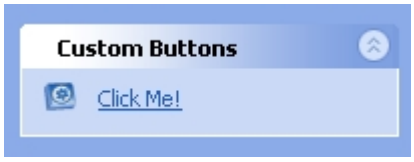
> **Note**
> If the default icon is associated with the button, then 4PSA DNS Manager displays 

- Label – The button's tag displayed in the interface on which the users can click in order to access the specified page. To modify the custom button's preferences, click the available label .
- URL – The URL linked with the button. On click, the specified page opens.
- Priority – The value that defines the order in which the buttons are displayed in the interface. A lower priority implies a higher position. For example, if there are two buttons, one with priority 50 and the other one with 35, then the second button will be displayed first.

## Add a New Custom Button

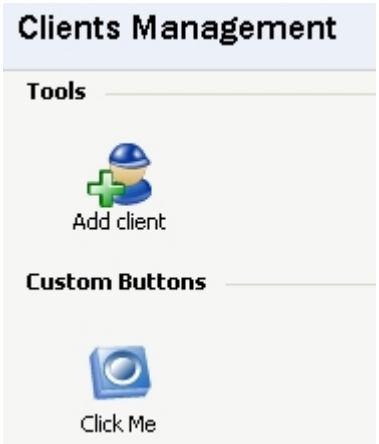
The Add Custom Button page allows you to fill in the information required to define the button. The customizable parameters are grouped into the following fieldset:

- Settings
  - Label – Use the available text box to specify the button's tag that will be displayed in the interface. The user will be able to click this label in order to access the specified URL .
  - Title – Here you can fill in the tool tip that will be displayed when the mouse is positioned on the button's icon.
  - Location – Use the radio buttons to choose where the new custom button will be displayed:
    - Navigation panel - The button will be displayed in the Custom Buttons section available in the left navigation panel.




> **Note**
>
> In the pictured example, a non-default image is used for the custom button.

    - User's context - The button will be displayed in the user's management page, in the Tools section.




> **Note**
>
> In the pictured example, the default image is used for the custom button.

  - Default image for all skins – If this check box is selected, then 4PSA DNS Manager will display the new custom button will be displayed in all the available skins using the default button icon. If you wish to load

custom icons, then deselect this check box. 4PSA DNS Manager will display additional controls:

- Use the Browse... button to locate a graphic file on your computer.
- Select the check box corresponding to the skin where you want the icon to be used.
- Select 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.

> **Note**
>
> You can upload image files up to maximum 10 KB per file. Exceeding this limit will trigger an error message.

- URL – Use this text box to fill in the URL that will opened when the button label is clicked from the interface.
- Context help – Here you can fill in the button description that will appear in the context help area on mouse-over.
- Action – Use the radio buttons to choose how the page whose URL you specified earlier will open:
  - In the Current window.
  - In a New window.

Click Ok to create the button. Click Cancel to go back to the previous page without adding the button to the system.

## Edit Custom Buttons

To edit the a custom button's parameters, follow the next steps:

1. Choose the button you want to modify and click its Label.
2. The editable data is grouped into the Settings fieldset.

   The following supplementary options are available when editing a button that has one ore more custom images associated:

   - Existing images - The currently used image and the skins where it is visible are displayed (e.g.: [All skins]).

- **Keep existing images** - If you deselect this check box, then you will be able to choose other images for the custom button using the controls available at the **Skin specific image** option.

> **Note**
>
> For more information, see the Add a New Custom Button section.

3. Click **Ok** to save your changes. Click **Cancel** to return to the previous page without modifying anything.

Chapter 6

# Manage the System Features

All the settings that define the system behavior, including the interface, the server preferences or the general options can be managed starting from this page by clicking the corresponding icons grouped into two functional sections.

As a client, you are able to control the following features:

- Options - Choose the desired core functionality you want to manage by clicking the corresponding icon.
  -  DNS templates
  -  Interface settings
  -  Custom buttons
  -  4PSA DNS Manager settings

- Database - This section groups all the database related options.
  -  XML export
  -  XML import

## Manage the System 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 all the DNS Zones that belong to the client account can be modified:

- Remote Updates Preferences
  - Remove zones no longer present in update source – When this option is enabled, the 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 that Zone. This setting helps you keep the 4PSA DNS Manager server perfectly synchronized with the remote update locations.

    
    Note

    This option is displayed only if the system administrator has given you the permission to manage it.

  - 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

    This option is displayed only if the system administrator has given you the permission to manage it.

  - 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. The default value is 3.

- Default DNS SOA Records
  - 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. The default value is 10,800 seconds.

    > **Note**
    >
    > RFC 1912 recommends 1,200 to 43,200 seconds, if your data is volatile, or 43,200 (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. The default value is 3,600 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. The default value is 604,800 seconds.

    > **Note**
    >
    > RFC 1912 recommends 1,209,600 to 2,419,200 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). The default value is 86,400 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. The default value is 604,800 seconds.

Click Ok to save your preferences. If you want to return to the previous page without committing the changes, then click Cancel. To revert to the default values, click Default SOA.

## XML Export

4PSA DNS Manager allows the client to export his account's database in .xml format. This feature can be used for backup or for migration purposes.

A client account will export all of the following items:

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

To export the database to a .xml file, simply click the 

XML export icon and confirm your choice.

## XML Import

4PSA DNS Manager allows the client to import an .xml file that is a database backup.

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.

A client is able to import from the .xml file his account's details and preferences and details about the Zones (existing or new ones).

Note

The existing client's account details will be updated.

Using the .xml file, new zones can be created. The records from existing zones are replaced with the records from the .xml file.

The 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 from a .xml file, simply click the 

XML import and use the Browse button to locate the backup file.

Chapter 7

# Manage the System Templates

The system templates are collections of predefined settings that can be used to easily configure DNS Zones, email messages or to manage various custom files. In your case, as a client account owner, you have access to only one template type that can be accessed from the Server Settings >> Options section:

-  DNS templates

## Manage the DNS Templates

**Note**

To be able to create and manage DNS templates, the system administrator must have enabled the appropriate permissions for your account.

The DNS templates automate the Zone configuration by inserting predefined, dynamically generated records.

The client DNS templates are available only to the current account. No other client is able to use them.

The DNS Templates of Client {client_name} management page allows you to:

- Visualize the existing Templates.
- Use the available controls to define a New DNS Template.
- Search for certain templates.
- Edit one of the existing DNS templates.
- Remove unused templates.

4PSA DNS Manager displays the following information about the available templates:

- Name – The name that identifies the template. Click the link to manage the template.

> **Note**
>
> There are some templates that the client account owner can only view and use in zone creation and cannot modify them because they were created by the system administrator.

- Type - The DNS Zone type that can be set up using the template:
  - Forward
  - Reverse
  - E.164

> **Caution**
>
> When you delete a template, the Zones created with it will not be affected!

## Add a New Client DNS Template

To create a DNS Template, you must follow the next steps:

1. Fill in a Template name.

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

2. Choose the template type using the available radio buttons:
   - Forward - A template for forward DNS zones.
   - Reverse - A template for reverse DNS zones.
   - Reverse IPV6 - A template for reverse IPV6 DNS zones.
   - E.164 - A template for E.164 DNS zones.
3. Click Ok. The DNS Template {tpl_name} of Client {client_name} page will open, allowing you to define the DNS records and the Template IPs.
4. Next, you should set up the DNS records by clicking the  Add DNS record icon available in the Tools section.
5. If you want, you can add now the  Template IPs .

### Edit a DNS Templates

When you want to edit an existing DNS template, you can modify and add new DNS records and template IPs, as described in the DNS Template Management page.

## Client's DNS Template Management

The DNS Template {tpl_name} of Client {client_name} page offers all the controls required to manage the DNS template:

- Visualize the existing DNS Record(s).
- Set up a new DNS record by clicking the  Add DNS record icon available in the Tools section.
- Add new  Template IPs .

- Search for certain DNS records.
- Edit one of the existing DNS records.
- Remove unused DNS records.

4PSA DNS Manager displays the following information about the available DNS records:

- Host – The DNS record's host name or the IP address.
- Record type – The DNS record's type .
- Value – Depending on the record type, this field displays an IP address, an alias, a name server, a host name, or a text.
- Priority - The Zone's priority.
- Weight - The Zone's weight.
- M – To edit a DNS record's details, click the  Modify icon.

## Add DNS Records

To add a record to a DNS template, you must first choose the Record type and next configure its specific parameters accordingly.

Note

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

The following DNS record types are available:

- Forward DNS Zones
- Reverse DNS Zones
- Reverse IPV6 DNS Zones
- E.164 DNS Zones

## Edit a DNS Template Record

The Edit Record from Template {tpl_name} page offers you the required tools to modify the chosen record:

- Record Type
  - Record type - To change the record's current type, use this drop-down list that contains all the supported record types.

- {record_type} Record

> **Note**
>
> All the parameters displayed in section depend on the previously chosen. **Record type**

> **Note**
>
> The domain name can be automatically replaced by the name of the newly created domain if [domain] is specified in the domain name field. In order to have an IP address automatically replaced the [ip] tag must be used.

### Removal Confirmation

To finalize the removal, you have to review the list, select the Confirm removal check box and click Ok. If you do not want to delete these records, click Cancel to return to the previous page.

### Managing a Template's IPs

The Server Global DNS Template {tpl_name} - IP Management page allows you to:

- Visualize the existing Template IPs.
- Add new master IPs.
- Search for certain IPs.
- Remove unused IPs.

4PSA DNS Manager displays the following information about the available template IPs:

- Type - The IP address type:
  -  Master
  -  Slave (allow transfer)
- IP Address - The IP address.

To add an IP address to the template, fill in the information required in the Add Template IPs fieldset:

- Add the following master IP - For master IPs assigned to slave zones.

- **Add the following allow transfer IP or IP/Mask to master zones** - For allow transfer IPs assigned to master zones.

  To add/remove multiple IP addresses, use the  icons.

### Removal Confirmation

To finalize the removal, you have to review the list, select the **Confirm removal** check box and click **Ok**. If you do not want to delete these records, click **Cancel** to return to the previous page.

Chapter 8

# Manage the DNS Zones

To access the DNS Zones page, click the  DNS Zones link available in the left navigation panel.

## Client Management Page

This page displays the list of all the DNS Zones defined for your account and it allows you to add new ones or to manage an existing Zone. Also, using the available controls, you can control your account's preferences:

- Tools

  This section contains all the controls required to manage your own account:

  -  Edit account details
  -  Add DNS zones

-  Remote updates
-  Backup DNS Zones

- Custom Buttons - This section is displayed only when there is at least one custom button with the Location set to User's context defined both by the system administrator or by you.
- DNS Zones - 4PSA DNS Manager displays a list with all the client's DNS Zones.

  4PSA DNS Manager displays the following information about each Zone:

- S – The Zone's status:
  -  Enabled
  -  Disabled

  Click this icon to enable/disable the DNS Zone.
- T – The DNS Zone type:
  -  Master
  -  Slave
- DNS Zone name – The name of the DNS Zone. Click the link to enter the Zone's management page .
- First name server – The host name of the first name server registered on this DNS Zone.

Note

The first name server of slave zones is not displayed.

- Created – The date and time the Zone was added to the system.

## Searching the DNS Zones List

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

Search {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.

## 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. To do so, follow the next steps:

1. Choose the desired DNS Zones by selecting their corresponding check boxes available on top of the table.
2. Click the  SPF rules link.
3. 

   Note

   SPF rules can be defined only for forward master Zones added from the control panel.

   Use the controls to manage the Global SPF Rules:

   - First, to create a SPF for one of the origin's subdomains, you have to fill in the subdomain in the Host text box. The format must be subdomain.[domain].

     Leaving this field empty generates the TXT record for $ORIGIN.
   - Next, define the rule. The standard rule format is:

     {qualifier} {mechanism} {URL}

     where:

     - {qualifier} - Use the drop-down list to select one of the available qualifiers:
       - + Pass
       - - Fail
       - ~ SoftFail
       - ? Neutral

- {mechanism} - Use the drop-down list to select one of the available mechanisms and modifiers.

  The following mechanisms are available:

  - all
  - ip4
  - ip6
  - a
  - mx
  - ptr
  - exists
  - include

  And the following modifiers:

  - redirect
  - exp

- {URL} - Use the available text box to specify the target URL.

- Use the  icons to add/remove rules from the list.

4. Click Ok to confirm the rules or Cancel to return to previous page without committing anything.

## 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, the glue records are used for two purposes:

1. 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.
2. To break the query deadlock for referrals which return name servers within the domain being queried.

Note

The **Glue Records** can only be defined for forward master DNS Zones managed from the interface.

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

- 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 8.1. Required Records

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

### Table 8.2. Resulting Glue Record

| Host | Record Type | Value |
|---|---|---|
| ns.sub.example.com | A | 1.2.3.4 |

To create a Glue Record, you must follow the next steps:

1. Choose the desired DNS Zones by selecting their corresponding check boxes available on top of the table.
2. Click the  Glue records link.
3. Review your selection and click Ok confirm or Cancel to go back to the previous page without gluing the records.

## Global Operations on DNS Zones

4PSA DNS Manager allows you to simultaneously change records belonging to two or more DNS Zones:

1. Choose the desired DNS Zones by selecting their corresponding check boxes available on top of the table.

2. Click the Global operations link.
3. The Global Operations page displays, depending on the type of DNS Zones you have selected, one or more of the following sections:
   - Forward Zones
   - Reverse Zones
   - E.164 Zones

   Each section offers the controls required to specify the rules for the respective Zone type.

   The general formula is:

   If {record_type} {matching_algorithm} {search_criteria} {action} {new_value}

   where:

   - {record_type} - Use the drop-down list to choose the type of the 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.
   - {matching_algorithm} - Use the second drop-down list to choose the matching algorithm:
     - equals when the value parameter of the records must be identical to the given value.
     - contains when the value parameter of the records must contain the given value.
   - {search_criteria} - Use this text box to specify the search criteria.

     Note

     * can be used to match any set of characters.

   - {action} - Use the third drop-down list to select the action you would like to perform on the matching records. The available options are:
     - replace with if you want to modify the matching records.
     - drop record if you want to erase them.
   - {new_value} - 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 previously selected drop record.

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

For MX forward Zones, the global operations formula is:

If {Mail exchanger MX} {item} {matching_algorithm} {search_criteria} {item} {action} {new_value}

This allows you to change both the Zone's value and priority using the {item} drop-down list.

4. Use the  icons to add/remove rules from the list.
5. Click Ok to confirm the rules or Cancel to return to previous page without committing anything.

## Edit Client Information

You can edit your contact details at any time. More details about the options available in the Client Account Information fieldset can be found here .

> **Note**
>
> The **Login** name must be unique in the system.

The mandatory fields are marked with an asterisk. Click Ok to add the commit the changes. Click Cancel to return to the previous page without saving anything.

## Add a New DNS Zone

4PSA DNS Manager allows you add a single DNS Zone, multiple DNS Zone names from a local file or multiple DNS Zones with complete DNS Records.

Note

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

## Add a Single DNS Zone Name

In order to add a single DNS Zone name, you must fill in all the information required in the Add DNS Zone name fieldset:

- DNS Zone name – Use the available text box to fill in a valid and unique DNS Zone name. Here are some examples for all the supported DNS Zones types:
  - For a forward Zone, you must use the following format:

    `<lower level domain(s)>.<top level domain>`

    For example:

    - `racksoft.com`
    - `wikipedia.org`
    - `amazon.co.uk`
  - For a reverse Zone, you must use the following format:

    `<lower level domain(s)>.IN-ADDR.ARPA.`

    For example:

    - `2.85.64.IN-ADDR.ARPA`
    - `4.3.2.1.IN-ADDR.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 the IPs between `3.2.1.192` and `3.2.1.255`; or `4.3.2.1.IN-ADDR.ARPA` for a complete /32 delegation.

According to the recommendations specified in RFC 4183, 4PSA DNS Manager supports both **/** and **-** as mask delimiters. The delimiter can be:

- Included in the **DNS Zone name**, for example `128/25.27.116.87.IN-ADDR.ARPA.` or `128-25.27.116.87.IN-ADDR.ARPA.` In this case, the delimiter is stored in the data base as provided and the **Reverse zone separator** option is disabled.
- Not included in the **DNS Zone name**, for example `3.2.1.IN-ADDR.ARPA.` In this case, you can choose the **Reverse zone separator** **/** and **-**.

  For the Class C(/24) reverse Zones, the separator can always be chose according to your requirements.

◦ For an IPV6 reverse Zone, you must use the following format:

`<reverse_ipv6_chunk_nibbles>.IP6.ARPA.`

where `<reverse_ipv6_chunk_nibbles>` can contain from 1 to 32 nibbles. A nibble is half an octet that corresponds to a single hexadecimal digit.

For example:

- `8.b.d.0.1.0.0.2.IP6.ARPA.` (/32 = 8 nibbles)
- `b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6` (/128 = 32 nibbles)

◦ For an E.164 Zone, you must use the following format:

`<lower level domain(s)>.E164.ARPA.`

For example:

- `2.2.3.E164.ARPA`
- `1.1.1.E164.ARPA`

- DNS Zone template – Use the drop-down list to select one of the available DNS Zone templates to be used to create the Zone. You can select Do not use DNS Zone template if you want to manually set it up.
- Template IP – This field is available only when a DNS Zone template is selected. All [ip] occurrences in the DNS Zone template will be replaced by this IP.
- DNS Zone type – Use the radio buttons to choose the DNS Zone type:
  ◦ Master
  ◦ Slave

> **Note**
>
> A slave zone will acquire it's 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 it is recommended to set up notifications on master zones.

- Reverse zone separator - When the separator is included in the reverse Zone's name (e.g.: 128/25.27.116.87.IN-ADDR.ARPA.), you cannot change the selection as the drop-down list is disabled. In this case, the separator detected in the Zone's name will be selected (for our example, /).

  If the Zone's name does not include the separator (for example, for the Class C(/24) reverse Zones), then you can use the drop-down list to select the records separator:

  - /
  - -

> **Note**
>
> This option is displayed for **Reverse zones** only.
>
> 4PSA DNS Manager is compliant with the recommendations specified in RFC 4183.

- Forward zone - Regular zone.
- Reverse Zone – Zone used for reverse DNS lookup (i.e. a zone in the IN-ADDR.ARPA domain).
- E.164 Zone - 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).

> **Note**
>
> This option is enabled only if the previously chosen Zone type is master.

- Slave DNS servers IP addresses – When the Allow DNS Zone transfer option is enabled, you can enter the IP addresses of the slave DNS servers

in this text box. Use the  icons to add/remove slave IP addresses. The DNS Zone will be transferred only to these IP addresses.

> **Note**
>
> This option is enabled only if the previously chosen Zone type is slave.

- 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.

> **Note**
>
> This option is available for slave DNS Zones only.

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

> **Note**
>
> This option is available for slave DNS Zones only.

Click OK to create the new DNS Zone. Click Cancel to return to the previous page without adding anything.

## Adding Multiple DNS Zones with Complete DNS Records

In order to add multiple DNS Zones with complete DNS Records, click the  Full zones from file icon available in the Tools area. The following fields will be displayed:

- Select file – Use the available text box to fill in the name of the file containing the DNS Zone names or click the Browse icon 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 it's 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.

- 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 IP or IP/Mask to master zones - The IP addresses specified in this field will be recorded in the allow transfer clauses of the namedropping file for master DNS zones
- Add the following master IP - The IP addresses specified in this field will be recorded in the masters clauses of the namedropping file for slave DNS zones

Click OK to create the new DNS Zones. Click Cancel to return to the previous page without adding anything.

## Edit a DNS Zone

> **Warning**
>
> The records of the zones added from a remote location cannot be modified from the interface. In this case, 4PSA DNS Manager displays the following warning message:
>
> This zone is managed by Remote Update and cannot be edited in the interface.

All your DNS Zone can be fully managed from the DNS Zone {name} of Client {client_name} page. Here you can find all the controls required to control the DNS Zone and its records, grouped into the following sections:

- New DNS Record
  - Click the  Add DNS record icon to define a new record for the current Zone.
- Tools

Using the icons available in this section you can manage the current DNS Zone:

- Change the DNS Zone type by clicking:
  -  Switch to slave if the Zone is master.
  -  Switch to master if the Zone is slave.
- Change the DNS Zone status by clicking:
  -  Zone is enabled to disable the Zone.
  -  Zone is disabled to enable the Zone.
-  Transfer IP addresses
-  Backup DNS zone

> **Note**
>
> A disabled Zone or without any records CANNOT be backed up. The  icon is displayed instead.

-  DNS round robin

> **Warning**
>
> This feature is only available for forward Zones added from the 4PSA DNS Manager control panel.

> **Note**
>
> If the forward Zone is not allowed **Round Robin management**, then the  icon will be displayed instead.

-  Zone SOA records
-  Check name servers

> **Note**
>
> When the domain has no name servers defined, the  icon is displayed instead.

- DNS Zone Information

  The following information about the current Zone are displayed:

  - DNS Zone type – The DNS Zone type: Master or Slave/ Forward, Reverse or E.164. The number of transfer IPs for master Zones and the number of master IPs for slave zones respectively are also displayed, between parenthesis.

> **Note**
>
> A slave zone will acquire it's 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.

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

> **Note**
>
> This line is displayed for reverse DNS Zones only.

  - 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, the  icon is displayed. Click this icon to access the configuration page of the respective remote update location.

- DNS Records

  This table displays all the records defined for the current DNS Zone. The following information is available:

  - S – The DNS record's status:

    -  Enabled
    -  Disabled
    -  Temporarily disabled

      This icon indicates that the record has been temporarily disabled by round robin who was not able to access it.

    Click this icon to change the record's status.

    > **Warning**
    >
    > The record's status can be modified only for Zones added from the 4PSA DNS Manager control panel.

  - P - This icon shows whether there are any round robin polls monitoring the record or not.

    - 

      This icon indicates that there are round robin polls set up for the corresponding record. On click, the record's Round Robin Polls for DNS {record_name} management page opens.

    - 

      This icon indicates that there are no round robin polls set up for this record.

    > **Warning**
    >
    > This column is available only for forward Zones added from the 4PSA DNS Manager control panel.

- Host – The host name or the IP address of the DNS record.
- Record type - The DNS record type, defined based on the DNS Zone type .
- Value – Depending on the Record type, this field displays an IP address, an alias, a name server, a host name or a text.
- Priority - The target hos priority. The lower the value, the higher the priority level.
- Weight - A relative weight between records with the same Priority.
- Last update - The date and time the record was last modified either from the web based interface or by updateurl.
- M – Click the  Modify icon if you want to edit the DNS record.

> **Warning**
>
> The records can be modified only for Zones added from the 4PSA DNS Manager control panel.

## Add a New DNS Records

> **Warning**
>
> Records can be added only for Zones added from the 4PSA DNS Manager control panel.

Depending on the Zone type, the Add NEW Record to DNS Zone {zone_name} page displays the following sections:

- The DNS Zone Information section is available for reverse zones only:
  - Hosts in this zone - The first and last available IP addresses. These parameters depend on the reverse Zone IP class.
- The {record_type} Record section is displayed for all Zone types:
  - Record type - Use the drop-down list to select one of the record types available for the current Zone:
    - For Forward DNS Zones
      - IP Address (A) - This record type maps a hostname to a 32-bit IPv4 address.

        The 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 record type, see RFC 1035.

- AAAA Record (AAAA) - This record type maps a hostname to a 128-bit IPv6 address.

  The 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 record type, see RFC 3596.

- Alias for record (CNAME) - The 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.

  The 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 a MX record.

For more information about this record type, see RFC 1035.

- Nameserver (NS) - This record type maps a domain name to a list of DNS servers authoritative for that domain. The delegations depend on the NS records.

  The 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 chosen 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 from the interface the primary nameserver on a zone (required for some local TLDs). In order to set up an NS record as primary, select the **Make primary** check box 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 that zone.
>
> For best practice, it is recommended to have at least two NS records defined for each public domain.

For more information about this record type, go to RFC 1035.

- Mail exchanger (MX) - This record type maps a domain name to a list of mail exchange servers.

  The 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 record type, see RFC 1035.

- Text record (TXT) -This record type 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.

  The TXT rules have the following format:

  `hostname. IN TXT "Text information"`

  where:

  - hostname. is the zone name or one of ts 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 record type, see RFC 1035.

- Service Record (SRV) - This record type specifies the servers' location for a specific protocol and domain.

  The 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 here.
  - Protocol is the desired service's protocol. This is usually TCP or UDP, but 4PSA DNS Manager supports all the protocols listed here.
  - 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 . (point), the service is unavailable.
  >
  > The Target can be in another domain if you use for it a FQDN domain name.

  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

_service._tcp.domain.com. IN SRV 0 1 9 anotherdomain.com.

For more information about this record type, see RFC 2782.

- For Reverse DNS Zones
  - Nameserver (NS) - Specifies a host which should be authoritative for the chosen 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 from the interface the primary nameserver on a zone (required for some local TLDs). In order to set up an NS record as primary, select the **Make primary** check box 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 that 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, but 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).

    The 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 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 that 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 record type, see RFC 1035.

- Reverse record (PTR) - This record type 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.

  The 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 record type, see RFC 1035.

- 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.

  The 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 record type, see RFC 1035.

- Text record (TXT) - This record type 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.

  The 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 record type, see RFC 1035.

- For E.164 Zones
  - Nameserver (NS) - This record type maps a domain name to a list of DNS servers authoritative for that domain. The delegations depend on the NS records. The 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 that 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 from the interface the primary nameserver on a zone (required for some local TLDs). In order to set up an NS record as primary, select the **Make primary** check box 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 that zone.

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

For more information about this record type, see RFC1035.

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

  ```
  order preference services flag regexp replacement
  ```

  where:

  - order indicates the order in which the 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 record type, see RFC3403.

- **Note**

  Since IPv6 addresses are natively classless, there are no **CNAME** based naming conventions when setting up delegated reverse DNS for your netblock. Thus, there is only one method of IPv6 rDNS naming.

  For more information, see the Non-Terminal DNS Name Redirection (primarily IPv6) RFC 2672.

### For Reverse IPV6 DNS Zones

- **Reverse record (PTR)** - This record type maps an IPv6 address to the canonical name for that host. Setting up a PTR record for a hostname in the IP6.ARPA. domain that corresponds to an IPv6 address implements reverse DNS lookup for that address. The PTR rules have the following format:

  IPv6 address IN PTR hostname.

  where:

  - IPv6 address is the IPv6 address in the IP6.ARPA. domain.

    **Note**

    Each time you define a new record for an IPv6 DNS Zone, 4PSA DNS Manager displays under the **IP address** text box the number of nibbles that have to be filled in to have a valid record.

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

  For example:

  ```
  8.b.d.0.1.0.0.2.IP6.ARPA. IN PTR test.com.

  1.1.1.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.B.D.0.1.0.0.2.IP
  IN PTR test.com.
  ```

  For more information about this record type, see RFC4291.

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

  The NS records can be defined only for $ORIGIN.

> **Note**
>
> The NS records of $ORIGIN are displayed in bold characters.
>
> 4PSA DNS Manager allows to choose from the interface the primary nameserver on a zone (required for some local TLDs). In order to set up an NS record as primary, select the **Make primary** check box 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 that zone.
>
> For best practice, it is recommended to have at least two NS records defined for each public domain.

The NS rules have the following format:

```
ipv6_part.host_ipv6_addr.IP6.ARPA. IN NS servername.
```

where:

- ipv6_part is the IP section that completes the IP address when prepended to host_ip_addr.
- host_ipv6_addr.IN-ADDR.ARPA. is the zone name.
- servername. is a domain name which specifies an authoritative host for the defined zone.

For example:

```
8.b.d.0.1.0.0.2.IP6.ARPA. IN NS example.com.
```

```
5.5.1.3.2.1.0.2.3.4.5.6.7.8.9.0.1.2.3.4.5.6.7.8.9.0.A.B.C.D.E.F.IP
IN NS example.com.
```

For more information about this record type, see RFC4291.

You can choose whether you would like the record to be enable after you create it by selecting the check box next to the drop-down list. By default, every record is enabled.

> **Note**
>
> The domain name can be automatically replaced by the name of the newly created domain if [domain] is specified in the domain name field. In order to have an IP address automatically replaced, the [ip] tag must be used.

> **Note**
>
> All the other parameters displayed in section depend on the **Record type** previously chosen.

You can add up to 10 multiple similar records in the same time using the  icons.

Click Ok and the new record(s). Click Cancel to return to the previous page without adding anything.

### Edit a DNS Record

The Edit DNS Record page allows you to change the record type and its specific parameters, depending on your requirements. To do so, you can use the controls grouped into the following fieldsets:

- The DNS Zone Information section is available for reverse zones only:
  - Hosts in this zone - The first and last available IP addresses. These parameters depend on the reverse Zone IP class.
- Record Type
  - Record type - To change the record's current type, use this drop-down list that contains all the supported record types.
  - Record is enabled - You can also enable or disable the record by selecting or deselecting this check box.
- {record_type} Record

> **Note**
>
> All the parameters displayed in section depend on the **Record type** previously chosen.

## 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.

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

The controls available in the DNS Zone Transfer of {record_name} page are grouped into three sections:

- DNS Zone Information
  - DNS Zone type - The DNS Zone type can be:
    - Master
    - Slave
  - 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.

> **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.

- New Transfer IP Address

  To add new IP addresses, you must simply specify the desired address or the IP/Mask address in the Slave DNS server IP or IP/Mask address text box (e.g: 192.168.14.11/24, 192.168.1.1/16) and click Ok.

  To add multiple IP or IP/Mask addresses in the same time, use the  icons.

- Transfer IP Addresses

  4PSA DNS Manager displays the following information about the available transfer IPs:

  - IP Address - The IP or the IP/Mask address of the DNS server allowed to transfer Zone information from the server.

## DNS Zone Backup

4PSA DNS Manager offers you the possibility to save a backup copy with all the DNS Zone's preferences and existing records. The .dnsm file that will be stored on your local drive has the following naming convention:

{zone_name}-{date}.dnsm

where:

- {zone_name} is the name of the current DNS Zone, for example 1.2.3.IN-ADDR.ARPA.d..
- {date} is the date when the file is saved, for example 20110216. The default format is yyyymmdd.

## Manage the Round Robin Polls

The round robin is a load balancing technique in which balance power is placed in the DNS server instead of a strictly dedicated machine as other load techniques do. Round robin works on a rotating basis in that one server IP address is handed out, then moves to the back of the list; the next server IP address is handed out, and then it moves to the end of the list; and so on, depending on the number of servers being used. This works in a looping fashion.

The Round Robin Polls for DNS {zone_name} management page allows you to:

- Visualize the Current Polls.
- Define a New Round Robin Poll by clicking the  Add new poll icon.
- Search for certain polls.
- Edit one of the existing round robin polls.
- Remove unused polls.

4PSA DNS Manager displays the following information about the available polls:

- S – The round robin poll's status:
  -  Enabled
  -  Disabled

  Click the icon to modify the poll's status.
- Name - The round robin poll's name. Click the link to edit the poll.
- Monitored records - The number of monitored records.
- Active records - The number of active records out of the total monitored records.
- Last update - The date and time the poll was last updated.

### Add a New Round Robin Poll

Follow the next steps to add a new poll:

1. Use the controls available in the Add New Resource Poll fieldset to define the poll's behaviour:
   a. Fill in the poll's Name.
   b. Use the drop-down list to select the Tested protocol. The available options are:
      - HTTP
      - IMAP
      - MySQL
      - PING
      - POP3
      - SIP
      - SMTP
   c. Fill in the number of minutes between two subsequent tests in the Monitoring interval text box.
   d. Use the Tested resource text box to specify a resource corresponding to the protocol that is to be tested. You can type in 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.

   e. Last, decide for how long the round robin will attempt to access the resource before failing in the Try resource for {x} seconds field.
2. Next, choose the DNS record(s) you wish to add to the poll from the DNS Records table by selecting the corresponding check box(es) available in the M column. If you want to select all the records in the list, then simply select the check box displayed in the top header.

   For more details on the information displayed about each DNS Zone, see this section.
3. Click the  Apply changes link to associate the selected records with the new poll.

4. To finalize the process, click Ok and return to the previous page. Click Cancel if you do not want to create the round robin poll.

### Edit a Round Robin Poll

The Poll {poll_name} for DNS {zone_name} page allows you to edit the round robin poll using the controls described in the previous section.

### Removal Confirmation

To finalize the removal, you have to review the list, select the Confirm removal check box and click Ok. If you do not want to delete these records, click Cancel to return to the previous page.

## Set the 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:

- Serial - The DNS Zone serial number that must be a natural value between 1 and 4,294,967,295 (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.

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

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, than 4PSA 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, than 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 {x} seconds
- Retry time {x} seconds
- Expire time {x} seconds
- Minimum TTL {x} seconds
- Default TTL {x} seconds

Note

More details about these last fields can be found in this section.

Click OK to confirm the changes or Cancel to return to the previous page without modifying anything.

## Checking the Nameservers

Clicking the  Check name servers icon to verify the availability of the name servers for the current zone triggers the display of a new section, Check Name Servers, that lists all the name servers and shows their availability using the following parameters:

- 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 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 these files using the HTTP, HTTPS and FTP protocol in order to load DNS Zone information from remote servers.

Note

For more details about remote update locations, including integration with a current infrastructure see the Remote Update Location Configuration chapter.

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.

The Remote Update Locations page allows you to:

- View all the Remote Update Locations currently available in the system.
- Instantly update the DNS Zone information with data from the remote location by clicking the  Update Now icon available in the Tools section.

- Visualize a list of the events that occurred during the remote updates by clicking the  Remote logs icon.

> **Note**
>
> If no update operation was ever performed, then the  icon is displayed.

- Add a New Remote Update Location.
- Search for certain remote locations.
- Turn on/off an existing remote update location.
- Edit the parameters of any available location.
- Remove unused location.

4PSA DNS Manager displays following information about the available remote locations:

- S - The remote update location's status:
  - On
  - Off

  Click this icon to change the location's status.
- Remote location - The URL where the file that contains update information can be found.

> **Note**
>
> The remote update locations can also be in IDN format.

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

- Priority – When one zone is defined in two files that can be found in two remote locations, the remote location with the highest priority will be taken into consideration.
- Update interval – The number of minutes between two consecutive retrievals of the remote location - the refresh interval.

- Last updated - The date and time the remote location was updated for the last time.
- M – Click the  icon to edit the remote update location's details.

## Add a New Remote Update Location

To add a New Remote Update Locations to the system, you must fill in all the required details:

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

> **Note**
>
> The remote update locations can also be in IDN format.

> **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 – Use the available drop-down list to select the number of minutes between two consecutive retrievals of the remote location. The possible values range from 2 to 2,880 minutes. The default value is 2.
- Remote URL priority – The priority of the zone definitions downloaded from this URL over other (duplicate) zone definitions. Using the drop-down list, you can choose one of the five priority levels:
  - very low
  - low
  - medium
  - high
  - very high

> **Note**
>
> When there are two or more locations that update the same zone(s) having different priorities, the location that last updates a zone is called the **Owner location**.
>
> If the **Lock zones to an update source** setting is:
>
> - **disabled** - Then the zones will be updated by the remote update URL with the highest priority.
> - **enabled** - Then the zones will be updated by the remote update owner location, ignoring the priorities.

- Username - The HTTP, HTTPs or FTP authentication username.
- Password - The TTP, HTTPs or FTP authentication password.
- Add the following master IP - The IP addresses specified in this field will be recorded in the masters clauses of the namedropping file for the slave DNS Zones. Use the  icons to add/remove several records in the same time.
- Add the following allow transfer IP or IP/Mask to master zones - The IP addresses specified in this field will be recorded in the allow transfer clauses of the namedropping file for the master DNS Zones. Use the  icons to add/remove several records in the same time.

Click OK to add the new remote update location. Click Cancel to return to the previous page without adding anything.

## Editing Settings of a Remote Update Location

The Remote Update Location: {location_name} page allows you to:

- Change the status of the remote update location by clicking the corresponding icon available in the Tools area:
  -  Switch Off - Disable an active update location.
  -  Switch On - Enable a disabled update location.
- Visualize a list of the events that occurred during the remote update of the current location by clicking the  Remote Logs icon.

Note

If no update operation was ever performed, then the  icon is displayed.

- Change the Remote Update Location parameters.

Note

For more information about these fields, see the Add a New Remote Update Location section.

Note

If the remote location details are modified, then the application will force the update of the remote locations.

## Remote Logs

The Remote Update URL Logs page displays a list of events that occurred during remote updates.

The following information is available:

- Date - The date and time the event occurred.
- Level - The event type.
- Message - An explanatory message regarding the event.
- Log data - Specific information regarding the event.

You can clear the remote update logs by clicking the  Clear logs icon.

## Removal Confirmation

To finalize the removal, you have to review the list, select the Confirm removal check box and click Ok. If you do not want to delete these records, click Cancel to return to the previous page.

## DNS Zone Backup

4PSA DNS Manager offers you the possibility to save a backup copy with all your DNS Zones' preferences and existing records. The .dnsm file that will be stored on your local drive has the following naming convention:

{zone_name}-{date}.dnsm

where:

- {zone_name} is the name of the current DNS Zone, for example 1.2.3.IN-ADDR.ARPA.d..
- {date} is the date when the file is saved, for example 20110216. The default format is yyyymmdd.

Chapter 9

# 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 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 straightforward job.

Let us 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 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 include the IP of the 4PSA DNS Manager in the Global Transfer IPs page (available only to the system administrator) or 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 4PSA database. This way you can be sure that the named.conf file will remain correct. To do this, execute the following commands in the 4PSA 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 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. The list of scripts that must be used on remote servers will be updated by 4PSA and the scripts will be placed 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`.

Chapter 10

# Contact and Support

For online help and support please visit:

- Support Zone: https://help.4psa.com
- Knowledge Base: http://kb.4psa.com
- Documentation: http://help.4psa.com/docs/

For mailing addresses and phone numbers from our offices:

http://www.4psa.com/contactus

If you have any question, do not hesitate to contact us.

# Appendix A. Supported Dump File Examples

Starting 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 4PSA 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.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| ||
}
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.com.| ||
    |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| ||
}
```

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, then 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 written on last position of the NS record from the 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 a record, as shown 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| ||}
```

Example for an E.164 reverse zone that contains all three supported record types, NS, PTR and TXT:

```
6-28.3.2.1.IN-ADDR.ARPA.|master {

    |REFRESH| |10800| || ||

    |RETRY| |3600| || ||

    |EXPIRE| |604800| || ||

    |MIN_TTL| |86400| || ||

    |DEFAULT_TTL| |86400| || ||

    |NS| |6-28.3.2.1.IN-ADDR.ARPA.| |test.com.| ||

    |PTR| |14.6-28.3.2.1.IN-ADDR.ARPA.| |example.net.| ||

    |TXT| |17.6-28.3.2.1.IN-ADDR.ARPA.| |Some text| ||

}
```

Example for an IP6.ARPA reverse zone that contains both supported record types, NS and PTR:

```
1.2.3.IP6.ARPA.|master {

    |REFRESH| |10800| || ||

    |RETRY| |3600| || ||

    |EXPIRE| |604800| || ||

    |MIN_TTL| |86400| || ||
```

```
    |DEFAULT_TTL| |86400| || ||
    |NS| |1.2.3.IP6.ARPA.| |example.net.| ||
    |PTR| |1.2.3.4.5.6.7.8.9.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.2.3.
}
```

# Index