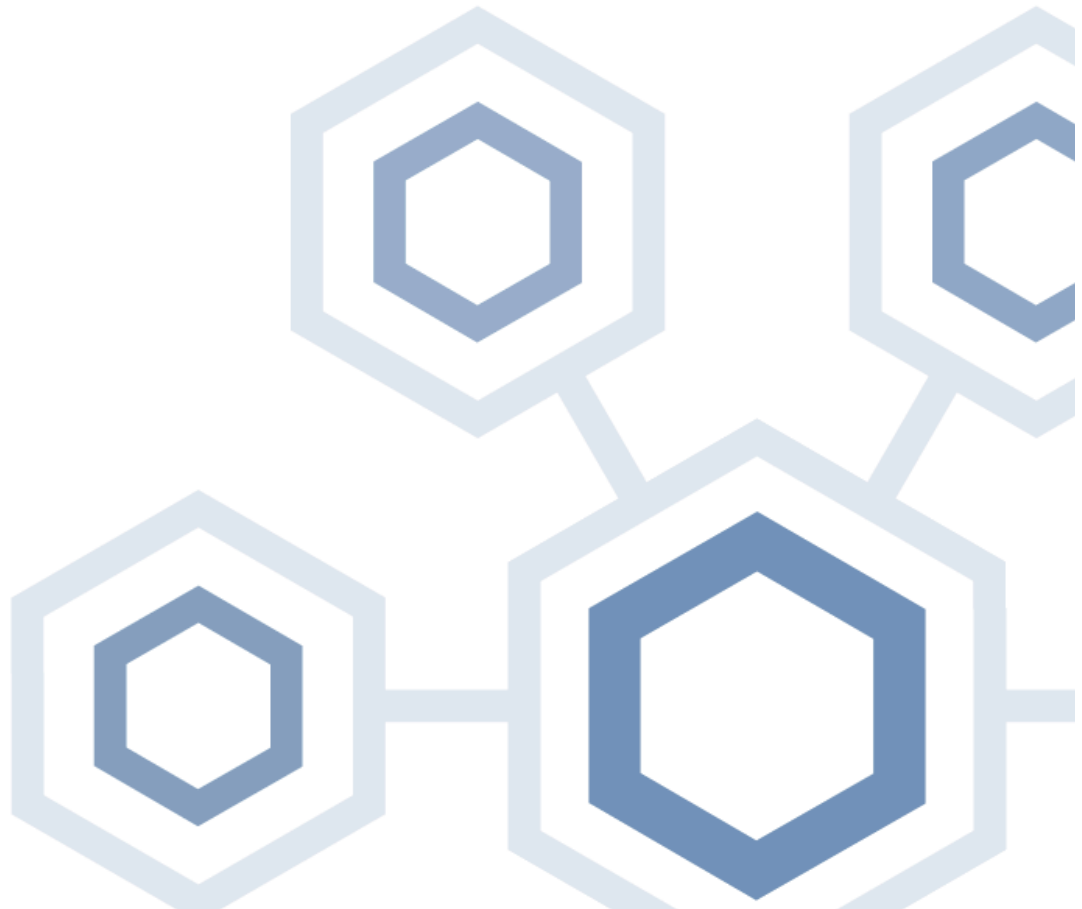




Managing Microsoft® Active Directory® DNS with BlueCat

The Benefits of Deploying BlueCat Address Manager and BlueCat DNS/DHCP Server for DNS Services supporting Windows® Active Directory®





Contents

Executive Summary	3
Introduction	4
Challenges with Windows Server DNS and DHCP	5
Challenge 1: Risk of Human Error	5
Challenge 2: AD Replication Problems Effect DNS Resolution	5
Challenge 3: No Effective Delegation Controls or Auditing.....	5
Challenge 4: DNS Maintenance and “Scavenging”	5
Challenge 5: Unnecessary Complexity	5
BlueCat Solves These Challenges	6
BlueCat and Active Directory	6
BlueCat Fully Supports Active Directory DNS	6
Decoupling Your DNS and DHCP from Windows Server and Your Active Directory Infrastructure	6
DNS Architecture Best Practices.....	6
BlueCat Offers Elegant DNS Architectures, Fully Integrated Management, and Advanced Security Controls	
Compared to Windows Server DNS.....	11
Advanced DNS, DHCP, and IP Address Management.....	12
Referential Integrity	12
Centralized, Model-Based Management.....	13
Preventing Outages Caused by Human Error.....	14
Auditing and Reporting.....	14
Advanced Security Capabilities	15
Advanced Secure Dynamic Update Control.....	15
Hardened DNS/DHCP Servers and Software	15
Granular Security and Delegation	15
Network and DNS Zone Templates.....	15



Executive Summary

Microsoft Windows® Active Directory® has become the de-facto standard for directory services across all sizes of enterprises. Microsoft-based Active Directory's name resolution is the DNS standard Internet name resolution is based on. Many IT personnel errantly believe that Active Directory is integrated with Microsoft DNS but nothing could be further from the truth. Active Directory depends on DNS and can act as the data store and replication technology for Windows Server DNS data but is in no way integrated with DNS^{1,2}.

Most enterprises have deployed Active Directory utilizing Windows Server DNS, abandoning best-practice DNS topologies. By tying DNS design to the Active Directory hierarchy they have created a poor DNS design. Larger enterprises feel the pain of these design deficiencies most acutely, experiencing poor DNS performance, poor reliability, and difficulty managing DNS as part of their larger DNS, DHCP, and IP Addresses Management (IPAM) needs.

Windows Server DNS architectures and capabilities create numerous challenges including a high risk of human error, service impacting replication problems, a lack of effective delegation controls or auditing, maintenance challenges, and overly complex DNS topologies based on Active Directory topologies.

BlueCat offers an integrated and centralized solution that reduces the operational burden of managing DNS, DHCP, and IP Address Management to solve these challenges. A best-practices infrastructure built on BlueCat provides higher performance, less complexity, eliminates human errors through robust validation, and adds significant technical and security capabilities not found in Microsoft Windows.

BlueCat provides the most robust and integrated platform for Active Directory DNS as well as your enterprise DHCP and IP Address Management needs.



Introduction

Microsoft Windows Active Directory has become the de-facto standard for directory services across all sizes of enterprises since its introduction with Windows 2000 Server. Nearly every business from small businesses to the Fortune 500 uses it in some part of their business.

When Microsoft designed Active Directory they abandoned their legacy NetBIOS name resolution service in favor of the Domain Name System (DNS), the name resolution technology the Internet is built on. Since the launch of Active Directory, many IT personnel have come to believe that Active Directory is somehow integrated with Windows Server DNS. Nothing could be further from the truth. Active Directory depends on DNS and can act as the data store and replication technology for Windows Server DNS data (LDAP replication), but it is in no way integrated with DNS ^{1,2}.

Active Directory servers are not aware of which DNS server platform they are using. Active Directory servers simply use the DNS servers configured in their network card settings and then create and manage their records using non-proprietary secure dynamic update technologies.

Most enterprises have deployed Active Directory utilizing the local Windows Server DNS service, abandoning an independent, best practice based, DNS topology. Tying DNS design to the Active Directory forest and domain hierarchy creates a poor DNS design. Larger enterprises feel the pain of such design deficiencies most acutely, experiencing degraded DNS performance, poor reliability, and difficulty managing DNS as part of their larger DNS, DHCP, and IP Addresses Management (IPAM) needs.

BlueCat offers an integrated and centralized solution that reduces the operational burden of managing DNS, DHCP, and IP Address Management. A best practice infrastructure built on BlueCat provides higher performance, less complexity, eliminates human errors through robust validation, and adds significant technical and security capabilities not found in Microsoft Windows.

BlueCat's additional capabilities include elegant and highly available topologies using Anycast and clustering, referential integrity between IPAM, DNS, and DHCP configuration data, full pre-deployment validation to protect against human error, improved security through inherently granular change permissions and delegation, full auditing, reporting, and more.

BlueCat provides the most robust and integrated platform for Active Directory DNS as well as your enterprise DHCP and IP Address Management needs.



Challenges with Windows Server DNS and DHCP

Challenge 1: Risk of Human Error

The greatest operational risk with Windows Server DNS using Active Directory replication is changes made live immediately on the local server and then replicated to all other servers hosting that DNS zone. Depending on the Active Directory configuration, which could mean every DNS server in the domain or the entire forest. Any accidental deletion will replicate across the domain or forest with no undelete capability. Prior to moving to a BlueCat solution, many customers have had to restore their Active Directory in order to recover DNS data lost by accidental deletion.

Microsoft's management tools provide no data validation to prevent human errors, and have poor auditing capability and security delegation controls. Determining which administrator made a particular change is difficult or impossible, further complicating troubleshooting processes.

Gartner and other industry analysts estimate human error as the root cause of at least 30% of network related outages^{3, 4}.

Challenge 2: Active Directory Replication Problems Affect DNS Resolution

The replication of DNS changes across Microsoft DNS servers can take from seconds to nearly an hour. This can result in inconsistent data across the enterprise until the replication completes. Replication is especially slow across low bandwidth or highly utilized links. These inconsistencies during replication can cause system failures and make validating DNS record changes difficult.

Challenge 3: No Effective Delegation Controls or Auditing

Large enterprises with global infrastructures find it difficult to secure access to all Windows Server DNS servers across business units and geographic regions. Microsoft provides only server-centric views of DNS and DHCP data that require large numbers of administrator-level accounts for management across teams and business units. This lack of control dramatically increases the number of administrators that can make changes, which are replicated across the domain or forest. When changes are made there is very little audit information available, and it is often quickly lost as local audit logs rollover and cannot be natively centralized.

Challenge 4: DNS Maintenance and “Scavenging”

In order to remove outdated DNS records, Microsoft DNS uses a “scavenging” process based on the last update time of the record. This process is notoriously unreliable in determining the validity of the record and most Active Directory administrators do not use it for fear of removing valid DNS records and causing a service outage. This can cause secondary issues, such as duplicate or outdated DNS information.

Challenge 5: Unnecessary Complexity

Companies that have grown through acquisition can have dozens or even hundreds of Active Directory domains, each with a number of Domain Controllers also running DNS. Maintaining Microsoft DNS on a multitude of servers is operationally daunting and results in a DNS architecture based on complex conditional forwarding and DNS delegation scenarios. Decoupling DNS design from the Active Directory topology can significantly reduce the number of servers needed to support any environment while providing DNS best-practice based resiliency and performance.



BlueCat Solves These Challenges

BlueCat provides the centralized management and intelligence needed to solve these challenges. BlueCat's IPAM, DNS, and DHCP solution delivers integrated management and advanced security and validation controls not available with Microsoft. Human error is the root cause of at least 30% of network related outages^{3,4}. Why continue to allow the level of complexity created by these challenges without any central management, data validation, effective delegation, or auditing? BlueCat and Active Directory

BlueCat Fully Supports Active Directory DNS

Before a client computer can connect to Active Directory it uses DNS queries to find an Active Directory server that hosts the services it needs. It is critical that these DNS resource records are accurate and highly available across the enterprise.

Active Directory servers register and maintain DNS host and service records which are necessary for these client and server interactions to succeed. The records are created and maintained using secure dynamic DNS updates. These dynamic updates comply with RFC 2136 but utilize the GSS-TSIG security extensions described in RFC 3645. BlueCat supports all possible interoperability scenarios with Active Directory using GSS-TSIG and provides more granular update security policies than Windows Server DNS can support natively, including update policies that specify which GSS-TSIG attributes to identify update clients by, and explicit controls on which record types that client can update. This improved granularity allows deeper inspection and control of dynamic updates.

- Microsoft Active Directory servers updating BlueCat DNS Servers securely using GSS-TSIG.
- Microsoft Active Directory clients updating BlueCat DNS Servers securely using GSS-TSIG.
- Microsoft DHCP servers updating BlueCat DNS Server securely using GSS-TSIG.
- BlueCat DHCP servers updating Microsoft DNS Servers securely using GSS-TSIG.

Decoupling Your DNS and DHCP from Windows Server and Your Active Directory Infrastructure

DNS Architecture Best Practices

The Domain Name System (DNS) was designed to be a hierarchal system to federate and distribute load and provide high-performance name resolution across hundreds of thousands of servers with distributed administration, all in a reliable and high performance manner.

Microsoft has been recommending a single forest, single domain model for even their largest customers. This may simplify the Active Directory hierarchy, but it defeats the hierarchal design efficiencies of DNS.

Deploying DNS as it was designed provides far-reaching benefits to the organization, as does revisiting your DNS domain hierarchy if you have moved to a single Active Directory forest and domain. Microsoft fully supports several models wherein you can create an independent disjoint DNS namespace that is optimized for your business topology and infrastructure independent of your Active Directory forest and domain structures⁵.⁶ This technique can be used to create regional or business unit specific DNS namespaces for desktops and clients across your global enterprise.



DNS Services

DNS can be logically divided into the following services:

External DNS Services

- **External Authoritative DNS**

These DNS servers host the public facing DNS records for your enterprise. These servers should never offer recursive services: open recursive servers can be used in DDoS attacks.

- These servers should be highly available, hardened against attack and distributed across the organizations facilities with Internet egress. Servers in this role should be placed in a DMZ as they will be available to the Internet DNS Servers.

- **External Outbound Recursion and Caching**

These DNS servers provide recursive lookup services for internal DNS queries needing to resolve external DNS names on the Internet and cache the results for response time optimization the next time the records are needed.

- These servers should be hardened against cache poisoning and should provide DNSSEC validation services to protect internal client's outbound queries from redirection. DNSSEC validation protects internal clients from being redirected to malicious sites due to the other company's DNS being compromised or cache poisoned.
- Recursive servers can also perform Response Policy Zone (RPZ) processing to provide alternate responses to queries. RPZ policies allow you to respond to business partner or other private link or VPN NAT'd clients with appropriate responses for their view into your network. Servers in this role should be placed in a DMZ as they will interact with the Internet and partner DNS servers directly.

Internal DNS Services

- **Internal Authoritative DNS**

These DNS servers host the internal facing DNS records for your enterprise. These servers may also offer recursive services and be directly accessed by clients, but a dedicated internal caching layer provides better scalability and security controls.

- These servers should be highly available for dynamic updates from Active Directory and clients.

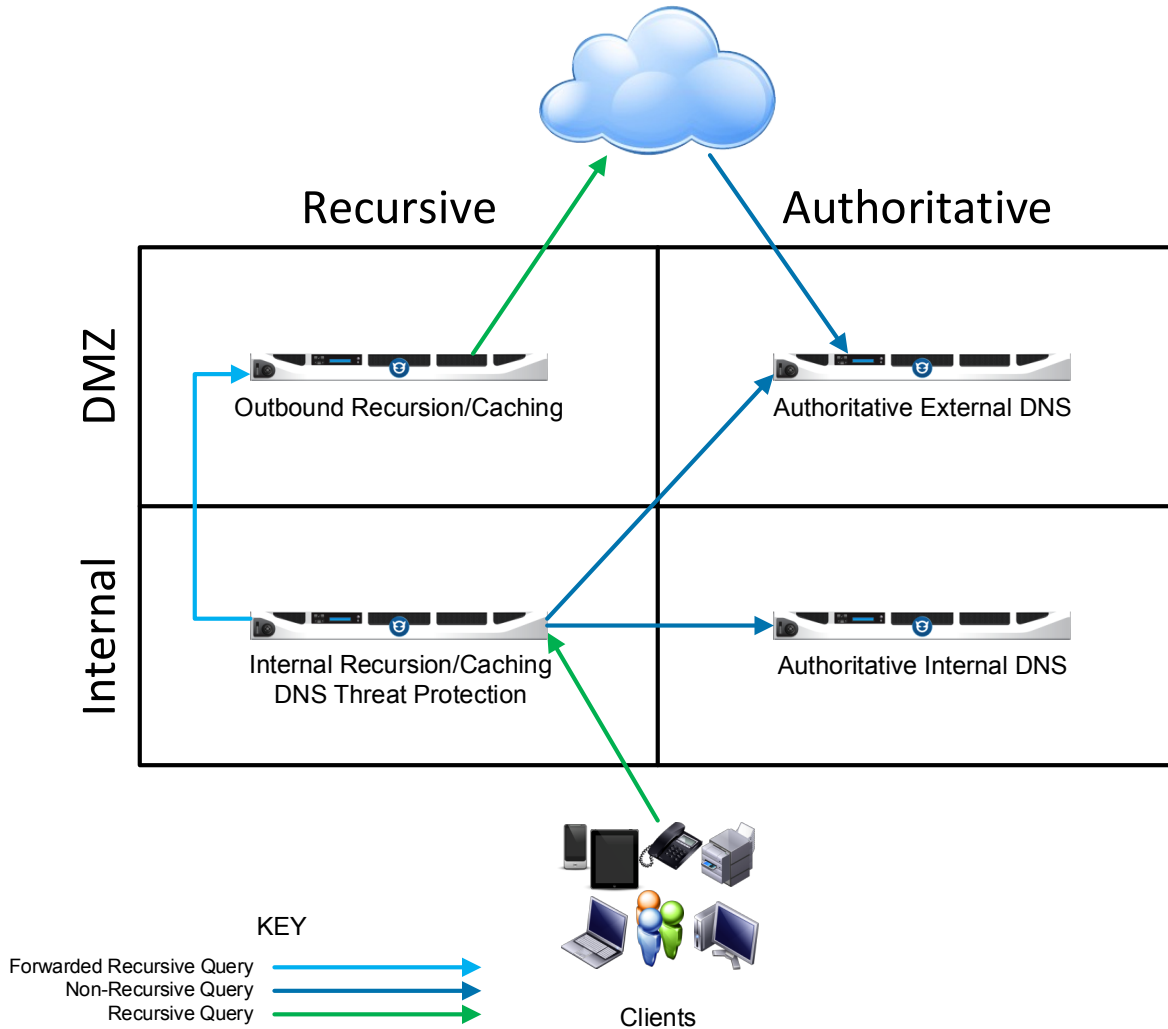
- **Internal Recursion and Caching**

These DNS servers provide recursive lookup services for internal DNS queries and forward any queries your domains your organization is not authoritative for to the External Outbound Caching and Recursion servers. Having dedicated caching servers in each geographic region allows you to direct queries to the appropriate resources in region.

- Dedicated caching servers can also perform policy Response Policy Zone (RPZ) processing to provide alternate responses to queries. RPZ is very valuable in providing correct DNS responses across internal NAT boundaries such as those necessitated by network overlaps from merger and acquisition activities.

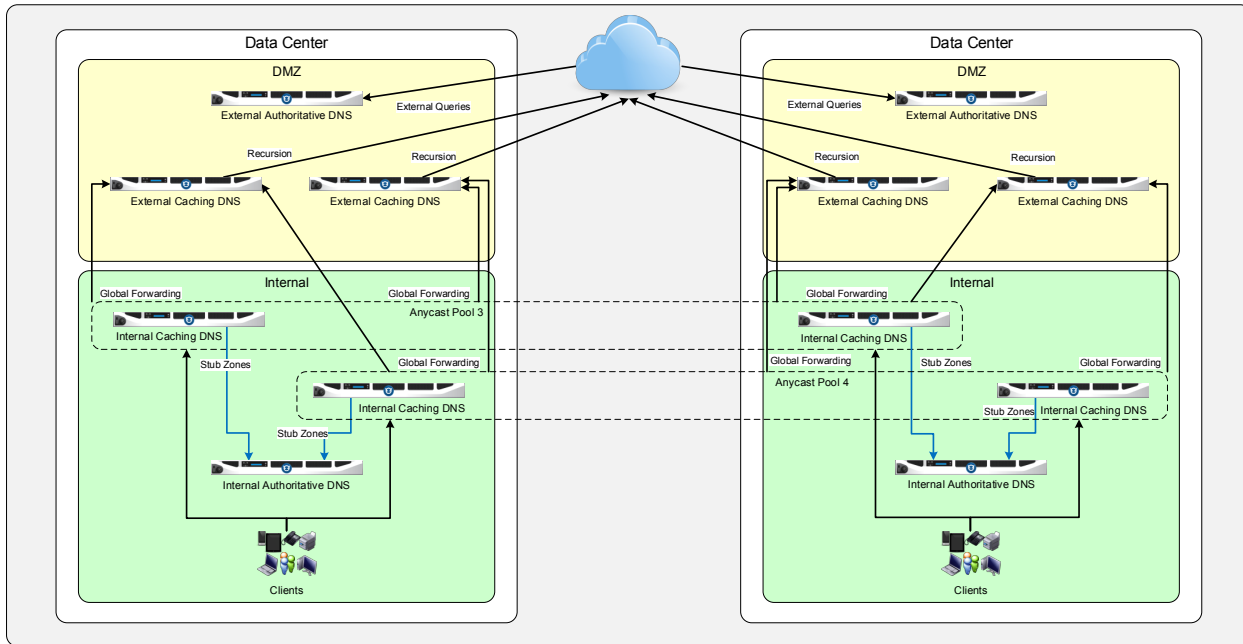


- BlueCat Threat Protection is also available on recursive servers to block and identify internal clients attempting to contact malware, virus, command and control, SPAM, and other known malicious or user-defined sites.





Best Practices for DNS Design



External Authoritative DNS Design

External Authoritative DNS servers should be distributed across the organization's Internet facing data centers to provide faster responses to all geographic regions. These servers should be hardened against all known DNS exploits and attacks as well as have operating system hardening. The DNS Master server for your external DNS should be on an internal network as a Hidden Master. A Hidden Master further abstracts the source of the DNS data behind your internal firewalls. Only DNS Slave servers should be deployed to the DMZ to service Internet queries for your public domains.

Security best practices are to deploy authoritative external DNS Slave servers in a DMZ protected by a firewall and Distributed Denial of Service (DDoS) protection systems. At the very least, these servers should have fourth generation firewall or load-balancer DDoS protection in front of them. No DNS server can provide protection against DDoS within itself; DDoS protection requires a defense-in-depth approach that includes off-premise protections at the ISP as well as third party security providers ⁷.

External Outbound Recursion and Caching Design

Outbound recursion and caching servers are an important element of your security and DNS design. These servers are the final stop for queries leaving your network for the Internet and should be leveraged as a point of security control. Outbound recursion servers should have DNSSEC validation enabled to protect your internal clients from falling victim to cache poisoning redirections due to poorly secured DNS servers at business partners or their upstream ISPs. BlueCat Threat Protection can also be leveraged here or at the Internal Recursion and Caching layer to block and identify devices attempting to access known malicious sites and IP addresses.

These DMZ-based DNS servers can also be configured to provide recursive lookups for a limited subset of internal DNS domains in support of DMZ application servers.



Best Practices for Internal DNS Services

Internal Authoritative DNS Design

Internal authoritative DNS Servers should be highly available and protected from direct configuration changes. Changes made on these servers can affect many aspects of DNS operation and should be carefully reviewed using change management and approval workflows. BlueCat recommends that master DNS servers be located in highly available data centers and should be clustered for physical redundancy. Multiple internal DNS masters should be deployed for static and dynamically updated zones to separate the workload from dynamic updates. Where possible, DNS hierarchies should represent geographical or business unit boundaries to collocate the DNS master servers in those regions.

In most Microsoft Active Directory DNS infrastructures, clients are configured to use the Domain Controller for DNS directly. This makes the client configuration brittle and introduces unnecessary overhead in managing DHCP options to ensure clients use the closest DNS server.

BlueCat recommends that DNS client devices not be configured to use the internal authoritative DNS servers. Instead we recommend they be configured to use an internal recursion and caching server layer.

Internal Recursion and Caching DNS Design

Internal recursion and caching servers should be deployed in a minimum of two Anycast pools throughout the enterprise office and data center locations. If your enterprise operates internationally, then regional pools should be deployed to ensure geo-aware control and Anycast routing optimization.

Deploying an internal caching layer greatly simplifies device configuration and is fully optimized for device roaming. Client queries are routed to the nearest DNS server and that server caches responses from the internal authoritative and external recursive servers. This local caching ensures the fastest possible response time while minimizing load on internal authoritative servers and minimizing traffic to the DMZ-based external recursion and caching servers. Anycast provides the highest possible availability for client queries and is the proven foundation of all core Internet DNS infrastructure.



BlueCat Offers Elegant DNS Architectures, Fully Integrated Management, and Advanced Security Controls Compared to Windows Server DNS.

Deploying DNS on BlueCat separately from the Active Directory topology provides the following key benefits:

- Central management and visibility of all DNS data with full referential integrity between devices, IP addresses, DNS names, and dependent DNS records.
- Three levels of data and configuration validation to prevent human errors from impacting production systems.
- Built-in workflow and approval processes.
- A flexible DNS topology that provides faster replication and response times.
- The ability to identify and block clients attempting to connect to malware, phishing, spam or other malicious sites.
- The ability to control and provide alternate responses to DNS queries for geographic or business specific optimizations.
- A reduction in operational costs and the number of DNS servers needed to support Active Directory DNS infrastructure.
- Higher availability of DNS and DHCP services provided by Anycast and our Crossover High Availability (XHA) clustering.



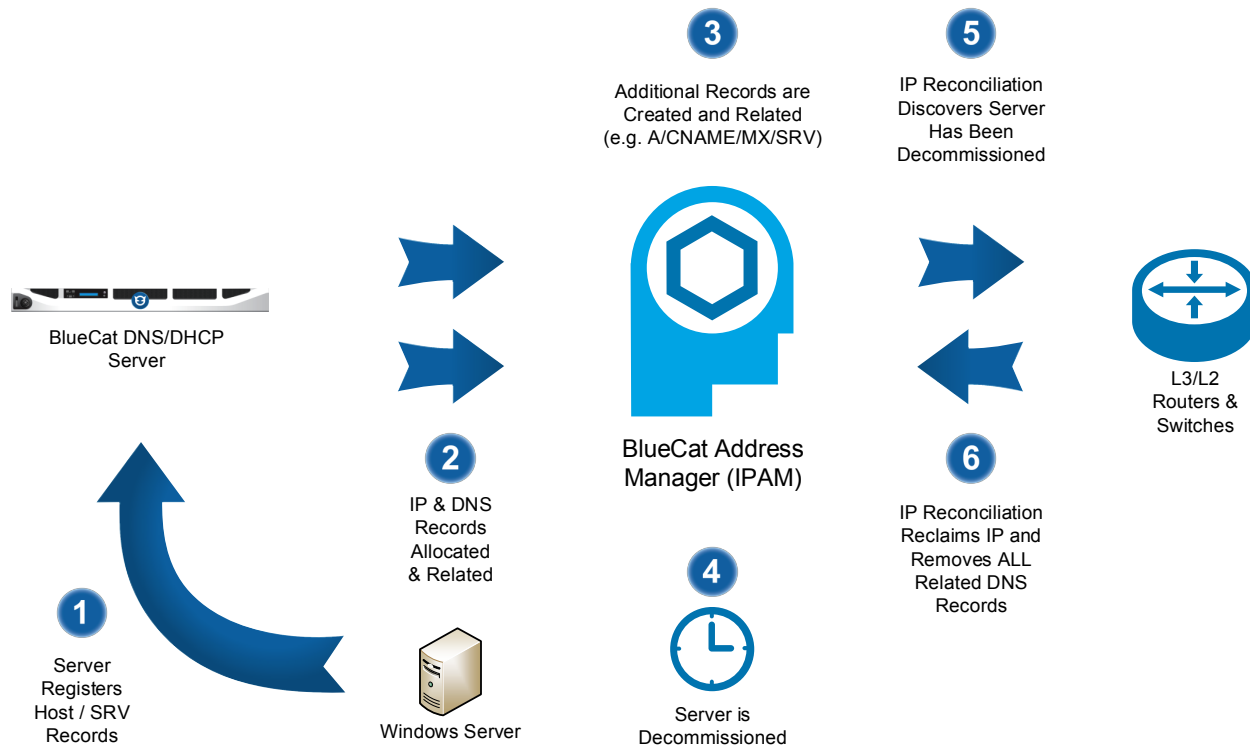
Advanced DNS, DHCP, and IP Address Management

Referential Integrity

BlueCat Address Manager enforces referential integrity in DNS, DHCP, and IPAM data. Address Manager maintains integrity between device hardware addresses (MAC & DUID), their related IPv4 & IPv6 addresses, their related host and PTR reverse lookup records, and any dependent DNS records such as Active Directory service records (SVR) or other dependent records (CNAME, MX, etc.).

Referential integrity eliminates orphaned and outdated data, whether dynamically or statically configured. This includes automatic cleanup of dynamically created DNS records when DHCP leases expire or are released by the client device. Address Manager also provides a single point of truth for all DNS, DHCP, and IPAM data in the environment, regardless of how many DNS/DHCP servers or where they are located.

Address Manager also provides manual and automated IPv4 and IPv6 network discovery and reconciliation, to ensure the data in the IPAM system is accurate and current, another capability not available in Microsoft Server.





Centralized, Model-Based Management

BlueCat Address Manager builds on its referential integrity model to provide hierarchal inheritance and template-based management of all IPv4 and IPv6 Allocations, physical networks, DHCP configuration, DNS Views, Zones, and Response Policy Zone (RPZ) policies. Address Manager's logic-based actions permit non-destructive resize, move, update, and merge actions which optimize network transformation, consolidation, and Cloud infrastructure provisioning projects.

Moving a DNS Zone

Moving a zone allows you to quickly rename all the records within a zone by simply specifying the new zone name.

Lab Internal > Registered > com > example.com > Move/Duplicate Zone

Move Zone

Destination


Address Name:

Assigning a Global or DNS View Level Zone Template


Global and DNS View level templates allow you to easily populate common record names into multiple zones. Records created by the template can be altered later and the template summarily or selectively reapplied to the zones that use it to update the records.

Assign / Apply Zone Template

Template

 Assign Template from View

OR

 Assign Template from Configuration



Preventing Outages Caused by Human Error

BlueCat Address Manager helps ensure BlueCat DNS/DHCP Servers always remain available by preventing human errors from impacting production with three levels of data validation. All management changes are performed offline and controls provide limited deployment or scheduled deployment of the changes into production.

Data Entry Validation.

Address Manager provides data entry validation, so users cannot enter invalid characters or other bad data when creating or changing DNS resource records, DHCP configuration options, or IPAM structures. Any user input that references another configuration object uses search and selection logic, not free text fields for data entry.

Data Checker Service

Address Manager includes the Data Checker service that verifies the entire enterprise configuration for human errors. Data Checker finds logical errors: items that may be technically valid, but that may result in undesired behavior or those that are not valid without other configuration work being completed.

Deployment Validation

BlueCat DNS/DHCP Servers generate and validate all configuration data files upon deployment from Address Manager. These final checks occur before the new configurations are put into effect to ensure that no technical errors can result in a production outage.

Auditing and Reporting

BlueCat Address Manager provides auditing of all changes in the environment. Changes made by administrators and non-administrators through the web UI, command line, and API, or by the system itself, as part of automated processes like IP Reconciliation. The audit history can be filtered by search criteria to quickly find information about what devices, belonging to which employees were on the network at any given time.



Advanced Security Capabilities

Advanced Secure Dynamic Update Control

BlueCat Address Manager provides advanced update policies for Active Directory and authenticated secure dynamic updates to DNS zones using the GSS-TSIG protocol. BlueCat update policies allow administrators to restrict dynamic DNS updates on any aspect of the Service Principle Name (SPN), MIT or Microsoft Kerberos principal, TSIG key, etc. Update policies also allow administrators to match a client update to a policy and explicitly specify which types of DNS resource records the policy allows to be updated. These controls far exceed Microsoft's secure update configuration options and allow simultaneous GSS-TSIG and TSIG based updates to the same zone for mixed environments with non-Windows DHCP or application servers.

Hardened DNS/DHCP Servers and Software

BlueCat DNS/DHCP Server (BDDS) is a purpose-built appliance, available as a 1U rack mount for data centers and branch offices, and as a software virtual appliance for Xen, KVM, Hyper-V, and VMWare environments. BlueCat DNS/DHCP Server provides a solid foundation for reliable and secure service delivery with no local access to DNS/DHCP configuration data. Each rack mount appliance comes with an industry-leading 5-year, 24-hour response time on-site repair warranty, and the option to upgrade to a 5-hour on-site repair response time, available in most of the developed world.

Granular Security and Delegation

BlueCat Address Manager is capable of very granular permissions for management delegation of DNS, DHCP, and IPAM configuration data. Administration can be delegated down to individual objects, including IP addresses and DNS resource records, or can be granted on whole classes of objects – at any level in the IP or DNS hierarchies. The least privileged permission is “hide”, not “read only”. This level of access ensures that users do not have to be trained to ignore configuration data or interface commands that they do not have permissions to use. If the user's permission on an object or command is “hide”, in addition to not being able to modify the object or execute the command, they won't see it at all.

BlueCat Address Manager supports multiple-authenticator configuration for access to the administrative web interface and API by users and groups from Kerberos, LDAP (Active Directory, OpenLDAP, etc.), Radius, and TACACS+ directory sources. This support includes the ability to authenticate users from any number of Active Directory forest or domains, regardless of AD trust relationships between them.

Network and DNS Zone Templates

Network and DNS zone templates allow administrators to define network structures, configuration options, and DNS resource records in templates that can be used in provisioning new networks or zones in a consistent and updateable way. Networks and zones created or updated with a template can be updated again later when the template changes, with administrative selection of exactly which attributes of the template should be reapplied.



References:

1. Carver, Bob. "Linux to Windows Migration." Configuring BIND to Support Active Directory Services. June 1, 2001.
<https://technet.microsoft.com/en-us/library/dd316373.aspx>
2. "Interoperability Issues." Domain Name System (DNS). January 21, 2005.
<https://technet.microsoft.com/en-us/library/cc755717.aspx>
3. Lerner, Andrew. "Network Downtime." Network Downtime (blog), July 11, 2014.
<http://blogs.gartner.com/andrew-lerner/2014/07/11/network-downtime/>
4. Network Barometer Report 2014. Report. Johannesburg, ZA: Dimension Data, 2014.
<http://www.dimensiondata.com/Global/Global-Microsites/NetworkBarometer>
5. "Disjoint Namespace." Disjoint Namespace. August 17, 2011.
<https://technet.microsoft.com/en-us/library/cc731125.aspx>
6. "Create a Disjoint Namespace." Create a Disjoint Namespace. April 11, 2008.
<https://technet.microsoft.com/en-us/library/cc731929.aspx>
7. Modern DDoS Defense Toolkit: Advice from Arbor Networks and Gartner. Technical paper no. 1. December 15, 2014.
<https://www.gartner.com/doc/1759917/enterprise-strategies-mitigating-denialofservice-attacks>