ironDNS®

diversity in your DNS infrastructure

Service Specification

ironDNS® DNS infrastructure

Service Specification

Content

ironDNS® DNS infrastructure

Service Specification

Standard Feature List

1

ironDNS® provides diversity for your DNS infrastructure

ABOUT ironDNS®

Overview

ironDNS® places special emphasis on stability, robustness and security. The high-availability platform relies on name server locations around the globe and offers Unicast and Anycast services. Of course, IPv4 and IPv6 are both supported.

Data Protection

As Knipp, the company providing ironDNS®, has its headquarters in Germany, ironDNS® is operated under the strict privacy policies of the European Union. In addition, Knipp holds a DIN ISO/IEC 27001:2015 certificate demonstrating its comprehensive security concepts.

Mixed Set-Up

In the mixed set-up, consisting of your own name servers and ironDNS® name servers, ironDNS® name servers can either be secondary name servers receiving the master zone from one of your name servers; or your name servers can work as secondary name servers receiving the zone (including notifies) from ironDNS® name servers.

DNSSEC

ironDNS® fully supports DNSSEC. Customers can choose either the active or passive mode depending on their individual needs. In the active mode, ironDNS® handles all necessary steps. In the passive mode, ironDNS® validates the zone without changing any DNSSEC-related resource records.

Diversity

Software diversity is the basic protection against malfunction and attacks. ironDNS® is a name server software and service that is wholly independent of all other name server implementations.

ironDNS® DNS infrastructure

PRODUCT SPECIFICATION

2

ironDNS® is designed to fully support DNSSEC

ironDNS® allows all Internet users world-wide to actually use domains. This is mainly done by converting human readable domain names into IPv4 and IPv6 addresses, which are used by the Internet communication protocols to address systems connected to the Internet.

Design Principles

- ***diversity*** in software (ironDNS® as proprietary solution and BIND as a fall-back solution)
- ***diversity*** in hardware
- ***diversity*** in operation systems (HP-UX and Linux)

Features

- ***Control Panel*** allowing extensive and easy zone management
- ***SOAP interface*** (for automatic high-volume zone provisioning)
- configurable ***E-Mail alerts*** in case of errors
- use of ***Unicast*** nodes
- use of ***Anycast*** networks
- ***IPv4*** and ***IPv6*** support (dual stack)
- all name servers are updated via a ***central manager*** component using the push principle; the manager always knows exactly which zone version is available on which name server, allowing for better control
- full fledged ***DNSSEC*** support including automatic rollovers of ZSKs
- support for ***arbitrary DNS resource record types*** (including unknown types)
- extensive ***zone validation*** and ***automatic correction of minor faults*** (configurable)
- ***two factor authentication*** for highly secured zones
- additional ***read-only accounts*** (e.g., for lower priviliged support staff)
- configurable ***DNS statistics***

ironDNS® DNS infrastructure

3

ironDNS® is compliant with standards

Implemented RFC standards

Adherence to and implementation of the following standards (among others):

- RFC 1034 Domain Names — ***Concepts*** and Facilities
- RFC 1035 Domain Names — ***Implementation*** and Specification
- RFC 1982 ***Serial Number Arithmetic***
- RFC 1995 ***Incremental Zone Transfer in DNS***
- RFC 1996 A Mechanism for Prompt ***Notification of Zone Changes***
- RFC 2181 Clarifications to the DNS Specification
- RFC 2182 Selection and Operation of ***Secondary DNS Servers***
- RFC 2671 Extension Mechanisms for DNS (***EDNS0***)
- RFC 2845 Secret Key Transaction Authentication for DNS (***TSIG***)
- RFC 3007 Secure Domain Name System (DNS) ***Dynamic Update***
- RFC 3225 Indicating Resolver Support of ***DNSSEC***
- RFC 3596 DNS Extensions to Support ***IP Version 6***
- RFC 3597 Handling of ***Unknown DNS Resource Record (RR) Types***
- RFC 3901 DNS ***IPv6 Transport*** Operational Guidelines (BCP 91)
- RFC 4033 DNS Security Introduction and Requirements
- RFC 4034 Resource Records for the DNS Security Extensions
- RFC 4035 Protocol Modifications for the DNS Security Extensions
- RFC 4343 Domain Name System (DNS) Case Insensitivity Clarification
- RFC 4472 Operational Considerations and Issues with ***IPv6*** DNS
- RFC 4509 Use of ***SHA-256*** in DNSSEC Delegation Signer (DS) Resource Records (RRs)
- RFC 4592 The Role of ***Wildcards*** in the Domain Name System
- RFC 5155 DNS Security (DNSSEC) Hashed Authenticated Denial of Existence
- RFC 5702 Use of ***SHA-2*** Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC
- RFC 6604 ***xNAME RCODE*** and Status Bits Clarification
- RFC 6672 ***DNAME*** Redirection in the DNS
- RFC 6781 DNSSEC Operational Practices, Version 2
- RFC 6895 Domain Name System (DNS) IANA Considerations
- RFC 7766 DNS Transport over ***TCP*** - Implementation Requirements
- RFC 7929 DNS-Based Authentication of Named Entities (***DANE***) Bindings for OpenPGP

Usage Scenarios

1. ***Replace your DNS infrastructure***; all your visible name servers are run by ironDNS®.
2. ***Enhance your DNS infrastructure*** by adding one ore more ironDNS® name servers seamlessly to your own name servers.

In both of the above cases you can

- enter and manage your zone file comfortably via the ***Control Panel***.
- run a (hidden) primary name server. The zones are transferred via ***IXFR/AXFR***.
- update your zones automatically via our ***SOAP interface***.

ironDNS® DNS infrastructure

Support for DNSSEC

Whatever mode of operation you choose, ironDNS® fully supports DNSSEC. If you sign your zones yourself, ironDNS® will simply use all DNSSEC-related resource records as provided and publish them on ironDNS® name servers. Alternatively, you can have ironDNS® sign your zone. In that case you can also use your name servers as secondaries by obtaining the signed zone from ironDNS. In the latter case ironDNS® will take care of the ZSK rollover autonomously and inform you (via Control Panel or SOAP poll message) about a due KSK rollover. Whenever it may be necessary you can always force a key rollover at your convenience.

Information Security

Knipp Medien und Kommunikation GmbH, the company providing ironDNS®, has its headquarters in Germany. Therefore, ironDNS® is operated under the strict privacy policies of the European Union. In addition, Knipp holds a DIN ISO/IEC 27001:2015 certificate demonstrating its comprehensive security concepts.

DNS infrastructure

DNS infrastructure

ironDNS® is a product of

Knipp Medien und Kommunikation GmbH
Technologiepark
Martin-Schmeißer-Weg 9
44227 Dortmund
Germany

www.irondns.net
info@irondns.net