Whether it’s the Internet at large or your directory services based network, DNS is the glue that holds it all together.

Organizations demand the best solution for their external DNS that lie exposed to Internet attacks. This can mean using non-Microsoft DNS.

This whitepaper takes you through the features of Microsoft and non-Microsoft DNS, making the case for a non-Microsoft DNS setup.
Executive Summary and Introduction

Whether it’s the Internet at large or your directory services based network, DNS is the glue that holds it all together. A simple DNS failure can translate into a business failure as well. If DNS isn’t working right, computers simply cannot talk with one another, leading to a “business blackout” until the problem is rectified.

It’s probable that you use a non-Microsoft solution for your external DNS service. If so, you aren’t alone. When it comes to choosing a DNS for use with Active Directory, most administrators simply pick “what’s in the box from Microsoft.”

But it doesn’t have to be that way, and indeed, there are incentives to utilizing non-Microsoft DNS, from a security and feature perspective.

- **Security:** Organizations demand the best solution for their external DNS that lie exposed to Internet attacks. Third-party DNS solutions are available which are designed and built from the ground up with security in mind. An organization’s internal DNS structure is equally open to malicious threats, malware, phishing and data exfiltration.

- **Visibility and Single view:** Most organizations have a heterogeneous mix of technologies and accurate, one-stop visibility is quintessential to efficient compliance and control.

- **Operational Efficiency:** Optimizing OPEX costs by utilizing automation and workflow vs manual spreadsheet management.

- **Intelligent Services:** Integrated DNS-based traffic control, network load balancing and service monitoring add great value to an organization.

In this whitepaper, you will learn about using non-Microsoft DNS with Microsoft Active Directory.

This paper includes customer stories where non-Microsoft DNS is used, where you can see how customers like yourself have increased their security and ability to manage DNS with non-Microsoft DNS.

This paper is for IT Managers and IT Pros and/or anyone who uses Microsoft Active Directory.
Must I use Microsoft’s in-box DNS?

In the case of your typical Windows domain network, it is “traditional wisdom” that only Microsoft DNS must be used with Active Directory for internal DNS resolution. Many times this is because:

- It’s convenient to use the in-box solution
- The MYTH that Active Directory requires Microsoft DNS to function properly
- Others are doing Active Directory-integrated DNS, and therefore that way must be the only way to do it.

However, these myths simply aren’t true. In fact, Microsoft even published a KB article dispelling this myth many years ago. The key point is iterated multiple times in multiple ways amongst Microsoft’s documentation surrounding Active Directory and DNS. This can be found in the full Microsoft Technet article here: https://technet.microsoft.com/en-us/library/cc755717(v=ws.10).aspx

Although the [Microsoft] DNS Server service is recommended to support Active Directory, you can use other DNS server implementations for this purpose.

Note that this article refers to BIND (Berkeley Internet Domain Name) type servers. But to be clear and specific, as the quote states you can use other DNS servers with Active Directory, and they don’t need to be specifically BIND. The third-party DNS server you choose simply needs to support Active Directory and some rudimentary RFC standards governing DNS communication that most non-Microsoft DNS servers support.

Adobe had a non-Microsoft BIND product long before I got here, before we migrated to yet another non-Microsoft DNS product.
- Brent Hetherwick Adobe. Technical Lead for DHCP, DNS and IPAM (DDI).

Other articles which clearly reference Active Directory interoperability with non-Microsoft DNS servers are:

Another place you can see that Microsoft-specific DNS is optional is in the Domain Controller promotion process. If you are creating an AD Forest for the first time, the wizard does not require you to select DNS. Notice how the wizard will allow you to continue with the DC promotion process despite not choosing to install the Microsoft built-in DNS server component as is shown in the screenshot below.

![Domain Controller Options](image)

There are some advantages of utilizing Active Directory-Integrated DNS for your DNS zone besides the mere convenience of the in-box wizard. The primary benefits are:

- Active Directory replication will take care of DNS zone replication automatically
- All DNS servers are writable

This reduces the necessity to configure and allot for separate DNS zone transfer traffic. Other benefits include secure updates and DHCP integration but these features are available in third-party solutions as well.

The fact is that Active Directory-Integrated DNS is an option but not required. In fact, even if you are currently utilizing Active Directory-Integrated DNS, Microsoft gives you the option to either add a secondary DNS or change the structure to one of the traditional DNS zone types as is shown in the screenshot below:
This built in feature is so that Windows DNS can integrate with an alternative non-Microsoft DNS server. Therefore, you can configure:

1. All of your DNS servers configured with Active Directory-Integrated zones
2. All of your DNS servers configured with a traditional primary/secondary zones
3. A hybrid of both Active Directory-Integrated zones and secondary zones

“We are not a part of the Microsoft Active Directory team, so when another team implemented Active Directory, we worked together. During the process, we never had any pressure from their end to utilize Microsoft DNS.
- Brent Hetherwick, Adobe. Technical Lead for DHCP, DNS and IPAM (DDI).
The case for non-Microsoft DNS

Active Directory administrators naturally want Active Directory to perform at its highest capabilities. The key activities that Active Directory and its domain controllers should be performing are:

- Authentication
- Authorization and
- Accounting (Logging)

Everything else that Active Directory and its DC are tasked with doing will take away from these critical aspects. By integrating DNS into your DCs, you are giving it a task which would necessarily take away from these critical activities.

Additionally, your DNS servers should be especially protected and especially secure. In the case of an attack on DNS, like a DDOS (Distributed Denial of Service) attack (akin to SQL Slammer and attacks like those, but expressly for DNS), a Microsoft Active Directory-integrated DNS could have issues; since it would be tasked with the DNS and the critical activities described above. Additionally, a flaw in DNS could have unintended repercussions for Active Directory if properly exploited. For instance, a recent Security Update (3164065) was specifically crafted to shore up a hole for Microsoft Windows DNS server. As noted in the security update:

*The vulnerability could allow remote code execution if an attacker sends specially crafted requests to a DNS server.*

Additional problems could occur in a blended Windows and Linux environment when using Active Directory-integrated DNS. The specific issue occurs when a Linux machine properly updates DNS but Active Directory DNS Scavenging is turned on. The problem occurs when Linux updates Microsoft DNS, but doesn’t continue to make DNS updates. This isn’t an intrinsic problem with Linux: The DNS protocol has no imperative for Linux to keep DNS updated. And in those situations, with Active Directory-integrated DNS and Active Directory DNS Scavenging turned on, those records could be unexpectedly eliminated. In the older Microsoft article entitled “Cumulative list of reasons that DNS records disappear from DNS zones” ([https://support.microsoft.com/en-us/kb/2985877](https://support.microsoft.com/en-us/kb/2985877)) the number one reason is listed as:

<table>
<thead>
<tr>
<th>Cause</th>
<th>Issue</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DNS Scavenging is misconfigured.</td>
<td>The Scavenging feature on one or more DNS Servers was configured to have overly-aggressive settings and is prematurely deleting DNS records for Active Directory-Integrated DNS zones.</td>
</tr>
</tbody>
</table>
Incentives for Moving from Microsoft DNS to non-Microsoft DNS

So what is the incentive to not utilize the convenience of exclusively utilizing Microsoft DNS servers?

Below is a list of some of the value added features offered by third party DNS solutions available today:

1. Proactive automated adaptive behavior protection from DNS attacks, malware, and data exfiltration through customized DNS firewall security
2. Utilize DNS and DHCP features that are unavailable from Microsoft in-box solutions such as Identity Mapping (linking IP addresses to users)
3. Intelligently resolve queries and direct traffic according to geographic location
4. Increased logging to help determine where issues and attacks are originating
5. Utilizing a single solution for external and internal DNS (aka “Single View”).
6. Operating system agnostic way to manage DNS.
7. Increased security by reducing admin privilege usage.
8. Increased granularity for control of dynamic DNS updates via IP-based access-control, as opposed to the Microsoft’s 3-level approach of “none”, “secure only” (ie, AD-integrated clients (GSS-TSIG)), or “secure and insecure” (ie, anyone, no TSIG or IP-based authentication required)

Let’s see how some administrators managed the last few items on this list.

About Single View

If you combine your DNS into a “Single View” you get the best of both worlds. First, you get a one-stop shop.

“We had two DNS solutions in house, so it made sense to have a single solution which handled everything. Since we had Windows with multiple forests and trusts and Linux computers, it was a challenge to get a single view pane of everything in our environment.

- Andrew Stein, contractor for Department of Defense

Second, you get the benefit of the DNS server responding to the queries differently based on who is asking the question.
Agnostic DNS management

If you use a non-Microsoft DNS platform, it could work for all team members to be on even ground.

“We consolidated to a single platform with a single interface. No matter our IT team’s skillset or background, it’s still DNS: we didn’t need particular Windows expertise to use a 3rd party DNS solution. In fact, no particular OS experience was required at all; the tool is 100% browser based.
- Andrew Stein, contractor for Department of Defense

Reducing Privilege Use in Active Directory

If you use a non-Microsoft DNS platform, you could potentially remove some un-needed privileges.

“Security was increased because we could use different role based access, instead of using traditional windows roles. We could set up roles for granular changes instead of perhaps too many rights within Windows.
- Andrew Stein, contractor for Department of Defense
Conclusions and What’s Next

Microsoft has always conceded that any compliant DNS solution will work alongside Active Directory. In short, there is no imperative to use Microsoft DNS with Active Directory. And real Active Directory customers are working just fine with this configuration.

“We’ve been using non-Microsoft DNS for more than 5 years, and no need to call Microsoft for any Active Directory support, DNS or otherwise.
- Andrew Stein, contractor for Department of Defense

There have been no support calls to my knowledge for Active Directory regarding or involving anything with our non-Microsoft DNS.
- Brent Hetherwick Adobe. Technical Lead for DHCP, DNS and IPAM (DDI).

And getting started with non-Microsoft DNS doesn’t have to be hard. Like anything, it’s a process, but that process doesn’t have to be particularly difficult.

“Once we made the decision, the process was a very straightforward migration. We were able to move multiple authoritative zones over, one at a time as we made a transition. We started with Linux initially then lastly, we migrated all of the Windows zones over.
- Andrew Stein, contractor for Department of Defense

If you’re interested in non-Microsoft DNS because of some of the items you’ve read here today, then you should investigate the features and functions you need and start a trial.

It’s my hope you have a new perspective on where non-Microsoft DNS can help you out.
About the Author

Jeremy Moskowitz is one of less than a dozen Group Policy MVPs worldwide, is the most-published author on Group Policy, and a prolific Group Policy speaker worldwide. He’s also the founder of GPanswers.com and PolicyPak software.

Since becoming one of the world’s first MCSEs, he has performed Active Directory desktop implementations for some of the nation’s largest organizations.

His books and articles have been read by millions and translated into multiple languages. Jeremy has written for Windows IT Pro Magazine, REDMOND Magazine, Microsoft Technet Magazine, Inside Technology Training Magazine, PC Magazine, and Ziff-Davis' Windows Professional Journals, among others.

Jeremy has spoken at just about every existing Windows conference about Group Policy, including Microsoft TechEd, Microsoft Ignite, Microsoft Management Summit, WinConnections, and TechMentor.

Brad Rudisail is a technical specialist at GPanswers.com and PolicyPak software. He has been an MCSE since 1999 and has served as a network engineer and manager in both the financial and education fields. He has been a leader in K12 education technology and has spoken at the national K12 Technology Conference in Washington DC and has been quoted in magazines such as T.H.E. Journal and ESchool News. He was formerly a university instructor and continues to serve as an IT Trainer on a number of subjects. He is a professional blogger and syndicated columnist.