DNS Management

DNS is critical to sipXcom operation.

NOTE: It is important that system administrators understand DNS Concepts to assure proper system operation.

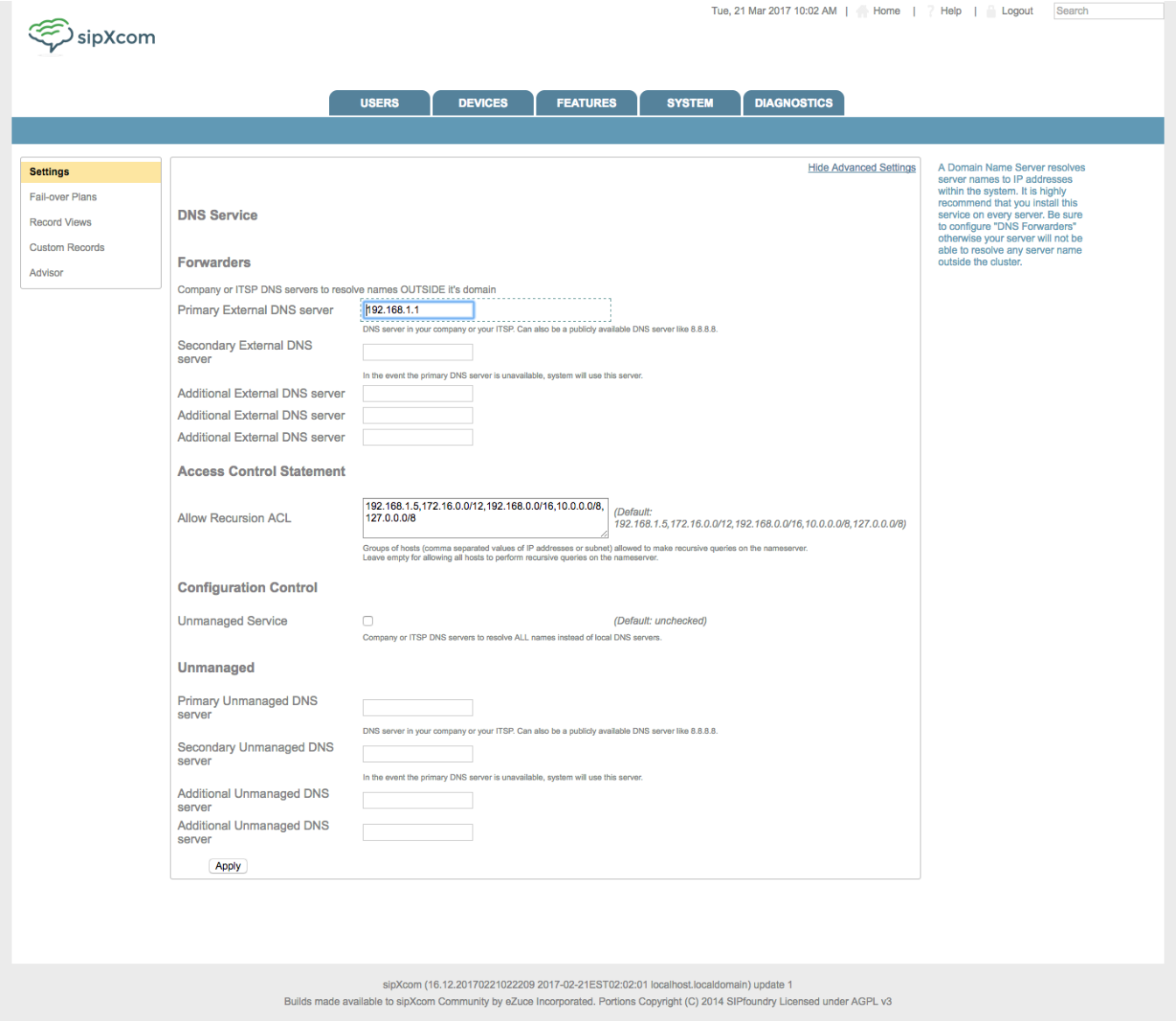
Introduction

sipXcom includes a comprehensive bind configuration management system that allows administrators to fully manage DNS as required by the communications cluster.

Specific bind documentation can be found here: https://kb.isc.org/category/116/0/10/Software-Products/BIND9/Documentation/

DNS Service Settings

DNS management can be found in the Admin Portal under SYSTEM -> DNS.



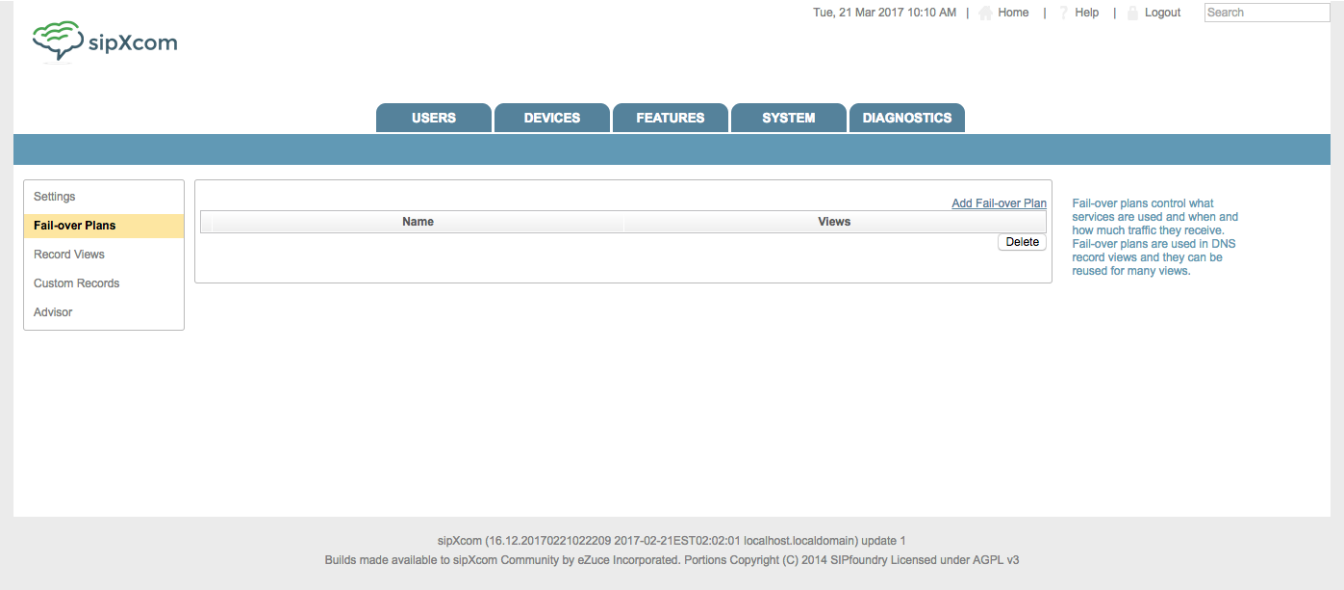
Make sure to configure at least one External DNS server for forwarding. A forwarder is used to send DNS requests to when the local DNS service can't resolve a DNS request locally.

If you wish to operate your own DNS servers (not recommended for servers, perfectly fine for phones) you can select 'Unmanaged Service' under "Configuration Control".

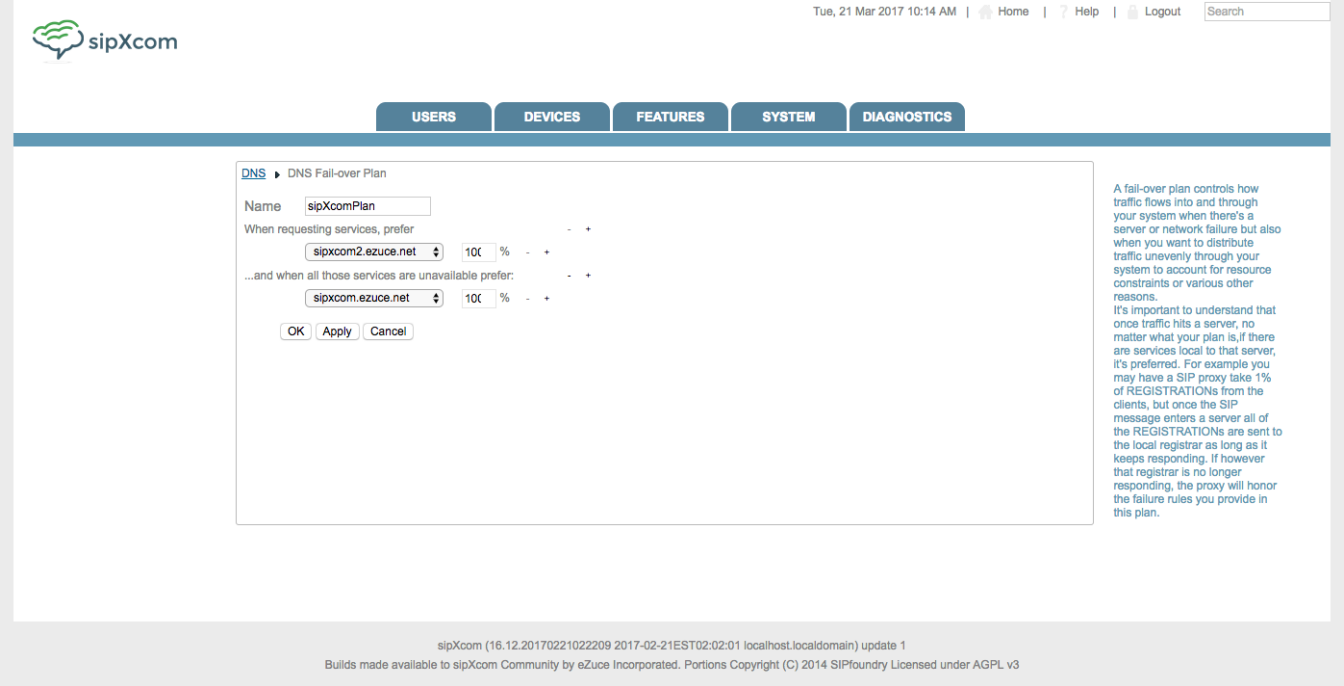
Fail-over Plans

Fail-over plans control what servers/services are used, when and how much traffic they receive. They really have no bearing in a single server system. Failover plans are use in Record Views. Fail-over Plans can also be used in multiple Record views.

Fail-over plans are also crucial when configuring Regions.

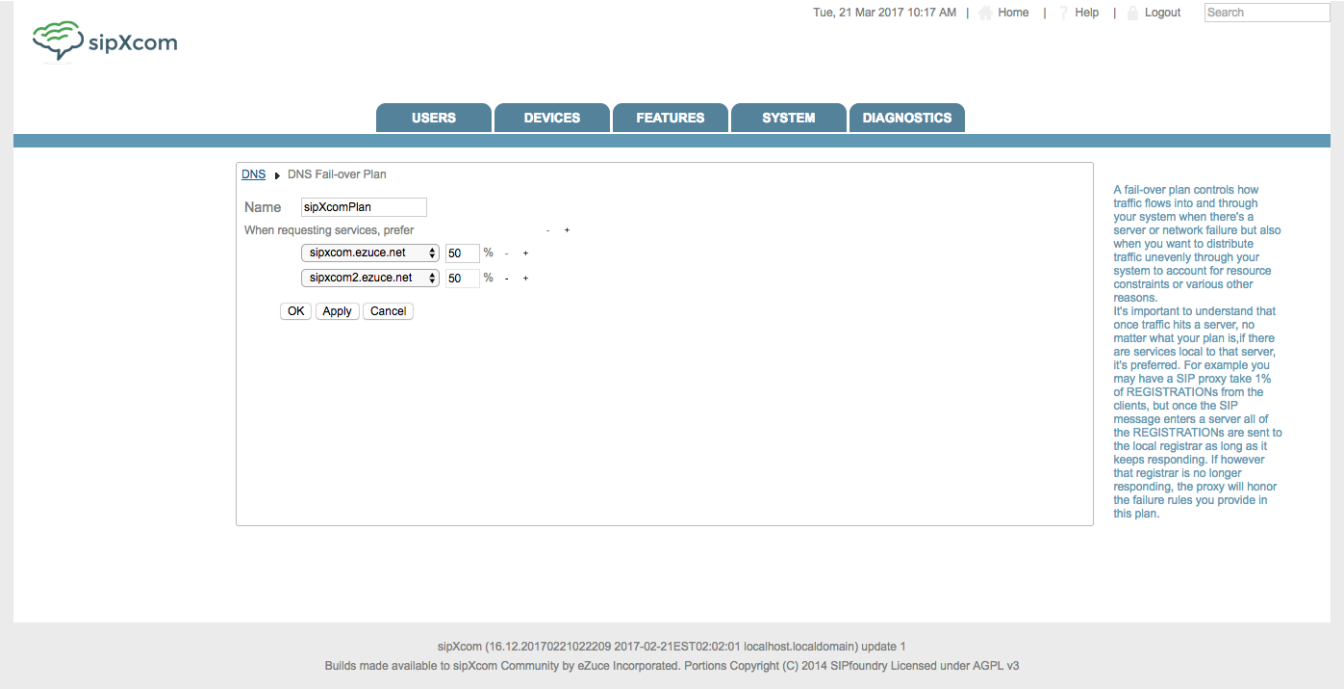


To add a Fail-over Plan, click the 'Add Fail-over Plan' in System -> DNS - Fail-over Plans.



In the above example we're creating a Fail-over Plan called 'sipXcomPlan' that will direct 100% of traffic to the server sipxcom2.ezuce.net and then fail over to sipxcom.ezuce.net.

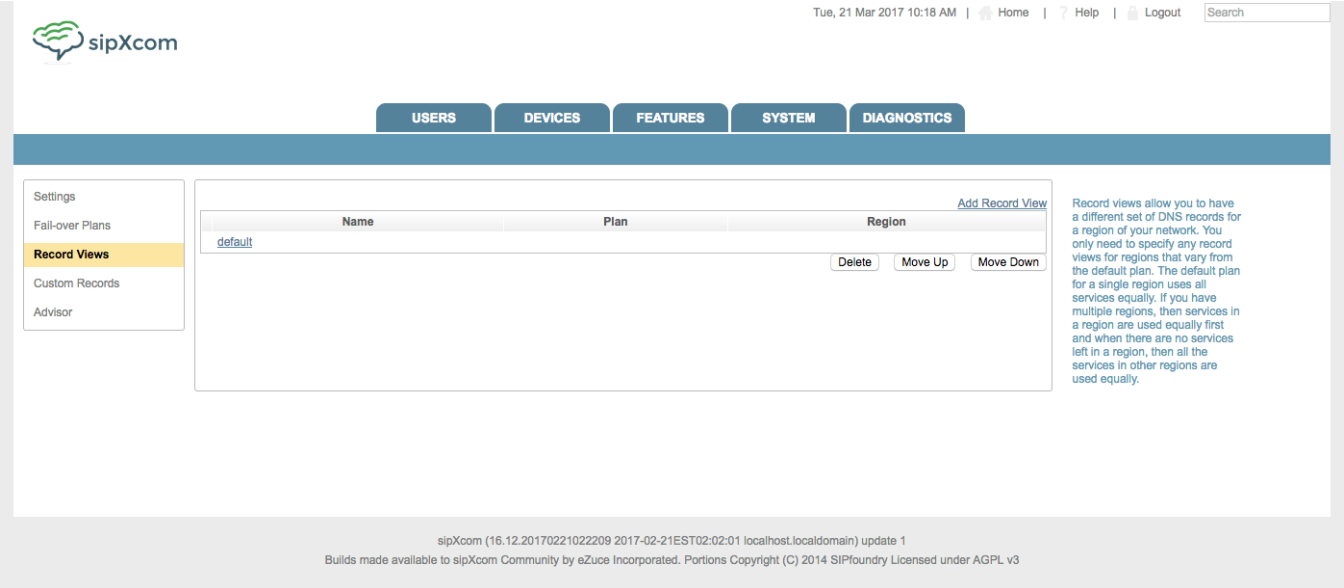
If we wanted to simply load balance and fail over across the two servers we could configure as follows:



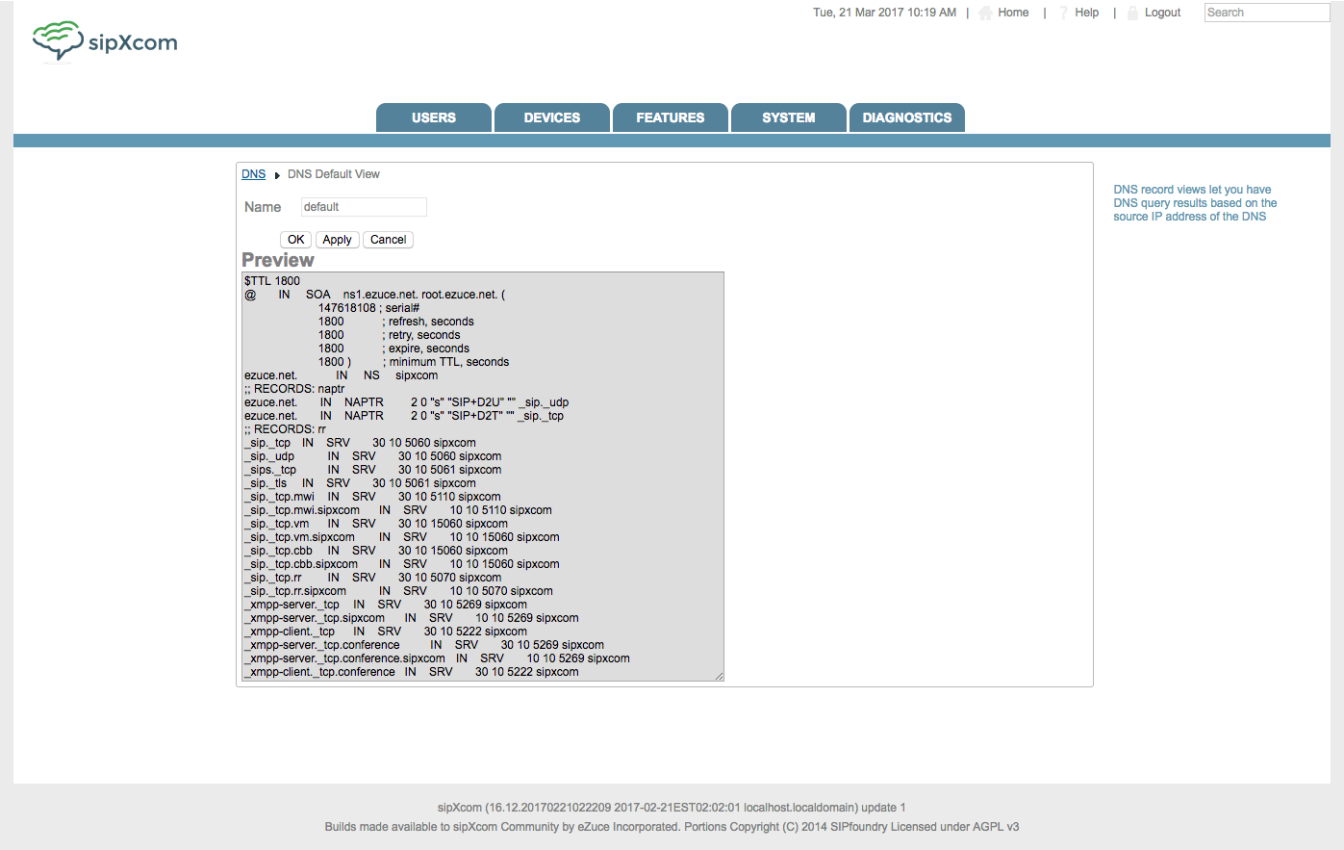
Record Views

Record views allow the administrator to configure different sets of DNS records for different segments of your network. Specify any record views for regions that vary from the default plan. If there is only a single region use the default plan. The default plan for a single region uses all services equally unless a Fail-over Plan is specified. If there are multiple regions, then services in a region are used equally first and when there are no services left in a region, then all the services in other regions are used equally.

A Record View is the equivalent of a 'bind view'. These views control how DNS responds to clients making DNS requests based on what IP addresses they come from. Before configuring new Record Views there should be some Regions defined in System -> Regions.



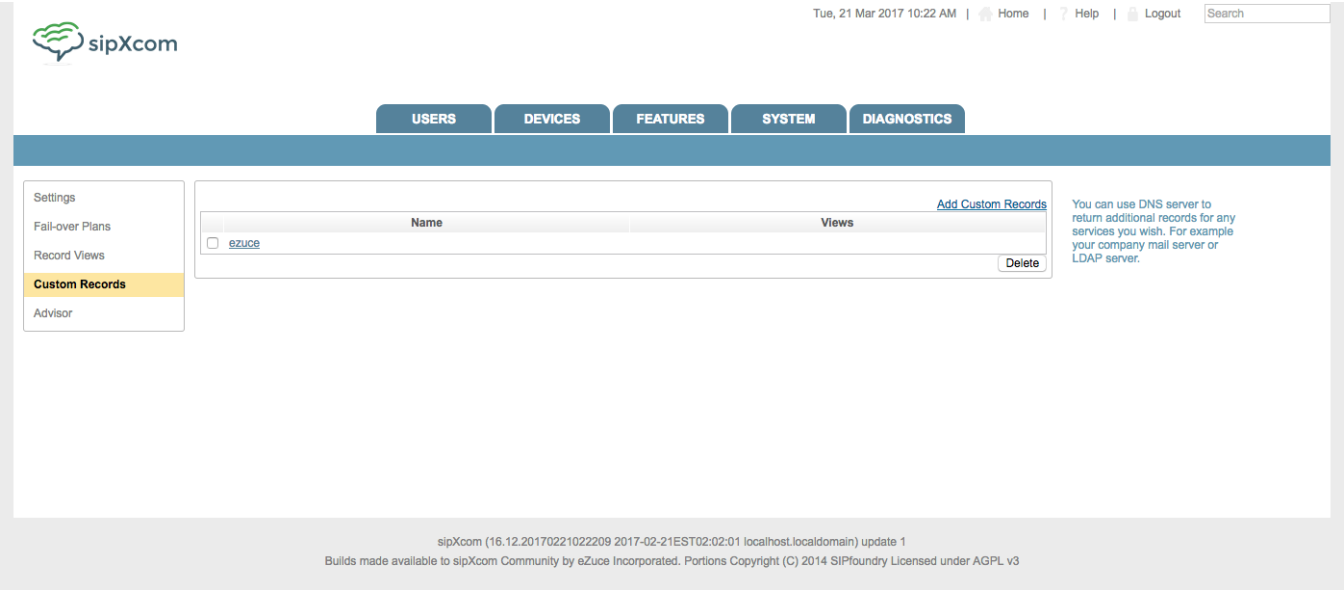
Clicking on the 'default' view provides the administrator the ability to include a Custom Record set (see following section) and provides a preview of the generated bind zone file.



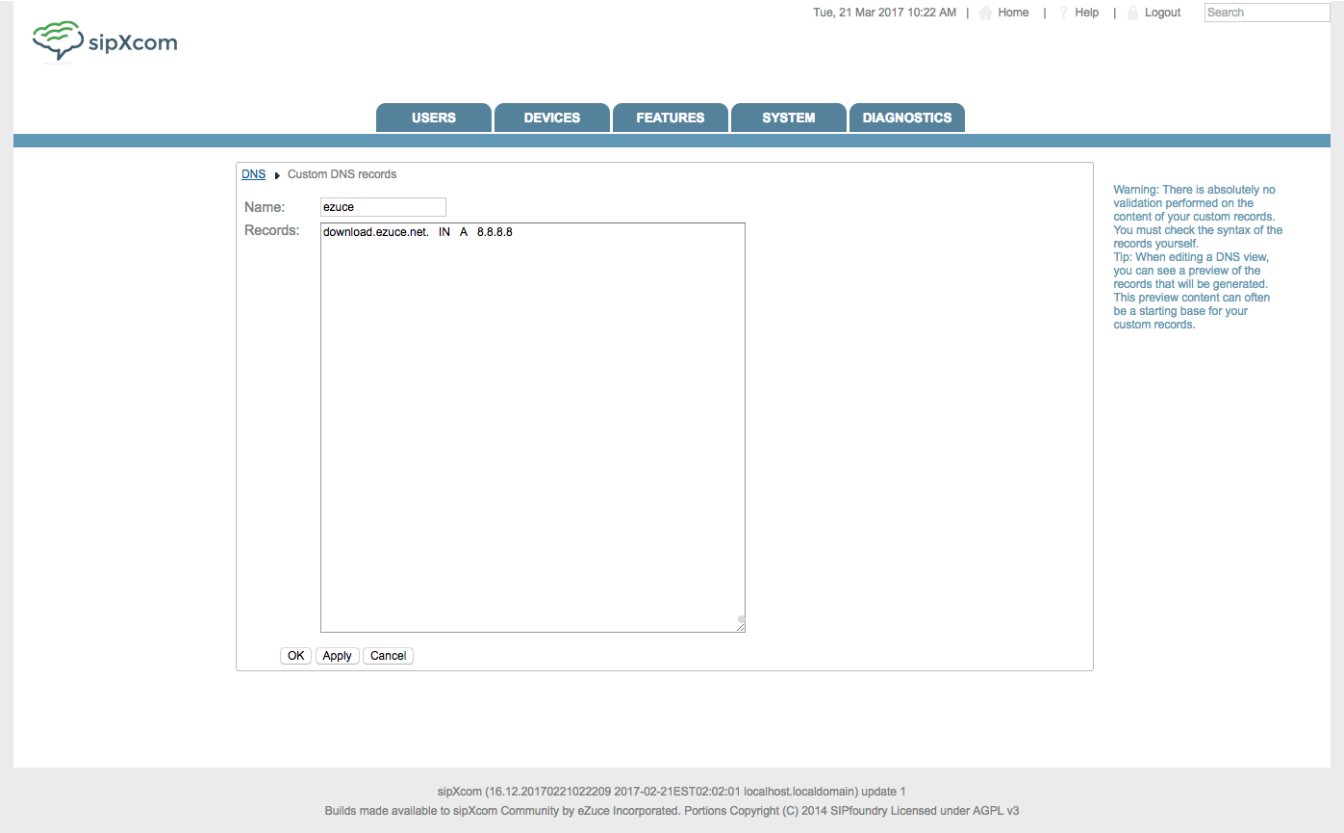
All bind zone files are located in /var/named.

Custom Records

You can use DNS server to return additional records for any services you wish. For example your company mail server or LDAP server. The typical use case for this is if sipXcom is configured with a SIP domain that is the same as the corporate DNS domain.



Click on 'Add Custom Records' to create a custom record set. The following example shows a host record added for 'download.ezuce.net' so that this server can find the external eZuce download server for ezuce.net. These are raw bind file entries (see bind documentation for information about bind records) that will get added to any Record View you add them to.



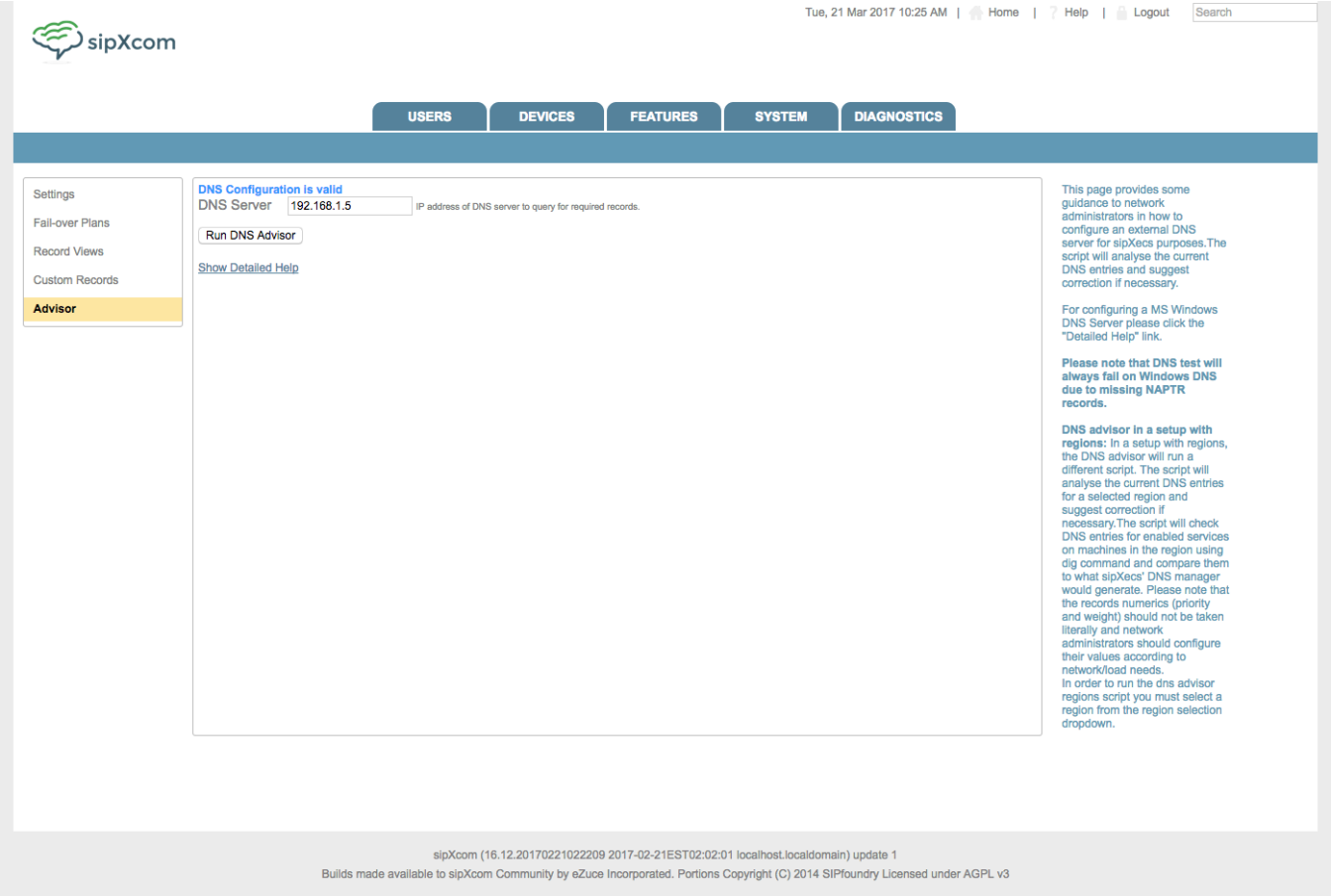
Pay attention to the warning: **There is absolutely no validation performed on the content of your custom records. You must check the syntax of the records yourself.**

Advisor

The DNS Advisor can check ANY DNS server for proper configuration for use with **uniteme**. The Advisor provides guidance to network administrators in how to configure an external DNS server for sipXcom purposes. The script will analyze the current DNS entries and suggest correction if necessary.

Please note: DNS test will always fail on Windows DNS due to missing NAPTR records.

DNS advisor in a setup with regions: In a setup with regions, the DNS advisor will run a different script. The script will analyze the current DNS entries for a selected region and suggest correction if necessary. The script will check DNS entries for enabled services on machines in the region using dig command and compare them to what sipXecs' DNS manager would generate. Please note that the record's numerics (priority and weight) should not be taken literally and network administrators should configure their values according to network/load needs.
In order to run the DNS Advisor regions script you must select a region from the region selection dropdown.



Clicking on the 'Show Detailed Help' will display the following info...

Detailed Help for Microsoft Windows DNS Servers

Using DNS Advisor you can natively take the output into a Linux server.

For Windows DNS you can use the output of DNS Advisor to configure DNS properly. The following is a guideline to assist with Windows:

1. In Administrative Tools and DNS

2. In the left-hand pane, single-left-click on the domain (under the Forward Lookup Zones into which the system will be installed.

3. To add an A record Right-click on the domain and select New Host (A).

4. In the dialogue box that appears, enter the name of the server (the fully qualified domain name field will populate automatically) and its IP address, and then click Add Host then Done.

5. The newly added A Record is displayed in the right-hand pane along with any other records already configured.

6. For SRV records do the following:

7. Right-click on the target domain in the left-hand pane and select Other New Records.

8. In the window that opens, scroll down the list and select Service Location (SRV) and then click on Create Record.

9. Enter the following values:

```
Service - enter _sip
Protocol - enter _udp or _tcp based on DNS advisor
Priority - taken from DNS Advisor value called priority
Weight - taken from DNS Advisor value called weight
Port number - 5060 - taken from DNS Advisor value called port
Host offering this service - taken from DNS Advisor value called server
```

10. Click OK.

11. For SRV RR records do the following:

12. Right-click on the target domain in the left-hand pane and select New Domain.

13. Name the new domain rr.servername and Click OK. Get these values from DNS advisor for each RR SRV record needed. The new sub-domain and its 'rr' folder are displayed in the left-hand pane.

14. Right-click on the 'rr' folder of your primary server and select Other New Records.

15. In the window that opens, scroll down the list and select Service Location (SRV) and then click on Create Record.

16. Enter the following values:

```
Service - enter _sip
Protocol - enter _udp or _tcp based on DNS advisor
Priority - taken from DNS Advisor value called priority
Weight - taken from DNS Advisor value called weight
Port number - 5070 - taken from DNS Advisor value called port
Host offering this service - taken from DNS Advisor
```

17. Click OK.

Notes:

A records - required

SRV records - HA requirement

NAPTR records - Not possible in Windows DNS and not required