Using BlueCat Adaptive DNS in the Cloud
Executive Summary

The following document describes the challenges that hybrid, multi-cloud architectures present for network teams, specifically related to IP address management, DNS and DHCP (DDI). These include:

**Achieving and maintaining universal, 360 degree visibility** into an organization’s IP space, namespace and DNS records without hindering rapid innovation and application development by cloud and devops teams;

**Establishing control of DNS resolution paths** to provide the best end-user experience and optimal network performance while minimizing architectural complexity and data conflicts that result in costly downtime.

**Securing access to critical applications and data** at the DNS layer by establishing intelligent least privilege security policies.

This paper discusses BlueCat’s approach to solving these challenges through application of its Adaptive DNS solution for full DNS visibility, control and security.
The Cloud Challenge

Being in the cloud means moving fast. Cloud and DevOps teams are constantly standing up new compute, tearing it down, and moving workloads. For developers, this is a pretty exciting situation to be in. The entire cloud environment is built to give them what they want, when they want it.

When all of this innovation is happening in the cloud, the consequences on core network infrastructure are usually an afterthought. Cloud and DevOps teams use default DNS services furnished by cloud providers, or DNS resources spun up on the fly. They often don’t know what that means for the rest of the network, and they probably don’t care. They just want to keep moving, no matter what happens on the infrastructure side. In addition, the dynamic nature of cloud development introduces risk that need to be managed with consistent security policies across the network.

Network administrators, on the other hand, care deeply about the infrastructure consequences of the cloud. They’re the ones who have to deal with the back-end chaos that results from everything the cloud and DevOps teams do. Cloud and DevOps teams expect all this stuff to “just work”. Network teams have to make it work.

Here are a few of the challenges network teams face when dealing with the consequences of cloud DDI infrastructure, and how BlueCat solves some of these challenges.
Visibility

Infrastructure teams at large organizations have a mandate to understand holistically how the business is allocating IP space in order to optimize network performance and deliver critical services to the business. But all too often, network teams have precious little insight into what’s going on in the cloud. Trying to discover and manage DDI data across multiple clouds and on-prem resources is a significant challenge – one that can manifest itself in two ways:

Cloud integration with on-prem networks: Whenever cloud/DevOps teams stand up networking components of the cloud, they assign IP space to those areas. In the absence of a single source of truth for assigning IP space across environments, those IP ranges may already be assigned to another area of the on-prem network. These conflicts cause network outages which reduce productivity (and profitability) to zero for as long as they persist.

Creeping fragmentation of DDI: Maintaining centralized visibility and control over core infrastructure resources is critical to error-free, rapid delivery of network services across the enterprise. When the cloud creates autonomous areas of the network with their own DDI resources, that centralized system begins to erode, and with it the ability to deliver services efficiently and effectively.

Simply imposing change controls on application developers doesn’t work. Even asking these teams to simply document their rapid changes and feed these back to teams responsible for network infrastructure is viewed as archaic and bureaucratic. So it just doesn’t happen.

So IT is left with a black hole in their plans to properly manage IP space across single clouds or hybrid cloud environments. Or worse, when the lack of a centralized authority for DNS resolution results in data conflicts that bring down the network, it is not the Cloud and DevOps team that get blamed. No, network teams are faulted for “slowing things down.” It’s a classic problem of network admins having all the responsibility but only some of the authority over network infrastructure.
Control

In order to overcome the challenges associated with a patchwork of hybrid cloud infrastructure, the network team sets about building and managing conditional forwarding rules to bridge the gap between all these different environments. The scale and speed of cloud adoption at many large enterprises means that there will be thousands of conditional forwarding rules developed in short order. As workloads move and new applications are developed, these rules will need to be constantly updated, requiring a lot of admin time to manage. This creates unmanageable complexity at many organizations. Often, teams responsible for maintaining this rat’s nest of routing and forwarding rules can point to a single or small group of experts that actually understand how it was built. They’re full time job becomes the maintenance of these rules, pulling resources away from more important things.

Ordinarily, customers want to apply some kind of automation to sort out this mess. The challenge is that none of the cloud-native DDI services support automation outside of their own environment. And nobody wants to manage separate DDI automation engines for each of their clouds – that’s just more trouble than it’s worth.
Security

Network security is a hard-enough task when all the infrastructure is on premise. Moving to the cloud introduces even more complications.

Suddenly customers are securing information in someone else’s data centers, triangulating against someone else’s infrastructure, and dealing with someone else’s software running through the network. On top of that, there’s that whole class of cloud-specific malware, which takes advantage of the unique architecture of the cloud to introduce new security vulnerabilities.

The shared responsibility model used by most public cloud providers offers cold comfort for network security teams. On one hand, the sheer scale of resources cloud providers devote to physical and data security is beyond what most companies or even governments could deliver on their own. On the other hand, cloud customers are on the hook to secure everything outside of the cloud provider’s infrastructure – not an easy task by any means.

In an ideal world, customers should be able to simply extend the security architecture created for on-prem environments into the cloud. Everything would be consistent, and the security controls would simply scale into a new environment. In reality, most security teams don’t even have visibility into what’s happening in the cloud – actual control over events seems like a pipe dream.

DNS is the common denominator which can bridge the security gaps inherent in hybrid cloud environments. That’s because every query on the network – whether on prem or in the cloud, legitimate or malicious – uses DNS.

When customers have visibility into what’s happening in DNS, they can create consistent security controls across the enterprise. More specifically, if customers have visibility into internal DNS records – DNS at the level of devices, VMs, and containers – they can apply security policies regardless of where individual assets sit.
BlueCat
Adaptive DNS
BlueCat’s mission is to reduce the complexity caused by inefficient, disconnected network services in the cloud through an approach called Adaptive DNS. This approach gives customers the power to thrive in a complex, hybrid cloud world – not get buried in the avalanche of conditional forwarders, disparate DNS services, and conflicting sources of information.

When it comes to implementing DDI in the cloud, there’s no single architecture that works for everyone. Every network is different, and the goals supported by every network vary widely. So a more flexible architectural approach is needed that doesn’t rely on boxes in the data center. It requires the flexibility of offering integration with the cloud-native tools already in use, or BlueCat solutions. It needs to be a ‘deployed anywhere’ solution – in the cloud or at the network edge – with a pricing model that doesn’t lock buyers into rigid deployment choices.

BlueCat help organizations find the cloud visibility and control they need without disrupting the pace of innovation by:

**Establishing a consistent approach to DDI:** BlueCat’s unified platform acts as a single source of truth of IP, namespace and DNS records, regardless of how or where it is assigned on the network. With BlueCat, administrators can extend core DDI infrastructure into the cloud or integrate it with cloud native DDI services. This isn’t necessarily an either/or decision, and there are several strategies which offer different paths to the same goal. BlueCat provides the flexibility to tackle this issue in the most appropriate way.

**Deploying network automation and orchestration tools:** Once a single source of truth for DDI is in place, cloud and DevOps teams can operate quickly at scale by calling on those DDI resources with BlueCat’s network automation tools and orchestration platforms. Self-service provisioning connected to an automated DDI infrastructure is a prime example of the value that fully integrated infrastructure can provide to cloud and DevOps teams, giving them the power to get the resources they need quickly without creating more problems for their network infrastructure colleagues.
Enabling Universal Discovery and Visibility in Hybrid Environments

From a DNS perspective, the common challenge organizations face in supporting a hybrid cloud architecture is the ability to enable bi-directional resolution and maintain complete visibility across all platforms. Resolution and dynamic visibility is essential because of the cloud vendors control of IP distribution. The ability to achieve resolution and visibility is the key challenge to seamlessly enable on-prem to cloud, cloud to on-prem, cloud to cloud, within tenant, across tenants, and out to the internet resolution use-cases.

BlueCat provides the IT team with automated workload discovery, IP addressing and DNS deployment within existing clouds deployed, and then real-time visibility of dynamic workload changes and moves within multi-cloud environments. This enables a return to DNS consistency and IP visibility over the entire network, reducing provisioning errors and DNS name space collisions.

Dynamic visibility means not just cloud DNS record assignment, but the creation of entire Address Blocks/Networks, Private Network Blocks/Subnets in VNETs/VPCs, Workload Instances and related IP addresses and DNS names.

To do this, BlueCat first polls the cloud provider in order to fully document the cloud IP infrastructure prior to starting continuous visibility. Discovery first occurs against a cloud provider region, a unique configuration within BlueCat is created for each region being discovered. All public address space network blocks and subnets within Cloud Provider region are then dynamically created. This occurs independently of whether space is actually being utilised, in order to allow for dynamic allocation/reallocation of internet facing public IP addresses that may be utilised on compute workloads.

Any private address space contained with any discovered private networks (VPC/VNETs) is then dynamically added to Bluecat at Network Blocks and Subnets.
IT teams do not have to manually create Network Blocks and Subnets - an automated documentation of IP address space utilised by the enterprise within their clouds provides, for the first time, a single pane of glass of both internal address space and any in the cloud utilised address space. This includes visibility into cloud address space that may have been running for extended periods without being formally documented by any organisations.

The second phase of the discovery process focuses on workloads within the private networks. Any compute discovered, whether started or not, is added dynamically to the Bluecat solution as a device instance. These instance devices hold additional meta-data gathered such as machine size, owner and whether the instance is started or stopped. When the device instance is added to Bluecat, any IP addresses, both public and private, are added to the infrastructure discovered already in the first phase.

BlueCat’s is unique in how it dynamically represents cloud compute that is currently running and disassociated from internal corporate DNS domains. BlueCat documents DNS records that are automatically allocated by Cloud solutions upon device instance creation as meta-data. But even more importantly, it appends BlueCat domain to the meaningful instance names. This brings these compute resources in line with corporate naming policy and allows for easier service discovery by internal resources.

Dependent on the Cloud provider, BlueCat also:

- Creates unique DNS views and zones in its Address Management solution for any public or private hosted zones with the Cloud DNS services, such as Amazon Route 53 or Azure DNS.
- Documents any IP-based load-balancer devices utilising cloud native capabilities as special device instances.

BlueCat’s approach to phased discovery will allow for future discovery enhancements, such as documenting actions initialized in the cloud, like CloudFormations or Azure Templates.

Effectively, BlueCat ensures that any change to network infrastructure done in the cloud - from cloud assignment of a single IP address to creation of entire networks
via orchestration tools - is reflected in BlueCat’s address management system. This allows application and cloud teams to operate unfettered in hybrid environments, while ensuring that infrastructure teams can see, and get out ahead of, potential IP conflicts that may cause errors and pose serious risk to business continuity.

Taming Complexity with Intelligent Networking

BlueCat gives network teams the control they need over pathways of data and compute flowing through hybrid cloud environments. Once the foundation of a standardized DDI infrastructure is in place, BlueCat uses automation to solve the problem of conditional forwarders with Intelligent Forwarding.

The Intelligent Forwarding concept is simple. Instead of managing a complex and changing set of single-option DNS resolution paths, network teams can provision multiple resolution possibilities. If the first DNS query comes back with an NXDOMAIN, the query will automatically re-route to the next priority location, and so on, attempting multiple pathways until it finds the right answer.

Managing these multiple resolution pathways across a hybrid cloud environment is much easier when they are all in a single place. When the DDI system supersedes the siloed services in each cloud or on-prem habitat, customers get the enterprise-level visibility and control that is needed to operate hybrid cloud environments at scale, taking full advantage of the nimble DevOps and cloud development tools.
Please see our video for more information on how BlueCat’s intelligent forwarding system works.

Enabling Cloud Security through DNS Query Logging and Policy Management

BlueCat creates a consistent security posture across the enterprise by leveraging the information flowing through DNS infrastructure. It does this by managing DNS right at the client level, logging and applying security policies to DNS queries at the “first hop”. This provides the baseline visibility which security and network teams need to implement needed controls in the cloud and on-prem.

BlueCat’s DNS security policies reduce attack surface by blocking malicious or inappropriate queries at the source. This functionality can be used as a form of role-based access control (RBAC) – preventing unauthorized access and ensuring that data sets and areas of compute are only available to users with the need to know.
BlueCat also uses DNS security policies to prevent lateral movement between clouds, underneath the external filters and firewalls which many advanced persistent threats and malicious insiders seek to avoid. The policies applied to DNS can vary according to the threat – customers can monitor, redirect, or block queries based on how the threat should be treated.

BlueCat allows security teams to triangulate threat data against a source IP to quickly identify the origin of cloud-based threats. BlueCat provides the detailed DNS logs and query data security teams need to identify patterns and anomalies which are the first indicators of compromise. For example, BlueCat can identify DNS tunneling which could be hiding data exfiltration. In addition, these DNS logs can be easily passed to leading SIEM solutions and data analysis tools for further analysis and remediation.

To extend the scope of this security and control, Cisco and BlueCat have integrated to deliver comprehensive visibility and control across all platforms from the end point to the cloud with an insightful defense architecture. This powerful new integration between Cisco Umbrella and BlueCat Adaptive DNS gives customers answers to the most critical questions in network security: Who, What, When and Why, with a non-intrusive solution deployment.

Please see our DNS Edge video for more information on how BlueCat’s DNS Security application works at the first hop.
Conclusion

The adoption of hybrid and multi-cloud architectures by enterprise organizations is creating unprecedented opportunity for delivering mission-critical services to internal stakeholders and customers alike. But it is also introducing compounding complexity for networking teams struggling to keep up with rapidly changing environments. Too often, the result is network and data conflicts, errors and costly outages, or at the very least, a poor user experience when customers cannot get access to the services or applications they need.

BlueCat’s Adaptive DNS platform helps overcome these challenges, allowing networking, cloud and application delivery teams to manage through this complexity and take advantage of the obvious benefits of hybrid cloud environments. Key to all this is maintaining a single source of truth for namespace, IP address and DNS record information in a centralized DDI platform. Whether by extending this critical service from the data center to the cloud, or recognizing and reflecting new IP space allocation in the cloud in BlueCat’s IP Address Management solution, Adaptive DNS ensures network connectivity, business continuity and data security, no matter where workloads and compute reside.
Today’s networks are drowning in complexity. If your DNS infrastructure isn’t adaptable by design, your network - and your entire business - is fragile. Think outages. Downtime. Data loss.

BlueCat helps your business thrive on complexity with Adaptive DNS. Move beyond static, manually-controlled, off-the-shelf DNS that breaks under network complexity, and move to a DNS that embraces it. Adaptive DNS is powered from the edge of your network, scaling to meet escalating demands by users, applications and services. It’s open and automated, giving you the power to enforce business policies, manage security, analyze data, and remediate threats.

Thrive on complexity from edge to core with BlueCat Adaptive DNS™.