COMMON CHALLENGES WITH MICROSOFT® DNS

Integrating Microsoft Active Directory® with BlueCat DNS Services

BLUECAT™

bluecatnetworks.com

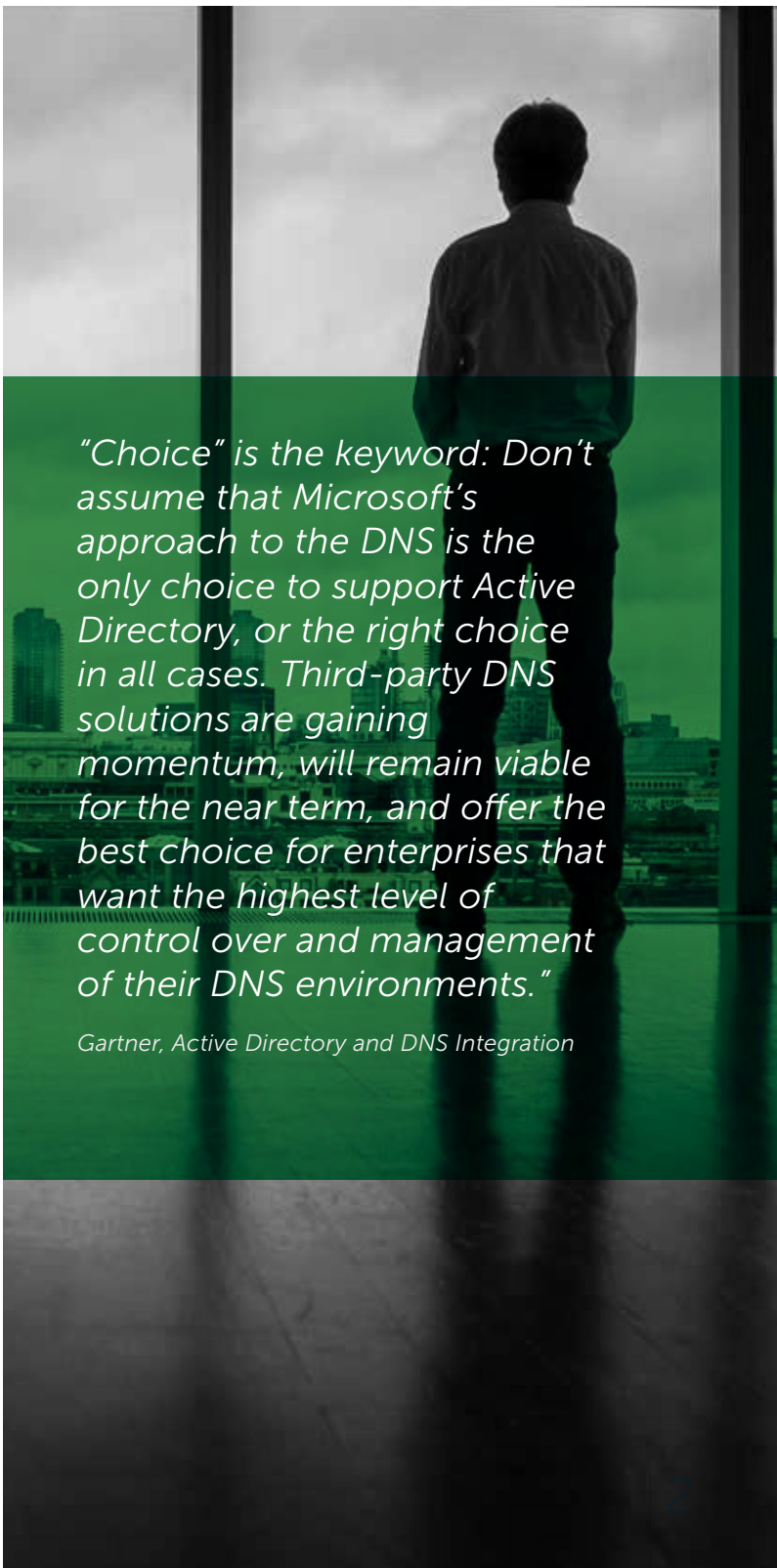
COMMON CHALLENGES WITH MICROSOFT DNS

Since its introduction with Windows 2000 Server, the Microsoft Active Directory has become the de-facto standard across organizations of all sizes for their directory services.

When Active Directory was designed, Microsoft discontinued their legacy NetBIOS name resolution services and replaced them with the Domain Name System (DNS).

It is a common misconception within many IT groups that Active Directory is by default integrated with Windows DNS server. The reality however, is that Active Directory itself is dependent on DNS. It can act as the data store and replication technology for Windows DNS server data (LDAP replication), but it is in no way integrated with Microsoft DNS[1,2]. Active Directory servers are not aware of the DNS server platform they are using. They simply use whatever DNS servers are configured within their network card settings and create and manage their own records by using non-proprietary secure dynamic update technologies.

Many organizations have deployed Active Directory utilizing the local Windows DNS service, which bypasses DNS topology best practices. They generally tie DNS design to the Active Directory forest[3] and domain hierarchy[3], which creates a poor DNS design altogether. This poor design significantly impacts larger enterprises as they experience degraded DNS performance, poor reliability and difficulty in managing DNS as part of their larger DNS, DHCP and IP Address Management needs.



"Choice" is the keyword: Don't assume that Microsoft's approach to the DNS is the only choice to support Active Directory, or the right choice in all cases. Third-party DNS solutions are gaining momentum, will remain viable for the near term, and offer the best choice for enterprises that want the highest level of control over and management of their DNS environments."

Gartner, Active Directory and DNS Integration

Challenge 1: Risk of Human Error

The greatest operational risk with Microsoft DNS using Active Directory replication is that changes are made live immediately on the local server and are then replicated to all other servers hosting that DNS zone. Depending on the Active Directory configuration, this could mean every DNS server in the domain or the entire forest. Any accidental deletion will replicate across the domain or forests with no undelete capability. To mitigate against this, many enterprises end up restoring 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. Further, the auditing capabilities and security delegation controls are not robust. For example, the capability to determine which administrator made a particular change is either difficult or impossible, which further complicates the troubleshooting and error resolution processes.

Challenge 2: Active Directory Replication Problems

The replication of DNS changes across Windows DNS servers can take just seconds to nearly an hour. In the latter case, this results in inconsistent data across the enterprise until the replication completes. For example, DNS servers that are located close to each other may get quick updates, but those that might be located across the globe may not replicate for hours. 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 DNS servers across business units and geographic regions. Microsoft DNS 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. Having various administrators with full access who can make changes to the system without the necessary controls in place not only adds to the security risk but results in complexity and potential errors that are replicated across the domain or forest (as described in Challenge 1 above). When changes are made, there is very little audit trail available and any available information often gets lost quickly as local audit logs rollover and cannot be centralized natively.

"We initially chose BlueCat to avoid the 'worst case,' a costly DNS or DHCP outage that would cripple our network, delay our production and put our business at risk. BlueCat is also saving us administration time and effort. With our previous Microsoft solution, there was more work for our staff to do each week to administer the DHCP service. "

Markus Vetter,

System Administrator, Tyrolit

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. As a result, most Active Directory administrators do not use this function due to fear of removing valid DNS records and causing a service outage. This then results in 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.

Challenge 6: Security

DNS security is often overlooked for private networks because an internal network is seen as secure and separate from the outside world. The real problem lies with the sheer volume of exploits in the Windows operating system that plague network administrators. Worm viruses can unload payloads that attack internal systems and replicate while bringing a network to its knees. For example, the SQL Slammer work that exploited a known vulnerability in the Microsoft Data Engine (MSDE) attacked available root servers by generating bogus queries. These queries resulted in a large number of ICMP packets being sent out which eventually caused some of the root servers to be offline. Many organizations also discovered that their own internal DNS servers were being attacked in a similar manner.

BlueCat supports a wide variety of interoperability scenarios with Active Directory using GSS-TSIG and provides more granular update security policies than Microsoft DNS can support natively. With BlueCat, you can be sure of superior performance delivery, less complexity and elimination of human-errors through robust validation. As well, BlueCat adds significant security capabilities that are not found in Microsoft DNS.

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

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

CLICK HERE TO LEARN MORE ABOUT DNS AND DHCP BEST PRACTICES

References:
1. Carver, Bob. "Linux to Windows Migration." Configuring BIND to Support Active Directory Services. https://technet.microsoft.com/en us/library/dd316373.aspx
2. "Interoperability Issues." Domain Name System (DNS). https://technet.microsoft.com/en-us/library/cc755717.aspx
3. What are Domains and Forests? https://technet.microsoft.com/en-us/library/cc759073(v=ws.10).aspx