Infoblox
CONTROL YOUR NETWORK

CASE STUDY

Infoblox DDI Migration Strategy

How to Migrate from VitalQIP to Infoblox

Brian Alaimo, Principal Engineer
Infoblox Professional Services

The Purpose

The purpose of this document is to describe the major facets in a migration of DNS, DHCP, and IP address management (DDI) services from VitalQIP to Infoblox. The goal is to give enterprise DDI administrators detailed information on the Infoblox migration methodology and best practices, so they can further articulate the highlights to others inside their organizations. The model presented is an example, based on real-world migrations. It summarizes the strategies employed to ensure success.

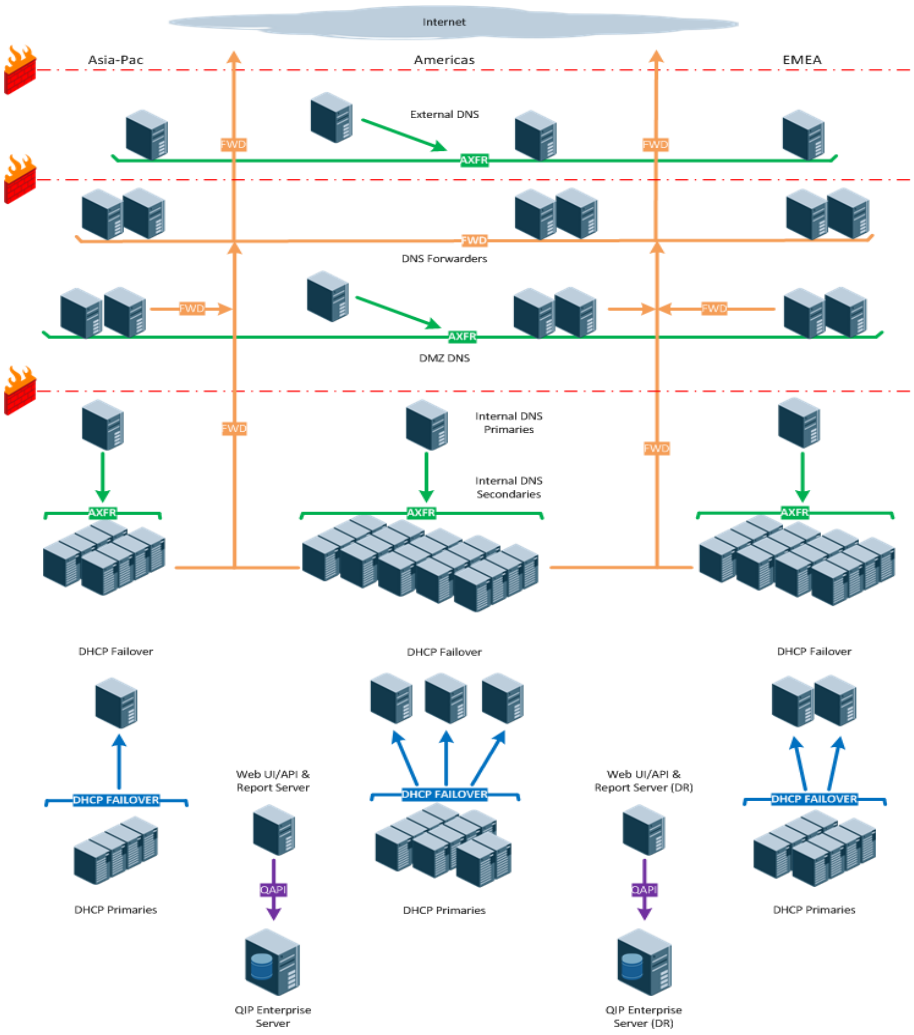
The Customer

To create the migration model this white paper uses a hypothetical organization name, "CX." CX is a global financial services firm with branches and remote offices in 17 countries divided across 3 regions: the Americas, EMEA, and Asia-Pacific. Its DDI environment, illustrated in Figure 1, runs on the VitalQIP platform and consists of:

- 2 enterprise servers (production and disaster recovery)
- 3 VitalQIP organizations (internal, external, and DMZ)
- 92 remote servers running DDI services
  - 5 primary DNS servers: one for external, one for DMZ, and one for each region
  - 3 external secondary DNS servers: one in each region
  - 6 DMZ secondary DNS servers: two in each region supporting multi-layer DMZs
  - 6 cache-only DNS forwarders: two in each region
  - 44 internal secondary DNS servers: two in each country/hub location
  - 22 primary DHCP servers: one in each country/hub location
  - 6 failover DHCP servers: located in regional data centers

- 775,000 managed objects in QIP
- 230,000 subnets, a large portion being point-to-point networks used by the ATM machines
- 2,500 internal DNS zones
  - Mostly reverse zones
  - A few dozen static forward zones for applications, apps behind load balancers, and BUs
  - 22 forward zones updated by DHCP
    - 1 for each country/hub location
    - 95 percent of the QIP objects in these zones
  - 40 minutes required to "push" all zones to a server with VitalQIP

- 1,100 external and DMZ DNS zones, mostly vanity domains consisting of a handful of records
- 2 Apache web servers (production and disaster recovery)
  - VitalQIP web UI for helpdesk and support teams
  - Self-service portal for end-user IP address assignment
  - Custom IP utilization report scripts
  - Web-services API invoked by in-house network automation tools



– *Figure 1* –

CX has invested heavily in automation of business processes to improve the bottom line. Over the years, Information Technology has developed a rich, enterprise-wide toolkit/API to provide automation and self-service functions for end users. Because day-to-day IT business activity has evolved to depend highly on the services provided by this toolkit, the self-service/ reporting/ automation portal for IP management must function without interruption.

As a business, CX is risk-averse and in some locations under regulatory mandate to introduce as little risk through change as possible. Information technology changes are tightly controlled by a change advisory board, and all proposed changes are thoroughly reviewed before being accepted. Migrations must be completed with no impact to end users or to the business whatsoever.

CX's version of VitalQIP is near its end of life, so the company is investigating alternatives. After evaluating several DDI vendors' products, CX has chosen an Infoblox Grid™ solution as the new DDI platform for its advanced database replication technology, easy-to-use clientless UI, and rich set of features.

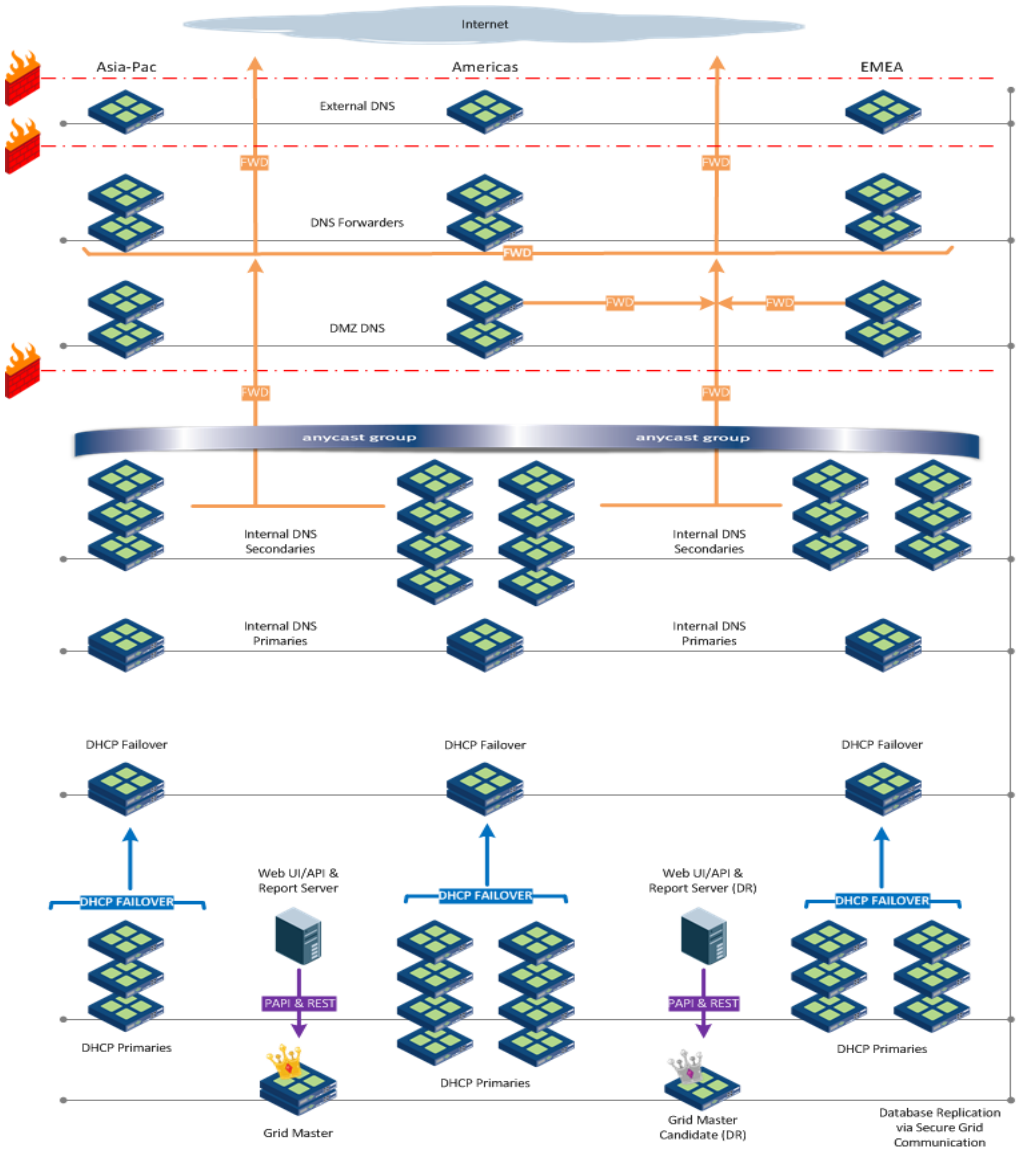
The Design

CX feels its DDI environment is excessively large and wishes to consolidate its infrastructure and move services for small locations back into major datacenters. Wide-area networks have evolved since the VitalQIP system was architected and deployed at CX, and the advanced WAN technology enables them to continue to provide DDI services to these smaller locations in a reliable manner. As most critical applications reside in the major datacenters, the adverse effects of a WAN connectivity failure for these smaller sites wouldn't matter much and would be tolerable for short periods of time. Illustrated in Figure 2, the new Grid architecture for CX consists of:

- 2 Grid Masters: one high-availability pair for production, and 1 Grid Master candidate for disaster recovery
- 1 Grid with 3 DNS views (internal, external, and DMZ)
- 55 Grid members running DDI services
  - 3 internal primary DNS servers, one high-availability pair in each region
  - 3 external DNS servers, one in each region
  - 6 DMZ DNS servers, two in each region supporting multi-layer DMZs
  - 6 cache-only DNS forwarder, two in each region
  - 17 internal secondary DNS servers, one in each large country/hub location
  - 17 primary DHCP servers, one in each large country/hub location
  - 3 failover DHCP servers, one high-availability pair in each region

This consolidated design centralizes DNS and DHCP services for small locations into major datacenters. It eliminates one secondary DNS server in each remaining country/hub location, cutting the number of DNS/DHCP servers by more than a third. Despite the reduced number of servers, redundancy and resiliency are increased by the introduction of new Anycast IPs for DNS.

The two Apache web servers providing reporting and web services remain an integral part of the overall system. The programs running on these servers are ported to the Infoblox platform. The web tools continue to use the same inputs and return the same outputs, but the middle logic is updated to use the Infoblox PERL and REST APIs. Fixing the code in this way provides a seamless transition for users and automated clients of these services.



– *Figure 2* –

The Approach

Infoblox's best practice is to migrate one VitalQIP organization at a time in a single cutover event, so CX's DMZ and external environments are migrated this way first, as they are relatively static and have a small number of servers. Starting with these smaller environments builds confidence in the system and the overall process.

Experience shows that migrating VitalQIP organizations all at once is less risky, fundamentally easier, and cost-effective, but there are cases where it is simply not feasible to migrate an entire organization in one event. This is especially true when it comes to very large VitalQIP installations. In the case of CX, the number of servers and the potential impact to their organization make it impractical to cut over in a single event, so a multi-stage approach is used.

To migrate, new primary DNS appliances are first installed in each region. As zones are migrated to these new DNS servers the existing VitalQIP primary servers are re-configured to transfer the zones from the Infoblox Grid,

and in turn they automatically re-distribute the Infoblox zone data to the remaining secondary VitalQIP servers as required. The other DNS and DHCP servers are migrated in groups of 10 to 15 locations at a time. As the VitalQIP servers are migrated, the Infoblox appliances are also made secondary for any zones still on VitalQIP, allowing users of the two systems to fully communicate throughout the transition. Static domains are migrated first, and then dynamic domains (i.e. those updated by DHCP) are migrated along with the DHCP servers that update them.

About DHCP Migrations

The key to migrating DHCP services is to reduce lease times. This reduction is done in steps until clients are renewing every one or two hours at the time of the migration. Reducing DHCP lease times gives precise control over when all the DHCP clients are migrated. It is simply a matter of placing the new server into production and waiting the hour for all the clients to renew with the new system. Having short lease times also provides an excellent back-out plan. If a roll-back is called, IT reverts the change and waits another lease cycle for all clients to renew back to the old system. This approach uses the built-in client behavior prescribed by the protocol to do the heavy lifting.

When migrating DHCP between systems, IT teams must also consider DNS, or more specifically, DHCP's role in performing dynamic updates to DNS. Because of the difference between the way that VitalQIP and Infoblox DHCP perform DDNS, the phases for DHCP migrations should be planned around DNS domains and all of the DHCP servers that update them. In addition, because the systems are different, the Infoblox best-practice is to remove DNS records that fall within DHCP ranges (i.e. Dynamic-DHCP objects in VitalQIP) during the DNS data import. Removing these records has the advantage of cleaning out all the invalid names generated by VitalQIP's naming polices and any names left over from VitalQIP's FIRST/LAST-IN policy. Then, when combined with short DHCP lease times during the migration, the records are re-registered by Infoblox DHCP when the clients renew their leases, leaving only valid DNS records in the zones. In addition, unlike VitalQIP, Infoblox DHCP will remove these records when the leases expire, so the zones stay clean going forward.

Infoblox's implementation of DHCP failover is also not compatible with VitalQIP's failover. VitalQIP's failover uses an active-passive model, where one server issues IP leases and the other is a hot standby, waiting for the primary DHCP server to fail. By comparison, Infoblox DHCP uses an active-active model, where both servers simultaneously handle lease requests from DHCP clients. The Infoblox servers function as peers and load-balance requests between each other. When migrating DHCP where failover is involved, the failover server must be migrated with the primary. Otherwise the VitalQIP failover server will become active when its primary is migrated, and then two separate systems will be serving DHCP for the same address ranges, which increases the likelihood of duplicate IPs being assigned. If many-to-one DHCP failover is in use, all of the primaries served by a single DHCP failover server must be migrated together with that server, or redundancy is lost for DHCP services on the ones not migrated.

So, ultimately, the phases for a DHCP migration are planned around the VitalQIP DHCP failover servers. Each DHCP phase consists of:

- One or more DHCP failover servers
- All of the primary DHCP servers to which they peer
- All of the DNS domains these groups of servers update

About Multi-phase DNS Migrations

DNS migrations that encompass all zones and resource records in an entire VitalQIP installation are fairly straightforward. Each is imported into its own Infoblox DNS View and brought online separately with minimal regard to the others, as they are generally independent environments. This is by far the simplest and least error-prone approach. However, when a single organization must be split into multiple stages (e.g. the internal organization is migrated over multiple cutover events), what may not be obvious are the challenges presented by the way the Infoblox DNS servers share a common database, which is distributed in real time from the Grid Master.

When migrating a single DNS view in stages, the first stage is easy. Import the stage-one zones, add secondary/delegation/forwarder zones for those remaining on QIP, validate the data, and cut over. Additional stages are more difficult because zone definitions already exist in the Infoblox database for the zones still on QIP. The Infoblox Grid will not allow a zone to be imported if it already exists, so those zones must be deleted first before the next stages' zones can be imported. However, deleting the secondary/delegated zones may result in an outage for them, which is unacceptable for any extended period, if at all.

To prevent a resolution outage for zones in subsequent stages, the zone data is not imported directly into the "production" Infoblox DNS View following the first stage. Instead, a new DNS View is defined in the Infoblox database, and the zone data for the next stage is imported into this "staging" view. With a staging view, the zone data can be imported, validated, and tested prior to the next migration event without affecting the general user population. Then during the cutover window, the QIP-based zones are quickly deleted from the production view and the new zone data is immediately copied in their place from the staging view. Using this technique, downtime for the zone is minimal while the zone is being copied from one view to another.

The Plans

The migration plans are structured to avoid any downtime of services to clients. Downtime during the cutover is avoided by taking advantage of the built-in client behaviors and the redundancy and resiliency built into the protocols. DNS clients are typically configured with multiple servers in their resolver lists and will retry them several times before timing-out on a query. DHCP clients attempt to renew their leases at 50 percent of the lease time and will retry again if a lease request isn't answered right away. By working one server at a time and allowing the clients to gracefully time out and retry, the migration can be performed without any perceived interruption of services.

Migration Plan

The following is a description of the steps typically performed during a migration from VitalQIP to Infoblox.

Stage the Appliances

The Infoblox Trinzic appliances are racked, powered, and cabled on their destination networks.

Reduce Lease Times

If DHCP is being migrated, gradually reduce DHCP lease times until all clients are renewing leases every hour or two.

Migrate the Data

It is all about the data. If the data imports properly, DNS will serve the records, and DHCP will hand out leases. Migrating the data involves the following tasks:

- Commence change freeze for affected subnets and domains.
- Export data from VitalQIP.
- Import data to Infoblox.
- Verify the data was imported correctly using special validation tools and techniques.
- Migrate the services

Services are moved from the legacy servers to the Infoblox appliances using one of two methods, depending on whether the servers are being replaced one for one or whether servers are being consolidated or moved.

Change-the-Server Method

The change-the-server method is used when the Infoblox appliance assumes the IP address of the legacy server (i.e. a one-for-one replacement). This type of migration is the simplest and has the least impact on clients, as they continue to resolve DNS and renew DHCP leases from the same server IPs, just different hardware. Performing this type of migration involves the following tasks:

- Infoblox appliances are staged on the same subnets as the legacy servers using temporary IPs.
- For each server being migrated:
  - Disable switch port of the legacy server.
  - Use Infoblox GUI to change IP from temporary to production value.
  - Wait for appliance to automatically restart and commence serving clients on the new IP.

Change-the-Client Method

With the change-the-client method, the IP address the clients use to obtain DNS or DHCP service is changed to that of the Infoblox appliance. This type of migration is more complex, and more risky as a result, as it involves making changes on both client and server systems. This method is generally used for server relocation or for consolidation/centralization of services to fewer servers. Performing this type of migration involves the following tasks:

- Infoblox appliances are staged with new, permanent, IPs on their target subnets.
- For each DNS server:
  - Back up configuration files.
  - Modify the named.conf file on the legacy VitalQIP server, making it a secondary to the Infoblox appliances for migrated zones.
  - Restart DNS on the QIP server.
  - Verify that the zone transfers succeed and that the data is loaded.
  - Disable DNS Generations (aka “DNS push”) to the legacy server to avoid overwriting the named.conf file changes.
  - Modify DHCP services to direct dynamically configured clients to the new IP addresses for DNS resolution.
  - Notify personnel responsible for managing statically configured DNS clients that use the legacy servers (e.g. servers, desktops, other DNS servers, etc.) of the change in IP address.
  - Enable DNS query logging on the legacy DNS servers and monitor the DNS logs to verify that all DNS clients and servers have switched over to using the Infoblox appliances.

- For each DHCP server:
  - In the week(s) prior to the migration, add IP addresses of Infoblox DHCP members to the existing DHCP helper lists on network devices.
  - Disable DHCP services on legacy servers.
  - Enable DHCP services on DHCP Grid members.

Observe Logs and Test

The Infoblox DNS and DHCP daemons write copious amounts of information to syslog. After each server is migrated, review the syslog on each of the appliances for client activity and any errors resulting from it.

If the logs are clean, perform basic user-acceptance testing. Reboot PCs, printers, and phones and verify that they obtain IP address from DHCP, and that their DNS records get added. Use tools such as dig or nslookup to verify DNS resolution for authoritative and non-authoritative names. Test critical applications for proper operation.

Wrap-up

After acceptance testing confirms that the system is fully functional and operational, perform the following tasks to conclude the migration:

- For DHCP, wait one full lease cycle for all clients to renew.
- Declare success.
- End change freeze.
- For DHCP, restore lease times to production values.
- For DHCP servers decommissioned after a change-the-client migration, remove IPs from network device configurations.
- Decommission legacy hardware when appropriate.

Back-out Plan

In the unlikely event that the migration has irrecoverably failed, the legacy systems can be reinstated relatively quickly when the migration is performed using short DHCP lease time as previously described. Depending on the lease time being used, the change can be reverted in about an hour or two by performing the following steps.

- If a change-the-server migration was performed:
  - Use Infoblox GUI to revert appliance IP back to temporary value.
  - Re-enable the switch port of the legacy system.
  - If migrating DHCP, wait one full lease cycle for all clients to renew.
- If a change-the-client migration was performed:
  - For each DHCP server, stop Infoblox DHCP services and re-enable DHCP on the legacy server. Wait one full lease cycle for all clients to renew.
  - For each DNS server, restore configuration from the backup taken just prior to the migration and restart the service.
- Observe logs and perform user-acceptance testing:
  - Reboot PCs, printers, and phones and verify that they obtain IP address from DHCP, and that their DNS records get added.
  - Use tools such as dig or nslookup to verify DNS resolution for authoritative and non-authoritative names.

The Result

Following the Infoblox methodology and best practices, CX has successfully migrated from VitalQIP. Using a combination of change-the-server and change-the-client methods and working one server at a time, the Infoblox Grid members were brought into production with no impact to clients. By reducing lease times, the DHCP migrations were performed in a highly controlled manner with an easy back-out strategy. Loading DNS data into a temporary staging view allowed the migration of the internal zones to be split into stages without affecting production systems. The self-service/reporting and web services components were ported to use the Infoblox API. Deploying new features such as DNS Anycast and DHCP load sharing through active-active failover led to a 30 percent reduction in server count, and new state-of-the-art IPAM features are currently being tested to enable CX to better control its network in the future.

About Infoblox

Infoblox delivers critical network services that protect Domain Name System (DNS) infrastructure, automate cloud deployments, and increase the reliability of enterprise and service provider networks around the world. As the industry leader in DNS, DHCP, and IP address management, the category known as DDI, Infoblox (www.infoblox.com) reduces the risk and complexity of networking.

Corporate Headquarters: +1.408.986.4000 1.866.463.6256 (toll-free, U.S. and Canada) info@infoblox.com www.infoblox.com