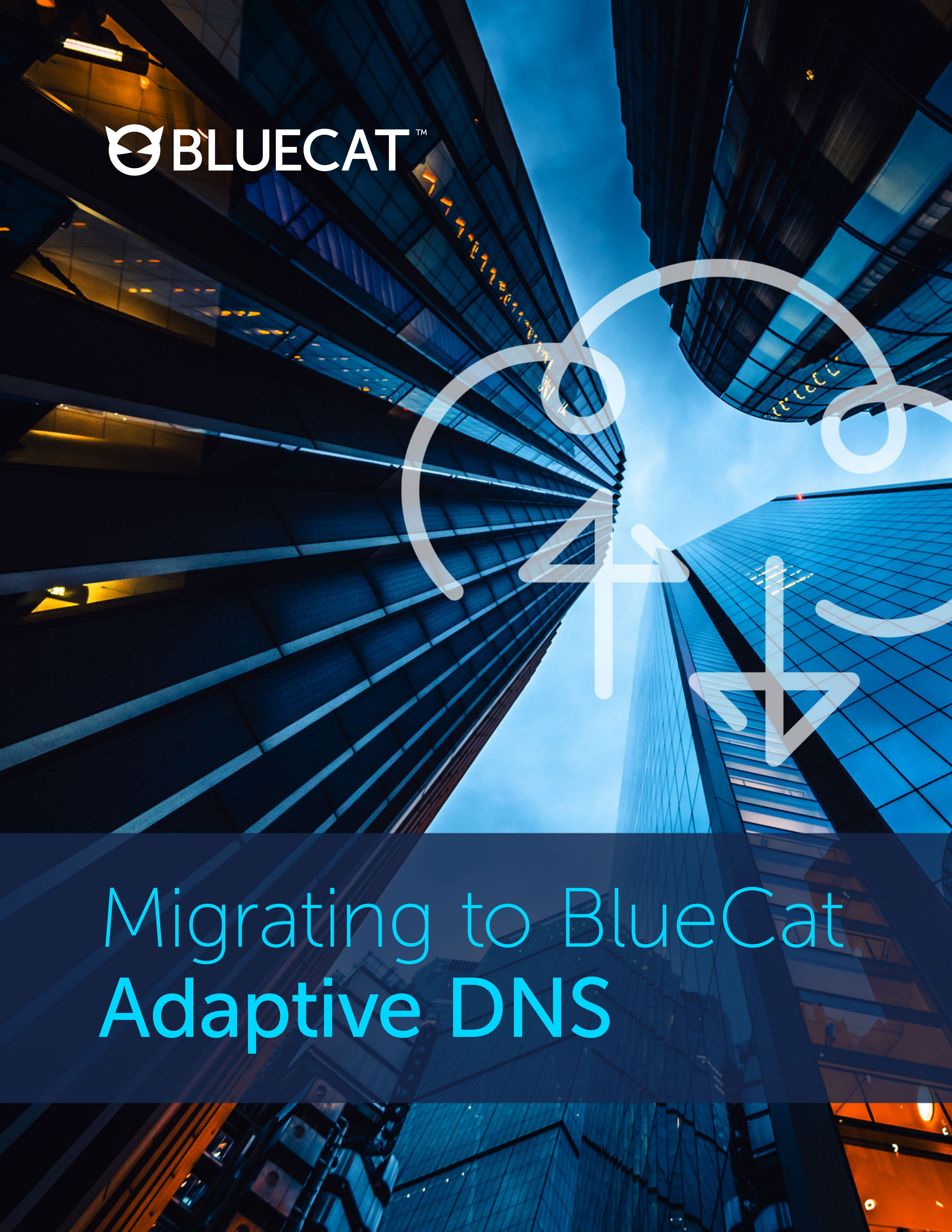


BLUECAT™

Migrating to BlueCat Adaptive DNS

Contents

Introduction

DNS, DHCP, and IP address management (IPAM) are business-critical components of reliable and secure network infrastructures. Given its importance, migrating DNS, DHCP, and IPAM—together known as DDI—infrastructure is an inherently risky business. With the amount of data, configurations, and routing pathways involved, there's a lot that can go wrong. Successful DDI migrations go beyond simple lift-and-shift from one platform to another—they align core infrastructure around business requirements.

Here are a few examples of the details that a successful DDI migration needs to get right:

- Disparate and conflicting data sources, bad records, and erroneous data cannot simply be discovered—they also need to be corrected.
- Customizations, automated workflows, and API calls need to be accounted for to ensure operational continuity and efficiency.
- To ensure continuity of operations, network teams need to be equipped to manage and maintain the new solution.

To account for all these factors, BlueCat has a proven, repeatable process for seamless, low-risk migrations. We use this process to migrate some of the largest and most complex environments in the world, accounting for a wide variety of data sets, project timelines, and business requirements.

In fact, in its 2022 Radar Report for DDI, GigaOm recognized BlueCat for offering "safe, secure migrations backed by decades of experience and proven migration tools, providing customers with predictable, low-risk cutovers."

BlueCat's migration record

Microsoft migrations	VitalQIP migrations	Other migrations
facebook United States Postal Service fiserv. DELL DISCOVER SONY Uber ups EY TOYOTA NetApp	NIKE pwc Ministry of Defence PNC NOVARTIS JPMorganChase United Technologies CSC VOLVO THE HOME DEPOT Coca-Cola Agilent Technologies Sun Life Financial	3M SAP NISSAN ZURICH SONY TESCO SuperValu Manulife Roche AIG DISCOVER experian. Ameren

This white paper outlines BlueCat's proven methodology and details the specific processes we use to ensure successful migrations to BlueCat's Adaptive DNS solution.

BlueCat's migration methodology and approach

Customers are at the heart of BlueCat's migration process. In each phase of project execution, the BlueCat team works side-by-side with customers to understand their needs and deploy systems that meet those needs. This approach not only ensures that your team gains the knowledge to maintain the solution over the long term, but also leverages your in-house expertise.

Each engagement is broken down into phases to minimize implementation risks and ensure that objectives are met at each stage of the process.

Initiate

Our consultants work one-on-one with members of your team to review the current and proposed environments or architectures, as well as the business goals behind transitioning to BlueCat. This generates a RAID (risks, actions, issues, decisions) conversation to be considered at all points of the project. This stage includes preliminary pre-kickoff calls, burn-through analysis of sample datasets, and a project kick-off.

Provision

We guide you in the deployment of BlueCat appliances according to previously defined architectures (known as rack-and-stack) and assist with configuring them for future functionality where applicable (known as box prep). Firewall testing and communication testing are conducted during this stage to ensure consistent behavior.

Process data

This is the bulk of any migration process—where most of the actual transition work happens. In this stage, fresh data is extracted and analyzed, transformed and sanitized, and pre-loaded into BlueCat Address Manager. This process is cyclical and usually occurs multiple times during a migration project.

Every BlueCat migration uses our professional tools to minimize migration workloads, optimize transition times, and correct common issues. After transitioning so many customers to BlueCat, we've found that dealing with minutiae up front—such as orphaned PTR records, bad delegations, invalid CNAMES, or redundant and inconsistent DNS/DHCP options—makes management of your DNS and IP space far easier in the long run. This is likely the only opportunity that an enterprise will ever have to properly purge or correct the junk inherently hiding in your systems.

After the data has been optimized and transformed, we import it into your staging environment or our BlueCat DNS/DHCP lab for full validation and testing during a dry run. Our tests include a thorough record comparison against the original data source, DNS resolution functionality, and the customer's own testing and validation plan.

Move to production

Our consultants collaborate with you to define and design cutover (known as go-live) strategies using best practices and risk mitigating techniques customized for specific environments. Change control/change freeze processes, go-live, and post go-live monitoring occurs during this phase. Production cutovers are also cyclical, proceeding together with the process data stage. Dry runs on lab-based systems ensure that the transition will achieve the expected results.

Closeout

Our consultants and project managers collaborate to provide an engagement recap that includes an executive summary, technical and architectural overview, migration summary, and next steps. When appropriate, a closeout call is initiated, and the documentation and project are signed off on.

Depending on the scope of our engagement, BlueCat DDI migrations may include internal DNS, external DNS, DHCP, IPAM frameworks, and/or caching/recursive servers. Each of these environments involve specific requirements, validations, and standard project management practices. Some of the migration steps may require multiple activities given the size, scale, and complexity of the environment.

Three BlueCat migration strategies

Every migration project involves unique business needs and architectural considerations. Depending on the requirements involved, BlueCat takes different approaches to infrastructure migrations. At a high level, we group these approaches under three broad strategies:

- Migration through intelligent forwarding
- Stealth DNS migrations
- Migration with BlueCat's proprietary toolset and processes

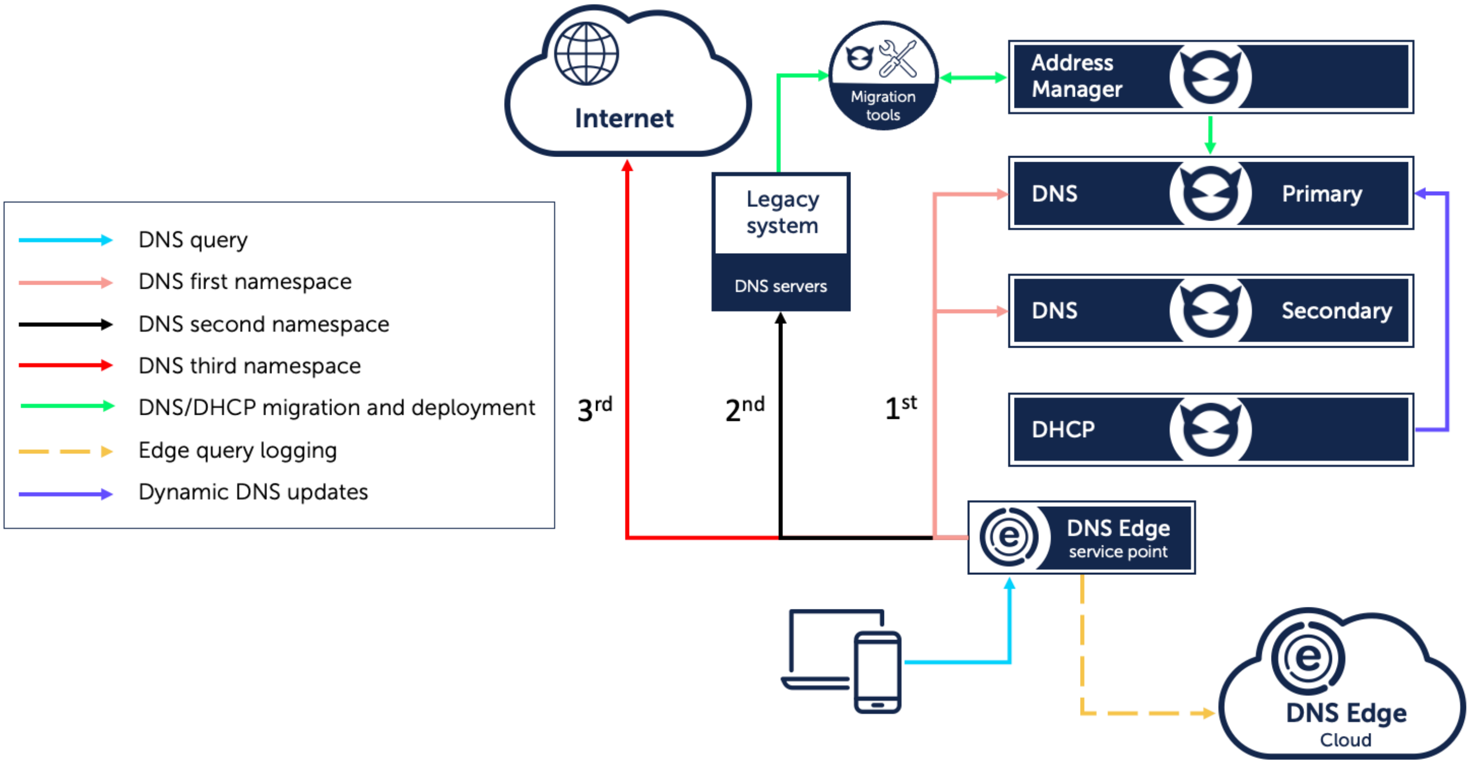
Strategy No. 1: Namespace migration with intelligent forwarding

In this strategy, BlueCat deploys its DNS Edge product to control DNS resolution paths. This adds unmatched transitional redundancy, reduced complexity, and elimination of costly errors during migration activities. The risk of missing data during the migration process is virtually eliminated. This strategy also dramatically simplifies the ability to roll back a migration if unanticipated issues arise.

DNS Edge uses namespaces to map domain names to forwarders. These forwarders facilitate the resolution of defined domain names. For instance, a client can query a migrated copy of BlueCat DNS and, if the expected answer is not returned, it then queries the legacy DNS. A failure to resolve in one environment is automatically retried in a second environment with no intervention by the client. Only a failure on both systems to return an answer is considered a non-response (NXDOMAIN, for example).

Throughout this process, BlueCat Professional Services works together with your team to identify the best configuration, namespace functionality, and operational approach.

Figure 1: Namespace migration with intelligent forwarding



Configuring namespaces

Namespaces give users more flexibility to configure DNS resolution paths during the migration process. They can easily route queries targeting select domains to a specific group of forwarders using match and exception domain lists. Not only can they name up to three default namespaces, but they can set different namespaces at the site level, with each namespace able to handle hundreds of domains.

A namespace is configured with a (non-empty) default group of forwarder servers to employ in the resolution of that namespace. Administrators can also use namespaces to limit resolution options based on a domain list.

- If no domain lists are configured as match lists to the namespace, then all queries are eligible to be resolved employing the namespace's defined forwarders.
- If domain lists are attached as exception lists, then the queries targeting the domains in these lists will not be forwarded to the namespace's defined forwarders.
- If one or more domain lists are configured as match lists, then the namespace will apply to all queries targeting the domains in these lists, except for the queries matching the domains in the exception lists (if defined).

Namespaces are defined in DNS Edge—any site can be set up to employ namespaces. DNS Edge service points will continuously pull and update namespace configurations, which are defined at the site level they are registered with.

Namespace resolution path behavior

To increase the success rate of a DNS query, DNS Edge can reroute traffic along a given number of defined paths until the query successfully resolves. The DNS Edge service point queries against all matching namespaces in the order they are defined until a response other than NXDOMAIN (the default) or a user-selected response code is returned.

- By default, when any response other than NXDOMAIN is returned, no further namespaces are evaluated.
- If the currently employed namespace returns NXDOMAIN, the request will continue with the next namespace to resolve the query.

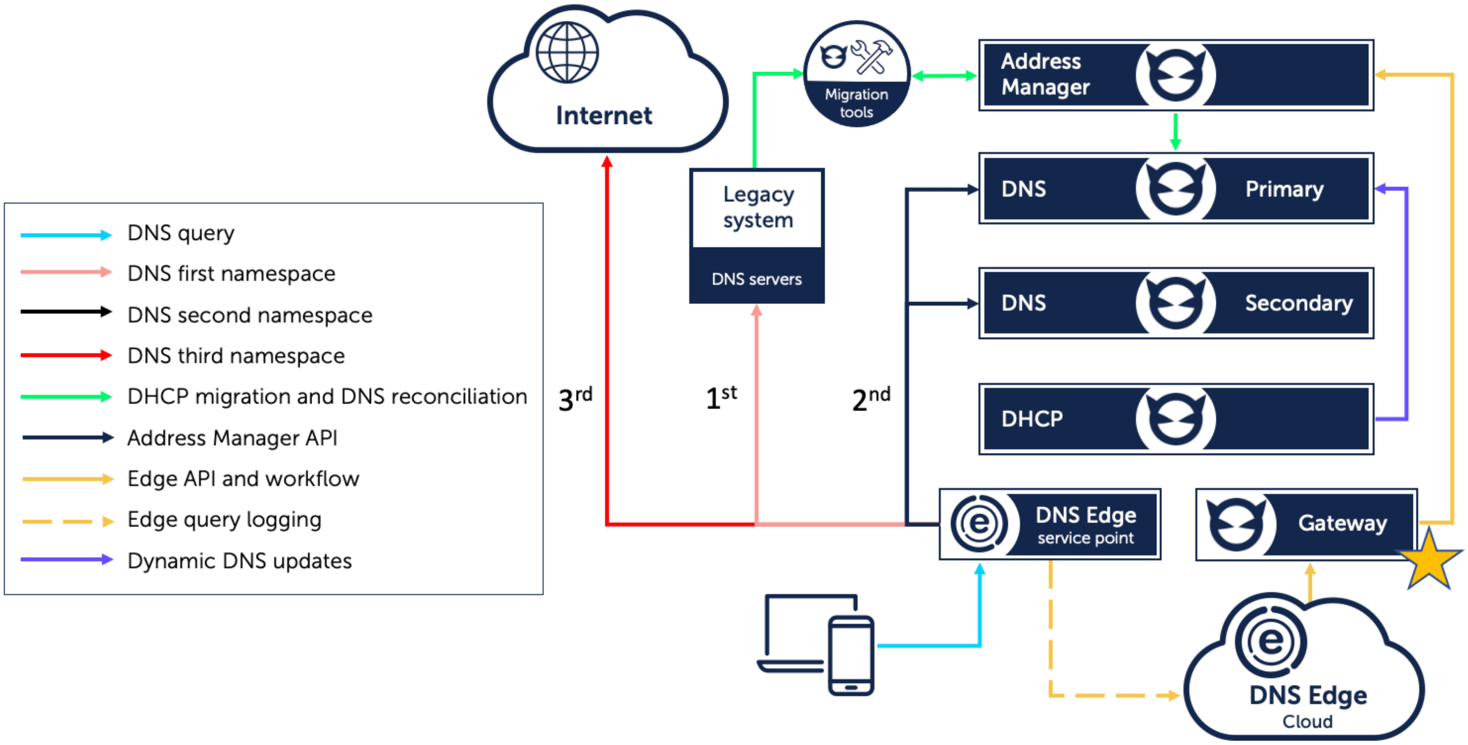
If all the namespaces are evaluated and none return a non-NXDOMAIN response, the last namespace's NXDOMAIN is returned. If the query cycles through all the selected namespaces and no match is found because the query does not match the match domain list(s) on any namespace, or it is included in an exception list, then an artificial NXDOMAIN response is returned.

Strategy No. 2: DNS stealth migration

DNS Edge service points also allow for a secondary migration strategy, whereby resolvable DNS queries are automatically migrated into the new BlueCat environment. This strategy reduces the number of stale records, ensuring a clean data set as records are populated into the new BlueCat Adaptive DNS platform.

In this migration strategy, DNS Edge service points run with previously configured namespaces. These namespaces look for every record in the incumbent authoritative DNS server first. If no record is found, they query BlueCat systems. During a stealth migration, as DHCP services are migrated to BlueCat, dynamic records begin to register with BlueCat rather than the legacy system.

Figure 2: DNS stealth migration using Gateway and DNS Edge service points



Using BlueCat's automation platform, Gateway, to synchronize queries, every query that passes the DNS Edge service point will be recorded and written into the BlueCat system as resolution happens from the legacy system. Query by query, Address Manager and BlueCat DNS will learn of and add all records that are successfully queried on the legacy DNS system without disrupting normal operations.

Over time, during the DHCP migration phase, BlueCat DNS is populated with all records that clients actually query. This allows you to obtain a report of records that do not get queried in order to better determine what is stale versus what is rarely used. Namespaces allow these stale records to be carried over to a quarantine namespace for further analysis and management.

Strategy No. 3: Migration with BlueCat's proprietary tools

In this strategy, DHCP data migrates from legacy infrastructure to BlueCat through one or a series of cutovers based on resource availability, maintenance window availability, individual network risk profiles, and other business factors. Ideally, individual sites are migrated as units rather than split across multiple migration events.

In the days leading up to each migration event, DHCP lease duration on legacy subnets/ scopes is reduced, causing more frequent lease renewals within the change window.

This allows for faster active lease migration from legacy DHCP to BlueCat, as well as confirmation that migrated scopes are functioning as expected during the migration process.

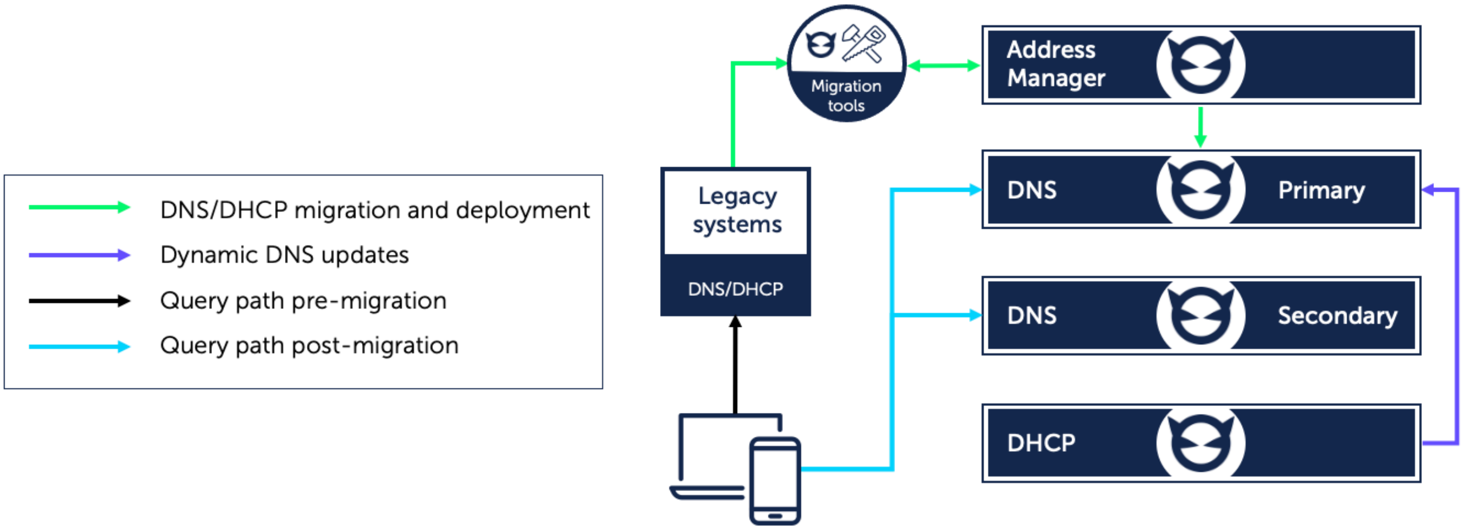


Figure 3: Migration with BlueCat's proprietary tools

For each migration event, current legacy exports will be provided to BlueCat Professional Services. We then analyze and migrate the appropriate subset of DHCP data for deployment to BlueCat infrastructure. IP helpers are added (or have previously been added) to support the BlueCat DHCP server(s) for the migrated scopes. The legacy DHCP scopes/servers are disabled and then the new DHCP configuration is deployed from Address Manager to the new DHCP servers.

As new devices join these subnets, or as leases from existing devices are renewed, they will receive leases from BlueCat DHCP servers. BlueCat DHCP will pass lease information to Address Manager in real-time. Optionally, Dynamic DNS is also updated via BlueCat DHCP and BlueCat DNS. Dynamic DNS data is also passed down to Address Manager.

After all the DHCP subnets have been fully migrated, legacy DHCP services are completely removed to eliminate any risk of multiple DHCP instances attempting to manage the same lease pools.

Once DHCP has been migrated (and optionally, any existing IPAM data), DNS is then migrated from the legacy system to BlueCat DNS. This is normally done in phases. First, a pilot migration gets the end user comfortable with the mechanics of the transition. That is then followed by one or more substantial migrations. Active Directory-integrated DNS is often a standalone event, but not necessarily. If the end user has purchased Edge, it can be leveraged for added redundancy in traditional migrations.

Migrating from VitalQIP, Microsoft DNS, and other solutions

BlueCat has extensive experience in migrating customers from VitalQIP, Microsoft DNS, and other solutions. We have a library of tools available to not only help with migration but also to shift operations to BlueCat's Adaptive DNS solution. This combination of tools, processes, and approach mitigates risks and enables customers to quickly proceed toward a target architecture and functionality while ensuring system integrity.

Based on our experience with a wide range of customers, we've found that the namespace migration strategy using DNS Edge is the ideal way to reduce risk and ensure a successful migration. For Microsoft DNS users, BlueCat also offers the option to introduce a BlueCat Microsoft overlay that provides immediate visibility through Address Manager.

Historically, Windows DNS (especially Active Directory-integrated DNS) has been migrated in the same way that BIND and other DNS systems are migrated. Today, if DNS Edge cannot be implemented, the traditional approach is still used.

Phased migration approach

Whether your current platform is VitalQIP, Microsoft DNS, or another legacy solution, BlueCat's phased migration approach is the same. Below are the seven major steps that we employ.

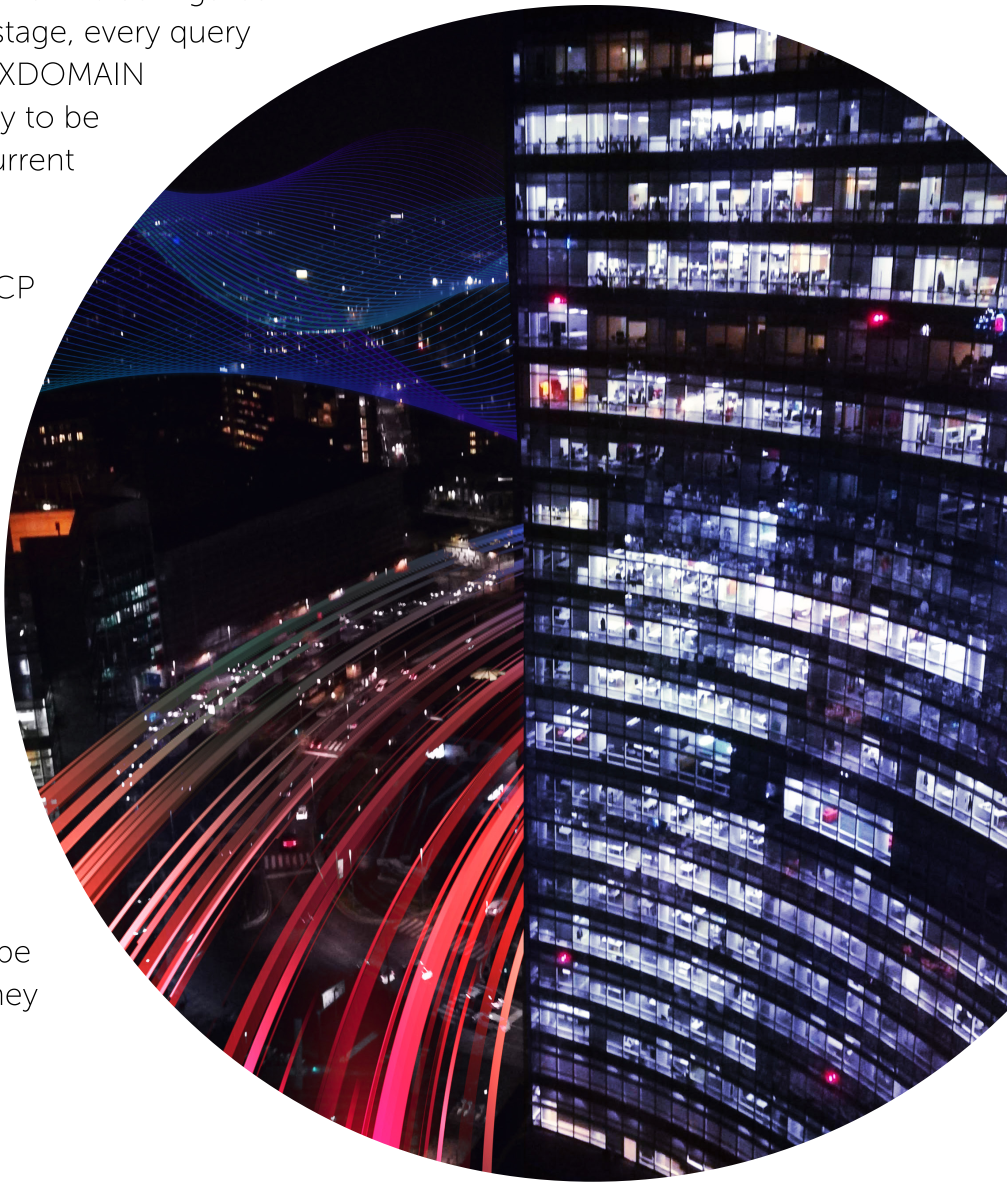
1. **IPAM data migration:** Using an export from the current platform provided by the customer, BlueCat Professional Services leverages BlueCat's migration and analysis tools to migrate all IPAM data to the BlueCat environment. Validation tools ensure

that the IPAM data is represented correctly in the BlueCat configuration. This data will provide a framework for DNS and DHCP migrations.

2. **DNS zone framework duplication:** Leveraging BlueCat's migration and analysis tools, BlueCat Professional Services creates duplicate DNS zones for the current platform's authoritative zones based on export data. Accuracy of the deployed zones is ensured by using validation tools to compare zones deployed in the current platform to the BlueCat configuration. Initially, these zones are configured and deployed as empty copies of the current platform's zones. They will mirror the current platform in structure. But they will not contain any actual resource records beyond NS records necessary for DNS resolution to function properly, as resource records are later populated.

3. **DNS Edge query routing:** DNS Edge service points are configured with two namespaces. They will look for every record in the BlueCat system first and, if not found, try the current platform's configured authoritative servers. At this stage, every query to BlueCat will result in an NXDOMAIN response, forcing every query to be truly resolved through the current platform. This stage sets up the environment for DHCP migrations. The BlueCat DHCP will register every BlueCat-issued DHCP lease into the BlueCat environment, making resolution possible through both systems.

4. **DHCP migration:** Static DHCP reservations and DHCP structures and options are pre-loaded into Address Manager. In the days prior to a migration cutover, lease times are reduced on legacy systems so that all active dynamic records can be monitored to confirm that they



renew on the new BlueCat DHCP systems at cutover time. At the same time, any static differences that may have occurred since a change freeze or data export will also be migrated over.

5. **DNS record migration:** Every record queried through the system will be captured, logged, processed, and written into the BlueCat system. Duplications and changes to records are identified and dynamic records are ignored. This creates a clean, up-to-date, and reliable record of all DNS objects that are used in the environment. Since this process is non-intrusive, the entire DNS migration can happen without any service interruption or additional maintenance planning.

6. **Merge final data:** Once the specified time for dynamic migration has passed, BlueCat Professional Services leverages analysis tools to produce a report reflecting a delta between records in the primary and alternate BlueCat DNS configurations. This report will provide a list of DNS records remaining in the alternate configuration that haven't been queried during the entire DNS migration process. The customer then reviews the report to determine if any of the remaining records are still needed. Once that list of records has been compiled, BlueCat Professional Services will migrate those records and verify accuracy, thereby consolidating all validated DNS zones and records onto the BlueCat platform.

7. **Decommissioning:** At this stage, we validate that records are no longer queried from the current platform's infrastructure. BlueCat migrates all remaining data from the current platform into a secondary configuration in BlueCat. A new namespace points to the secondary BlueCat configuration, ensuring that even very rarely queried records can be captured. This setup will operate for a period to verify that no queries are still being resolved by the current platform. As soon this is validated, the namespace pointing to the current platform is removed and it can be safely decommissioned.

Custom VitalQIP REST endpoints for automation

BlueCat investigated more than 200 VitalQIP-specific endpoints that exist in customer environments and created equivalent mappings to help your operational team continue the work already in place at your organization. It is easy and quick to implement a set of endpoints that mimic some of your VitalQIP endpoints, allowing for a more seamless migration when moving to BlueCat.

Endpoints cover several key functions and can be grouped into the following key areas:

Validation: These validation endpoints are used to see if networks, zones, IP addresses and other data sources exist. It will only validate the payload provided; no changes are made. This collection of REST endpoints is usually executed before the creation or deletion of data.

DDI operations: A collection of endpoints used to add, update, or delete data. Actions include IP address management, resource record management, and network management. These endpoints are run after verifying the data set in the above validation endpoints.

Bulk actions: This provides the same actions in DDI operations except in bulk data processing. This is usually used when opening or closing an office or rolling out a new zone.

Custom VitalQIP reporting through Gateway

VitalQIP provided some unique reporting capabilities that BlueCat has recreated and added to ensure a reportable environment. The following standard reports are included for our VitalQIP to BlueCat migration customers:

Report name	Details
BlueCat appliance model report	Shows list of BlueCat servers in Address Manager with each server’s name, models/profiles, and IP addresses
DHCP utilization report	Shows the number and percentage of DHCP addresses in use by the network
Multiple default gateway detection report	Finds networks that cause issues during start-up for Windows DHCP clients due to multiple gateways defined
NTP stratum and offset report	Shows NTP statistics (peer, offset, stratum, jitter, delay) for BlueCat servers
Patch report	Shows patches applied on BlueCat servers

Report name	Details
CAPm (capacity) subnet report	Various statistics related to DHCP utilization (max utilization over five days, actual utilization, allocation, etc.)
Servers by firmware version report	Shows BIOS, iDRAC, and fiber NIC firmware versions, as well as DNS/DHCP services
Subnet report	Shows subnet region, ID, name, subnet, and subnet mask when searching by IP or network name
User login report	Shows user sessions in Address Manager (username, timestamps of login/logout, session state, IP, and authenticator used)
Version report	Shows current running BlueCat software version for all servers

Best practices for physical deployment of BlueCat systems

To ensure a smooth deployment of BlueCat systems, BlueCat Professional Services employs several best practices.

- Address Manager is deployed as the central management system in primary and secondary data centers.
- Migration-focused Gateway instances are deployed as a pair wherever Address Manager is deployed. These instances are not only the required framework for our toolsets, but also central to automation activities that help customers operationalize the new system.
- BlueCat DNS and DHCP Servers (BDDSes) are deployed based on architectural decisions.
- DNS Edge service points are deployed behind a load balancer or in load balancing enabled Anycast between the current platform's internal recursion (caching) layer and the current platform's authority layer, or as the first hop DNS server for clients to handle query loads (horizontal scaling architecture). This can be based on regional considerations as well as expected query loads.
- DNS Edge service points are enabled to have HTTPS access to the BlueCat DNS Edge Customer Instance hosted by BlueCat in AWS.
- BlueCat connects systems according to documentation and makes them ready for production use.

Are you ready to migrate from VitalQIP, Microsoft DNS, or other legacy providers to BlueCat's Adaptive DNS solution?

Look no further.

We're ready to help you get started.

Contact us to discuss your migration today

bluecatnetworks.com