Boost Your Cloud Infrastructure Agility With Integrated DDI

Highlights:

The ever-increasing need for competitiveness has had a significant impact on the IT department's mission and budget. Supporting the business with fewer means has led to industrialization through advanced IT automation.

Virtualization and open API(s) have been the key technologies enhancing this transformation, introducing the abstraction layer required to build a simpler orchestration schema, democratizing the cloud.

Outline:

While infrastructure becomes more and more complex, mixing public and private resources, businesses require more and more interconnected services that are highly available and easily scalable, with very low time-to-service.

The most efficient way to provide such services is to automate the most of the deployment, offering self-service IT products to the business. But how do you automate a process when even your in-house experts cannot find a reliable source of information - the single network source of truth (NSoT) - about fundamental resources amongst the multiple, sometimes contradictory, databases that store your infrastructure's current state? IP address assignment and DNS registration are key configuration items that directly impact service accessibility and visibility. Unfortunately, the criticity of DDI (DNS-DHCP-IPAM) services is often underestimated, as they can be very simple to configure and maintain in small environments. IP address assignments are often delegated and then listed in difficult-to-share Excel datasheets. DNS registry is maintained manually, as are DHCP configuration files. DDI complexity and criticality increase as quickly as a network grows, putting IT services continuity and deployment capacity at risk when not managed properly.

In this context, as the DevOps approach is widely adopted, network teams need to provide a reliable service for network resources provisioning. Modern DDI is a starting point. It provides a centralized way to maintain a complex addressing plan - based on IP Data Lakes - and automating DHCP and DNS configurations. It strengthens foundations of cloud infrastructures to enhance their scalability, resiliency and management agility, allowing network engineers to focus on the infrastructure's future upgrade plan to absorb the incoming workload.

IP Data Lake
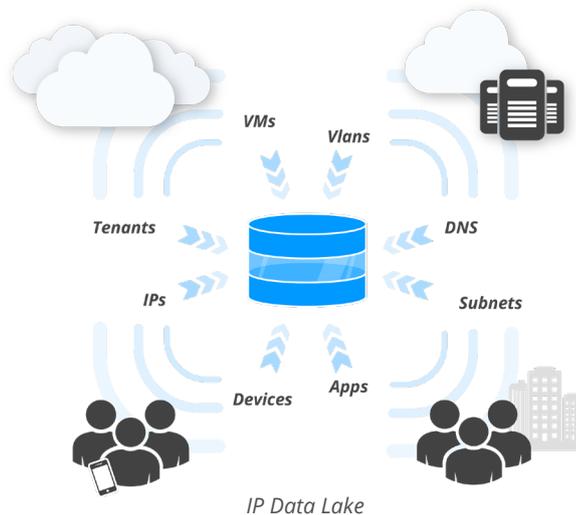
In this paper, we will discuss these subjects, and explore the common automation models and tools available to you in your hybrid cloud automation journey.

DDI Services and Cloud Automation

Enterprises' IT departments are now providing self-service portals to their users to fulfill business needs. They embrace the DevOps approach that reduces time-to-deployment, delegating the capability to publish services to non-administrative roles.

The current standard is to deploy the IT workload in highly industrialized environments running on top of cloud infrastructures, where the service's components are commonly distributed across one or more virtual machines following an SOA approach (Service Oriented Architecture).

According to this model, any service can be built on top of other components, remaining independent of their implementation according to a clearly specified middleware accessed through API, relying on IP network communication.

But if this tends to improve agility, the underlying infrastructure is increasingly distributed and dynamic, making it challenging to manage.

In the meantime, under financial engineering pressures, cloud hybridization is becoming the solution to lower expenses. IT workloads are now hosted according to their properties:

- Static business critical workload is hosted on private cloud
- Highly dynamic workload is hosted on public cloud

In some advanced cases, mature cloud users even spread their dynamic workload across several cloud providers, making the information system and its addressing plan to ensure network accessibility even more complex.

There is only one way to deal with such a complicated system: industrialization. In this case, it relies on the automation of the resource provisioning workflow.

The Requirement To Automation: Insight

Automating a provisioning workflow is not as easy as it seems. Before deploying any kind of service, you need information about its properties and a proper way to manage the affected resources that are limited in quantity, or which have to be unique:

- Storage capacity (storage that can be used to store the data)
- System CPU/memory (hypervisor cluster that suits to host the service)
- IP addresses (available addresses that suit security and accessibility needs)
- FQDN (unique available human-readable addresses that fit the service name)

These are needed in order to ensure that a service will be provisioned on top of the appropriate provider (public or private), according to predefined business rules. It also optimizes resource usage while preventing conflictual assignments such as conflicting IP address or FQDN deployments, putting IT services availability at risk.

This insight level is generally obtained through several tools:

- IP address management
- DNS resource records management
- Licences available in provisioned pools
- System Inventory (Currently Provisioned Compute/Storage Resources)
- System Monitoring (Compute/Storage Resources Usage)

These are key components of a database commonly named CMDB (Configuration Management DataBase), which is the core of any automation engine. Yet a vast number of organizations lack modern DDI, and even more lack a modern CMDB infrastructure to properly manage IP resources. This limits them in their cloud industrialization, preventing the implementation of an efficient and fully automated service deployment workflow. Implementing a DDI solution is one of the first steps of a successful IT automation project.

It might be possible to start automating a service provisioning workflow without a CMDB, relying instead on existing tools to manage a limited set of compute and storage resources. But as a company's address plan and the DNS registry are global, a DDI solution is more highly recommended to ensure network consistency and reduce the development cost of automating IP addresses and DNS records management.

Therefore, every CMP (Cloud Management Platform) product on the market integrates some sort of IPAM/CMDB, even on their lowest level of implementation. But when dealing with an entire information system, these embedded tools are limited. They only deal with delegated resources management, leaving the intricate development of the integration workflows in the overall infrastructure up to you.

Orchestration Models and Tools

Orchestration is a process- ideally automated- coordinating and managing complex computer systems and services. It is a key to the current IT industrialization approach allowing the automation of deployment workflows. It can be introduced in the following abstract model:
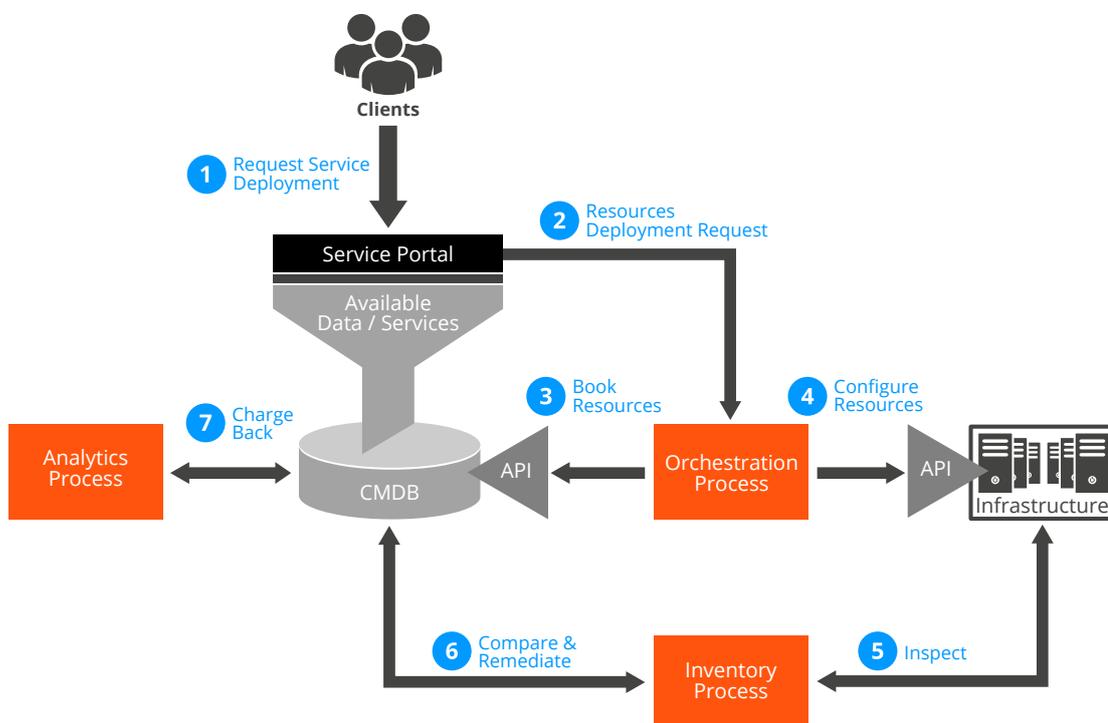
Abstract Orchestration Model

Orchestration has been developed based on ITIL recommendations, focusing on service lifecycle management. Such processes require insight on your platform's current state, to decide which available resources suit the needs of the service about to be deployed (such as where to host your workload and the data while ensuring service accessibility to the intended audience).

In this model, handling resources can be managed in three ways:

- **Delegation:** A limited set of resources is assigned to a specific orchestration platform without any control from the upper level. These resources are managed through embedded, limited CMDB. Insight is rarely consolidated at the enterprise level, therefore such a platform generally lives on the side of the enterprise information system with limited integration. Data then grows more disparate across the available databases and becomes out of sync amongst each "ecosystem". Still, as it is the easiest way to proceed, many platforms are deployed this way.

- **In-sync delegation:** a hypervision or sub-cloud system uses its internal IPAM system to manage dynamic allocation of IP addresses to its compute components, mainly virtual machines or containers. This internal IPAM uses a well known set of address blocks configured statically and reported in the central IPAM. The provisioning process is able to synchronize information from its internal repository to the external world, typically a full central DDI service in order to provide visibility and help in automating complex processes outside of the sub-cloud system, such as naming of the communication endpoints, security through filtering or more basically cost control and billing of used resources to customers.

- **Central dynamic booking:** Resources are managed through a central CMDB, and are allocated dynamically and supervised from a central point of view. Orchestration takes place in a global environment, ensuring the cohesion of the information system. This kind of deployment requires a certain level of maturity and extended integration of the related processes.

In all three cases, DDI has an essential role to play and needs to be tightly integrated into the process, to allow you to manage limited resources that require an accurate dynamic inventory (IP data lake) to ensure the efficiency of your applications and provide the visibility over the entire IP addressing plan and device resources.

Orchestrating With DDI

As we have already seen previously, the cloud has brought a new and unprecedented level of agility to the IT infrastructure, reducing costs and time-to-service. It is now possible to provision services within minutes, when it previously took days or weeks.

However, deploying a service still requires deploying virtual machines connected to the IP network to handle the workload. These virtual machines will only be accessible once they are assigned an IP address and network name (FQDN – Fully Qualified Domain Name).

Assigning and releasing these resources is a cornerstone to a service provisioning workflow that must be integrated in any orchestration process that wishes to automate it. But, as often, the challenge is more complex than it seems. In today's networks reflecting a company's organization, it is common to deal with multi-tenant architectures where the IP addressing plan and VLAN mapping are used to enforce security policies and segregate network flows.
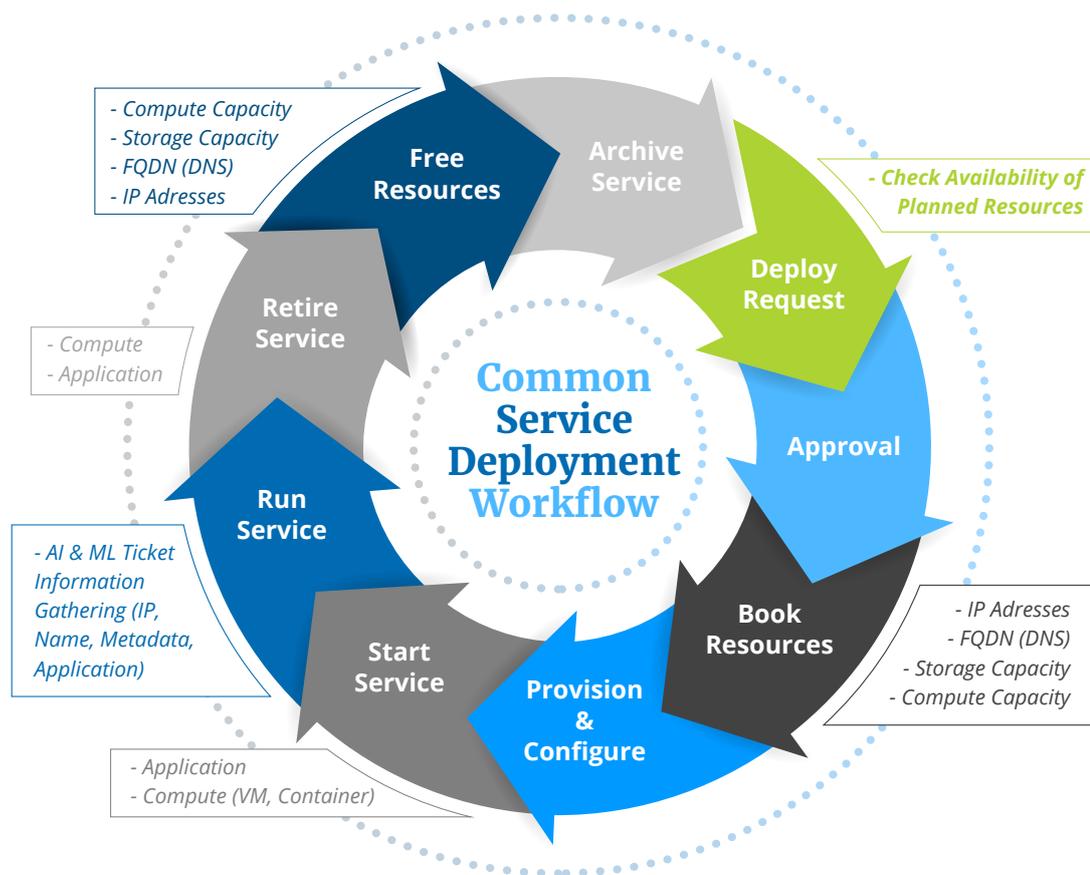
Therefore, IP addresses must be allocated in a precise and consistent way within the overall IP network schema. Keep in mind that any process' choice or action which cannot be addressed automatically implies human interaction, reducing your agility. This creates several challenges:

- Managing IP addresses in multi-tenant environments dealing with overlapping addressing plans (Service Providers / Hosting providers / DSI managing several subsidiaries) requires interacting with different databases, while maintaining important relationships such as subnet to VLAN association. Handling this complexity in a workflow requires advanced customization-modern DDI products already deal with such complexity.

- Managing multi-vendors, distributed DHCP and DNS services require developing a custom sub-orchestration process to address each case. Modern DDI products offer unified built-in advanced automations, handling the inner orchestration required to manage DHCP and DNS services.

- Ensuring IP addresses are mapped to DNS records (in both Direct and Reverse zones) so that users know they are accessing the correct version of the service.
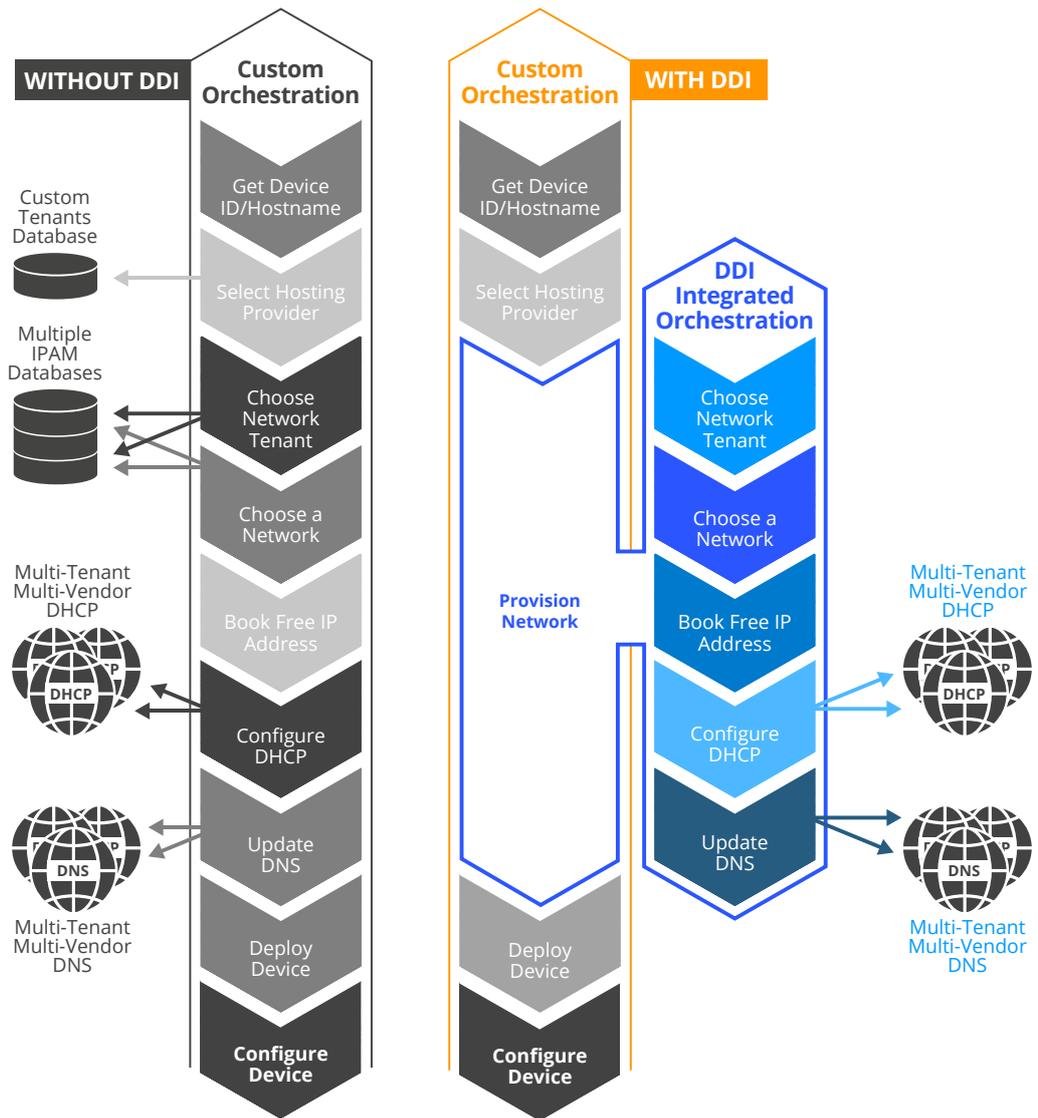
Device Deployment Workflow

Addressing these challenges correctly allows you to reduce IP space fragmentation and avoid dead-end routing and duplicated addresses, ensuring your capacity to quickly deploy new applications that are always accessible to authorized users.

By allowing any IT tool from the ecosystem to interact with the DDI solution through API and data access, the automation process is sure to be taken into account in all the IT processes. Security can use rich metadata to ensure application access is not compromised, supervision can automatically add deployed components based on DNS records and IPAM information, accounting can update the inventory for costing redistribution.

The automation intrinsically embedded in the DDI solution is also made available to any external service using API and automated event notification. This in-and-out messaging solution between IT components and a central repository or IP information acting as a single source of truth is very important to ensure seamless deployments and help digitalization of the processes.

The important topic of decommissioning is largely simplified by the presence of a central repository (data lake) containing all IP related information and associated metadata. Using cloud services implies cost control; limiting the lifetime of deployed resources helps with this and is made far more simple with an automated DDI solution.

An Efficient Solution

EfficientIP is aware of the challenges of orchestration in cloud environments, and SOLIDServer™ product that can easily integrate your orchestration schema, using any of the below tools:

- Top market orchestrators (plugins and API)
    - HP-OO/HP-CSA
    - BMC SoftWare - Cloud Life Manager Orchestrator
    - Cisco
    - Microsoft - System Center
    - VmWare - Vrealize
    - Red Hat - Cloudform
    - OpenStack - Neutron (through custom driver)
    - Hashicorp - Terraform
- Common configuration management/enforcement tools (API)
    - Chef
    - Puppet
    - Ansible
    - Salt
- Custom orchestration workflow developed internally (API)

Through product integration, you are provided with a centralized and resilient management tool allowing you to drive your entire network infrastructure.

Orchestrating private cloud services in multi-tenant environments is made easier with DDI. It provisions IP addresses in the appropriate spaces and subnets on demand, optimizing the fragmentation of your network while ensuring the availability of the application from the authorized tenants.

In the meantime, you do not need to develop advanced orchestration schemas. Embedded DDI orchestration processes are easily tunable through GUI, allowing you to extend an existing object's behavior using customized templates and inheritance, with the ability to trigger custom rules to enforce your own policies. The inner complexity of driving multi-vendor/multi-tenant DNS-DHCP environments is then masked. The product takes care of registering the necessary static DHCP reservations while creating the appropriate DNS and reverse DNS records, ensuring your application accessibility. This allows you to focus on your business process, not on the supply chain.

As a result of implementing this centralized orchestration, you gain visibility into your platform's behavior, enhancing your network provisioning process. Using IPAM alerting rules, you can now be notified when your IP address pools are about to be exhausted, before being unable to deploy new applications. You are offered the ability to easily compare which resources have been provisioned against the real resource usage of your infrastructure. Using the NetChange solution and its dynamic discovery process, you get clear reporting to identify and correct these possible inconsistencies and release unused resources.

Your application's accessibility and your ability to deploy are dependent on your DNS and DHCP services. Securing their availability is critical. SOLIDserver, through its smart architecture, automates deployment and management of resilient DNS-DHCP architectures to ensure services continuity. Still, it is remiss to talk about availability without talking about security. SOLIDServer™ also provides protection against advanced DNS security threats such as DoS and zero-Day exploits, enhancing your DNS service resiliency.

EfficientIP provides you with the required agile solutions for simplifying and automating the relationships between your IPAM, VLAN plan, and DHCP and DNS services, while interacting with your overall cloud platforms to accelerate your deployments. In today's world, where both scalability and availability of front/backend services of the business is critical, DDI from EfficientIP could be one of the competitive advantages.

efficient iP®

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752