This document is an annex to the Cloudband onboarding questionnaire.

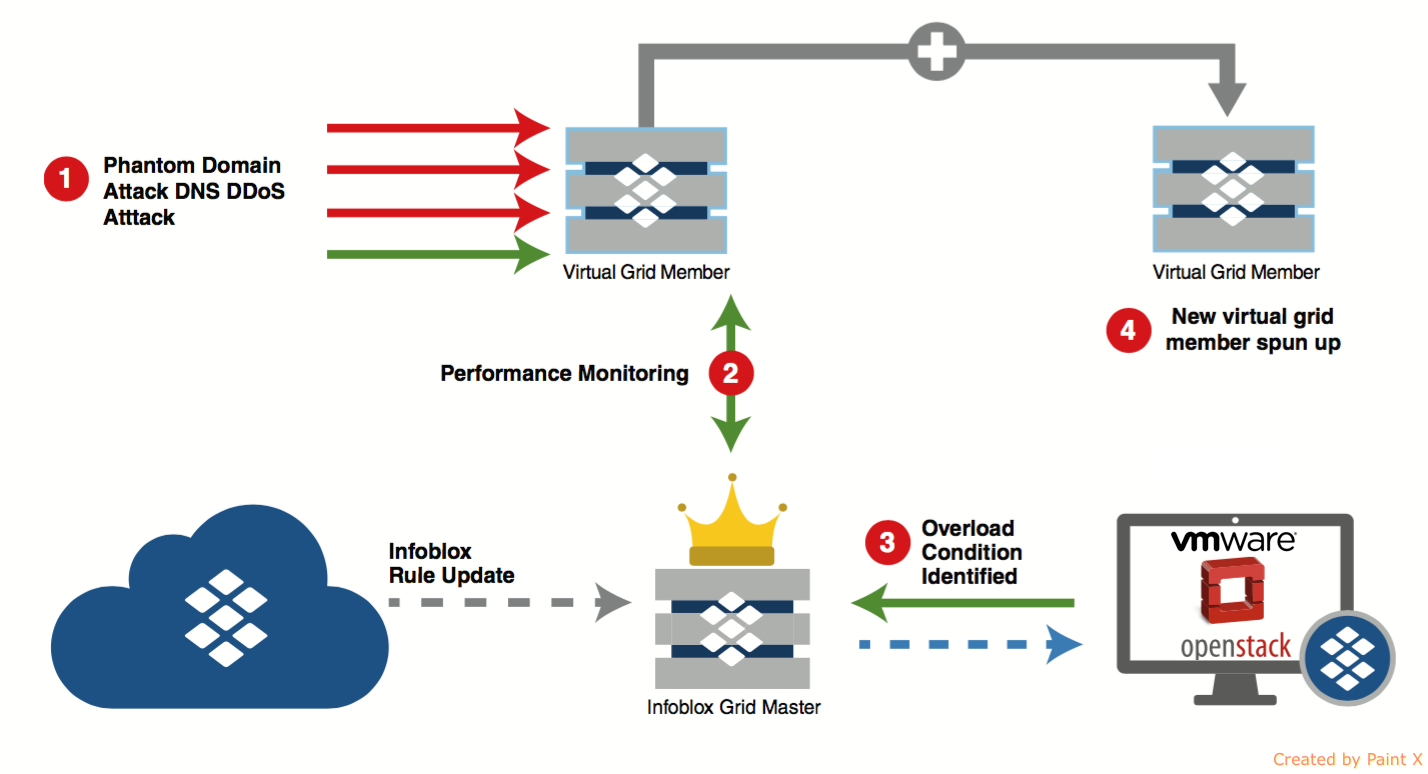
**A2**

Operators have embraced network functions virtualization (NFV) as key technologies to promote service agility and fast roll-out, simplify network operations, provide cost-effective and elastic scalability, and reduce costs. This extensive network transformation, combined with new security and competitive challenges, requires a redefinition of the role of DNS, which was initially designed to provide simple mapping of application and service names to IP addresses. Infoblox has grown DNS into a robust technology, which supports new services, protects against escalating threats, and supports service-provider network strategies. Today Infoblox Virtual Secure DNS Solution includes enhanced capabilities that support existing physical and hybrid networks and a smooth network transition to NFV and SDN.

Infoblox Virtual Secure DNS Solution

The Infoblox Virtual Secure DNS solution for service providers is a hardened, proven solution that provides mission-critical functionality while reducing the business and operational risk during the network transition to NFV and SDN. The Infoblox solution redefines DNS, once regarded simply as a rugged, scalable network utility, and incorporates the function into a strategic platform that supports next- generation operator services, network transformation strategies, and business goals.

The Infoblox Virtual Secure DNS solution employs security rules to detect, report upon, and stop DoS (Denial of Service), DDoS (Distributed Denial of Service) and other network attacks targeting DNS caching and authoritative applications. This solution helps minimize “false positives” and ensures that your mission-critical DNS services continue to function even when under attack. Advanced DNS Protection is designed to provide visibility and protection against network floods and DNS threats. It detects DNS attacks through predefined and custom threat protection rules, and mitigates DNS threats by dropping problematic packets while responding only to legitimate traffic. You may also manually perform the rule update process based on your configuration.



Elastic Scalability

Infoblox Virtual Secure DNS provides the elastic scalability of DNS virtual network functions (VNFs) and the carrier-grade reliability, flexibility, and operational control required in virtualized networks. The solution ensures seamless, multi-service operations and delivers superior subscriber experience and new services in a timely manner—even under evolving market conditions.

Protection of often highly distributed DNS functions is a top priority. The solution allows you to quickly view and control all points in the DNS infrastructure network, pinpoint areas under attack or subject to other traffic surges, and then elastically scale up DNS instances in the specific local area where they are needed. This ability to prevent disruption or impairment of DNS functionality is fundamental to achieving the business advantages of NFV and SDN.

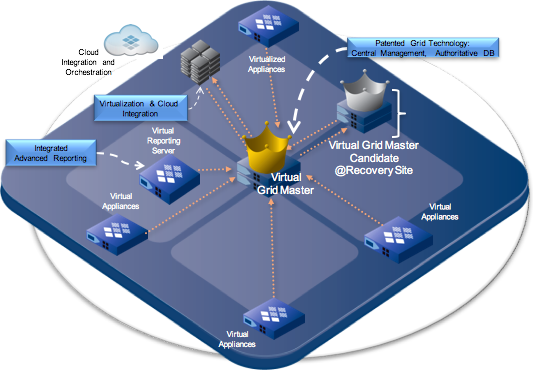
Infoblox Virtual Secure DNS Solution is built from standard Infoblox virtual appliances.

Infoblox NIOS

All Infoblox appliances run on the Infoblox NIOS Operation System. Security is built into the very fabric of Infoblox. The Infoblox NIOS operating system is built from the ground up, taking a Linux kernel and then adding only those components necessary for delivering services and features. Some vulnerable applications and utilities often used as attack vectors have been excluded from NIOS. This purpose built, hardened operating system differs from standard off-the-shelf Linux builds which must be strip hardened before use. By deploying NIOS within a closed, hardened appliance with no root access, direct access to the database is denied. This protects against commonly exploited attack vectors and against human error. Infoblox NIOS comes as part of every Infoblox DNS appliance, whether physical or virtual, providing a truly secure solution.

The Infoblox Grid Architecture

At the core of the Infoblox solution is the patented Infoblox Grid™. The Infoblox Grid links member appliances together securely across the Provider’s network. The Grid is not a separate management and reporting application that merely overlays the individual appliances. Rather, appliances in an Infoblox Grid are linked to form a control plane, using a distributed database embedded in each appliance as part of the NIOS operating system. This transforms the appliance population into a unified system with unique and beneficial attributes.



The Grid delivers the core automation behind an Infoblox deployment, enabling rapid automated updates for security patches or software updates and eliminating the need for individual per-server patches for OS or software updates or security patches. The Infoblox Grid Master is first updated by the operator and all Grid Member appliance updates can then be applied automatically by the Grid Master. This also has the benefit of eliminating outage risk due by eliminating manual configuration errors. This significantly reduces operational support costs and staff can save time by avoiding frequent manual but complex administrative tasks.

At the centre of the Grid is the Grid Master (GM). The GM co-ordinates the activities, management and maintenance of the Grid and provides central administration for DNS. All DNS changes are made through the Grid Master; via a single, central GUI interface. The GUI can be accessed by most Web 2.0 compliant browsers and provides a collection of wizards simplifying the complexities of DNS configuration. Progressive syntax and semantics checking is provided as DNS data is entered, ensuring the correctness of each entry. Changes are transmitted to each DNS member in real-time, unless scheduled otherwise, ensuring that all records throughout the deployment are uniform and up to date.

The NIOS triple commit strategy ensures the accuracy of the data before it is put into production. Infoblox provides updates from the Grid Master to the member appliances using secure database updates. Each transmission is verified for accuracy, written to disk and verified again for accuracy. If needed the DNS member appliance will request a re-transmit of the data before committing the change.

Operations

The NIOS administration GUI removes the complexity and provides accuracy when engineering or operations staff are required to perform a small number of modifications. However, Providers are constantly rolling out new services and updating existing services and applications. For each new service or change, DNS data has to be modified. This results in addition and modification of many hundreds of records a week. The administration GUI also facilitates bulk changes via a well-defined and documented CSV import format. Engineering and Operations staff can produce CSV files with hundreds or thousands of entries for mass input. Data entry checks ensure the accuracy of the data. As the data is loaded, the operator can view the import as it progresses or run it in the background. Individual errors are recorded in a log file with the row number, the import string and an explanation of the error.

A workflow can be enabled, “holding” any changes for approval by a separate administration group, before the changes are committed to live operation, providing additional checks and balances.

Infoblox NIOS provides both a Perl API and a RESTful API. This can be used to integrate with 3rd party systems for provisioning or back-end tasks. These rich APIs enable tight integration with existing or legacy operator-specific OSS systems, providing synergies not available on competing platforms. Infoblox realized OSS integration with wired, EPC and 3GPP environments.

Workflow

NIOS has Role Based Access Control (RBAC) built-in. RBAC is built around users, groups, roles and permissions. A user can be part of a group. A role can be associated to a group. A group can be associated to permissions. On top of this RBAC, workflow can be implemented. With workflow tasks prepared by one group have to be approved by another group. The workflow allows delegated tasks to be executed after explicit approval.

Smart Folders for Organizing Data

Smart folders provide an easy way to organize and categorize networks. In conjunction with extensible attributes that allow administrators to define and assign custom properties to objects, Smart Folders provide a powerful way to hierarchically view and manipulate data.

For example, administrators may define a custom attribute called “PoP” with syntax “City-DC-xxxx” and associate this attribute with all DNS records. A smart folder can then be created that show all DNS RRs associated to a DC in a PoP.

Smart Folders are dynamic in nature e.g. when a new device is added or removed from the network, it is also added to or removed from all associated Smart Folders automatically.

Maintenance

Upgrades are done centrally through the Grid Master. The new revision is loaded onto the Grid Master, then distributed and built on each member through an automated process. Once complete the administrator can the centrally initiate the upgrade process where each node is rebooted on to the new software revision. Infoblox allows for staged upgrades and can specify an upgrade order so that not all DHCP/DNS services are down simultaneously. Further, any member on the Grid can be offered as a high availability pair of appliances, in an active passive format. This allows for continued service by one appliance in the pair, while the other is upgraded.

The Grid Master contains the entire database, which includes the configuration for each member appliance. Should a unit be replaced with a new unit, it will be automatically be provisioned with the same IP address, and directed to the join the Grid. Once the unit’s credentials have been verified, the Grid Master will automatically upgrade and provision the unit with the exact information that was on the replaced appliance. Since the Grid Master contains the entire database, including member configurations, only the Grid Master needs to be backed up. Any member can be reconstituted from the Grid Master. Backups can be scheduled to third party servers or ad hoc.

At no time is the administrator required to individually maintain or upgrade each DNS server.

Reporting

Now that a single centralized control plane has been established using the Grid, the centralized visibility of all DNS servers and parameters from a single viewpoint enables operators to gain management visibility and create reports for capacity planning and troubleshooting. Infoblox offers a comprehensive reporting server for use within an Infoblox Grid. Trending reports, threshold alerting and DNS statistics are included.

Some of the “out of the box” reports are as follows:

* CPU Utilization Trend
* DNS Query Rate by Query Type
* DNS Query Rate by Server
* DNS Daily Query Rate by Server
* DNS Daily Peak Hour Query Rate by Server
* DNS Response Latency Trend
* DNS Cache Hit Rate Trend
* DNS Replies Trend

Note: The reporting member and data will remain on premises. The reporting member and data is accessed from the Grid Member (Central Point of Control).

Service Agility

The ability to launch or modify services quickly, is one of the primary drivers of NFV and SDN adoption. Service providers need to quickly launch new competitive services where and when they are needed, in response to dynamic market demands or other business changes. Rapid, accurate provisioning is an essential component to enabling this capability.

This highly reactive, dynamic virtualized environment requires tight integration of IP address assignment, with the creation of DNS records as new VMs are deployed.

Improve Subscriber and Network Protection

Infoblox specializes in DNS-specific attack prevention and visibility. Virtual Secure DNS provides broad protection against DNS-based malware and other DNS-specific attacks including DNS tunneling, data exfiltration, NXDOMAIN, and phantom domain. The solution also protects subscriber devices from becoming infected if they access malicious domains and identifies infected clients for cleanup. The solution takes a live reputation-feed service from the Infoblox global threat ecosystem to create a dynamically updated list of known malicious URLs and IP addresses. When a DNS query reaches an Infoblox DNS server virtual appliance, any match to the reputation-feed list results in redirection or blocking according to the service provider’s policy rules configured on the appliance. All actions are logged, and reports can be generated showing all malicious activity.

Automated Kill Chain

Automated threat mitigation removes limitations of manual updates, significantly improving protection levels. The volume and diversity of attacks has exceeded the ability for administrators to manually keep up with the changing landscape. Petabytes of data need to be examined in order to identify attacks and mitigate individual security incidents. The Infoblox global security ecosystem provides early detection and automatic updates. The unique automated update of both reputational and identified threats enables an automated kill chain, effectively blocking zero-day threats and often mitigating attacks before they can cause any damage to subscribers or service availability.

**Redundancy**

A typical design provides redundancy at 4 levels:

* Level 1. Per Data Center (DC). Anycast IPs will be announced by DC router to subscribers, subscribers will go to the closest DC based on BGP/OSPF and in case of DC failure the request are dynamically routed to the next closest one. With BFD this failover is under a second
* Level 2. Inside DC. Behind the router it will be used a second anycast cloud using ECMP (Equal Cost MultiPath) with BGP and BFD. This option allows to avoid the LB utilization, reducing complexity and latency. Multipath allows to spread the load among the servers behind, with persistency. If one servers fails traffic is spread among the remaining nodes.
* Level 3. Elasticity. With the integration with the orchestrator and the metrics it will be possible to detect a change in the load due to an increase of traffic because one or more nodes are down, and automatically spin new instances to cope with the traffic and reduce the load per instance using NFV scale-out/scale-in functions.
* Level 4: Infoblox also supports other approach for High Availability like HA based on VRRP.

Scaling

The solution can horizontally scale by adding capacity within a datacenter or by adding data centers. With the use of Anycast, the added capacity will be automatically taken in production.

* Per Data Center (DC). Anycast IPs will be announced by DC router to subscribers, subscribers will go to the closest DC based on BGP/OSPF metrics. Additional DCs can be enrolled in this anycast cloud.
* Inside DC. Behind the router it will be used a second anycast cloud using ECMP (Equal Cost MultiPath) with BGP and BFD. Additional appliances can be enrolled within the DC Anycast cloud.

HEAT Integration

Infoblox Grid integrates into Openstack via HEAT. The Infoblox API is used for integration.

Infoblox Heat templates and resources are open source: <https://github.com/infobloxopen/heat-infoblox>

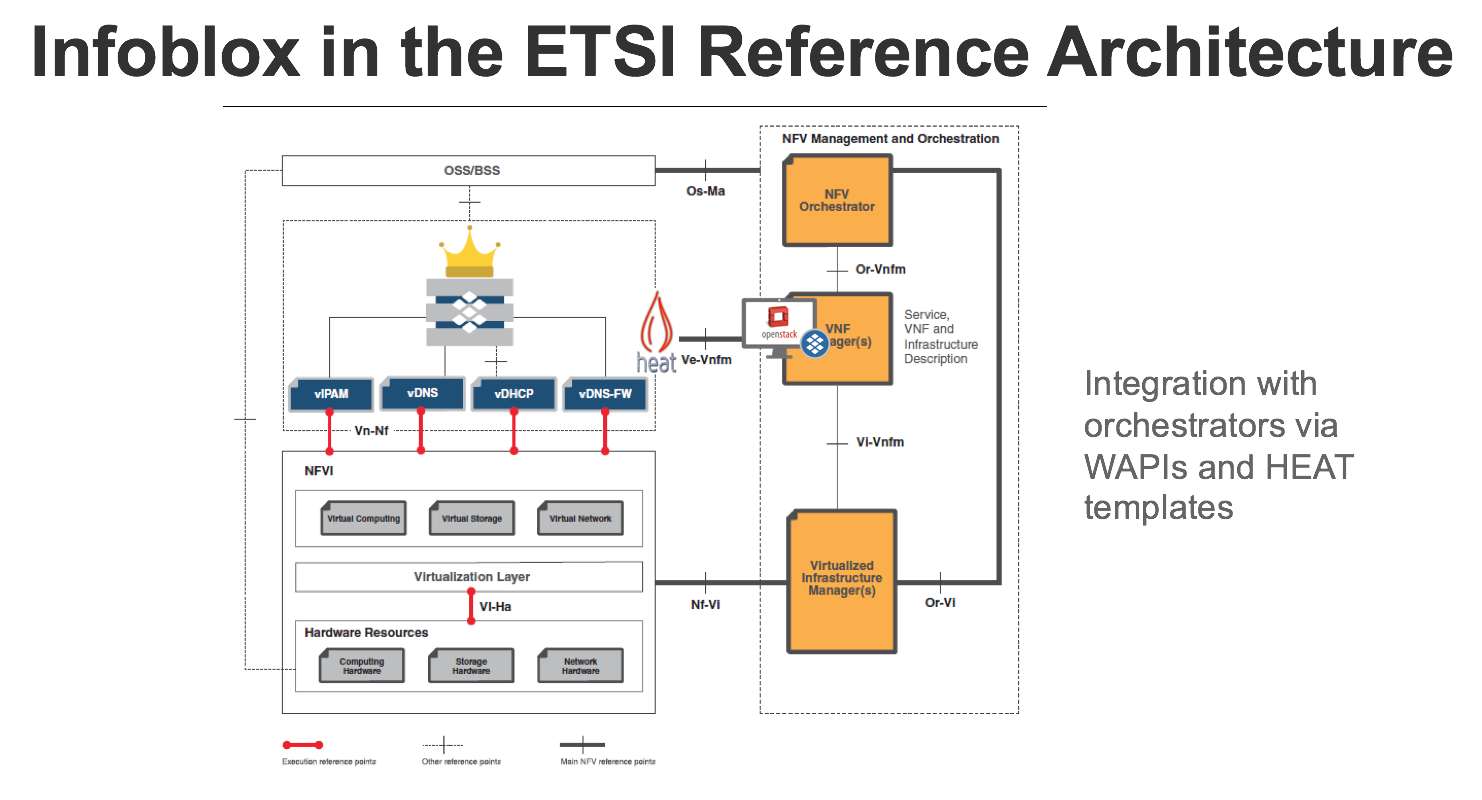
The proposed solution can be fully managed (including configuration) via the Grid Manager web GUI it can be accessed via any standard web browser available on the market.

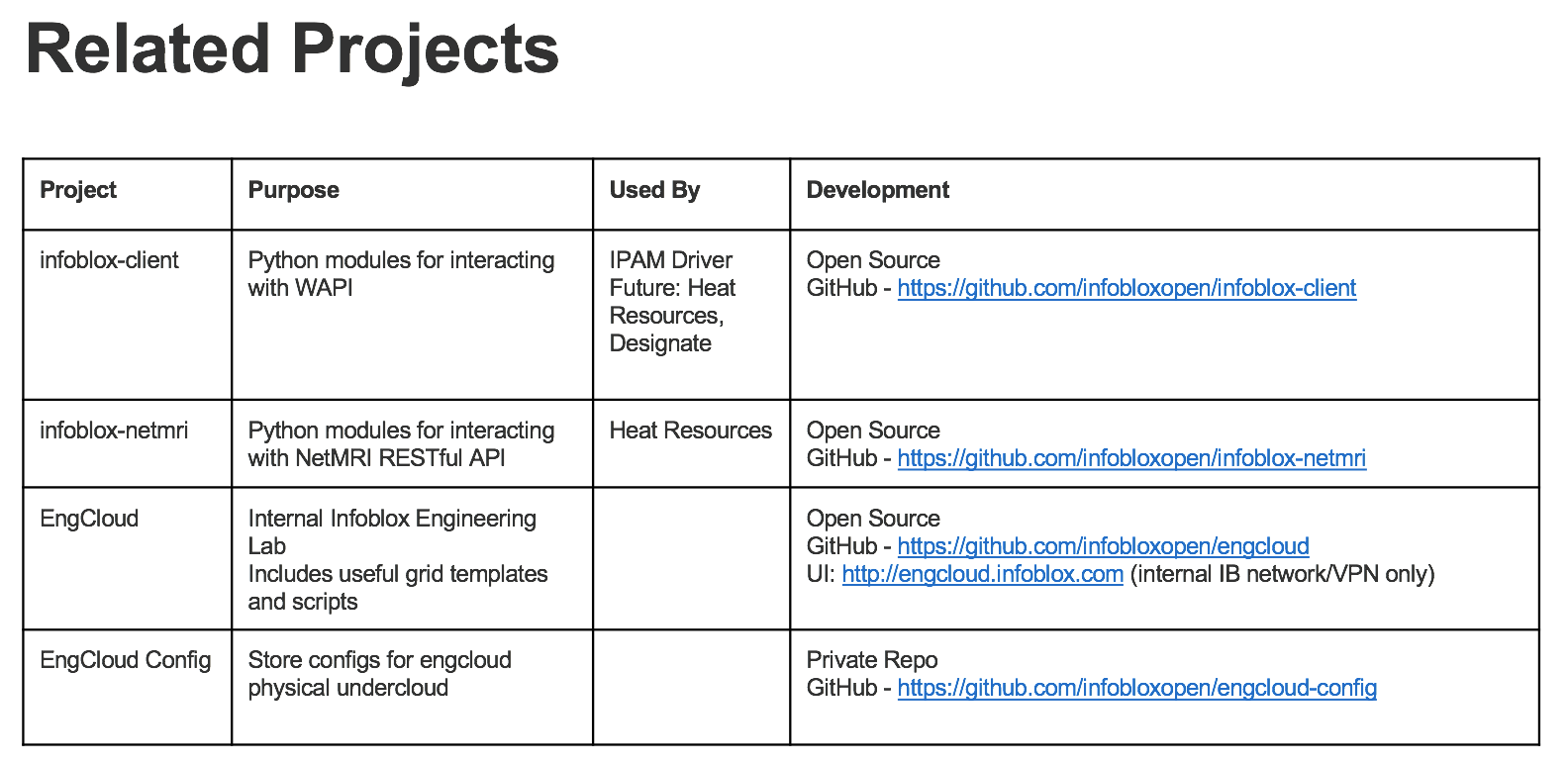
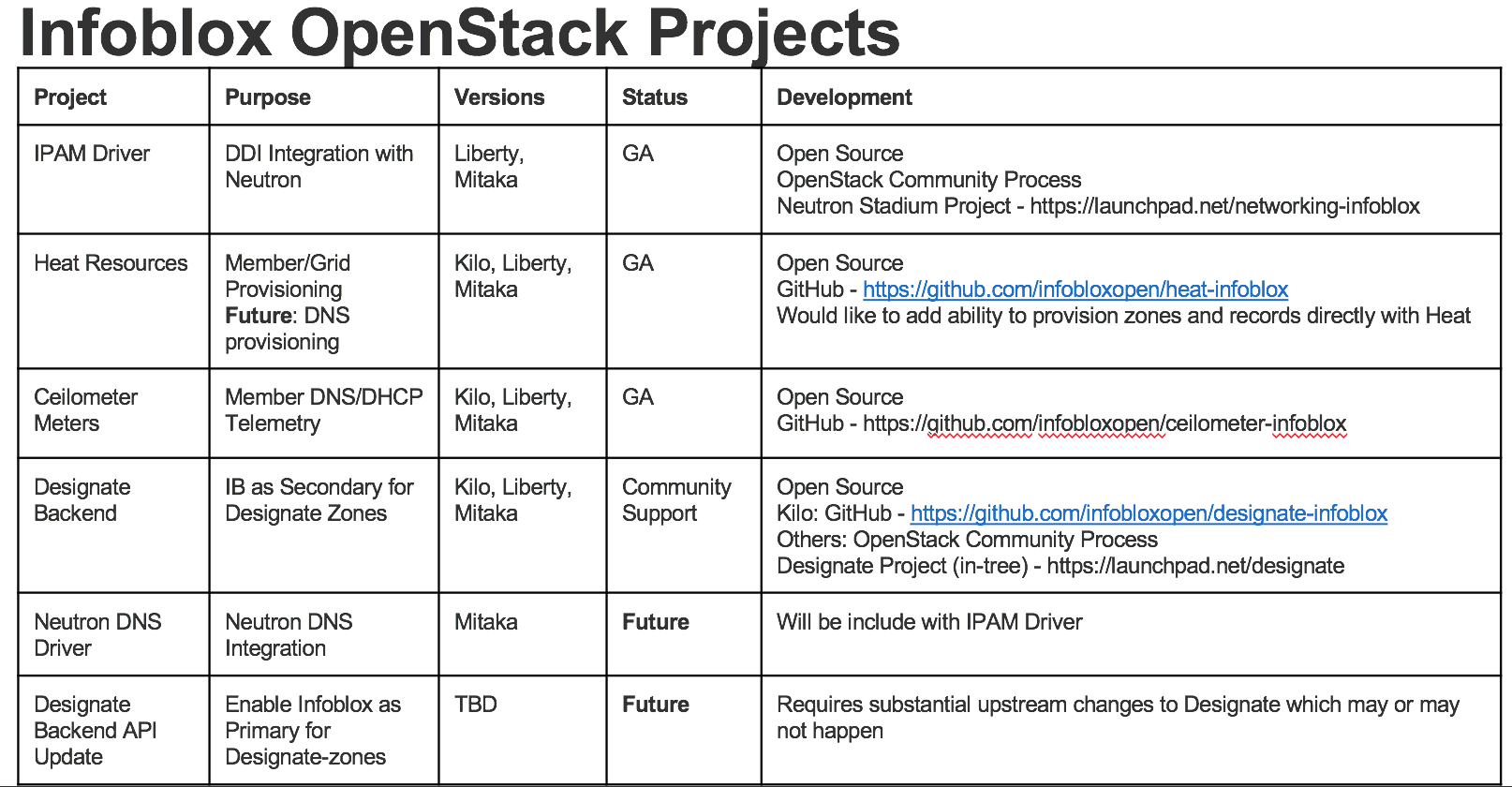
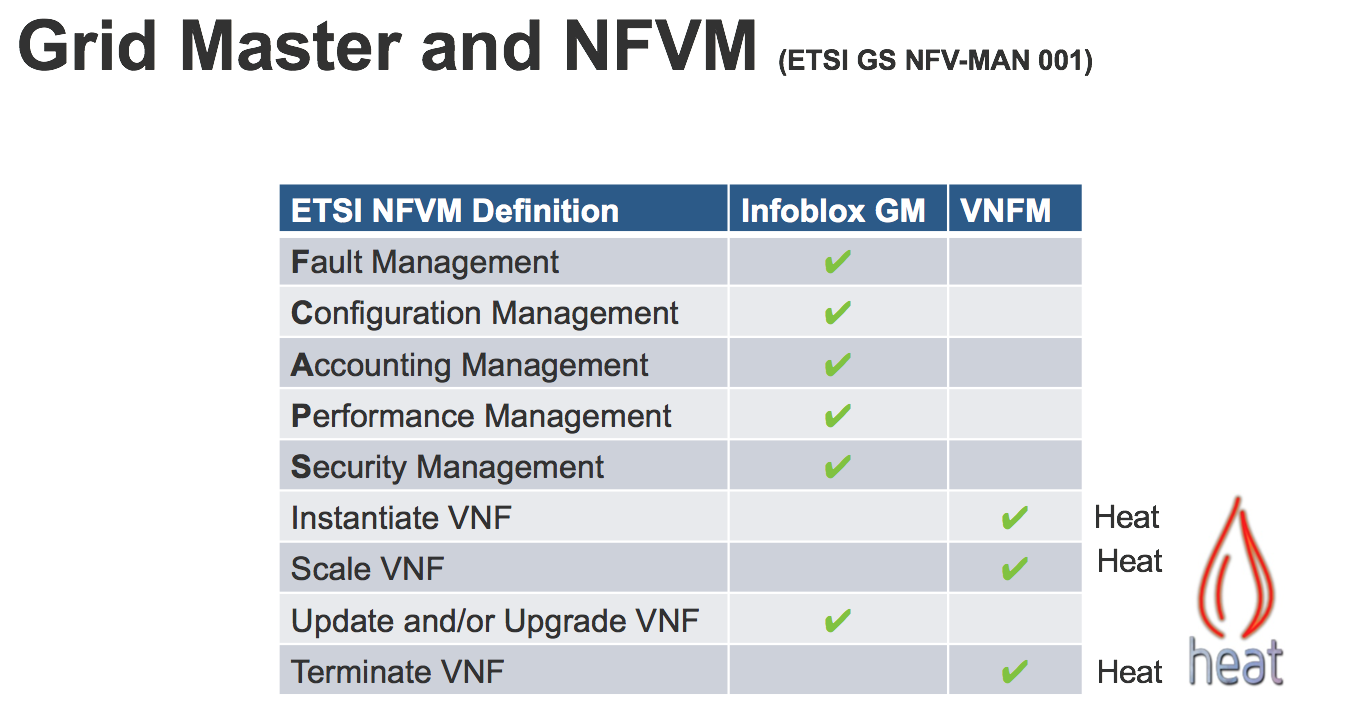
The proposed solution includes a configuration management interface, based on an open standards API that could be used for integration with an Element Management System. The Infoblox WAPI (Web API) is a RESTful (representational state transfer) interface used by Infoblox customers for automation and integration purposes. Infoblox itself uses this to provide customers with plug-ins for integration with cloud management orchestration systems such as VMware, System Centre Orchestrator and OpenStack. Other vendor companies, for example, ServiceNow and IBM, have used the RESTful interface to provide an integration point for their customers. In addition, Infoblox is aware of end customers creating their own integrations; for instance to link asset management systems to DNS, DHCP and IP Address Management so that devices can be provisioned.

The Web API is fully supported by Infoblox, including documentation and examples of supported objects and methods. As a RESTful interface it is not dependent on a specific language so customers are free to use whatever language suits the integration purpose and skill set within an organisation. Infoblox has seen integration take place using Python, Perl, Java, JavaScript and Powershell for instance. The WAPI has a versioning scheme that is independent of the NIOS software versioning scheme, meaning there is no need to change/upgrade code or components when Infoblox software is updated. The current WAPI version 2.3 is backward compatible with WAPI releases that have the same major WAPI version or with designated earlier major versions. Though the protocol itself may not be strictly backwards compatible, the server emulates the correct behaviour, when necessary.

Extending the OAM functionalities to the more comprehensive level of FCAPS (fault, configuration, accounting, performance, security), the proposed solution include a rich web gui that offer specific tabs for all the above functionalities:

* **Fault**. The web gui allow to visualize the status of all the elements of the Grid and the DNS services they deliver. Specific reports are available to view the fault statistics. The solution include also full SNMP support for fault management.
* **Configuration**. All the functionalities of the Grid can be configured from the web gui in a centralized “Grid wide” approach, for example the DS services can be configured centrally and then applied to all the Members/tenants. The Grid include also the Extensible Attribute (EA) and Smart Folder (SF) that will allow KPN operation team to organize the Grid configuration elements in a personalized way, EA are metadata data that can be added to configuration elements to quickly organize, visualize, search, configure parts of the services. All the configuration made by any interface (web gui, SSH, API) are recorded.
* **Accounting**. The proposed solution include reporting services that provide detailed and granular visibility of the DNS traffic serviced by the infrastructure. Many off the shelf reports and many customizable reports are available.
* **Performance**. The proposed solution include reporting services that provide detailed and granular visibility to the performances of the networks. Many off the shelf reports and many customizable reports are available to monitor and control the performance of the entire network, of the single Members, of the single instances. Many performance figures are available via SNMP MIBs.
* **Security**. The proposed solution include embedded security functionalities to protect KPN DNS infrastructure from (DNS-based attacks such as DNS DDoS, exploits, NXDOMAIN, DNS tunneling, and DNS hijacking attacks), it include also the DFWF acticvation license that allow KPN to load its blocked domain list. All the security functionality are managed from the web gui, specific off the shelf security reports and customized one are available.





Integration with Standard Orchestrators and Hypervisors

Infoblox has been deployed in cloud and virtualized environments for a number of years. In addition to tight VMware integration, Infoblox also offers OpenStack support for Icehouse, Juno, and Kilo. In fact, Infoblox is included in the OpenStack Liberty platform. Supported hypervisors include VMware, KVM, Xen, and Hyper-V. Vmware integration include:

vRealize Automation, vRealize Orchestrator, vCloud Automation Center, vCloud Orchestrator. OpenStack integration include: Red Hat, SUSE, HP

Infoblox proposed solution is integrated with the major VNF Manager/Orchestrators available on the market (Openstack. Vmware and others). Infoblox allow an easy and fast integration with any VNF manager and is available to discuss with KPN any specific requirements on this topic.

Infoblox has attained VMware Ready™ status for network functions virtualization (NFV), certifying interoperability with the complete VMware vCloud® NFV platform. Infoblox DDI (DNS, DHCP, and IP address management) is certified with VMware’s industry-leading virtualized compute, networking, and storage solution as well as both of VMware’s virtual infrastructure managers—VMware vCloud Director® and VMware Integrated OpenStack. This designation indicates Infoblox DDI with support for NFV has achieved VMware’s highest level of endorsement, and is now included in the VMware Solution Exchange (VSX).

Infoblox supports NFV work for Kilo and later. Heat Version 1.0.0 for Kilo releases and version 2.0.0 is for Liberty releases are both supported and functionally equivalent.

The following are examples of supported OpenStack/KVM distributions and releases as they

adhere to the Heat Versions above:

Red Hat OpenStack Platform 7 (Kilo)

Red Hat OpenStack Platform 8 (Liberty)

SUSE OpenStack Cloud 6 (Liberty) (note, SUSE skipped the Kilo release and went straight

from Juno to Liberty)

Mirantis OpenStack 7.0 (Kilo)

Mirantis OpenStack 8.0 (Liberty)

HP Helion OpenStack 2.0 (Kilo)

HP Helion OpenStack 3.0 (Liberty)

Infoblox can verify support for platforms not listed on request.

**IN 14 Licencing**

Network Function Virtualisation decouples the hardware from the service. Infoblox adapts to this model by offering a virtualised solution not licensed by the number of appliance usage. Infoblox can license VNFs based on peak QPS, number of authoritative records and the number of provisioned subscribers.

Infoblox calls this Service Provider License Agreement (reflected by SPLA in the SKUs). The SKUs allow operators Io deploy any number of virtual appliance instances on the new Infoblox Flex appliance model. Price will be determined by peak capacity or number of provisioned subscribers as indicated on the appropriate SKU.  
  
Recursive DNS is licensed based on QPS. This is indicated by the -Q- in the SKU. Examples:  
IB-SPLA-REC-Q-100K covers 100K Q–S Recursive DNS  
IB-SPLA-DCA-Q-100K covers 100K QPS DNS Cache Acceleration   
IB-SPLA-SUB-ADP-Q-100K covers 100K QPS Advanced DNS Protection for recursive DNS  
  
So the price for 100 K QPS Recursive DNS with cache acceleration and ADP is the sum of the three SKUs.

Authoritative DNS is licensed by the number of resource records referred to as Objects. The O in the SKU indicates Objects. Examples:

IB-SPLA-AUTH-O-100K covers 100,000 resource records for authoritative DNS.

IB-SPLA-SUB-ADP-AUTH-O-100K covers 100,000 records for authoritative DNS with Advance DNS Protection.  
  
Services like Active Trust and Parental Control are licensed per subscriber. Those SKUs have the -S- in the SKU name. Examples:  
IB-SPLA-SUB-AT-ST-S-1M cove–s Active Trust (aka DNS Firewall) Service for 1 M provisioned subscribers the are entitled to use this service (aka opt-in subscribers)  
IB-SPLA-SS-S-1M covers Subscriber Secure for 1 M subscribers  
IB-SPLA-PC-S-1M covers Parental Control for 1 M subscribers

The license model is a pure “Pay as you Use” model and allows the operator to pay only for the real use of the capacity and services provided by the solution. The two main parameter of this licensing model are Capacity and Features. The capacity is related to the base services the DNS is requested to perform (i.e. Recursive, Authoritative). For Recursive services the capacity dimension is the QPS (Query per Second), for Authoritative is the Object Records. These are the only parameters to take into account for licensing and pricing.

For example for Recursive Service the license is related the number of QPS requested by KPN and is independent from the number of virtual appliance, management, reporting or anything else needed to build the architecture. It is also independent from the number of sites. If at any time KPN decides to spread the architecture from 4 to 8 or more DCs no additional cost will incur.

The license is network wide and is perpetual for the base services and is trusted based. No blocking applies when the threshold is exceeded. Every year will be verified jointly with the customer the real number of QPS that has incremented and the license extension will be negotiated. Infoblox believes this approach could be very useful for KPN as it allows to buy the year 2-5 expansions considering the real capacity after it is really used and not as an upfront investment that can be affected by incorrect planning estimation or by competition or regulation.

The value added services license scheme differs from services and can be summarized in the following:

* **vADP (vSecure):** with this license all the ADP features are made available to the customer with the right to have constant update by Infoblox Threat Intelligence Cloud. The license model is per QPS per Year and is a subscription based services.
* **vDCA (Cache acceleration):** with this license the cache acceleration feature is made available to the customer. This feature allows the DNS response time to dramatically decrease from milliseconds to microseconds hence greatly improving the customer experience. The license model is per QPS perpetual.
* **Subscriber Services/Parental Control/In line messaging:** with these licenses can be enabled the features to deliver subscriber services. In particular, security filtering for mobile and fixed users, parental control and inline messaging per users. These are value added services and are meant to produce additional revenues for the Service Providers. The license model is per opt-in subscriber per year and they are subscription based services.

**PRE 14**

**IN**

Infoblox provides the hardware footprint of some sample configurations. The design consists of:

* Service Delivery: Caching DNS appliances
* Service Delivery: Authoritative DNS appliances
* Management: Grid Master and Grid Master Candidate
* Management: Reporting appliances

Caching DNS performance is based on the Cache Hit Ratio CHR). The lower the CHR, the lower the QPS performance. We have assumed 95% CHR in the examples below. DNS Cache Acceleration (DCA) can increase the QPS. In below examples, you see caching DNS + virtual Advanced DNS protection enabled with and without DCA.

Caching DNS with vADP and DCA (900 K QPS at 100% CHR, 300K QPS at 95% CHR)  
  
26 Gig Memory  
  
250 Disk  
  
10 Cores

Seven of those appliances deliver 7 \* 300 = 2.1 M QPS

Caching DNS vADP, no DCA (275K QPS at 100% CHR, 120K QPS at 95% CHR)  
  
18 Gig Memory  
  
250 Disk  
  
8 Cores  
  
  
  
Caching DNS with vADP and DCA (2.7M QPS at 100% CHR, 400K QPS at 95% CHR)  
  
44 Gig Memory  
  
250 Disk  
  
22 Cores  
  
  
Caching DNS vADP, no DCA (490K QPS at 100% CHR,  180 K QPS at 95% CHR)  
  
30 Gig Memory  
  
250 Disk  
  
16 Cores

For authoritative DNS the appliance model is driven by the number of resource records and QPS. We have assumed 2M RR objects.

Authoritative DNS with vADP 275K QPS and 2M objects:  
  
30 Gig Memory  
  
250 Gig Disk  
  
16 cores

The GM and GMC appliances are sized by the number of objects in the entire grid. Below you find two sample configurations for 2M and 5M objects in the grid.

GM/GMC 2M Objects  
22 Gig Memory  
250 Gig Disk  
12 cores  
  
  
GM/GMC 5M Objects  
  
14 Cores  
250G Disk  
28 Gig Memory

Reporting v1405-5G

4 Cores

250G Disk

32 Gig Memory

|  |  |
| --- | --- |
| **NVI Item** | **vDNS** |
| *Overbooking* |  |
| Overbooking | No |
|  |  |
| *Stack* |  |
| OS (VM) | NIOS 8.1 |
|  |  |
| *Compute* |  |
| CPU Cores | Caching (see examples above)  Authoritative (see examples above)  GM/GMC (see examples above)  Reporting (see examples above) |
| CPU Speed | Caching 2.6GHz and higher  Authoritative 2.6 GHz and higher  GM/GMC 2.6 GHz and higher  Reporting 2.6 GHz and higher |
| Memory | Caching (see examples above)  Authoritative (see examples above)  GM/GMC (see examples above)  Reporting (see examples above) |
| NUMA pinning | May Recommended: CPU pinning  Must not: virtual NUMA nodes spanning across physical NUMA nodes |
| Hyperthreading | May and Recommended |
|  |  |
| *Storage* |  |
| Disk | Caching 250G  Authoritative 250G  GM/GMC 250G  Reporting 250G |
| Local storage |  |
| Distributed storage | Only if reporting clustering is required |
| Remote storage | Only if remote Syslog is enabled and for backups |
|  |  |
| *Networking* |  |
| Interfaces | 4 |
| Interface types | NIANTIC or Higher |
| Traffic Mirroring |  |
| SR-IOV | Caching/Authoritative: Recommended  GM/GMC: Must Not be enabled  Reporting: May be enabled/Don’t care |
| DPDK | Caching/Authoritative: Recommended  GM/GMC: Must Not be enabled  Reporting: May be enabled/Don’t care |
| PCI Pass-through | Don’t care |