Virtualized Domain Name System & IP Addressing Environments

White Paper by FusionLayer, Inc.

September 2016

Virtualized Domain Name System & IP Addressing Environments

by FusionLayer, Inc., August 2016

Any comments relating to the material contained in this document may be submitted to:

FusionLayer, Inc.

keilaranta 1, FI-02150 Espoo, Finland.

or by email to:

info@fusionlayer.com

Virtualized DNS & IPAM Environments

Virtualized DNS and IP Addressing Environments

As organizations initiate virtualization projects in their operating environments, common edge services such as Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) make a perfect candidate for virtualization.

Because of the high costs and inflexibilities associated with traditional, hardware-based DNS and IP addressing computing appliances, most organizations have implemented existing D-services (DNS, DHCP) by utilizing unsupported open source software (BIND, DHCPD) or generic Microsoft server products (Microsoft AD) on industry standard servers. These home-grown servers typically utilize a very low percentage of their CPU. They are also prone to vulnerabilities, unnecessarily tedious to manage, and require on-going maintenance. Virtualization is an excellent way to streamline these inefficiencies.

Rather than re-building new virtual machines manually, the easiest way to virtualize any network service is to use productized software packages known as virtual or software appliances. A software appliance is a self-installing server optimized for a specific task. It contains all software components required for an installation from a hardened operating system to all necessary tools and application(s). Distributed as an installation media (ISO image) that can be used to boot up new virtual machines in just minutes, software appliances automate installation and maintenance processes thereby translating to higher productivity and lower total cost of ownership.

FusionLayer specializes in virtualization-ready software appliances that provide an end-to-end solution for DNS and IP addressing needs. This White Paper suggests a route for virtualizing DNS and DHCP services in an enterprise network. For further details on individual FusionLayer Products, please visit www.FusionLayersoftware.com

Benefits of Virtual DNS and DHCP Infrastructure
1. Optimization of CPU utilization and consolidation of computing resources as DNS and DHCP servers are migrated on virtual platforms
2. Savings in hardware and maintenance costs through decreased number of physical servers in the network, software appliance usage, and centralized management
3. Enhanced availability through continuous uptime offered by advanced virtual environments such as VMware® Virtual Infrastructure 3
4. Rapid and flexible deployment, improved scalability through software appliance usage
5. Higher level of information security thanks to

Virtualized DNS & IPAM Environments

Virtualization Enables Better Security, Efficiencies

In traditional network environments, DNS and DHCP services are typically run on industry standard servers that host a number of different network services. While pragmatic, this deployment strategy involves several disadvantages:

1. Scalability issues: running several network services on a single server translates to limited scalability during busy-hours and traffic peaks.

2. Single point of failure: if the hardware platform fails, all network services provided by that server will become unavailable.

3. Vulnerabilities: when running several network services on a single server, vulnerability in any one piece of software can make all services running on that server vulnerable to exploitations.

4. Compromises in server and system management: running several network services on a single server translates to compromises in management and maintenance processes.

5. Inflexible deployment processes: making changes or new additions to network architecture is unnecessarily complicated as different network services have been bundled together.

The easiest and the most cost-efficient way to eliminate these problems is to install and run DNS and DHCP software appliances in virtual infrastructure as dedicated virtual machines. Thanks to their purpose-built design and automated software updates, software appliances are less prone to vulnerabilities and provide efficient tools for uncompromised server and system management. By auto-installing on advanced virtualization platforms such as VMware® Virtual Infrastructure, they offer better scalability, higher availability, and flexible deployment options.

Software Appliances for DNS, DHCP and IP Addressing (DDI)

FusionLayer NameSurfer IPAM is a secure management system designed for efficient distributed management of organizations' DNS data and IP address space.

FusionLayer DNS is a secure stand-alone virtualized server that can be operated as an authoritative and/or as a caching/recursive DNS server.

FusionLayer DHCP is a secure, stand-alone virtualized DHCP server with configuration validations and built-in support for DHCP failover pairs.

FusionLayer Discovery has been designed to extract VLAN, MAC, Port ID and other information produced by routers and switches, in real time, and push that data to Nixu NameSurfer Suite IPAM.

Virtualized DNS & IPAM Environments

Proceeding with DNS and/or DHCP Virtualization

For organizations that have already implemented VMware® Server, ESX Server or Virtual Infrastructure in their operating environment, virtualizing DNS and DHCP servers using FusionLayer Products is very straight forward. Generally speaking, the three-step installation process involves:

1. Booting up a new virtual machine with a FusionLayer Product installation media available at www.FusionLayersoftware.com (ISO image with CentOS Linux inside). After the first virtual machine has been booted, it can be cloned into VMware Template simplifying the installation process even further.
2. Typing in basic network configurations such as an IP address, and installing VMware tools on the software appliance platform
3. Importing existing DNS data or DHCP configurations to the new virtual machine

Solution Architecture and Related Considerations
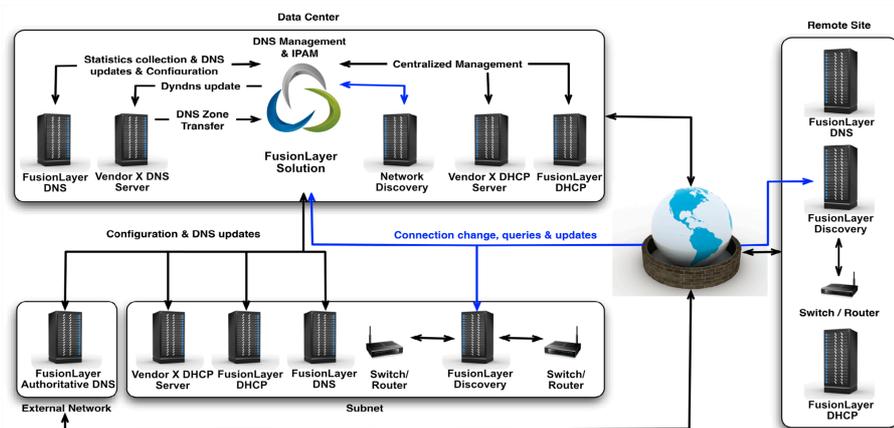
Illustration: *DNS and DHCP services in a typical enterprise network*

The graph above provides a simplified illustration of DNS and DHCP services in an enterprise network environment. The descriptions below provide general guidelines on how DNS and DHCP services can be virtualized in a typical enterprise network environment.

Data center: VMware Virtual Infrastructure provides an excellent foundation for virtualizing DNS and/or DHCP services in enterprises. In order to ensure redundancy and availability, FusionLayer recommends the following solution architecture:

I. I. Centralized DNS and IP address management system that is used to manage the entire name and address space. This system would consist of single virtual machine with support for DNS views, so that internal and external authoritative DNS zones can be managed separately. '
II. Two or more virtual machines for internal authoritative DNS
III. Two or more virtual machines for internal recursive/caching DNS
IV. Two or more virtual machines running DHCP servers as failover pair

5

If an enterprise has several data centers, it is recommended that a number of DNS and/or DHCP servers are distributed to different geographical locations for added redundancy.

Subnets: typically, subnets are workstation networks that rely on Microsoft AD for DNS and DHCP services. An alternate solution for providing DHCP and caching/recursive DNS services in subnets is to run software appliances as dedicated virtual machines on VMware Server or ESX server platforms. If this is not an option, management of authoritative DNS zone files in Microsoft AD servers can be centralized by configuring these zones files as slave zones for master zone files residing and managed in the centralized DNS management system described in paragraph 1 above.

External network / DMZ: external authoritative DNS servers residing in DMZ can be run on VMware Virtual Infrastructure as dedicated virtual machines. The data (authoritative external DNS zones) on these servers is managed using the centralized management system described in paragraph 1.

Remote Site(s): typically, remote sites are small(ish) networks that rely on Microsoft AD for DNS and DHCP services. An alternate solution for providing DHCP and caching/recursive DNS services in subnets is to run software appliances as dedicated virtual machines on VMware Server or ESX server platforms. By adopting the alternate approach, also other network services and resources can be run as virtual machines on the same virtualization platform.

About FusionLayer, Inc.

FusionLayer is a VMware Technology Alliance Partner specializing in virtualization-ready DNS, DHCP and IP address management software appliances. All FusionLayer Products are certified for VMware® Virtual Machine environments and can be used to build end-to-end DNS and IP addressing solutions.

Headquartered in Helsinki, Finland, and with regional contact points in Americas, Western and Central Europe, and Asia Pacific, FusionLayer's mission is to offer the best value in industry by creating virtualization-ready DNS and IP addressing solutions that set the benchmark for combined security, ease of use and low cost of ownership.

FusionLayer Products have an installed base of more than 6.000 instances worldwide. Our technology is used by nearly one third of all 4G mobile operators worldwide as well as by enterprises large and small from practically all industry verticals.

Support Statement for VMware® Virtual Machine Environment
FusionLayer confirms that we will support customers running FusionLayer NameSurfer, FusionLayer DNS, FusionLayer DHCP and FusionLayer Discovery on supported Operating Systems in a VMware virtual machine environment.

FusionLayer will provide unqualified support for FusionLayer NameSurfer, FusionLayer DNS, FusionLayer DHCP and FusionLayer Discovery running in a VMware virtual environment in an identical manner as with FusionLayer Products running on any other major x86 based system without initially requiring reproduction of issues on native hardware. Should FusionLayer suspect that the virtualization layer is the root cause of incident; the customer will be required to contact the appropriate VMware support provider to resolve the VMware issue.

While FusionLayer Products are expected to function properly in a VMware virtual environment, there may be performance implications which can invalidate FusionLayer's typical sizing and recommendations.