ZoneControl

User Guide

Apr 23, 2024 *Release 1.6.1*

©2024 by Open-Xchange AG and PowerDNS.COM BV. All rights reserved. Open-Xchange, PowerDNS, the Open-Xchange logo and PowerDNS logo are trademarks or registered trademarks of Open-Xchange AG. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

CONTENTS

1	1.1	Steps with ZoneControl Main window Adding a zone	1 1 2
2	Editi 2.1 2.2 2.3 2.4 2.5 2.6	ng Zones Zone details page	5 8 9 10
3	Sche	duled Tasks	17
4	Zone	e Templates	19
5	Glos	sary	21
нт	TP Ro	outing Table	23
Ind	dex		25

CHAPTER

ONE

FIRST STEPS WITH ZONECONTROL

ZoneControl is a web-based tool that facilitates the editing of DNS domains, known as "zones". It also supports modifying secondary notification settings, AXFR settings and enabling DNSSEC on these zones.

1.1 Main window

After logging in, the main screen is presented.

POWERDNS	Zone Control		Add Zone Reload	1 admin .
Y		2		3
Zone	Kind	Serial	Server	Actions
catalog.example.	Producer (Primary)	1710857408 🛧	auth0	E 2 0
catalog.example. read-only	Consumer (Secondary)	1710857408	auth1	i≣ ^ 1
catalog.example. read-only	Consumer (Secondary)	1710857408	auth2	4 5 -6
cryptokeys.org.	Primary	2009071301 💠	auth0	i≡ <u>2</u> û
cryptokeys.org. read-only	Secondary	2009071301	auth1	i≣ <u>₹</u>

Fig. 1.1: The main window of ZoneControl.

This window lists all the zones on all the servers. Each zone line consists of the following elements:

Name shows the full name of the zone. An additional label indicates it is read-only.

Kind is one of "primary", "secondary", "native", "producer" or "consumer" (the last two only when catalog zone support has been enabled). A "secondary" or "consumer" zone cannot be modified, as its data is retrieved from a primary server. A "primary" or "producer" zone can be edited and is generally distributed to other DNS servers that serve as secondaries or consumers. The "native" zone kind indicates data replication is not done via DNS-based replication, but via another mechanism, like database level replication.

The **Serial** is the serial number in the *SOA* record of this zone. This number is used by "secondary" servers to check if their copy of the DNS data is still up to date. On "primary" zones – and "secondary" zones that are configured to send notifications – a cloud shaped icon is shown. A blue icon indicates that the serial number for which a notification was sent does not match the current serial number. A notification will be sent at a later moment (the exact time depends on the DNS server configuration), at which point the icon will turn green.

In the **DNSSEC** field, a label is present if this zone is DNSSEC secured.

The **Server** field shows the server on which this zone resides. A zone with the same name can be on multiple servers, for instance as a "primary" on one, and as a "secondary" on many others.

The **Actions** field has several buttons for quick access to some actions for the zone. These buttons are:

- 4 History. Shows the history of all changes made to records in this zone.
- **5** Export. Exports the zone to a *zonefile* format. (*only shown when the user does not have RRSet limits*)
- 6 Delete. Deletes the zone from the server.

When more than 25 records exists, the list is paginated. The page-controls are at the bottom of the list and the hotkeys *ctrl+f* and *ctrl+b* can be used to go a page forward or backward, respectively.

Above the list of zones, several other fields and buttons are visible.

Number 1 is the search field. This can be used to filter the list of zones.

Clicking on **2** shows a dialog to add a new zone. This dialog is explained in another chapter.

The username is displayed at **3**. Clicking the username will open a menu with several options, depending on the user's permissions. This menu also contains the logout button.

1.2 Adding a zone

OWERDNS

When clicking on the "Add zone" button in the main screen of ZoneControl, the "Add new zone" dialog window is shown. This dialog window has all the fields required to add a new zone.

To add a zone, first select a server where this zone shall live (1). Then fill in the zone name at 2, with a trailing dot. Select the kind of zone this is at 4. Depending on the type of zone, one of two things will need to be filled in at 5.

Instead of filling in the details above it is also possible to select a template at **3**. Please see *Zone Templates* for more information.

For native and primary zones, fill in the *NS records* for this zone (with trailing dots).

Note:

No corresponding secondary zones are created on the specified servers, these need to be added manually.

For a secondary zone, fill in the IP address(es) of the primary server(s) for this zone.

After clicking the "Add" button (**6**), the data in this dialog is checked. If there are any input errors, they will be displayed in within this dialog. After the zone is added, the zone will appear in the *main window*'s zone list.

Once added, a secondary zone will be retrieved from its primary, and a primary zone will send out notifications to its (potential) secondary servers.

	. 1
Add new zone	×
Server	
Server	h
	נ
Zone Name	
somezone.example.com.	ן ן
Template(optional)	es
Zone name	
Native	
O Primary	
○ Secondary	
Catalog Zones	
○ Producer (Primary)	
⊖ Consumer (Secondary)	
Name servers to use in NS records (one per line, must be a fully qualified domain name ending in a dot)	
ns1.example.com.	
ns2.example.com.	
	đ
5	_
Cancel Add	

Fig. 1.2: The "Add zone" dialog window.

CHAPTER

TWO

EDITING ZONES

Editing zone contents is done in the zone details page, which is openend by clicking on the name of a zone in the *main window*.

2.1 Zone details page

POWERDNS Zone	Control 2	3	4 5 Add Record Reload	1 admin -
	DNSSEC disabled	Primary	. Export I≣ History	
Ŧ 6				
Member of catalog.example. producer ca	italog.			
Name	Туре	TTL	Records	
example.com.	SOA	1D 3H 46M 40	primary ns1.example.com. email ahu.example.com. serial 2847484148 refresh 8H retry 2H expire 1W negative 1D	+ /
example.com.	NS	2M	ns2.example.com. +-	- /
example.com.	MX	2M	15 smtp-servers.test.com. + 10 smtp-servers.example.com.	- /
∟_imaptcp.example.com.	SRV	2M	0 1 143 blah.test.com. +	- 🖉
cname-to-insecure.example.com.	CNAME	2M	www.insecure.dnssec-parent.com.	- 🖉
double.example.com.	А	2M	192.168.5.1 192.168.5.1	- /

Fig. 2.1: The zone details screen of ZoneControl.

This page lists all the DNS records in the zone in a table.

11 shows which catalog ("Producer") this zone is part of. If the zone is not part of a catalog this element will not be shown.

Each row has the following elements:

Name (**7**) shows the exact name of this record. It is *fully qualified*, which means that it includes the parent zone's name.

The **Type** field shows the type of the record.

TTL: The Time to Live value of this record, shown in a shorthand if possible. Possible value suffixes for this shorthand are: 'H' for 'Hours', 'M' for 'Minutes', 'D' for 'Days' and 'W' for 'Weeks'. If no unit is present, the value is given in seconds.

The **Records** column shows the record's data for **Name** and **Type** and contains several buttons to manipulate this record. **8** is a shortcut for **1** and opens the *New record* dialog window with the current domain prefilled. Pressing **9** slates the record for deletion and **10** opens the *Edit record* dialog. When the logged-in user's permissions are insufficient, or when the zone cannot be edited (e.g. because it is a secondary zone), these buttons are not visible.

When more than 200 records exists, the list is paginated. The page-controls are at the bottom of the records and the hotkeys *ctrl+f* and *ctrl+b* can be used to go a page forward or backbrad, respectively.

DNSSEC disabled

Fig. 2.2: The DNSSEC button when DNSSEC is disabled for this zone.

At the top of this window, next to the zone name, several buttons provide additional information about the zone. These buttons can be clicked to open a dialog window with relevant configuration items.

2 shows the DNSSEC state of the zone. It is green when DNSSEC is enabled and white when it is disabled. Clicking this button opens the *DNSSEC dialog* window.



Fig. 2.3: Native and Secondary zone buttons. The Primary zone button is not shown here.

The zone kind button (**3**) shows what kind of the zone this is. This is one of *primary*, *secondary* or *native*. Clicking this button opens the *Zone kind dialog* window.

Clicking the Export button (4) generates an export of the zone in *zone file* format. (*this button is **not shown** when the user has RRSet limits)* Your browser will offer to download this file.

The History button opens the zone history window, where all the past changes to this zone are listed, with the latest changes on top. This view can also be used to restore a previous version of the zone if necessary.



Fig. 2.4: The Save changes button.

Any changes made to the zone in this window are not directly sent to the PowerDNS Authoritative Server, but kept within the browser. When there are pending changes, a button appears at the top of the window displaying the number of pending changes. Clicking this button opens the "Confirm Save" dialog.

Note: If you close the browser window without saving, your pending changes will be lost.

2.1.1 Catalog Zones

POWERDNS**** Zone Control		Add Record	Reload	👤 admin 🗸
catalog.example. zone DNSSEC disabled Producer	Z Export I≣ History		? for k	eyboard shortcuts
Y zz1				
Catalog Records				
Member Zones				
zz10.example.com.				-
zz11.example.com.				-
zz12.example.com.				-
zz13.example.com.				-
Candidate Zones	Catalog			
zz1.example.com.	none			+
zz14.example.com.	none			+
zz15.example.com.	none			+
zz16.example.com.	none			+
zz17.example.com.	none			+
zz18.example.com.	none			+
zz19.example.com.	none			+
zz100.example.com.	none			+

Fig. 2.5: The catalog editing section of a Producer zone.

The zone page of a Producer zone has one extra element compared to other zone kinds: the "Catalog" tab. Inside this element zones can be added and removed from the Producer's catalog. The [+] button will add a candidate zone to the catalog and the [-] button will remove a member zone from the catalog.

The "Records" tab shows the zone's records similar to other zone kinds.

Both the "Member Zones" and the "Candidate Zones" lists support pagination and filtering.

The "Candidate Zones" also has a "Catalog" column showing whether a candidate is already part of another catalog. *A zone can only be part of a single catalog.*

Not shown here but member zone screens have a little extra element showing which catalog zone they are part of.

2.2 Adding a new record

When adding a new record, several pieces of information need to be filled in.

Field **1** contains the name of the record. The name on the record must always be relative to the zone, as alluded to in the dialog. Leaving this field empty creates a record at the top of the zone.

The selector at **2** specifies the type of record that will be added. The buttons to the right of this field are shortcuts to frequently used DNS types.

The TTL field (**3**) sets the Time to Live for this record. This field accepts a number of seconds, or a shorthand notation like "10M" for a 10 minute (600 second) TTL. To the right you will find several shortcuts for frequently used TTLs.

Note: In DNS, the TTL applies to the *record set*, not to a single record.

New record					×		
Name [1]			.p	owerd	ns.com.		
Type [2] A AAAA CNAME	TXT	MX	HT	TP Re	direct		
TTL [3] M=minutes, H=hours, D=days, W=weeks	5M	1H	4H	1D	1W		
Records (one per line, prefix with # or ; to disable) [4]							
Schedule changes [5]							
<pre>cmd/ctrl + s to save, esc to cancel</pre>			Car	ncel	ОК		

Fig. 2.6: The New Record dialog window.

The Records field at **4** is used to input the contents of the record(s), one item per line. You can prefix individual records with ; to disable them, in which case they will not be server by the DNS server.

Note: Disabled records will be validated on save, just like active records. You cannot use this for adding arbitrary comments.

When adding IPv4 and IPv6 addresses (A and AAAA records), the IP addresses can be suffixed with a * to indicate a PTR ("reverse") record should be created for this address.

Note: On save, the server will check if a zone exists to store the PTR. If none exists, the whole save transaction is aborted.

Check the box at **5** to schedule this change for the future. See the chapter on scheduled changes for more information.

Upon clicking the "OK" button, the new record is added to the pending changes.

2.3 Editing a record

After clicking the edit button (**10** in Fig. 2.1), the Edit record dialog is opened.

Editing demo2.powerdns.com. A					×			
The A record contains an IP address. It is stored as a decimal dotted quad string, for example: 203.0.113.210.								
TTL								
1H [1]	5M	1H	4H	1D	1W			
M=minutes, H=hours, D=days, W=weeks								
Records (one per line, prefix with # or ; to disabl	e)							
198.199.127.127								
[2]								
Schedule changes [3]								
[cmd/ctrl] + [s] to save, [esc] to cancel								
			Car	icel	OK			
	_	_	_	_				

Fig. 2.7: The Edit record dialog window.

This dialog is a stripped-down version of the *New record* dialog. The name and type of the record are fixed and shown in the header of the dialog.

The TTL field (**1**) sets the Time to Live for this record. The field accepts a number of seconds, or a shorthand notation like "10M" for a 10 minute (600 second) TTL. To the right you will find several shortcuts for frequently used TTLs.

Note: In DNS, the TTL is per *record set*, not per single record.

The Records field at **2** is used to edit the contents of the record(s), one item per line.

Check the box at **3** to schedule this change for the future. See the chapter on scheduled changes for more information.

2.4 Saving pending changes

When editing, adding or deleting records, changes are not immediately saved to the DNS Server. Instead, these are 'staged' inside ZoneControl.

2.5 Changing DNSSEC settings

Pressing the DNSSEC button (**2** in Fig. 2.1 or Fig. 2.2 when DNSSEC is disabled) opens the DNSSEC dialog.

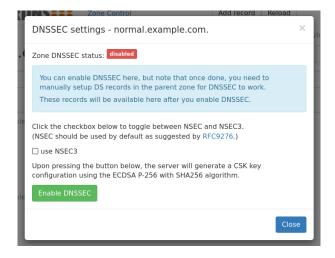


Fig. 2.8: The DNSSEC dialog for an unsecured zone.

By default NSEC will be used for DNSSEC. Checking the "use NSEC3" box will show an expanded dialog where one can edit the NSEC3PARAM.

DNSSEC settings - normal.example.com.	×				
Zone DNSSEC status: disabled					
You can enable DNSSEC here, but note that once done, you need to manually setup DS records in the parent zone for DNSSEC to work. These records will be available here after you enable DNSSEC.					
Click the checkbox below to toggle between NSEC and NSEC3. (NSEC should be used by default as suggested by RFC9276.)					
▼ use NSEC3 NSEC3PARAM 100-					
The default NSEC3PARAM as suggested by RFC9276 is 1 0 0 - NSEC3PARAM has the following format: hash-algorithm flags iterations salt and the following conditions: • hash-algorithm: must be 1 • flags: must be either 0 or 1 (suggested: 0) • iterations: must be between 0 and 65535 (suggested: 0) • salt: must be either - or an even number of hex digits (no more than 254!) from the following group 1234567890ABCDEFabcdef Please see RFC5155 for more detailed information.					
Upon pressing the button below, the server will generate a CSK key configuration using the ECDSA P-256 with SHA256 algorithm.					
I	Close				

Fig. 2.9: The DNSSEC dialog for an unsecured zone with expanded NSEC3 settings.

Clicking the "Enable DNSSEC" button will enable DNSSEC for the zone. This adds cryptographic keys based on the settings of the PowerDNS Authoritative Server.

On a DNSSEC secured zone, the dialog displays the DNSSEC information that can be uploaded to the zone's *registry* (see Fig. 2.10 for an example).

Note: Both the DS records and DNSKEY record are shown. Which of these need to be uploaded depends on the domains's *registry*. Some registries require the DNSKEY to generate the DS records themselves.

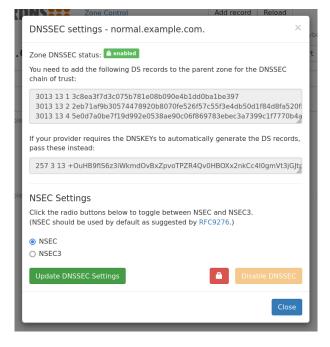


Fig. 2.10: The DNSSEC dialog for a secured zone.

This dialog can also be used to update the DNSSEC settings or to disable DNSSEC. As part of updating the DNSSEC settings it is possible to switch between NSEC and NSEC3 (the cryptokeys will be kept). Clicking the NSEC3 radio button will show the expanded NSEC3 settings similar to those in Fig. 2.9.

It is possible to disable DNSSEC here but be very careful with this (as shown in Fig. 2.11) as we do not have backup functionality in place in this version of ZoneControl. The "Disable DNSSEC" button will be disabled until one enables it by pressing the red lock / unlock button.

The "Disable DNSSEC" button can be disabled again by pressing the, now green, lock button.





Fig. 2.11: The DNSSEC dialog with an unlocked "Disable DNSSEC" button

2.6 Zone settings

Clicking the Zone Kind button (**3** in Fig. 2.1 or Fig. 2.3) opens the Zone Settings dialog window. The options available in this dialog depend on the zone kind.

2.6.1 Native zones

Native zones have the fewest settings, as there are no settings required for data replication.

Zone Settings - foo.example.com.								
This is a Native zone. Native zones within PowerDNS do not use traditional Primary- Secondary AXFR transfers, but instead sync with a mechanism native to the underlying database system. Native zones will not send out DNS notifications to other servers when a change occurs.								
Settings	Settings Actions							
Convert zone Convert into a Primary zone								
		Cancel Sav	_					
		Caricei						

Fig. 2.12: The Zone settings dialog window for a native zone with an active Actions tab.

Long Gormon	7160 1	00010						
Zone Settings - foo.example.com.								
This is a Native zone. Native zones within PowerDNS do not use traditional Primary- Secondary AXFR transfers, but instead sync with a mechanism native to the underlying database system. Native zones will not send out DNS notifications to other servers when a change occurs.								
Settings	Actions							
Allow AXFR	zone transfer requests from	_						
10.0.0.3 or	10.0.0.0/8 or ::1 or 2001:db8:1::/64							
One IP or subnet per line 2 Cancel Sa								

Fig. 2.13: The Zone settings dialog window for a native zone with an active Settings tab.

The button at **1** converts the zone from a *native* zone to a *primary* zone. (Zone conversion to a Producer zone is not available.)

Note: Changing from a native zone to a primary zone might require extra configuration in the PowerDNS Authoritative Server. For instance, the primary configuration setting will need to be enabled before notifications are sent.

As it is possible for native zones to be replicated via *AXFR*, the field at **2** allows configuration of IP addresses that may transfer this zone.

2.6.2 Primary zones

For *primary* zones, the dialog in Fig. 2.14 is displayed:

Zone Setti	ngs - power	dnssec.org.		×				
This is a Primary zone. Primary zones hold the authoritive DNS entries for a zone, and usually notify Secondary zones of changes to its entries, so that a Secondary can fetch new zone through an AXFR transfer.								
Settings	Actions							
Convert ze	one		Convert into a Native zone					
Queue no	tifications to s	econdaries	Queue NOTIFY messages					
			Cancel Sav	/e				

Fig. 2.14: The Zone settings dialog window for a primary zone with an active Actions tab.

Zone Contion	Audi	necora
Zone Sett	ings - powerdnssec.org.	×
usually notify	mary zone. Primary zones hold the authoritive DNS entries for a zone, and Secondary zones of changes to its entries, so that a Secondary can fetch ough an AXFR transfer.	the
Settings	Actions	
Allow AXFR	zone transfer requests from	
10.0.0.3 or	10.0.0/8 or ::1 or 2001:db8:1::/64	
One IP or subm	et per line. These servers of changes	
10.0.0.3 or	10.0.0.3:5353 or ::1 or [2001:db8:1::1]:53	
In addition to n	ameservers defined in the VS records. One IP per line, with optional port number.	
	Cancel Sa	ve

Fig. 2.15: The Zone settings dialog window for a primary zone with an active Settings tab.

The button at **1** converts the zone into a *native* zone. (Zone conversion is not available for Producer zones.)

Note: Converting into a native zone will make the PowerDNS Authoritative Server stop sending notifications for zone updates. It will still allow zone-transfers.

In field **2**, IP addresses that are allowed to transfer the zone can be specified.

The IP adresses entered in the field at **3** will be notified when the zone has been changed, *in addition* to all the servers specified in the zone's NS records.

2.6.3 Secondary zones

The *secondary* zone dialog is show in Fig. 2.16.

Zone Sett	ings - cryptokeys.org.	×		
entries from a	condary zone. Secondary zones cannot be edited directly. They receive their a Primary server through an AXFR transfer, usually after getting notified of they will also check primaries according to the refresh interval set in the	r		
Settings	Actions			
Primaries to sync from				
172.18.0.3				
One IP per line, with optional port number 2				
Allow AXFR	zone transfer arests from			
10.0.0.3 or	10.0.0.0/8 or ::1 or 2001:db8:1::/64			
One IP or subnet per line.				
Also notify t	hese servere senanges			
10.0.0.3 or 10.0.0.3:5353 or ::1 or [2001:db8:1::1]:53				
In addition to n	ameservers defined in the NS records. One IP per line, with optional port number.	.10)		
	Cancel Sav	e		

Fig. 2.16: The Zone Settings dialog window for a secondary zone.

The field at **1** is used specify the IP addresses of the primary(s) of this zone. These addresses can be suffixed with a port, should be it different from the default of '53'.

Note: When adding a port to an IPv6 address, the address part must be wrapped in square brackets to disambiguate the address from the port:

[2001:0DB8:AA::1]:5300

If this server is also a primary for other secondaries, the other two fields can contain relevant settings.

In the field at **2**, IP addresses that are allowed to transfer the zone can be added.

The IP adresses entered in the field at **3** will additionally be notified when the zone has been changed. By default all servers in the zone's NS records are notified of changes.



CHAPTER

THREE

SCHEDULED TASKS

TBD

CHAPTER

FOUR

ZONE TEMPLATES

To simplify adding new zones it is possible to create "template zones". These are zones whose zone contents and metadata are used for the newly created zone.

Note: DNSSEC settings are **not** copied.

A template zone is created just like any other zone except its name should end in .template. as shown in the "Template" input in Fig. 4.1.

Add new zone	×
Server	
auth1	*
Zone Name	
use-a-template.example.	
Template (optional)	List all zones
default.template. (auth0)	Å.
	Cancel

Fig. 4.1: The "Add new zone" dialog showing template zones.

It is also possible to use any existing ("real") zone as template. When the "List all zones" box is checked all available zones will be shown to use as a template. See Fig. 4.2.

Add new zone	×
Server	
auth1	*
Zone Name	
use-a-template.example.	
Tomplate (antional)	list all zonas
✓ 1.zones.example. (auth1)	\$
10.zones.example. (auth1)	رر
11.zones.example. (auth1)	
12.zones.example. (auth1)	
13.zones.example. (auth1)	
14.zones.example. (auth1)	
15.zones.example. (auth1)	

Fig. 4.2: The "Add new zone" dialog showing all zones as template candidates.

CHAPTER

FIVE

GLOSSARY

Many terms in this document are specific to the DNS. This glossary contains short explanations of these terms. For more information, **RFC 7719** (DNS Terminology) can be consulted.

AXFR

The query type used to request a full zone transfer. Commonly used to refer to the act of transferring a zone.

fqdn

A Fully Qualified Domain Name is a domain name that specifies its exact location in the DNS hierarchy.

primary

primary server

A "primary" zone (or server) acts as a source of truth for a zone. *secondary* servers will check at the primary server if their zones are still up to date.

native

A "native" zone does not used DNS-based data replication but for instance database replication.

NS record

NS records in a zone declare the name of the nameservers authoritative for that zone.

record set

RRSet

A record set is the collection of DNS records with the same name, type and TTL.

registry

The organization that allows registration of names in the zone. These organization operate the *TLDs*. For .nl this is SIDN and for .com this Verisign

secondary

secondary zone

A "secondary" zone (or server) retrieves its zone data from a *primary* server.

SOA record

SOA

Only one "Start Of Authority" record exists in a zone. It indicates that this domain is indeed a zone.

TLD

Top Level Doman

A Top-Level Domain is a a zone that is one layer below the root, such as .nl and .com.

Zone file

Zonefile

The de-facto storage format for DNS zones. This format is text-based and lists all records in a zone, one per line.

HTTP ROUTING TABLE

/api

GET /api/v1/servers/{server_id}/zones/{zone_id}/_history,

??

- GET /api/zonecontrol/info,??

- POST /api/zonecontrol/login,??
- DELETE /api/v1/servers/{server_id}/zones/{zone_id}/_names/{name}/_comments/{rrtype}/_comment/{comment ??

INDEX

A axfr, **21**

F fqdn, **21**

Ν

native, <mark>21</mark> NS record, **21**

Ρ

primary, <mark>21</mark> primary server, <mark>21</mark>

R

record set, 21 registry, 21 RFC RFC 7719, 21 RRSet, 21

S

secondary, 21 secondary zone, 21 SOA, 21 SOA record, 21

Т

TLD, **21** Top Level Doman, **21**

Ζ

Zone file, <mark>21</mark> Zonefile, <mark>21</mark>