phoenixNAP Client Portal

DNS Management

Disclaimer

Please be aware that DNS management can be a confusing and complicated system. If you get something wrong, you might experience problems such as bouncing emails sent to your domain, or even cause your domain's website to malfunction. We recommend you use the DNS manager with caution, and ONLY if you understand at least the basic concepts in DNS management. PhoenixNAP, LLC does not assume liability for any damages you may suffer or costs you may incur as a result of manipulating your DNS settings via the PNCP DNS Manager.

Table of Contents

Introduction

Welcome to the phoenixNAP Client Portal DNS Management user guide!

The *Forward DNS / Reverse DNS* feature is a powerful, yet simple, tool for managing your domains and DNS records via the Client Portal. Paired with Client Portal's other features, such as the Load Balancer and IP Management, and with full support for IPv6, you will use PNCP as a one stop shop for all your IT business needs.
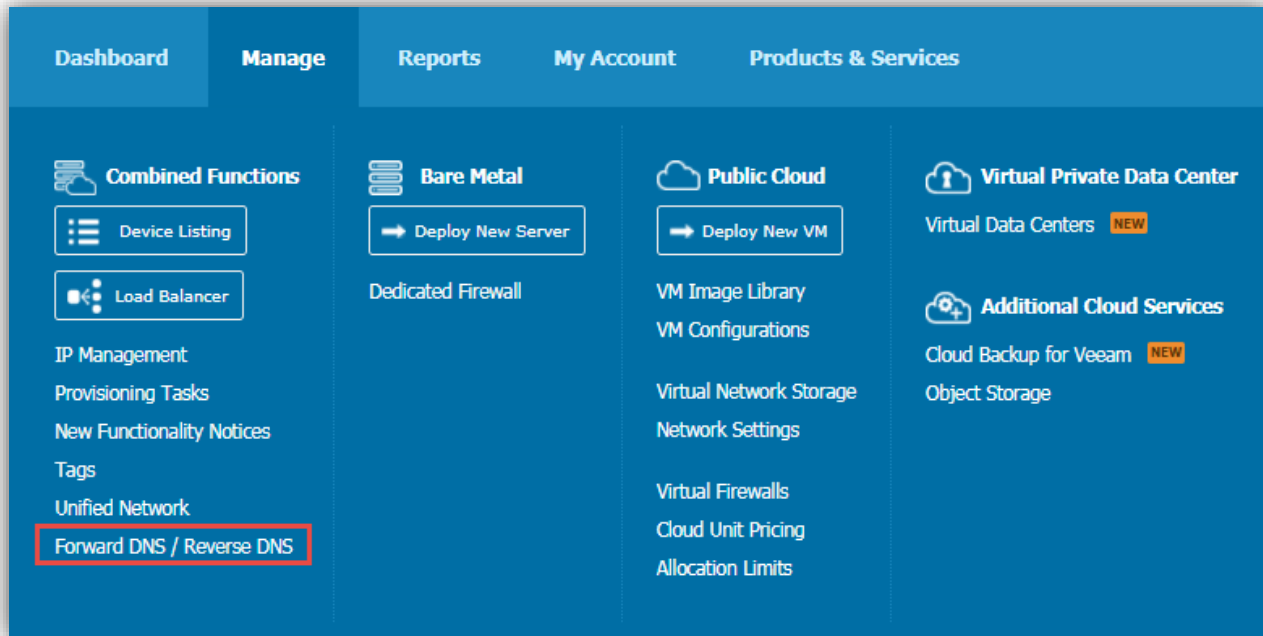
Forward / Reverse Domain Name System (DNS)

What is the difference?

Forward DNS

A forward DNS lookup will, when supplied with a domain name (for example google.com), return the IP address for the supplied domain. When you access Google, a DNS server is looking in its forward lookup zone for the IP address(es) of the site, and then returning them to you. This type of record is an A record, and is the most common one. A forward DNS lookup can contain other records, such as MX, C-Name, etc.

Reverse DNS

A reverse DNS lookup is used to lookup the domain name for a supplied IP address. You normally supply the IP address backwards and append .in-addr.arpa (more info at

phoenixNAP Client Portal
DNS Management

https://en.wikipedia.org/wiki/.arpa). This can be a useful feature to anyone, but it is particularly practical for those running an outgoing mail server.

A good tool for finding rDNS or normal DNS records is **dig**.

How to reach the DNS screen in the phoenixNAP Client Portal?

1. **Sign in** to the Client Portal.
2. Open the **Manage** mega menu.
3. Click **Forward DNS / Reverse DNS** under the *Combined Functions* heading.

| My Domains | Forward DNS Records | Reverse DNS Records |

Domain Name Listing

Add Domain Name/s   Search my Domains   ✖

⇅ Verified Status	⇅ Domain Name	⇅ Added On	Manage
✖	blbbababa.com	Aug/22/2016	Actions
✖	dingo.com	Aug/22/2016	Actions
✖	md.net	Mar/09/2017	Actions
✖	random123412351.com	Aug/22/2016	Actions
✖	random123413412.com	Aug/22/2016	Actions
✖	random21424312431.com	Aug/22/2016	Actions
✖	random23462352345.com	Aug/22/2016	Actions
✖	random235623542354.com	Aug/22/2016	Actions
✖	random235q23452345.com	Aug/22/2016	Actions
✖	random262462354.com	Aug/22/2016	Actions

phoenixNAP • 1.855.330.1509 • Email Support

How to add a domain name?

1. Open the **Forward DNS / Reverse DNS** screen.
2. Click **Add Domain Name/s.**
3. **Copy/paste** or manually enter domain name/s (use a comma to separate multiple entries).

NOTE: Identical domain entries will be ignored.

4. When you are finished adding domain names, click **Add.**

> **Verification**: All Domain Name Ownership must be verified! The names may not be published until this is completed. Find more information on this topic in the Domain Verification section of the help guide.

Domain Name Listing

The Domain Name Listing offers the following information:

1. **Verified Status**. This will show you if the domain has been verified or not.

   ❖ **Not Verified**. The Verification process has not begun yet. Please begin the verification process by choosing **Actions** > **Verify**. A verification email will be sent to you, the domain owner. Alternatively, complete the process via DNS String. Update your TXT record with the string provided. Once complete, click the **Actions > Verify** link to complete process. Click *Yes, I updated my Registrar*.

   ❖ **Warning**. This occurs after a domain has been verified for ownership and the system starts checking for NS entries at their registrar. If this fails, a warning status will appear. Update your NS entries to point to phoenixNAP's name servers. Once complete, click the **Actions > Resolve** link to complete the NS related entry process. Click *Yes, I updated my Registrar*.

   ❖ **Verified**. The Verification process has been completed successfully and the NS records at your registrar have been updated to point to our name serves.

2. **Domain Name**.
3. **Added On**. Date of adding the domain.
4. **Manage**. Click on the **Actions** icon to open a drop-down menu with the following options:

   ❖ **Modify**. ONLY non-verified domain names can be modified. You can modify a domain name as desired. After modifying the name click **Update** to confirm your changes. Be aware that Modified Domain Names must go through the entire Verification Process again.

   ❖ **Resolve**. Update your NS entries to point to phoenixNAP's name servers. Once complete, click the **Actions > Resolve** link to complete the NS related entry process. Click *Yes, I updated my Registrar*.

   ❖ **Delete**. Deletes Domain Name as well as any Forward DNS / Reverse DNS records associated with it. You will be asked to confirm this action.

   ❖ **Verify**. You can reset the verification process ONLY if domain ownership has not been verified yet.

> **NOTE:** Verified Status, Domain Name, and Added On columns are sortable.

Domain Verification

Any time you add a new domain name, you must verify it. An email will be sent to the domain admin (you), and you will need to verify ownership. Identical Domain Names will not be added!

You will receive a verification notice for your domains:

- ❖ **Not Verified**. The Verification process has not begun yet. Please begin the verification process by choosing **Actions** > **Verify**. A verification email will be sent to you, the domain owner. Alternatively, complete the process via DNS String. Update your TXT record with the string provided. Once complete, click the **Actions > Verify** link to complete the process. Click *Yes, I updated my Registrar*.
- ❖ **Warning**. This occurs after a domain has been verified for ownership and the system starts checking for NS entries at their registrar. If this fails, a warning status will appear. Update your NS entries to point to phoenixNAP's name servers. Once complete, click the **Actions** > **Resolve** link to complete the NS related entry process. Click *Yes, I updated my Registrar*.
- ❖ **Verified**. The Verification process has been completed successfully and the NS records at your registrar have been updated to point to our name servers.

Domain Verification is a two-step procedure:

1. Verify domain ownership, either via Email or via DNS String. Begin the verification process by selecting **Actions** > **Verify**.
2. Configure your Name Server (NS) Records to point to our phoenixNAP servers.

- ❖ ns2.phoenixnap.com
- ❖ ns1.phoenixnap.com

Verifying Ownership

> **EXPIRED DOMAINS:** Before verifying an expired domain, you must contact your current registrar for renewal instructions. After renewing the domain, you may start the verification process as you normally would.
>
> **IMPORTANT NOTE:** If you do not renew your domain name, you risk losing it!

Verifying Ownership via Email

An email will be sent to you with a link to verify the domain. Simply click on the link and follow the instructions.

If you didn't get the email, click the *Resend the Email* link on the Verify Domain Name (via Email) window, or opt for the Alternative Method (via DNS String).

Verifying Ownership via DNS String

If you didn't receive an email:

1. Select **Actions** > **Verify** again.
2. Select **Alternative Method**.
3. Click **Generate Verification String**. You will be required to verify the domain by entering a unique string as a TXT record with your registrar. You must use the string that we provide.
4. **Copy** the string.
5. Go to your domain name's registered registrar.
6. Enter the string as a TXT record.
7. Once you have updated your registrar, return to the phoenixNAP Client Portal and select **Actions** > **Verify** again – but this time select the *Yes, I updated my Registrar* link that indicates you completed this task.

> **NOTE:** This alternative option is always available to use if you prefer, even if an email was sent to you. If there is an error in the verification process, you will be notified.

Updating Your NS Records

> **IMPORTANT NOTE:** This is the second step, and updating your NS records is necessary to finish the verification process, as it connects our system to your domain. Only after both steps have been completed can you control your DNS via the phoenixNAP DNS manager.

Once domain ownership is verified, (either via email or string) you must continue to the **next step** and **update your NS records** at your registrar to point to the NS servers that are presented to you.

1. Go to your domain name's registered registrar.

2. Create two NS records:

   - ❖ ns1.phoenixnap.com
   - ❖ ns2.phoenixnap.com

3. Once you have updated your registrar, return to the phoenixNAP Client Portal and select **Actions** > **Verify** again – but this time select the *Yes, I updated my Registrar* link that indicates you completed this task.

   You should receive a confirmation message stating that the NS Record has been verified. You can publish your domain.

> **NOTE:** Keep in mind that it can take anywhere between 24h to 48h for the DNS manager to process domain verification. It depends on the root domain controller of the domain which will require the wait for the NS changes to be propagated. For example, for a *.com* domain the change to the NS records would need to be executed across the .com name servers.
>
> If you are experiencing difficulties, please contact Support which is at your disposal 24/7. When necessary, we can manually verify your domain in phoenixNAP's system.

Forward DNS Mappings

1. Open the **Manage** mega menu.

2. Click **Forward DNS / Reverse DNS** under the Combined Functions heading.

3. Click the **Forward DNS Records** tab.

Forward DNS Records List

By default the Forward DNS Records list will show all records. Use the **Search field** to narrow down the result. Know that **Verified Status, Domain,** and **Record Type** columns are sortable.

Available Actions

There are three (3) available actions:

1. **Add Forward DNS.** Click **Add Forward DNS,** located above the list to add a new forward DNS record. A popup menu will open:

   ❖ Select a domain from your domain list.
   ❖ Select DNS Record Type. For further information about DNS Record types follow this [link](#).
   ❖ Enter DNS Record Details:

      a) **Name.** You manually enter name as desired.

      b) **Record type-specific options.** Different type of DNS Records will provide various record-specific options. See the **Supported Forward DNS Record Types and Their Respective Record Values** section below.

      c) **DNS Time to Live Value.** Enter a value in the appropriate field and select a time unit from the drop-down menu.

Under the Manage column you will find two links:

1. **Actions.**

   ❖ **Delete.** Deleting a DNS record will delete all associated Forward DNS records.
   ❖ **Modify.** Click this link to modify an existing Forward DNS record.

2. **More Details.** Open the **More Details** link in order to get a list of all the external details that are not listed in the table.

   Supported Forward DNS Record Types and Their Respective Record Values

   You can add eight (8) different types of DNS records:

1. **A/AAAA Address (Host) Record.** These records specify the IP address (IPv4 or IPv6) for a given host and points to that IP address. Useful to use if you have sub-domains residing on various systems.

❖ **Name**. A record name is composed of a series of parts called labels delimited with dots '.'. Each label can contain up to 63 characters. The entire record name must not exceed 253 ASCII character length.

❖ **IP Address (v4/v6) or Add IP**. Enter an IP address of the FQDN. A valid IP address consists of a four octet 32-bit address. Use a comma to separate multiple entries. If you choose the **Add IP** option, specify **Node, Device**, and **IP**.

❖ **Select Pointer (PTR) Record Creation**.

   a) **Create PTR Records**. PTR Records created if there are no existing records associated to the IP Addresses added.

   b) **Always Create PTR Records**. PTR Records created regardless of existing records associated to the IP Addresses added.

   c) **Do Not Create PTR Records**.

❖ **TTL**. The DNS Time to Live must be greater than 0 and must not exceed 2,147,483,647 seconds.

Example Domain:	domain.com
Sample Format:	IN A 69.9.64.11
Where:	1. IN indicates Internet
	2. A indicates record type
	3. 69.9.64.11 indicates the IP address of domain.com

2. **CNAME (Canonical Name Record)**. Use to make domains and sub-domains an alias of another domain. It ties a host name to an A record. With a CNAME record, instead of making several A records, you can create one record and point them to one A record. The advantage of this approach is that when you need to change the IP address, all you need to do is change the A record's IP address.

❖ **Name**. A record name is composed of a series of parts called labels delimited with dots '.'. Each label can contain up to 63 characters (a-z, A-Z, 0-9 and hyphens '-'). Labels may not start or end with a hyphen. The entire record name must not exceed 253 ASCII character length.

❖ **Alias**. Enter a domain to be tied to an A record.

❖ **TTL**. The DNS Time to Live must be greater than 0 and must not exceed 2,147,483,647 seconds.

Example Domain:	mail.something.com
Sample Format:	IN CNAME mail.something.net
Where:	1. IN indicates Internet
	2. CNAME indicates record type

3. **MX (Mail Exchanger Record).** Use to specify to which mail servers should emails be routed to. The MX DNS record needs a priority value as a part of its entry - it sets the priority of a target host.

   ❖ **Name.** The Record Name must be composed of a series of parts called labels delimited with dots '.'. Each label can contain up to 63 characters. The entire record name must not exceed 253 ASCII character length.

   ❖ **Mail Exchange Server**. Enter mail server name.

   ❖ **Priority**. Enter a numerical value between 0 and 65535 indicating the priority level assigned to a server. Lower value means that a server is more preferred.

   ❖ **TTL**. The DNS Time to Live must be greater than 0 and must not exceed 2,147,483,647 seconds.

Example Domain:	thisdomain.com
Sample Format:	thisdomain.com. 14400 IN MX 0 thisdomain.com.
	1. This record shows that all mail @ thisdomain.com should be routed to the mail server at thisdomain.com.
	2. The number zero (0) indicates the priority level.
	3. Make sure that there is a dot at the end of the domain name in the MX record. If the dot is absent, emails are routed to "thisdomain.com.thisdomain.com".

4. **TXT (Text Record).** Use to insert any text-based information that can be called upon when necessary. Most commonly it is used to verify domain ownership and is used to implement SPF.

   ❖ **Name**. The entire record name must not exceed 253 ASCII character length.

   ❖ **Text**. A text-string which is to be passed in to the TXT record. Enter up to 4,000 characters. Apostrophes and dollar symbols "$" are not allowed.

   ❖ **TTL**. The DNS Time to Live must be greater than 0 and must not exceed 2,147,483,647 seconds.

Example Domain:	Example.com
Sample Format:	example.com. TXT @ "Random text"
Where:	1. TXT indicates record type
	2. @ indicates record name. (In this case it is blank, which is indicated by @.)
	3. "Random text" indicates the arbitrary text entered in the record.

5. **LOC (Location Record)**. Use the LOC record to specify geographical location information of a domain.

   ❖ **Name**. A Record Name must be composed of a series of parts called labels delimited with dots '.'. Each label can contain up to 63 Characters. The entire record name must not exceed 253 ASCII character length.

   ❖ **Geographic Location Text**. Specify a geographical location.

   ❖ **TTL**. The DNS Time to Live must be greater than 0 and must not exceed 2,147,483,647 seconds.

Example Domain:	mydomain.com
Sample Format:	mydomain.com. LOC 52 14 05 N 00 08 50 E 10m
Where:	1. LOC indicates record type
	2. 52 14 05 N 00 08 50 E 10m indicates the geographical location.

6. **NS (Name Server Record)**. Use to specify an authoritative name server for a given host.

   ❖ **Name**. The Record Name must be composed of a series of parts called labels delimited with dots '.'. Each label can contain up to 63 characters. The entire record name must not exceed 253 ASCII character length.

   ❖ **Name Server**. The Name Server is composed of a series of parts called labels delimited with dots '.'. Each label can contain up to 63 characters. The entire value must not exceed 253 ASCII character length. Empty spacing and asterisks "*" are not allowed.

   ❖ **TTL**. The DNS Time to Live must be greater than 0 and must not exceed 2,147,483,647 seconds.

Example Domain:	example.com
Sample Format:	example.com. IN NS ns1.phoenixnap.com.
Where:	1. IN indicates Internet

	2. NS indicates record type
	3. ns1.phoenixnap.com. is the authoritative server for the domain example.com

7. **SPF (Sender Policy Framework Record)**. The values of a SPF record specify what servers are allowed to legitimately use your domain name for the sending of emails. This serves as an email-validation record system designed to detect email spoofing.

   ❖ **Name**. A Record Name must be composed of a series of parts called labels delimited with dots '.'. Each label can contain up to 63 characters. The entire record name must not exceed 253 ASCII character length.

   ❖ **Rule**. Enter up to 4,000 characters. Apostrophes (") are not allowed (e.g. v=spf1 -all).

   ❖ **TTL**. The DNS Time to Live must be greater than 0 and must not exceed 2,147,483,647 seconds.

Example Domain:	Example.com
#1 Sample Format:	mydomain.com. TXT "v=spf1 -all"
Clarification:	This is the simplest possible SPF record. It means the domain example.com never sends mail. This would make sense to have if the domain never sends emails.
#2 Sample Format:	TXT "v=spf1 mx -all"
Clarification:	Designate MX servers, as they do send mail.
#3 Sample Format:	mydomain.com. TXT "v=spf1 mx ptr -all"
Clarification:	This designates all of the hosts whose PTR hostname matches example.com

8. **SRV (Service Locator Record)**. Use this to provide information on available services. For example, given a known domain name, you can define the port and hostname for a given service.

   ❖ **Name**. A Record Name must be composed of a series of parts called labels delimited with dots '.'. Each label can contain up to 63 characters. The entire record name must not exceed 253 ASCII character length.

❖ **Host Name**. The system which receives the service. This Host Name is composed of a series of parts called labels delimited with dots '.'. Each label can contain up to 63 Characters. '*' and empty spacing between characters are forbidden. The entire value must not exceed 253 ASCII character length.

❖ **Priority**. A numerical value between 0 and 65535 indicating the priority level assigned to the host. Lower values give higher priority (zero (0) gives highest priority).

❖ **Weight**. A numerical value between 0 and 1410065407 which is to be used as a load balancing mechanism.

❖ **Port**. Enter a numerical value between 0 and 65535. This is the actual port number of the service in offer.

❖ **TTL**. The DNS Time to Live must be greater than 0 and must not exceed 2,147,483,647 seconds.

Example Domain:	somedomain.com
Sample Format:	_service._proto.name. TTL class SRV priority weight port target.
Where:	1. "service" is the symbolic name of the desired service
	2. "proto" is the transport protocol of the desired service. This is usually TCP or http.
	3. "name" is the domain for which this service is valid. (Ending with a dot.)
	4."TTL" is time to live
	5. "class" is always IN
	6. "priority" indicates the priority level of the target host. Lower value equals greater importance.
	7. "weight" is used when more than one service has same priority. A higher value gives greater importance.
	8. "port" is the port number of the service in question.
	9. "target" The name of the host that will provide this service. Does not have to be in the same zone (domain).

DNS record value specifies where you want to point your record, or in some cases what you want to do with it. These values vary in type, depending on DNS record type.

> **Same as Zone:** Uncheck 'Same as Zone' if name differs from My Domain. If same as zone, "@" will indicate record name.

Time to Live Value (TTL)

For the TTL, enter a numerical value of how long a DNS record will be cached before it needs to be refreshed. The default value for TTL is 3600 seconds, but you can enter any value greater than zero (0) and specify it in seconds, minutes, hours, or days. Any changes you make to the value of a DNS record will take place in the specified time to live period. (e.g. If you make a change to a DNS record and the TTL is set to 600 seconds, it will take that time until the new information is in effect.)

Reverse DNS Mappings

Reverse DNS is a technique in which an IP address is resolved into a domain name.

To reach the Reverse DNS Mappings screen:

1. Open the **Manage** mega menu.
2. Click **Forward DNS / Reverse DNS** under the Combined Functions heading.
3. Click the **Reverse DNS Records** tab.

> **Reverse DNS Records List:** By default the Reverse DNS Records list will show all records. Use the Search field to narrow down the result. Know that the Verified Status, Domain, and IP Address columns are sortable.

Record Type

A **PTR record** is used to perform reverse DNS lookups. A PTR record or pointer record maps an IPv4/v6 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.

For example, www.random-site.com has the IP address 122.0.3.16, but a PTR record maps 16.3.0.122.in-addr.arpa. It is always advisable to have a proper reverse DNS record (PTR) set up for your servers, especially when you are running a mail / smtp server.

Creating PTR Records

Whenever you add an A/AAAA Address (Host) Forward DNS Record, you can create PTR Records.

1. Select a domain.
2. Choose an A/AAAA Address (Host) record.
3. **Enter or add IP addresses**. Use a comma to separate multiple entries.

4. **Select Pointer (PTR) Record Creation.**

   ❖ **Create PTR Records.** (ONLY if there are no PTR records associated to the IP address(es) added.)
   ❖ **Always Create PTR Records.** PTR Records created regardless of existing records associated to the IP addresses added.
   ❖ **Do not Create PTR Records.** PTR records will not be created and you will not have rDNS mappings associated to the IP address(es) added.

Additionally, you can create PTR records on the Reverse DNS page by clicking the **Add Reverse DNS** button. Select an internal or external domain and DNS record details.

> **NOTE**: External Domains will be marked as Unverified. You can always add them on the **My Domains** page in order to manage them in the Client Portal.

When you decide to create PTR records, they will be made available on the Reverse DNS page.

Available Actions

The phoenixNAP Client Portal enables you to modify or delete an existing rDNS record.

To modify an rDNS record:

1. Open the **Forward DNS / Reverse DNS** screen.
2. Click **Reverse DNS Records**.
3. Click **Actions > Modify** under the Manage column. Pay attention to the main three (3) pieces of information:

   ❖ **DNS Record Type.** This will display "PTR Pointer Record".
   ❖ **IP Address (v4/v6).** The IP address(es) associated to the A/AAAA record.
   ❖ **A/AAAA Address (Host) Record.** This displays the A/AAAA Address (Host) Record to which the IP address(es) maps to. Open the drop-down menu to select another A/AAAA Address (Host) Record.

> **Modifying rDNS Records:** Please be aware that you can select only those A/AAAA Address (Host) Records that share the same IP Address.

To delete an rDNS record:

1. Open the **Forward DNS / Reverse DNS** screen.
2. Click **Reverse DNS Records**.
3. Click **Actions > Delete** in the row of the PTR record you want to delete.
4. Click **Delete** to confirm you choice.

Glossary of Common Terms

Name Servers

A name server is a web server that has DNS software installed on it. It is a server that is managed by a web host specifically designated for managing the domain names that are associated with all of the hosting provider's accounts.

Fully Qualified Domain Names (FQDN)

FQDN stands for 'Fully Qualified Domain Name', and is often referred to as an absolute domain name. It means that it consists of the hostname and the domain name (e.g. example.ad.com).

Top-Level Domain Name

A top level domain, often referred to as TLD, is the most general part of the domain (e.g. 'com', 'org', 'edu', 'gov', etc.).

Forward DNS

A forward lookup zone will, when supplied with a domain name (for example google.com), return the IP address for the supplied domain. When you access Google, a DNS server is looking in its forward lookup zone for the IP address(es) of the site, and then returning them to you. This type of record is an A record, and is the most common. A forward lookup zone can contain other records, such as MX, C-Name etc.

Reverse DNS

A reverse lookup zone is used to lookup the domain name when supplied with an IP address. You normally supply the IP address backwards and append .in-addr.arpa (more info at http://en.wikipedia.org/wiki/.arpa).

Domain Verification

Every newly added domain name must be verified for ownership and connected to PNAP's NS records. Only after these two steps have been completed, can the admin manage the domain via the Client Portal.

Time to Live Value (TTL)

The numerical value which tells the system for how long will a DNS record be cached before it is refreshed. The default value for TTL is 3600 seconds, but any value greater than zero (0) may apply. Any changes you make to a DNS record will take place after the specified time to live period.

Priority

Priority is assigned to specific types of DNS records (e.g., MX and SRV). It is a numerical value between 0 and 65535 indicating the priority level assigned to the host. Lower values give higher priority (zero (0) gives highest priority).

Additional Resources

phoenixNAP Client Portal User Manual

https://help.phoenixnap.com/Client+Portal

DNS Management – FAQs

https://help.phoenixnap.com/Client+Portal+FAQ

phoenixNAP Client Portal FAQs

https://help.phoenixnap.com/Client+Portal+FAQ

phoenixNAP Client Portal – Glossary of Terms

https://help.phoenixnap.com/Glossary+of+Terms

phoenixNAP – Hosting FAQs

https://help.phoenixnap.com/Hosting

Network Uptime Guarantee

https://help.phoenixnap.com/Network+Uptime+Guarantee

Security FAQs

https://help.phoenixnap.com/Security

Contact Details

SUPPORT

If you encounter any unforeseen difficulties or need to contact phoenixNAP Support for any other reason, you can do so 24 hours, 365 days a year for your convenience.

- ❖ Toll Free: 1.855.330.1509
- ❖ Phone: 480.646.5362
- ❖ Email: support@phoenixnap.com
- ❖ Live Chat

ONLINE SALES (Bare Metal Servers, Public Cloud)

Monday – Friday

7AM – 7PM UTC -7

- ❖ Toll Free: 1.877.588.5923
- ❖ Existing Customers: customersuccess@phoenixnap.com
- ❖ New Client Inquiry: sales@securedservers.com

BUSINESS SOLUTIONS

(Colocation, Virtual Private Data Center, Managed Private Cloud, Hardware Leasing, Managed Services)

Monday – Friday

8AM – 5PM UTC -7

- ❖ Toll Free: 1.877.588.5918
- ❖ Sales Email: sales@phoenixnap.com