

Re: Restrict Dynamic Updates

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2008-05/msg00024.html>

- *From:* Robert Lindholm <RobertLindholm@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 2 May 2008 07:23:05 -0700
-

Ace:

Thanks for your continued assistance...

Is there a way to force the [WinXP] clients to update their A/PTR records directly with the AD/DNS server?

While I appreciate the win of using AD/DNS and AD/DHCP, it's not something I'm going to be able to implement in our environment.

If the clients do own the A/PTR records and can directly update AD/DNS, can the "stale" records be removed manually or by using scavenging?

I will definitely incorporate your recommendation of using a forward to the BIND/DNS server to minimize the exposure of the AD/DNS servers to the Internet.

Bob

--

Robert Lindholm
University of Rochester

"Ace Fekay [MVP]" wrote:

In <news:6DE7A001-E854-42D4-B274-58D828AABD6F@xxxxxxxxxxxxxxxxxx>,
Robert Lindholm <RobertLindholm@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> typed:

Ace:

Thanks for taking the time to respond with such a lengthy well intentioned reply...

I agree with your assessment that having internal AD/DNS servers/cleints exposed to the Internet is an inherently bad idea, but am in a position where I need to deploy AD in a timely a manner while doing it in as safe manner as possible given our environments

Re: Restrict Dynamic Updates

limitations.

For non-technical reasons, we currently don't have a perimeter firewall and won't have one in a time frame that coincides with the Active Directory deployment.

Our "internal" production network does use public IP addresses and this is not likely to change until we finally deploy a perimeter firewall.

A second complicating factor is that we have traditionally been a UNIX/Linux shop and almost all of of "server" services are hosted off of those platforms, including BIND DNS and DHCP for all of our Windows clients.

The only service we are currently hosting or will likely be hosting in the near future from the Windows platform is Windows authentication and any other necessary services required for AD.

Our production environment is extremely entrenched and I'm not going to be able to turn it "upside down" with the AD deployment, so I'm trying to integrate AD as best I can with our UNIX/Linux environment.

Initially, my thought was to leave the clients pointing to the BIND/DNS servers to resolve all non-AD queries and redirect them to the AD/DNS servers only for AD-specific queries, allowing the BIND servers to perform the majority of name resolution duties, but I may need to reconsider that strategy after reading the knowledge base articles[below], I'm going to try redirecting the clients to the AD/DNS servers to see how well that works.

However, I would still like to find a way to minimize exposure to the AD/DNS servers, while providing the AD clients access to needed AD resources and continuing to let the BIND/DNS servers act as our ISP/external DNS servers.

There may be a possibility of implementing a small dedicated AD server firewall, which would limit external exposure to our servers [at least]... while this isn't an optimal solution, this is probably better than our current situation.

One question I still have is what records are AD hosts [typically] updating with AD/DNS besides A/PTR records and what records do they need access to for AD authentication?

I realize in a more mainstream/native Windows AD environment, servers/clients may be offering a variety of Windows-based services, but we have not traditionally done that here, nor are we likely to in the near future.

Unfortunately, we cannot fully utilize the many benefits of AD right

Re: Restrict Dynamic Updates

now, even though we have a large/complex enough Windows client install base that dictates we utilize a domain oriented environment for administrative efficiencies.

My plan is to deploy a basic AD for now, but in a way that will allow for future development once we have some of the much needed security features in place.

Any further suggestions/comments would be greatly appreciated...

Bob

Hi Bob,

Sounds like you do have a fully entrenched Unix/Linux based system. I can understand the difficulty of moving such an embedded system.

The clients will register A/PTR records. Normally a client will register it's A record and Windows DHCP will register it's PTR. I usually like to force Windows DHCP to register both as well as force DHCP to 'own' both records. Advantage is when a client gets a different IP, Windows DHCP can update it instead of creating an additional record leaving the old one sit hence causing issues.

As far as DCs, this is a whole different issue. Besides the A/PTR records, they also register SRV records. BIND does support this, however, in many designs using BIND, there are certain disadvantages. BIND supports secure updates using TSIG, however Windows doesn't understand that. Windows DNS using AD Integrated zones, supports secured updates, meaning the client MUST authenticate to allow it to update. This is also an advantage using Windows DHCP and Windows DNS. The APIs work hand in hand as well as with secured updates. BIND and Unix DHCP does not offer this support for a Windows environment.

Your best bet is to use Windows DHCP and DNS. This would be an easier change over than completely changing the IP scheme to a private scheme at this time. Have all Windows and other machines ONLY use the Windows DNS server. This includes other Unix and Linux machines. Only have them use the AD DNS servers for their DNS address. At least for the Windows machines, this is very important, especially in light of the way the resolver service works, as you've read, to allow them to "find" domain resources and services. Having the other machines point to them gives you a common central location to create and manage internal host data in DNS.

To gain the advantage of Windows DNS Secured Updates, DNS must run on a DC. Secured Updates feature is only available when the zone is AD Integrated, and AD integrated zones are only available on a DC. The advantage of AD integrated zones, is the zone data is stored in the actual AD database, and NOT as a text file such as what a BIND server does, further securing the data.

Re: Restrict Dynamic Updates

Once you've setup DNS even before you setup a DC, configure a forwarder on the DC's DNS server to your BIND server. This will be your base DNS infrastructure design. This way BIND will take care of internet resolution for the AD DNS servers and completely masks and hides the AD DNS servers because they will NOT be exposed to the internet whatsoever. To further protect the BIND servers, forward them to your ISP's DNS server.

I hope this helps.

Ace