

Re: Creating a new Zone in DNS

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2008-06/msg00158.html>

- *From:* "Cyborg" <apollo13@xxxxxxxxxxxxxxxx>
 - *Date:* Thu, 12 Jun 2008 13:57:39 +0100
-

I think I understand, I don't need the resolution for the entire domain just one or two, like ftp.domain.co.uk or mail.domain.co.uk. I created a new primary zone called mail.cbsoutdoor.co.uk but can you tell me what the next step is as the only record under this is (same as parent folder), name server and the DNS server name. How can I add the private IP?

Thanks

"Herb Martin" <news@xxxxxxxxxxxxxxxx> wrote in message
news:eSGkFZHziHA.1772@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hi, we only have one forward lookup zone for our Active Directory domain, it's all Windows 2003 Native. Now we have many web servers on our DMZ (on our Cisco firewall) that external customers get to. They use addresses like ftp.domain.co.uk and webmail.domain.co.uk etc but my internal users can't get to these as the domain names resolve to external IP's on the firewall.

What do I need to do then? I only have one zone in DNS which is a different Domain name to this external one we use. Do I need to create a new primary zone?

Then how do you have a problem? If your internal servers are NOT holding the zone for the external servers, then you EITHER forward to the ISP or do recursion on the Internet and you will automatically get the same entries the rest of the world will get.

If you want to hold that zone to give out different IPs (private ones) to internal clients then you can do that if you provide ALL of the resolution for that external zone.

IF you wish to provide resolution that is different for just a few (or

Re: Creating a new Zone in DNS

many) of those external zone/domain names then you must create a DNS "zone" for EACH such INDIVIDUAL SERVER (that's right a ZONE PER SERVER) and add the "empty", "blank" or "Same as parent" entry with the correct IP.

This zone per server idea overrides JUST that server domain (now a zone) name and thus eliminates its lookup but ONLY that particular servers lookup, from the external or other DNS.

"Herb Martin" <news@xxxxxxxxxxxxxxxx> wrote in message
news:OgN0RMGzIHA.4040@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

"Cyborg" <apollo13@xxxxxxxxxxxxxxxx> wrote in message
news:234C796B-1CAD-47E7-ACBC-1087FB72742C@xxxxxxxxxxxxxxxxxxxx

Hi, we only have one forward lookup zone for our Active Directory domain, it's all Windows 2003 Native. Now we have many web servers on our DMZ (on our Cisco firewall) that external customers get to. They use addresses like ftp.domain.co.uk and webmail.domain.co.uk etc but my internal users can't get to these as the domain names resolve to external IP's on the firewall.

If you use the same Domain names (not addresses) internally and externally for your zones then YOU must manually add the external record names and address to your internal zone.

Such is termed "Shadow DNS".

My internal users however can get to these my using the private IP address of these server, so I thought is it possible to create a new zone called doamin.co.uk and then create ftp.domain.co.uk etc to point to the private IP address, so everyone is use the same FQDN?

Nice thing is when you do that extra manual work you can choose to give internal users the internal or the external address for them, as appropriate.

Re: Creating a new Zone in DNS