



DNS Service Implementation and Changeover

White Paper

Nixu Software Oy Ltd
A Nixu Group Company
Keilaranta 15
FI-02150 Espoo
Finland

www.nixusoftware.com

Importing Zone Data to Nixu NameSurfer

The zone data can be imported from existing master name server to Nixu NameSurfer in two ways: by using the *zone transfer* function, or by using zone files compatible with BIND.

The zone transfer option excludes the possible dangers of file corruption, or zone files containing false data due to mistake after editing, through zone data validation. Another benefit from using this method stems from the real-time data accuracy: when making a zone transfer, the user can be certain that the received data is up to date.

Regardless of the method used, the zone data can be imported to Nixu NameSurfer either via WebUI using *DNS / Import* feature or alternatively using *nsctl* command-line tool. The instructions for using import function are documented in Nixu NameSurfer's online help and Nixu NameSurfer Suite Reference Manual.

Nixu NameSurfer Initialization

Given the hierarchical structure of DNS and the hidden primary architecture of Nixu NameSurfer, the hidden primary DNS server can be modified without any significant changes visible to the network, or the authoritative name servers integrated with it. Therefore, our advice is to start the DNS changeover by installing and configuring Nixu NameSurfer as the hidden DNS primary for the new environment.

At this point, the NameSurfer import function can be chosen to act upon:

- a) only the private zone data
- b) only the public zone data
- c) both the private and public zone data

By importing the zone data in increments – for example only the internal zone data first – the chance of possible problems stemming from the changeover process interfering with external services can be narrowed down significantly. By using internal zone data, the new hidden primary DNS server can be tested thoroughly and its configurations validated. The imported zone data will be managed by using the tools included in Nixu NameSurfer after the import process.

If the existing BIND servers continue to be run alongside Nixu NameSurfer hidden DNS primary during the changeover, the master server IP address of their BIND configuration (named.conf) zone definition must be changed to match with NameSurfer's IP address. Below, please find examples of BIND name server configuration:

```
zone "corporation.com" {
    type slave;
    file "corporation.com.bk";
    masters {
        20.20.20.20; #original master
    };
};
```

Or if the server in question is a master name server for the particular zone:

```
zone "corporation.com" {
    type master;
    file "corporation.com.bk";
};
```

The zone definition must be changed so that the zone type is "slave" and the IP address in the masters definition matches the NameSurfer's IP address. Please also note that Nixu NameSurfer's hidden primary DNS process listens on port 8054. In other words, the definition should appear after modification as the following:

```
zone "corporation.com" {
    type slave;
    file "corporation.com.bk";
    masters port 8054 {
        20.20.20.21; #namesurfer IP address
    };
};
```

Along with the hidden primary DNS process, a local BIND process can be activated in Nixu NameSurfer installation. If activated, the local BIND can be viewed in as *localhost* in the Remote Servers section of Nixu NameSurfer's WebUI. The BIND instance running as localhost can be added to a zone as a *Remote Secondary* name server by ticking a checkbox located next to it in zone's root node view. This causes the local BIND process to control that particular zone, and the authoritative name servers can communicate via standard DNS port :53 using Nixu NameSurfer's IP address. In this case, the BIND server configuration does not require the port definition as shown in the example above. Please also note that old BIND servers are not integrated with Nixu NameSurfer by default, so new zones created in Nixu NameSurfer are not automatically pushed to existing BIND name servers.

Installing Nixu SNS Servers

If new Nixu SNS server instances are assigned new IP addresses (as opposed to utilizing existing IP addresses used by legacy BIND servers), they can be installed alongside the old BIND servers in the production network.

Nixu SNS servers should be integrated with Nixu NameSurfer using real IP addresses, rather than for example load-balancer or virtual IP address(es). If the Nixu SNS servers have both a public and a private address, one should decide which of the two addresses is used to communicate with Nixu NameSurfer, and configure other network equipment (e.g. firewalls) accordingly.

If Nixu SNS server's IP address is changed during the changeover from the installation environment to the production network, the IP addresses should be changed again using Nixu NameSurfer's WebUI. The instructions for this process can be found in both Nixu SNS Reference Manual and Nixu NameSurfer Suite Reference Manual.

After the integration process has been completed, adding a single zone is carried out by accessing the desired zone's root node page in Nixu NameSurfer; viewing *Remote secondary servers* section; and ticking the checkboxes of those Nixu SNS servers that will be authoritative for that particular zone. When adding a remote secondary server for several zones, the basic principle is the same; however, in this case, the operation can also be performed using NameSurfer's *Bulk changes* tool. After the selections have been made and the changes have been saved by clicking the OK button, Nixu NameSurfer automatically updates the configuration and sends it out to relevant Nixu SNS servers.

In the event that some of the Nixu SNS server instances are public and some private, one should make sure that the correct Remote secondary servers are chosen for each zone. Although the process of adding Remote secondary servers to the network should be the responsibility of a more experienced network administrator, the possibility of human error still remains. Therefore, as a precautionary measure, the private and public zones can be divided into their own *Views* in Nixu NameSurfer. A View can have the IP address ranges containing the SNS servers which have access to that particular View's zone data. With this configuration, the production network can have two DNS Views in use, for example Internal and External. When adding new zones, a user-specific *Zone template* (part of User Management) containing a proper set of pre-selected Remote secondary servers for a zone can also be utilized.

In order for the new Nixu SNS servers to be made authoritative for a given zone, please follow the steps below:

1. Add the Nixu SNS servers' NS records to the zone data
2. Update the new NS records throughout the domain hierarchy

Usually both the zone itself and the parent zone of the higher domain hierarchy contain the A records corresponding to the particular NS records. Because the A records point to specific IP addresses, it is important that these are also updated and notified to the higher levels of domain hierarchy.

To ensure that recursive name servers (caching DNS servers) in the Internet will be able to perform queries with cached name servers after the changeover, the legacy BIND servers can be run – assuming they have different names and IP addresses than the new name servers – alongside Nixu SNS servers until the old zone data has expired in caching name servers.

Recursive DNS and Nixu SNS Servers

Nixu SNS server instances can be configured to function as a caching/recursive DNS server by setting the *DNS / Options / Access / Inbound restrictions / Recursion* option's value to "Yes". The clients and networks allowed to make recursive name queries using the server in question can be defined using *DNS / Options / Access / Inbound restrictions* section's *Allow recursion – IP address or block* and *Allow recursion – ACL* options. When using access control lists (ACL), they must first be defined at *DNS / ACLs* section.

Changing IP Addresses

If the servers are using temporary IP addresses before the changeover to production environment – for example in a testing environment – they must be changed before the actual changeover. Although the examples below describe how to change the IP address with different server types, it is recommended to install Nixu NameSurfer using a real IP address if possible.

Nixu NameSurfer:

The IP address of the operating system can be changed by running *system-config-network* command in the CLI. This activates a text-only editor, allowing a new IP address and name servers to be defined. New network settings will come into effect after running *service network restart* command.

In addition to the operating system, the new IP address must also be specified in the Nixu NameSurfer configuration files, as follows:

```
/usr/local/namesurfer/config/server.conf:  
primary_addr
```

recursive_name_server

/usr/local/namesurfer/config/webui.conf:
primary_addr

It is also recommended to check, and modify if necessary, the *Default master server IP* value in *Server details* section located in integrated Remote servers.

Nixu SNS server:

Run *sns-network-config* using the Nixu SNS CLI. This allows new IP addresses for different network interface devices to be configured.