Software-Defined DDI solution for the Hybrid Enterprise

With FusionLayer Infinity and F5 BigIP DNS

Summary

The reference architecture outlined in this document introduces FusionLayer's hybrid network management design for enterprises that run Microsoft Active Directory (AD) in their networks and have implemented VPN connectivity to public cloud services such as Microsoft Azure and Amazon Web Services (AWS). The technical case study is based on a blueprint architecture FusionLayer has designed and deployed for Company Alpha (CA), a global enterprise within the logistics industry required to meet the stringent Payment Card Industry (PCI) requirements by its business infrastructure.

Introduction

During the pre-sales phase, FusionLayer carried out a discovery process whereby it analyzed CA's existing processes in the solution area. As an outcome of that assignment, three operational problem areas were being identified:

- Majority of CA's network data such as subnet and VLAN assignments, MPLS and NAT links to logical networks, and network segments activated in public cloud were managed in spreadsheets. This had led to errors causing downtime.
- Inability to automate DNS and IP address integrations with the existing VMware private cloud and the container-based application deployment model CA had on its roadmap. This led to slow service activation and increased OPEX.
- Lack of DNS security features that CA needed to consistently meet the network security requirements required by PCI.

CA's original Request for Proposal (RFP) had outlined a traditional DNS, DHCP and IPAM (DDI) architecture. Because deploying a traditional solution would have required a complete swap of the existing Microsoft DNS and DHCP infrastructure without solving all the business problems that CA was facing, FusionLayer recommended an alternate solution that allowed CA to retain its existing Microsoft core network services while addressing all the identified problems. The key business benefits of the proposed architecture involved higher levels of business continuity, operational efficiency and network security than any competing solution.

Architecture Overview

Based on the proposed architecture, FusionLayer Infinity was implemented as the single-pane-of-glass for the existing Microsoft DNS/DHCP services and the newly acquired F5 BigIP DNS instances. The FusionLayer management overlay made it possible to manage the network assignments for the Microsoft Azure VNETs integrated to the enterprise network via VPNs. Additionally, being the single source of truth for network data, Infinity was also the unified REST interface for existing VMware as well as the new Red Hat orchestrators used for container-based application deployment. Addressing the basic level of security provided by the Microsoft DNS servers, the F5 BigIP DNS servers deployed at the edge were used to protect existing DNS services against security threats.

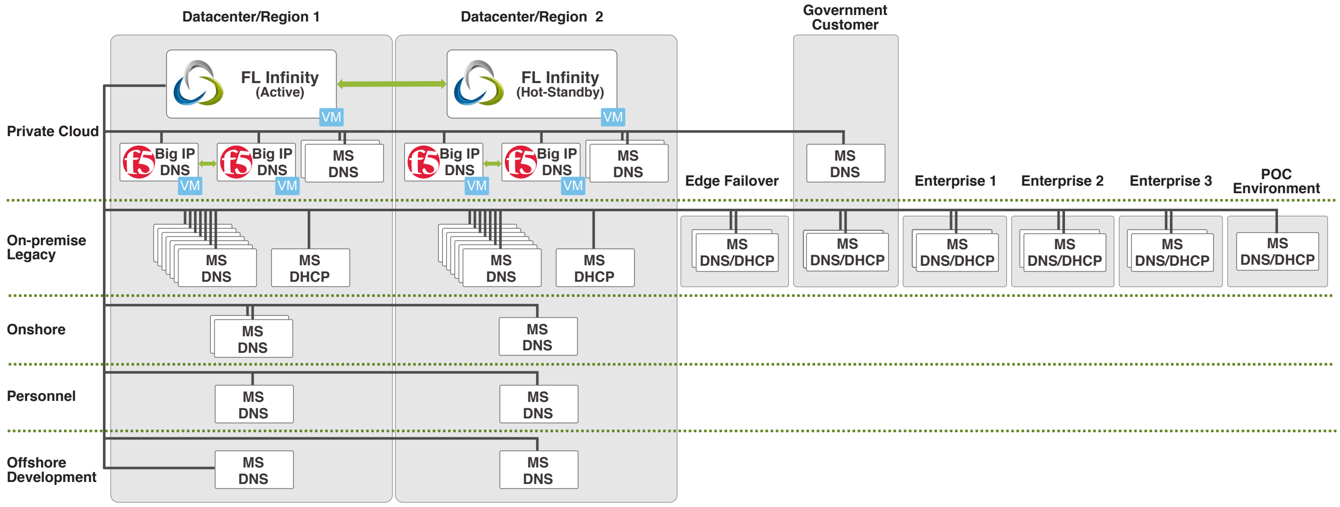


Figure 1: High level architecture depicting the proposed solution to CA

Summary of the logical design:

- Two FusionLayer Infinity (SD-IPAM) instances deployed as a HA-clustered management overlay for the existing Microsoft DNS/DHCP services and the new F5 BigIP DNS instances deployed at the edge of the network.
- Four F5 BigIP DNS instances
- Existing Microsoft Windows Server instances run by CA for DNS and DHCP
- Integration with NOC, SOC and Microsoft LDAP via FusionLayer Infinity overlay
- Option to integrate FusionLayer Infinity with subnets in public clouds such as AWS VPC and Azure VNET for multi-cloud use cases; and different orchestrators such as VMware, Kubernetes, and others for process automation.

Description of the high-level architecture:

- The two FusionLayer Infinity instances depicted in the architecture implement an HA cluster with one HA cluster member deployed in Location A and another HA cluster member in another region Location B. The two members of the HA cluster function using a primary – hot-standby replica model whereby the data in the two server instances are automatically synched up for redundancy. If the active server is lost, the hot-standby replica will automatically pick up the service and appoint itself as the new active primary server.

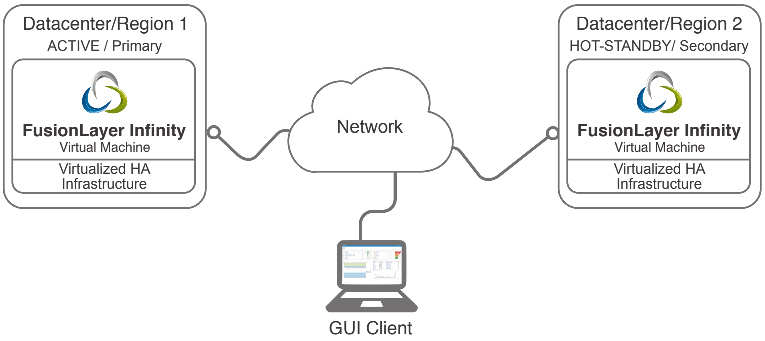
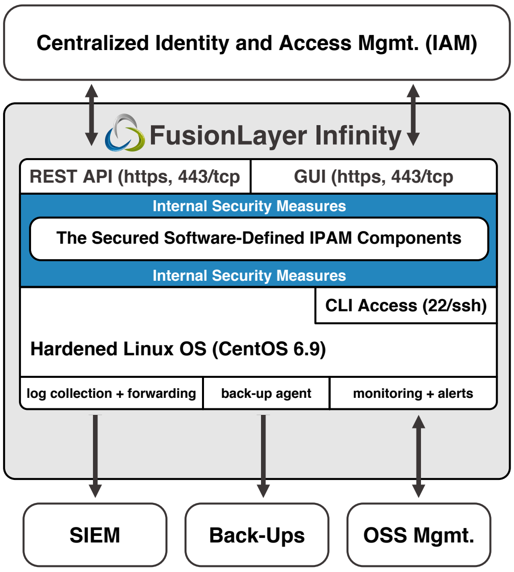


Figure 2: FusionLayer Infinity HA architecture

The FusionLayer Infinity HA cluster delivered visibility and manageability for the existing Microsoft DNS and DHCP and the new F5 BigIP DNS instances. Additionally, Infinity was integrated with Microsoft LDAP to provide centralized authentication/authorization and audit trails (who, what, when) of all changes. Finally, the Infinity instances were also integrated with CA's existing NOC (SNMP-based monitoring) and SIEM (log forwarding) to align with their current security and operational frameworks.


Centralized Identity and Access Mgmt. (IAM)
FusionLayer Infinity
REST API (https, 443/tcp
GUI (https, 443/tcp
Internal Security Measures
The Secured Software-Defined IPAM Components
Internal Security Measures
CLI Access (22/ssh)
Hardened Linux OS (CentOS 6.9)
log collection + forwarding
back-up agent
monitoring + alerts
SIEM
Back-Ups
OSS Mgmt.

Integrations with:

- OSS management
- Back-ups
- Identity and Access Management
- SIEM

Security Architecture:

- Principle of Defense in Depth
- Principle of Least Privilege
- Role-Base Access with:
  - Centralized Authorization
  - Centralized Authentication
  - Audit Trails

Figure 3: FusionLayer Infinity architecture and integration with NOC and SOC

Server Specifications:

- Two FusionLayer Infinity server instances virtualized as VMs running on existing VMware infrastructure. The per-VM specifications were 8 assigned cores; 8GB of RAM; and 200GB of disc space. These were deployed as virtual software appliances (based on CentOS Linux) with a hardened operating system provided by FusionLayer as part of the delivery.

- The Microsoft DNS/DHCP instances depicted in the architecture continue to run as previously. The integration between the Infinity overlay and Microsoft utilized existing XML API and secure DNS update mechanisms embedded into Microsoft Windows Servers (2008, 2012 and 2016) without requiring any changes to the existing architecture.
- The F5 BigIP DNS instances in the proposed architecture were integrated with FusionLayer Infinity management overlay using the REST API embedded into F5 BigIP and by using standard DNS protocols such as IXFR/AXFR and NOTIFY.
- The architecture additionally enables integrating public clouds (AWS, Azure) and on-premise orchestrators such as Kubernetes, Ansible or VMware to the FusionLayer Infinity management overlay at any time. Without any changes to the proposed architecture.

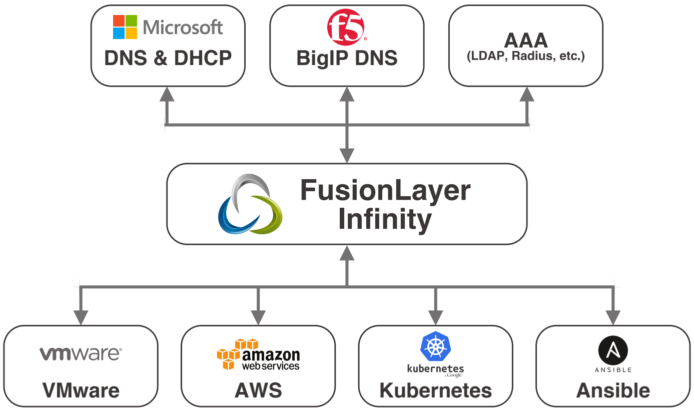


Figure 4: FusionLayer Infinity integrations with AWS, VMware, Kubernetes and Ansible

Data Migration Process

The new architecture considerably simplified the onboarding process for CA. With Infinity's standard integration with Microsoft DNS and DHCP, all of the data in the existing services automatically populated into Infinity within minutes of the completed integration.

The integration required only configuration changes and no architectural changes. The configurations required were as follows:

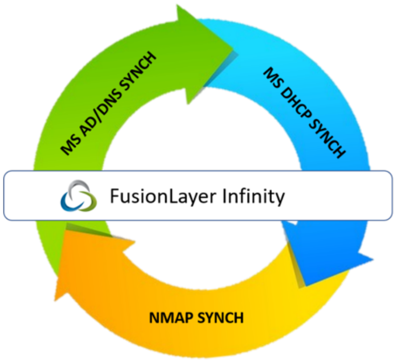
- The MS DHCP integrations used the built-in tools in Infinity’s Integrated Server functionality. Once any given Microsoft DHCP instance had been integrated and access permitted, the data synchronization happens automatically in Infinity.
- The MS DNS integration used built-in tools in Infinity’s Secondary Zone functionality. Once configured, Infinity read all AD / DNS data in the servers and automatically populated that data into the Infinity overlay. At any time, Infinity can also be configured to add hosts into existing Microsoft DNS zones using the secure DNS update functionality (Kerberos + GSS/TKEY) by Microsoft.

The data migration process was carried out as follows:

1. DHCP scopes/leases were exported from existing DHCP servers and imported into FusionLayer IPAM. The export happened with Infinity reading the networks from each MS DHCP using the XML API. After reading all the data, the discovered networks were then converted into managed. This means that they were added into IPAM and the contents of those networks were synchronized into Infinity.
2. Infinity synchronized with Active Directory (AD) DNS zones and imported the existing hostname + IP address pairs into Infinity. Those pairs then automatically populated into each matching network managed in Infinity. During the import, no duplicate hostnames were found. However, if duplicate hostnames exist during the discovery phase (DNS, DHCP scans),

they are displayed next to the IP address for clarity.

3. As a complementing discovery method, NMAP scans enabled Infinity to discover active hosts that were not in Microsoft DHCP or DNS. It is recommended to only run NMAP scans after MS DHCP data has been converted into managed. Running NMAP sweeps identifies which hosts within a given subnet are replying.



Note: If the same hosts are discovered from multiple sources, the specific synch methods used to discover the host (DNS, DHCP, scan) are shown next to the IP along with its name. This is to help simplify the resolution process.

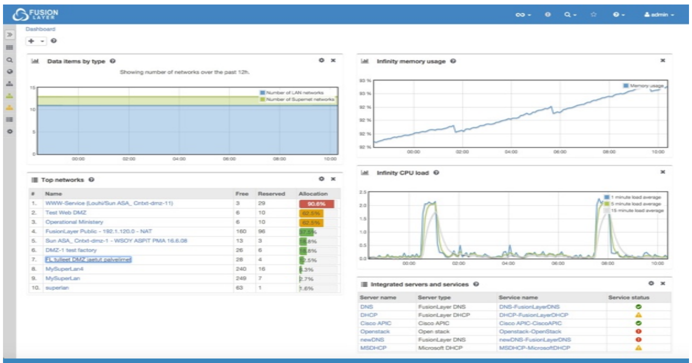
The Environment & Architecture

CA is a global Enterprise with a leading presence throughout EMEA and Asia-Pacific. As a result, the DDI solution plus existing technologies for Company Alpha include:

- 2 FusionLayer Infinity instances (HA) with:
    - Role-based Access Control (RBAC) and audit trails of all changes.
    - Network discovery tools for locating existing subnets and VLANs
    - DNS management tools for automated management of DNS zones
    - Zero-Touch DNS Provisioning for F5 DNS and Microsoft DNS
    - Integration possibilities to next-generation network services including:
        - Traditional DNS and DHCP network services (F5 & Microsoft)
        - On-premise SDN controllers (Cisco ACI, Nokia Nuage, & VMware NSX)
        - Orchestrators (Kubernetes, Ansible, & Puppet)
        - Public cloud services (Amazon Web Services & Microsoft Azure)
- 4 F5 BigIP DNS
- 30+ Microsoft DNS
- 10+ Microsoft DHCP

The Result

CA has successfully implemented visibility, manageability and additional security into their existing network architecture. CA has effectively eliminated the possibility of network downtime caused by manual DNS and DHCP management errors and solved their DNS security problems. With the cost of network downtime being estimated by Gartner at 5,600 USD per minute, CA is expected to save millions of dollars annually.



Top networks

#	Name	Free	Reserved	Allocation
1.	WWW-Service (Louhi/Sun ASA_ Cnbt-dmz-11)	3	29	90.6%
2.	Test Web DMZ	6	10	62.5%
3.	Operational Ministery	6	10	62.5%
4.	FusionLayer Public - 192.1.120.0 - NAT	160	96	37.5%
5.	Sun ASA_ Cnbt-dmz-1 - WSOY ASPIT PMA 16.6.08	13	3	18.8%
6.	DMZ-1 test factory	26	6	18.8%
7.	FL tulleet DMZ jaetut palvelimet	28	4	12.5%
8.	MySuperLan4	240	16	6.3%
9.	MySuperLan	249	7	2.7%
10.	superlan	63	1	1.6%

Integrated servers and services

Server name	Server type	Service name	Service status
DNS	FusionLayer DNS	DNS-FusionLayerDNS	✓
DHCP	FusionLayer DHCP	DHCP-FusionLayerDHCP	⚠
Cisco APIC	Cisco APIC	Cisco APIC-CiscoAPIC	✓
Openstack	Open stack	Openstack-OpenStack	❗
newDNS	FusionLayer DNS	newDNS-FusionLayerDNS	❗
MSDHCP	Microsoft DHCP	MSDHCP-MicrosoftDHCP	⚠

Global Toolset - Dashboard

About FusionLayer

FusionLayer streamlines cloud and application delivery in next-generation data centers. The company's vendor-agnostic technology bridges the gap between network infrastructure, orchestrated cloud, and network function virtualization workflows.

Our Software-Defined IPAM: manages and provisions changes to existing DNS and DHCP servers, performs L2/L3 network discovery and enables free networks to be pushed into SDN controllers for automated activation and configuration. It also powers real-time network parameter provisioning for multiple clouds and NFV orchestrators, enabling fully automated application and network service deployment inside shared or overlapping networks.

Nine out of 10 of the world's largest service providers leverage FusionLayer. Visit fusionlayer.com.