Technical Description:
Nixu Registry Server

Nixu Software Oy Ltd

A Nixu Group Company

Keilaranta 15

FI-02150 Espoo

Finland

1. Overview of Nixu Registry Server

Nixu Registry Server is a Domain Name Registry Solution (DNRS) developed for generic and mid-sized Top-Level Domains (TLDs). Designed as a solution framework with modular architecture, Nixu Registry Server can be configured and tailored on per-installation basis to meet the exact requirements of the customer. The configurable modules in Nixu Registry Server include:

- Web-based domain reservation portal for the registry operators
- Web-based self-service domain reservation portal for end-users
- Web-based API for dynamic integration with registrars (toolkits on request)
- WHOIS server with data replicator
- Domain accounting and billing integration module
- Domain checking and network tools available to end-users
- Choice between external or embedded SQL backend
- Support for agents of commonly used OSS and back-up systems

Nixu Registry Server comes with a number of reservation process automations, allowing registries running Nixu solution to provide a self-service reservation portal to the end-users, and a web-based API for its registrars. The underlying AJAX-based web framework and a built-in IDN support enable the localization of both look & feel and used languages, to align with the local business environment. To automate the related business processes and requirements, Nixu Registry Server supports various, configurable domain accounting rules and can be integrated with virtually any billing and/or other backend systems.

Depending on the project scope, Nixu Registry Server is delivered either as a highly-available standalone DNRS integrated with existing Domain Name System (DNS) primary platform, or as a part of a complete end-to-end DNRS & DNS Infrastructure turnkey delivery. The DNS part of a turnkey delivery can consist of:

1. Proprietary Nixu DNS Primary platform (Nixu NameSurfer Suite) integrated with existing DNS secondaries. In this scenario, the supported DNS secondary types include Nixu SNS, Secure64 DNS, BIND and NSD. Also other RFC-compliant DNS secondary types are supported; however, these remote servers and/or services cannot be controlled remotely from Nixu NameSurfer Suite.

2. Proprietary Nixu DNS Primary platform coupled with new DNS secondaries. Nixu can deliver either Nixu SNS (BIND-based), Secure64 DNS (NSD-based), BIND or NSD secondary servers.

3. A mixed delivery consisting of proprietary Nixu DNS Primary platform, new DNS secondaries and existing DNS secondaries and/or secondary services.

Nixu NameSurfer Suite used as the proprietary DNS Primary platform is the market-leading DDI solution used by Fortune 500 companies; more than 30 percent of all 2.5G (GPRS) and 3G (UMTS) service providers; and five Top-Level Domains worldwide. It has been designed for secure, centralized management of organizations' DNS data and IP address space, and can also be used for centralized management of remote DNS servers. Thanks to its proprietary DNS primary server process and powerful network-based API, it can be easily integrated with external applications and services, making Nixu NameSurfer Suite the DDI provisioning platform of choice

2. Deployment Descriptions and Recommendations

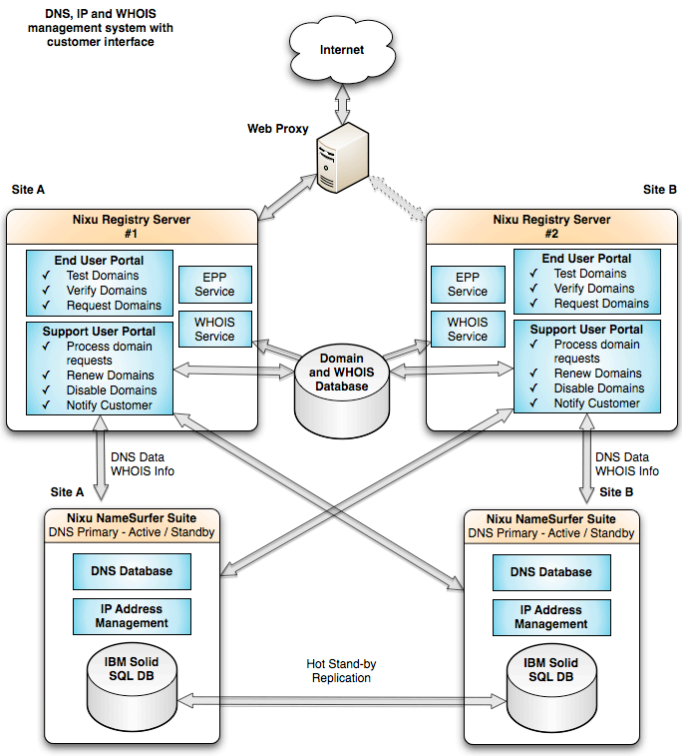
To achieve six-sigma availability in the deployment, Nixu recommends that both the DNRS (Nixu Registry Server) and the primary DNS (Nixu NameSurfer) platforms be deployed as highly available server pairs over two data centres, each with two network links and redundant load-balancer(s). With this deployment strategy, every component used in the installation is doubled, making sure that even if any one part of the solution – or indeed the entire data centre – failed, the operations would continue uninterrupted.

As far as the secondary DNS service is concerned, Nixu recommends the following approach:

1. For each DNS secondary node, one or two authoritative DNS secondary server instances should be run in both data centres. These servers would be run as a single secondary DNS cluster node behind a single public IP, utilizing either the load-balancers described in paragraph 1 or anycast technique. The exact number of secondary servers assigned to each node (two/four/more) depends on the level of performance and redundancy the TLD expects to achieve. Especially in situations where the companies operating local DNS secondary clusters do not have a data centre in the TLDs country of origin, this approach can be used to ensure that the public DNS service will continue to run uninterrupted even if the network connections to the overseas data centre / service provider were disconnected for any reason.

2. The secondary DNS server node(s) should ideally be complemented by running anycasted secondary DNS service procured from a specialist company operating such service. Nixu has relations with such companies and will be happy to make recommendations upon request.

Below, please find a diagram describing the solution architecture recommended by Nixu:



Below, please find an overview of the roles of the different servers used in the installations. The roles of these servers are assigned as follows:

Server 1: Nixu Registry Server running on native x86-based hardware on Site A
Server 2: Nixu Registry Server running on native x86-based hardware on Site B
Server 3: Nixu NameSurfer Suite (DNS Primary) running on native x86-based hardware on Site A
Server 4: Nixu NameSurfer Suite (DNS Primary) running on native x86-based hardware on Site B
Web-Proxy: The web-proxy running in front of Sites A and B in the diagram should be interpreted as a highly available proxy cluster.

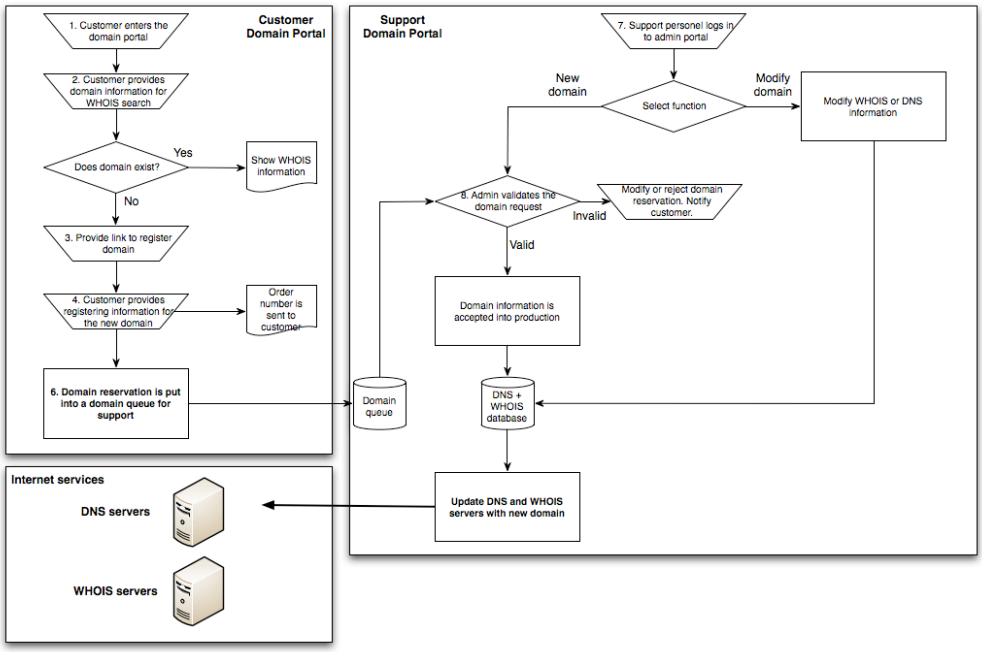
Server 1

Server 1 runs Nixu Registry Server. This server is used for self-service domain reservations and modifications as well as related tasks such as domain availability searches and DNS diagnostics (either universal or ccTLD / gTLD specific); to provide the registry staff with an administrative interface for the management of reserved domains and domain reservations; to push the reserved and/or amended domain information to the primary DNS platform; to generate the billing tickets required by the online payment service provider; and to provide the WHOIS service for the gTLD/ccTLD and possible subdomains. The embedded SQL backend is either an embedded Postgres db or an external Oracle db, and the contents of the databases are replicated between Servers 1 and 2. The network-based API included in the Nixu Registry Server supports EPP and can be used by registrars to automate the domain reservation processes between their own systems and the registry.

Server 2

Identical to Server 1. In order to make sure that the service provided by servers 1 and 2 shall be fault-tolerant and transparent to the end-user, these two servers shall be run in active-active or active-standby mode behind two load-balancers both of which advertise the same IP address, sharing load between the servers, and directing traffic to the remaining server in the event that either one of the servers fail for any reason.

Below, please find a process diagram depicting the related domain reservation process:



Server 3

Server 3 runs Nixu NameSurfer Suite. This server is used as the hidden DNS primary server supporting IPv4, IPv6, DNSSEC, ENUM and IDN. This server is integrated with Servers 1 and 2 over a network-based API (XML-RPC) included in the product, allowing dynamic updates to master zone file(s) from servers 1 and 2. Whenever changes to the zone file are made, Nixu NameSurfer Suite pushes those changes automatically to the secondary DNS servers using Incremental Zone Transfers (IXFR; please note, also AXFR is supported). The configurations of the secondary DNS services controlled by the Registry can be managed centrally using Nixu NameSurfer's Remote Servers management utility.

Furthermore, in addition to obtaining changes pertaining to the domain information from Servers 1 and 2, Nixu NameSurfer Suite also automates the DNS management tasks for the zones the Registry is authoritative for including creation of reverse entries and zone serial numbering. The server includes network-based API and command-line interface, and a web-based user-interface and User Groups functionality that can be used to provide a SSL secured connection to all DNS master data. The User Groups functionality includes an audit trail listing the WHO, WHAT and WHEN of any and all DNS changes made using the system, coupled with a convenient undo/redo functionality that can be used to reverse undesired changes. The collection period used in connection with the audit trail can be freely defined according to the policy requirements of the end-user organization.

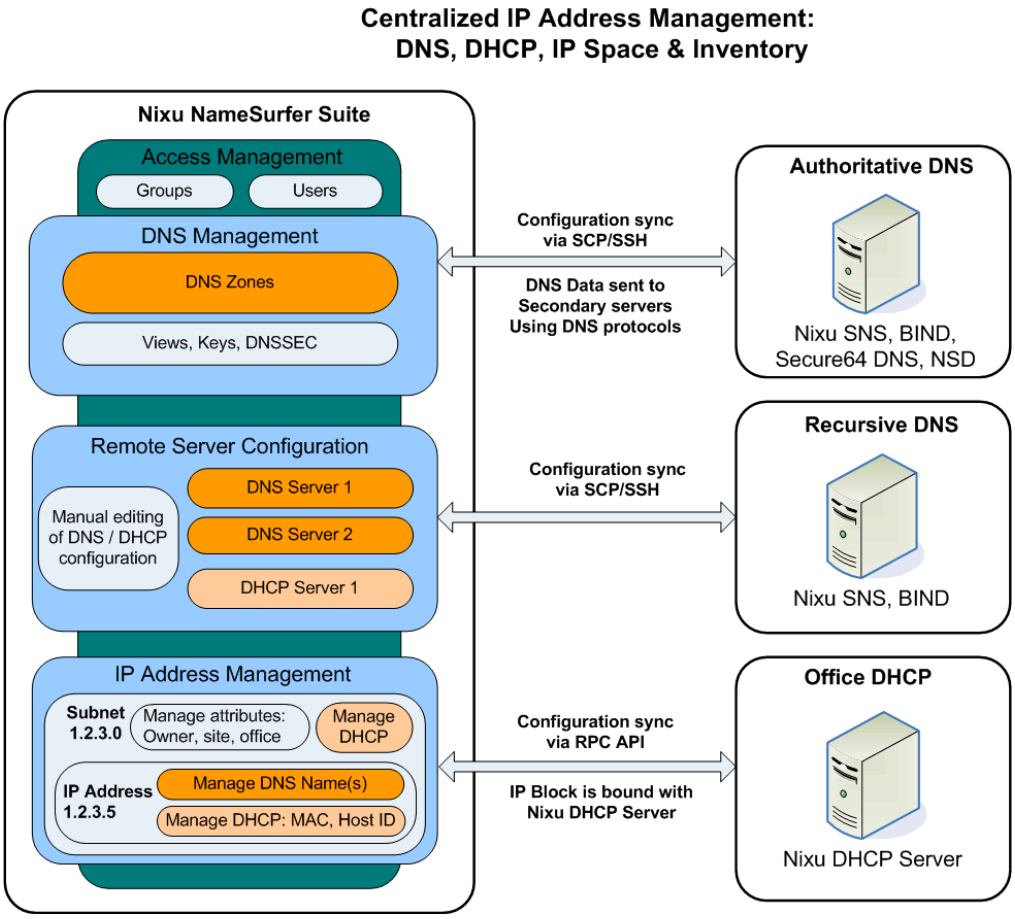
To assure the integrity and the security of the deployment, the proprietary primary DNS server is deployed as hidden primary, i.e. it will not be visible to the outside world, except for the secondary DNS servers to which connections are encrypted using SSH and authenticated using transaction signatures (TSIGs).

Thanks to its embedded SQL backend (Solid EmbeddedEngine by IBM), the hidden primary DNS server is capable of serving tens of millions of objects in its database when run on industry-standard hardware such as HP ProLiant Series. Since the SQL backend is embedded, no network traffic occurs between the DNS primary and external backends, thereby mitigating the possibility of data interception.

Server 4

Identical to server 3. The two hidden DNS primary servers in the installation (Servers 3 and 4) store all data in embedded SQL backends, and are run in active-passive mode. In other words, the active primary DNS server is used for all management routines and to obtain dynamic changes to DNS made using the API or dynDNS. Thanks to the hot-standby replication technology used in these servers, all changes made using the active primary are propagated in real-time to the SQL backend of the hot-standby replica, making the two servers identical at all times. In the event that the active server goes offline for a pre-defined period of time, watchdog software included in the delivery appoints the hot-standby replica as the new active primary, and the web-proxy on the servers starts forwarding users to the newly appointed active primary. Please note that in addition to hot-standby replication, the servers also support online back-ups of the configurations and the database, using simple CLI command coupled with utilities such as "cron".

Below, please find a diagram depicting the relationship between Nixu NameSurfer Suite primary server and the possible secondary DNS servers used in the deployment:



Web-Proxy

While the Web-Proxy included in the diagram on page 3 is depicted as a single machine, it represents a web-proxy / load-balancing cluster consisting of a number of machines split over two data centres, advertising a single public IP address for the services running on servers 1, 2, 3 and 4. Upon request, Nixu will be happy to make recommendations on proxy / load-balancing products suitable for this purpose.

Secondary DNS Service

The clustered (anycasted / load-balanced) secondary DNS nodes used in connection with Nixu delivery can be implemented using Nixu SNS (BIND-based), Secure64 DNS Authority (NSD –based), BIND or NSD. The recommended deployment would consist of different DNS server types (either NSD or BIND based), increasing the resistance to DNS server software vulnerabilities that could be found in any single DNS server type. In addition to the clustered DNS secondary nodes dedicated to a single ccTLD / gTLD, also globally distributed secondary DNS services can be used in connection with the Nixu solution. Below, please find a brief description of Nixu SNS (Secure Name Server) would be used in this context.

Nixu SNS is run as a secondary DNS server authoritative for the ccTLD / gTLD zone(s) and possible subdomains. The product supports all relevant RFCs pertaining to IPv6, DNSSEC, IDN and ENUM. Nixu SNS is a hardened, BIND-based purpose-built DNS server with Intrusion Detection / Intrusion Prevention system used to mitigate DDoS and similar attacks. While the scalability of Nixu SNS depends on the hardware platform it is being run on, a Nixu SNS server instances running on an industry-standard HP ProLiant DL360 or similar server is capable of answering more than 30,000 queries per second.

When deployed as a clustered node, four servers such as this running behind a single public IP are capable of answering more than 120,000 per second per clustered node.

To ensure their security, Nixu SNS servers are configured so that their configurations can be managed remotely from the DNS primary using SSH and SCP, and the zone transfers from primary DNS server are performed over a SSH secured connection using TSIG authentication. The DNS secondary servers support automated software updates that allow automated patching of the server software whenever new vulnerabilities are discovered.

Integration

The integration between Nixu Registry Server and Nixu NameSurfer Suite (Primary DNS Service) is carried out using a network-based APIs included in the products. In the event that an existing Primary DNS Platform is used, Nixu Registry Server can be integrated against the published API of that system.

The integration between Nixu NameSurfer Suite and the secondary DNS servers / services would be carried out and secured using RFC-based standards such as zone transfers (IXFR/AXFR), NOTIFY, transaction signatures (TSIGs), SSH and SCP. When running Nixu SNS and/or Secure64 DNS Authority in the deployment, both servers come with built-in support for remote & centralized management from Nixu NameSurfer's Remote Servers management utility.

The integration between the payment gateway and Nixu Registry Server is performed using a network-based API. This same API would also be used in communications between the Registry and Registrars.

3. About Nixu Software

Nixu Software is an affiliate of privately held Nixu Group founded in 1988. Headquartered in Helsinki, Finland, and with number of regional sales offices in Europe, the Americas and Asia Pacific, our mission is to offer the best value for money within the DNS and IP addressing industry. The execution of our mission is based on our DNS, DHCP and IP address management solutions and software appliances that set the benchmark for combined security, ease of use, and low cost of ownership.

Nixu Software leverages Nixu Group's world-class expertise in software development and information security by developing secure DNS and IP address management solutions and software appliances. Our products can be deployed either as standalone end-to-end solutions, or as components of more extensive turnkey solutions developed in co-operation with different OEMs.

Nixu Software stresses four fundamentals in all its product development efforts: security, scalability, availability and efficiency. Having longstanding blue-chip customers who have managed 100% DNS uptime for a decade while reducing the related management costs by more than 50% per year, our track record is second to none.

Nixu Software's DNS products have an installed base consisting of more than 3.000 server instances worldwide. Our technologies are used by more than 30% of all 2.5G and 3G mobile operators globally; dozens of Fortune 500 companies; and several generic and country code Top Level Domains in Europe and Asia Pacific.