DISCOVERY DNS

# Managed DNS Manual

6 February 2015

This document is provided pursuant to the disclaimer provided on the last page.

## Contact



| | |
|---|---|
| **Name** | Chris Wright |
| **Title** | Chief Technology Officer |
| **Address** | L8, 10 Queens Rd, Melbourne, Vic 3004, Australia |
| **Number** | +61 3 9866 3710 |
| **Email** | chris.wright@ariservices.com |



## Classification

Public

## About DiscoveryDNS

Based on client demand and leveraging over 11 years of experience ARI Registry Services launched DiscoveryDNS. DiscoveryDNS provides a global DNS service to ARI Registry Services' clients around the world.

## About ARI Registry Services

ARI Registry Services, part of the Bombora Technologies group of companies, is driving innovation and the expansion of the Internet through the delivery of world-class domain name Registry Services. With over 11 years of experience, ARI Registry Services is a leading provider of Domain Name Infrastructure Services and DNS Services for generic Top-Level Domain applicants and country code Registry Operators.

We help governments, major brands and entrepreneurs across the globe realise the full potential of the Internet by providing expertise, security and reliability in operating a core Internet infrastructure.

# Contents

# 1 Reseller System

Discovery DNS Reseller system is a wholesale DNS hosting platform designed to be used by Registrars and hosting providers for the provision and management of premium DNS services. It utilises a worldwide anycast network that has been built and tested to scale to 8 million Queries Per-Second. The system makes use of the same infrastructure and expertise that powers over 200 TLDs, including the .au country code TLD.

The DiscoveryDNS Reseller DNS System boasts the following features:

- Standard Compliant Anycast Network
- Web Interface and REST API (with Java toolkit)
- Query Usage Reporting
- Individual and Group Plans
- Reseller Branded Name Servers
- Zone Branded Name Servers
- DNSSEC Signing
- HTTP forwarding
- Email forwarding
- AXFR In Zone Transfer

# 2 Provisioning Interfaces

Two interfaces are available for resellers to use to interact with the system:

- Web Interface (an interface designed to be used by people)
- REST API interface

## 2.1 Web Interface

The Web Interface provides all functionality provided by the API as well as additional functionality. The Web Interface includes the ability to:

- Manage accounts and users
- View name servers and name server interface sets
- Access auditing information
- Access usage information
- View plans
- Manage zones

### Time-based One-time Password Authentication

The Web Interface requires Time-based One-time Password (TOTP) authentication. TOTP authentication provides for a 2nd factor of authentication beyond just your password. The second factor is a constantly changing 6 digit number which you get from your software TOTP device.

Typically a user will use a smartphone like an iPhone or Android phone with a TOTP application such as Google Authenticate. You will be prompted to set up your TOTP authentication device the first time you login to the system.

## 2.2 API Interface

The DiscoveryDNS API protocol is a 'REST like' protocol that operates over a secure HTTP connection. Entities are represented in JSON format, allowing easy integration using programing languages that support HTTPS and JSON. Many REST libraries will also function well with the protocol.

DiscoveryDNS provides an implementation of our API in the Java programming language for you to use: http://discoverydns.github.io/dnsapi-client/

### Certificate Authentication

Authentication is achieved using TLS client certificate authentication. As part of completing the TLS handshake the certificate presented must be one that is issued by DiscoveryDNS, and signed by the

DiscoveryDNS CA. It must include the Universally Unique identifier (UUID) of the user you wish to authenticate as in the Common Name (CN) field.

All the standard certificate checks are applied (expiry checks, revocation checks, etc.) as well as verification that the certificate was issued by the DiscoveryDNS CA. Certificates are valid for one year unless revoked earlier, and require yearly renewal on their issue date. Only the TLSv1.1 protocol is supported with STRONG or greater cipher suites.

For detailed information on the API interface, refer to the *DiscoveryDNS API* document at the following link: http://discoverydns.github.io/dnsapi-client/

## 2.3 Average Propagation Delay

Changes made to DNS information via the API or Web Interface are queued for propagation to the DNS network immediately, depending on the number of other changes queued, and if DNSSEC signing was requested or not – the information will propagate to the DNS almost instantly. In most cases the changes will be propagated before the response is received by your client. For performance reasons, the DNS back-end caches information for 30 seconds, therefore it can take up to 30 seconds before changes are visible on every node in the entire network.

If queries for resource records have never been received by a site, then the changed information is returned immediately; therefore changed information in the interfaces distributes to all sites in virtually real time.

If the changed information is already in the cache, there is a 30 second delay before it is released from the cache and changed information is populated. If the changed information is not in the cache, the changes are immediately visible.

# 3 Functionality

This document gives you a broad overview of the functionality of the system and is designed to be read in conjunction with the *DiscoveryDNS API* document which can be found at the following link: http://discoverydns.github.io/dnsapi-client/

The two documents together are required to be read to understand the full functionality of the system. Even if you are going to utilise our Java Toolkit we strongly recommend you read the API documentation as well.

## 3.1 Time

The system operates in UTC time. All timestamps of transactions, propagation times, create dated, last update dates, etc., are stored and displayed in UTC time format on both the Web Interface and the API.

## 3.2 Accounts and Users

Each reseller is assigned an account within the DiscoveryDNS system. This account and its initial Administrator and API users will be created for you as part of the on-boarding process. Once set up you can utilise the admin user to create as many additional Users as required.

Users can log into the Web Interface, authenticated by a password and a TOTP capable authentication device (e.g. Google Authenticate on iPhone and Android). Additionally the REST API can be accessed by obtaining a signed certificate from DiscoveryDNS that authenticates the user.

The client certificate must be generated and signed by the DiscoveryDNS certificate authority and include the UUID of the user you wish to authenticate in the CN field. Certificates will be valid for one year unless revoked earlier, and will need to be renewed yearly on issue date. Please contact the service desk to arrange allocation of certificates.

An Account will have a currency associated with it which influences the availability of plans, see Section 0.

### Roles and Status

User permissions are implemented via Roles which control what Users are permitted to perform. All operations performed by a User are logged and accounted to that User.

The Web Interface provides mechanisms for Administrators to manage the level of access of their Users, including suspension of Users whose access should be revoked. Administrators should periodically review that the level of access to the System aligns with current requirements.

### Passwords

The System will expire you user password every 6 months. You will be forced to change your password once it has expired.

The password complexity rules are explained via the Web Interface when changing or setting passwords.

### Email

If you associate an email address with your account, the system will send periodic messages such as over limit notifications and DNSSEC signing completion to the email address. All this information is also available via the Poll Message queue discussed in Section 3.6.

## 3.3 Name Server and Name Server Interface Sets

Name servers and name server interface sets are created and managed by DiscoveryDNS.

### Name Server Interface Sets

Name server interface sets represent the IP addresses allocated to the anycast clouds that are used to provision zone files. A name server interface set contains one IPv4 and one IPv6 IP address per anycast instance in the allotted clouds. Typically Resellers are allocated one name server interface set for their exclusive use. One name server interface set can have multiple name server sets associated with it.

### Name Server Sets

A name server set represents the information that is used to generate the name server records that are used with zones when they are provisioned on the system. The Name Server Set contains the information required to generate the DNS names of the name servers identified by the associated Name Server Interface Set. Additionally the Name Server Set will contain the information required to complete the SOA record of the zone.

Effectively the Name Server Set will allow a reseller to ‘brand’ the DiscoveryDNS name servers with your own naming. A Reseller with multiple brands can request to be allocated multiple nameserver sets, one for each brand, so that when the Reseller provisions a zone under the relevant brand, the name server information that is created is branded with the applicable brand.

For example, for a Reseller having Brand 1 and Brand 2, they are assigned one name server interface set for usage, therefore one set of IP addresses, but two name server sets, one being Brand 1 the other Brand 2. In creating a zone using the name server set Brand 1, then the name servers would be ns1.brand1.com with IP address 1.2.3.4, and ns2.brand1.com with IP address 1.2.3.5. If a zone is created using the Brand 2 name server set, then name servers for the zone would be ns1.brand2.com with the same IP address 1.2.3.4, and ns1.brand2.com with IP address 1.2.3.5.

This enables the correct branding in the DNS based on different brands, but with the use of one set of IP addresses only.

Resellers are able to search and view name server sets within the system, but only DiscoveryDNS can create and update them.

### Prefixes and Domain Names

Prefixes and Domain Names for name server names are able to be specified. A prefix such as ‘ns’ or ‘server’, etc, could be specified, resulting in the generation of ns1, ns2, ns3, ns4, etc, up to the number

of nodes in the cloud. The prefix will then be suffixed with the configured domain name to form the zones' NS records. The prefix, domain name and email address information included in a name server set is also used when generating the SOA record.

The prefix and email address information included in a name server set is also used when generating the name server and SOA records for zones that utilise the zone branding feature, see Section 3.4.

### Status

New zones can only be linked to name server sets that are linked to name server interface sets that currently have an active status.

Name Server Interface Sets can be in either an 'active' or 'inactive' status. Zones can only be assigned to Name Server Sets that are linked to Name Server Interface Sets that have an active status. Name Server Sets that are linked to Name Server Interface Sets with an Inactive status are not able to be used by zones. Once a Name Server Interface Set is changed to an inactive status existing association's stay in affect but no new association is allowed.

**Important:** Be aware that on changing away from a Name Server Set that is linked to an inactive Name Server Interface Set, you cannot change back to it.

## 3.4 Zones

A zone represents a DNS zone file that is to be provisioned on to the anycast network. You create a zone utilising the Web Interface or via the API. Once you create a zone, or make any changes to it, those changes will be propagated to the Discovery DNS anycast network. The changes are queued for propagation immediately, and depending on the number of outstanding changes and if DNSSEC signing was requested or not, are generally deployed to the network before the response to add or update is received.

The zones assigned to a name server interface set must be unique, duplicates are not allowed for obvious reasons. A zone has two collections of resource records, DDNS records are generated by us, User resource records are supplied by the system. All resource records in described in this section are supported.

Each zone or group of zones in the System must be associated with a plan—on creating a zone, the applicable plan it is to use must be specified; it may be updated at any time. For more information on plans and their association with zones, please see Section 0.

The system allows you to access the query summaries of a zone. These zone query usage records are available with to-the-hour granularity, and from the Web Interface as well as the API. The records are periodically removed so be sure to download the data you require. The most current months' data is always guaranteed to be available.

Certain operations on zones such as DNSSEC signing can take some time (due to the cryptographic requirements); when these operations are occurring no more changes can be made to the zone until they are completed. This is indicated by a pending operation flag on the zone. Additionally the zone has a last published property which tells you the last time the zone was published to the anycast network.

Once a zone is created it is your responsibility to create the relevant delegation and, if required, glue records in the parent domain (usually at the registry or registrar). To assist with this the zone contains a field which includes the required parent records. When DNSSEC signing is used, the DS record will only be in this set after the DNSSEC signing process is completed.

## Supported Resource Records

| Type | Definition | Value | Function |
|---|---|---|---|
| **A** Address record | RFC 1035 | 1 | Returns a 128-bit IPv6 address, commonly used to map hostnames to an IP address of the host. |
| **AAAA** IPv6 address record | RFC 3596 | 28 | Returns a 32-bit IPv4 address, commonly used to map hostnames to an IP address of the host, but also used for DNSBLs, storing subnet masks in RFC 1101. |
| **NS**** Name server record | RFC 1035 | 2 | Delegates a DNS zone to use the given authoritative name servers. |
| **MX** Mail exchange record | RFC 1035 | 15 | Maps a domain name to a list of message transfer agents for that domain. |
| **SOA*** Start of authority record | RFC 1035 RFC 2308 | 6 | Specifies authoritative information about a DNS zone, including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone. |
| **CNAME** Canonical name record | RFC 1035 | 5 | Alias of one name to another: the DNS lookup will continue by retrying the lookup with the new name. |
| **SRV** Service locator | RFC 2782 | 33 | Generalised service location record, used for newer protocols instead of creating protocol-specific records such as MX. |
| **TXT** Text record | RFC 1035 | 16 | Carries machine-readable data, such as specified by RFC 1464, opportunistic encryption, Sender Policy Framework, DKIM, DMARC, DNS-SD, etc. |
| **NAPTR** Naming authority pointer | RFC 3403 | 35 | Allows regular expression based rewriting of domain names which can then be used as URIs, further domain names to lookups, etc. |
| **SPF** Sender policy framework | RFC 4408 | 99 | Specified as part of the SPF protocol as an alternative to storing SPF data in TXT records, using the same format – considered for obsolescence as of August 2013. |
| **DS** Delegation signer | RFC 4034 | 43 | The record used to identify the DNSSEC signing key of a delegated zone. |
| **CERT** Certificate record | RFC 4398 | 37 | Stores PKIX, SPKI, PGP, etc. |
| **PTR** Pointer record | RFC 1035 | 12 | Pointer to a canonical name. Unlike a CNAME, DNS processing does not proceed, just the name is returned. The most common use is for implementing reverse DNS lookups, but other uses include such things as DNS-SD. |
| **SSHFP** SSH Public key fingerprint | RFC 4255 | 52 | Resource record for publishing SSH public host key fingerprints in the DNS System, in order to aid in verifying the authenticity of the host. RFC 6594 defines ECC SSH keys and SHA-256 hashes. |

| Type | Definition | Value | Function |
|---|---|---|---|
| **TLSA**<br>TLSA certificate association | RFC 6698 | 37 | A record for DNS-based Authentication of Named Entities (DANE). RFC 6698 defines "The TLSA DNS resource record is used to associate a TLS server certificate or public key with the domain name where the record is found, thus forming a 'TLSA certificate association'". |
| **LOC**<br>Location record | RFC 1876 | 29 | Specifies a geographical location associated with a domain name. |
| **DNSKEY***<br>DNS Key Record | RFC 4034 | | Holds the public key used to sign records in the zone. |
| **RRSIG***<br>Resource Record Signature | RFC 4034 | | Holds the generated cryptographic signature which can be used in conjunction with the corresponding public key DNSKEY record to verify that the response received from the DNS by a client is as intended by the zone administrator. |
| **NSEC***<br>Next Secure | RFC 4034 | | Points to the next secured entry in a signed zone file, used for authenticated denial of existence in DNSSEC queries for domain names that are not present. |

* These records cannot be provided by the client, they will be generated by the server as required and will be returned in responses only.

** These records at a zones APEX will be managed by the server as above, but can be used at other levels in the zone for the purpose of delegation.

## Features

A number of additional features can be used with a zone, if the associated plan allows. These are explored below.

## Branded Name Servers Feature

When you enable the Branded name servers feature on a zone, instead of the information contained within the name server set being used to generate the delegation name servers and SOA information, the name server and SOA records are generated based on the zone itself. So the domain is branded based on the zone name itself, rather than reseller branding.

## DNSSEC Signing Feature

When you enable the DNSSEC Signing feature on a zone, the system will generate a unique public/private key pair for the zone and cryptographically sign the zone and publish it to the DNS with its cryptographically secure signatures. Once complete, the required DS record will be present in the zones delegation information, as well as sent via the messaging system. The DNSSEC process complies with the *DiscoveryDNS DNSSEC Practice Statement* which can be found at the following link: http://discoverydns.github.io/dnsapi-client/

## AXFR In Zone Transfer Feature

When you enable the AXFR In feature on a zone, instead of providing the resource records via the Web or API Interfaces, the records will be imported via a recurring AXFR transfer. In such a case, the DiscoveryDNS system acts a secondary for the given zone. A list of Master Servers IP addresses as well as a TSIG Key must be provided on the zone creation.

The remote zone serial will then be evaluated regularly, based on the refresh attribute of its SOA record. If the remote serial is newer, an AXFR request will be issued to one of the Master Servers, and an AXFR import will occur.

The resource records will be imported 'as is'. They need to be of the 'IN' class, and of one of the 'Supported Resource Records' types listed above.

The DiscoveryDNS system also supports the reception of NOTIFY requests, on one of the provided Notify Modules endpoints. On reception of a NOTIFY request, the remote zone serial will then be evaluated, and if newer, an AXFR import will occur.

A 'Refresh' command is also made available in the Web and API Interfaces, to force an AXFR import, skipping the preliminary serial check.

A Message will be sent on the first successful AXFR import, as well as on an unsuccessful attempt on all provided Master Servers, or if an AXFR import contains records of unsupported types.

When enabling the 'DNSSEC Signing Feature' on such an AXFR zone, the DiscoveryDNS system then acts as a public master for the zone, providing "bump-in-the-wire" signing. It will then manage the zone as described in the 'DNSSEC Signing Feature' chapter above, re-signing the zone on each AXFR import. It will then automatically manage its own zone serial, separately from the remote zone's original one.

## Pseudo Resource Records Feature

Pseudo Resource Records enable advanced DiscoveryDNS features. These resource records are not 'real' DNS resource records, but ones created by us to allow the configuration of some advanced features. These pseudo resource records will be translated by the system into the actual records required to make the feature work as the zone is published to the anycast cloud. Each is explored below.

**Zone Apex CNAME Pseudo Resource Record (ZONECNAME)**

Placing a CNAME record at the apex of a zone is not allowed according to the DNS standards. The ZONECNAME pseudo resource record can be used at the apex of the zone (and the apex only) and emulates the behaviour of having a CNAME at this level. The emulation is achieved by periodically resolving the target of the ZONECNAME record and inserting the corresponding A and AAAA records into the zone file in its place when it is published. For example:

Zone 'test.com'

**test.com ZONECNAME www.domain.com**

Assuming www.domain.com resolved to the IPv4 address 203.78.65.6 then the deployed test.com zone will contain:

Zone 'test.com'

**test.com A 203.78.65.6**

Each time that the record for www.domain.com is changed, this will be detected by the system and the test.com record updated. This check is performed periodically. If the target cannot be resolved no record will end up in the published zone and the ZONECNAME is ignored. Both IPv4 and IPv6 records will be inserted in the target.

**HTTP Forwarding Pseudo Resource Record (URL)**

URL pseudo resource records allow a simple http redirect to be configured. By creating a URL record, the domain name created will be redirected to the resolved URL template specified. To make this occur once the zone is published the URL record will be translated into the A and AAAA records of our anycast HTTP redirect service. The redirect will also be published to the redirect service and our http listeners will serve redirects for the name. The destination of the redirect can be a standard HTTP or HTTPS URL, or can use special URL template parameters to dynamically generate the redirect URL. The template parameters that can be used are as follows:

| Parameter | Description | DNS Name | Example Template | Incoming Request | Resulting Redirect |
|---|---|---|---|---|---|
| {path} | This parameter is replaced with the path of the incoming request prior to its redirection | www.source.com | http://www.target.com/sub/{path} | http://www.source.com/one/two | http://www.target.com/sub/one/two |
| {wildcard} | When the URL record is used with a wildcard DNS record this parameter will be replace with the wildcard portion of the matched domain name | *.source.com | https://{wildcard}.target.com/ | http://s1.s2.source.com/ | https://s1.s2.target.com/ |
| ?{queryParameters} | This parameter is special, it must be prefixed with the '?' and can only appear at the end of the template. It will be replaced by ALL the incoming supplied query parameters | www.source.com | http://www.target.com/?{queryParameters} | http://www.source.com/?input1=cat&input2=dog | http://www.target.com/?input1=cat&input2=dog |
| Any query parameter surround by '{' and '}' | You can reference any incoming query parameter in the template by name. The parameter will be replaced with the value of that parameter in the incoming query | www.source.com | http://{input1}.www.target.com/?incoming={input2} | http://www.source.com/?input1=cat&input2=dog | http://cat.www.target.com/?incoming=dog |

You can mix and match parameters in templates as required, duplicates are allowed, parameters can be used in any part of the URL. However if you specify a parameter and the incoming request is not capable of fulfilling that parameter no redirect will occur and an error page will be displayed. So for example if you use the wildcard parameter with a non-wildcard record the redirect will never function. Similarly if you are using a query parameter name, and that query parameter is not supplied, the result will be an error.

The exception to this is the queryParameters parameter, which will work whether there are query Parameters supplied or not. Also it is your responsibility to ensure that after substitution a valid URL is created.

Several redirection types are currently supported:

- HTTP Redirect with status code 302 ("Moved Temporarily"),
- HTTP Redirect with status code 301 ("Moved Permanently"),
- HTTP Redirect with status code 303 ("See Other"),

- HTTP Redirect with status code 307 (“Temporary Redirect”),
- URL cloaking with iframe (destination URL is rendered in an invisible full screen iframe, so that original URL is preserved in the user’s browser address bar).

For the redirection by URL cloaking with iframe, some additional optional parameters can be set:

- Page title, which will be set in the output *<title>* HTML tag.
- Page description, which will be set in the output *<meta name="description" …>* HTML tag.
- Page title, which will be set in the output *<meta name="keywords" …>* HTML tag.

**Mail Forwarding Pseudo Resource Record (MAILFW)**

The MAILFW pseudo resource records allow a simple mail redirect to be configured. By creating a MAILFW record, any email destined for any mailbox at the domain name created will be redirected to the destination specified. To make this occur, once the zone is published, the MAILFW record will be translated into the required MX records. Additionally, if the Branded Name Servers feature is in use for the zone, the generated MX records will be branded as per the domain name, thus the required A and AAAA records will also be created. The mail servers used are our anycast SMTP redirect service. The redirect will also be published to the redirect service and our SMTP listeners will receive the mail for the domain and forward it to the configured destination.

The destination of the redirect can be a single email address, which will forward all email for that domain to that particular email address, or simply a domain name prefixed with an @ symbol, in which case the incoming mailbox name will be retained for the outgoing email. For example:

If you configure a redirect record as below:

**test.com MAILFW bob@example.com**

Then all email for test.com (bob@test.com, greg@test.com, or indeed any other address @test.com) will be sent to bob@example.com.

If you configure a redirect record as below:

**test.com MAILFW @example.com**

Then an email sent to bob@test.com will be sent to bob@example.com, email for greg@test.com will be sent to greg@example.com etc.

The redirection can also be performed on a specific recipient, if you configure the redirect records as below:

**test.com MAILFW admin admin@example.com**

**test.com MAILFW bob@example.com**

Then an email sent to admin@test.com will be sent to admin@example.com, and all other emails for test.com (bob@test.com, greg@test.com, or indeed any other address @test.com) will be sent to bob@example.com.

And as well, if you configure the redirect records as below:

**test.com MAILFW admin admin@example.com**

**test.com MAILFW @example.com**

Then an email sent to admin@test.com will be sent to admin@example.com, and otherwise an email sent to bob@test.com will be sent to bob@example.com, email for greg@test.com will be sent to greg@example.com etc.

## 3.5 Plans

Plans indicate the monthly fees payable for a zone, any excess fees, and which features a zone is permitted to utilise. Users can search for and view plans they have access to, however plans are only created and managed by DiscoveryDNS. These plans represent the fees negotiated with DiscoveryDNS. As part of the on-boarding process you will be provide with the details of the plans you have access to.

### Access to Plans

As plans represent your unique contract, plans will be created for you as part of the on-boarding process, or when any changes to your commercial arrangement are made – As such you will only see and have access to plans that are for you. This is all configured and managed by DiscoveryDNS. Additionally Plans have a currency associated with them; this is the currency that the fees for the plan will be charged in.

Accounts also have a currency associated with them. Therefore you will only be able to access plans that share the same currency as your account.

### Plan Types

There are three types of plans:

- **Base Plans** – These plans are designed to allow us to assign you one fee for a bulk purchase of queries that you can use for all basic domains hosted on your infrastructure. They behave similar to a group plan except that the group name cannot be specified. Only one 'instance' of a base plan can be created, which will happen automatically for you the first time you assign a zone to a base plan.
- **Standard Plans** – These plans support a single zone per plan instance, that is each time you associate a plan of this type (a plan without the grouping feature) with a zone there will be a monthly recurring charge based on the plans details and feature usage of that zone.
- **Group Plans** – These plans support more than one zone being associated with an 'instance' of the plan, that is a group of zones which all share the same 'group name' are associated with one instance of the group plan. Each time you associate a new group of zones (distinguished by their group names) with a group plan there will be a monthly recurring charge for that zone group based on the plan details and feature usage of the zones in the group. Zones can be moved between groups by modifying their group name; however the billing affect will not take place until the following month. All zones in one group should belong to the same customer.

At the initial create there is a pro-rata charge to the start of the next month, then at the start of each following month the plan fee will be charged for that month (or path thereof). If a zone (or zone group) is deleted part way through the month no refund is credited. Any excess fees are calculated at the end of the month and applied to the following month's bill.

You may change plan at any time, but the change does not take effect until the start of the next month (billing cycle).

### Status

Plans can be in either an 'active' or 'inactive' status. Zones can only be assigned to plans that have an active status. Plans with an Inactive status are not able to be used by zones. Once a plan is changed to an inactive status existing association's stay in affect but no new association is allowed.

**Important:** Be aware that on changing away from an inactive plan, you cannot change back to it.

### Billing

Billing is done on a monthly cycle from the start of the month until the end of the month. Zones created half way through a month are billed pro-rata.

### Plan Units

Plan units represent the 'metrics' than can be 'counted' for a particular instance of a plan. When the plan is a single zone plan, the metric will be counted for that zone, when it is a group plan the metric will be counted across all zones associated with the group of that particular instance of the plan. A Plan Unit defines the following:

- A base number of units that are included in the plan as part of the plan fee.
- The block of units used in calculating excess fees (the excess fee is charged for each block or part thereof beyond the included number of units).
- The charge per block used to calculate the excess fee.

Example:

- Included Units: 100
- Excess Block: 20
- Excess Block charge: $2

If you used 90 units the excess charge would be $0

If you used 120 units the excess charge would be $2

If you used 110 units the excess charge would be $2 (as 10 units is part of a block size of 20, and there are no partial charges)

If you used 180 units the excess charge would be $8

The units you may see configured on your plans are:

- **Queries** – the monthly number of DNS queries.
- **Resource Records** – the number of resource records utilised by the zone.
- **Zones** – the number of zones that can be included in the group plan, and excess fees for additional zones.

If no unit measure for a particular value is associated with a plan then that particular unit is not counted towards your billing.

### Plan Features

Plan features represent the functionality within the DiscoveryDNS reseller system that zones utilising that plan can access. A plan feature may have a corresponding charge associated with it. If the charge is zero then you can use the feature as part of the plan with no additional charge. If the charge is non-zero than if you turn on or utilise the particular feature then you will be subject to the extra charge each month

The features that you may see configured on your plans are:

- **Branded Name Servers** – enables the selection of branded name servers with a zone, which then generates the NS records for the zone based on the zones name itself (see branded name servers feature).
- **DNSSEC Signing** – enables the selection of DNSSEC signing on zones to cause them to be signed with DNSSEC (see DNSSEC later).
- **Grouping** – identifies the plan as a group plan (See explanation in this section).
- **Zone CNAME Record** – enables the usage of ZONECNAME resource records (see Zone CNAME pseudo resource record as described in Section 3.4).
- **URL Record** – enables the usage of URL http forwarding records (see URL pseudo record as described in Section in Section 3.4).
- **MailFW Record** – enables the usage of MAILFW email forwarding records (see MAILFW pseudo record as described in Section 3.4).

## 3.6 Messages

The DiscoveryDNS system will queue messages for your account based on events occurring in the system. You can 'poll' for the current message and then acknowledge it to get the next message. You should do this regularly to ensure you are up to date with what is occurring in the system.

The messages that you can expect to receive from the system include:

- **Zone/Group Usage Warning** – this will be sent when the query usage of a zone/group reaches the warning level.
- **Zone/Group Usage Critical** – this will be sent when the query usage of a zone/group reaches the critical level.
- **Zone/Group Usage Over Limit** – this will be sent when the query usage of a zone/group exceeds the queries included with its associated plan.
- **Zone DNSSEC Signing Complete** – this will be sent when the DNSSEC signing of a zone has been completed and the DS record is available to be retrieved.

More information on the messages is explained in the API documentation

# 4 Auditing

Object version and transaction record auditing information is maintained within the System.

## Object versions

Every time a change is made to an object (account, zone, user, plan), its history is maintained via a version of the object. All versions of the object from its creation up to its current version are kept, representing the object's full history.

## Transactions

All transactions performed have an associated client and server transaction ID, and a record of the user who performed the transaction, the IP address it was performed from, and the interface used (Web Interface or API).

All command and transaction records are recorded with the above details against the transaction ID and a timestamp, and include the changes to the objects involved in the transaction.

A log of all incoming and outgoing JSON is set to the API, as well as the standard HTTP request logs for the Web Interface.

**Viewing Transaction Data**

The log of transaction is searchable from the Web Interface. Also each object has a link to its own history which you can view in the Web Interface. The Web Interfaces shows you basic details about the transaction performed including:

- What transaction was performed
- When it was performed
- Who performed
- How they performed
- Which objects were affected by the transaction

The full details (input and output parameters, before and after object states) are available from support staff on request.

# 5 Service Level Agreements

Service Level Agreements (SLAs) are offered on the overall DNS service as well as on a plan specific basis.

## Overall service SLAs

SLAs for overall service cover availability of the API/Web Interface and the processing time performance of the API/Web Interface.

Resellers' overall service SLAs relate to the ability to use the interfaces to manage the zones under a reseller's control.

## Plan SLAs

Service level is also plan specific, with different plans having different SLAs. Each Plan that a zone can be on can have a specific service level.

**DNS service availability SLAs**

Higher priced plans offer higher DNS service availability percentages than lower priced plans.

**Plan based UDP and TCP performance SLAs**

Performance is based on the percentage of queries responded to within a certain amount of time. The performance SLA varies dependent on the applicable plan.

**Definitions**

We, us and our means any or all of the Bombora Technologies Pty Ltd group of companies, their related entities and their respective officers, employees, contractors or sub-contractors.

**Disclaimer**

This document has been produced by us and is only for the information of the particular person to whom it is provided (the Recipient). This document is subject to copyright and may contain privileged and/or confidential information. As such, this document (or any part of it) may not be reproduced, distributed or published without our prior written consent.

This document has been prepared and presented in good faith based on our own information and sources which are believed to be reliable. We assume no responsibility for the accuracy, reliability or completeness of the information contained in this document (except to the extent that liability under statute cannot be excluded).

To the extent that we may be liable, liability is limited at our option to replacing, repairing or supplying equivalent goods or paying the cost of replacing, repairing or acquiring equivalent, or, in the case of services, re-supplying or paying the cost of having such re-supplied.

**Confidentiality Notice**

This document contains commercially sensitive information and information that is confidential to us. This document is intended solely for the named recipient, and its authorised employees, and legal, financial and accounting representatives (collectively, Authorised Recipients).

The recipients of this document must keep confidential all of the information disclosed in this document, and may only use the information for the purpose specified by us for its use. Under no circumstance may this document (or any part of this document) be disclosed, copied or reproduced to any person, other than the Authorised Recipients, without our prior written consent.

**Trademarks Notice**

Any of our names, trademarks, service marks, logos, and icons appearing in this document may not be used in any manner by recipients of this document without our prior written consent. All rights conferred under law are reserved.

All other trademarks contained within this document remain the property of their respective owners, and are used only to directly describe the products being provided by them or on their behalf. Their use in no way indicates any relationship between us and the owners of those other trademarks.




ARI REGISTRY SERVICES