

Re: Should DC's with DNS point to self first?

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-02/msg01663

- *From:* "Joe Richards [MVP]" <humorexpress@xxxxxxxxxxxx>
 - *Date:* Mon, 19 Feb 2007 12:42:00 -0500
-

- > IMO: No. There's no reason (in common scenario) to use other
- > DNS server
- > when you have all locally, by doing so IMO you're wasting server
- > resources and network traffic just for fun (Bad configuration)

We are going in circles here, but no, this is not a bad configuration. It is just something you apparently don't like.

- > Again, the shutdown/restart reason stated before is definitely not a
- > good reason to do so IMO.

Since it isn't bad to do so, any reason to do so is fine if that is what the Admin decides.

- > The poster didn't stated anything about replication issues
- > or something
- > like that, if it was that would be a different story.

It wasn't a topic at all, you can't assume it is fine or not. My stating that replication issues is A reason to do it, not the only reason to do it is just that, giving but a single reason why someone would definitely want to lean that way. Again, there are far more issues associated with pointing a DC at itself for primary DNS than pointing at something else. It tends to work fine much of the time, but that isn't a reason to say that is the best or only way to do it which you seem adamant in doing.

- > The story would be the same, it doesn't matter,
- > if no specific scenario IMO the DNS should always point to itself
- > otherwise it's just a waste of resources.

Yes this is your opinion, and again, I absolutely do not agree with it. DCs should sometimes point at themselves for primary, sometimes point at other DNS servers for primary. It depends.

- > Note: I never said that the DCs never do reboots, but the
- > purpose should be that one.

Why? Reboots are not inherently bad. In the last 11 or so years I have run Windows servers that reboot weekly due to corporate policy and others on protected secure networks that rebooted once per year during required data center shutdowns. I have worked on UNIX boxes with the same rules. In fact, one very large

Re: Should DC's with DNS point to self first?

multinational I know actually rebooted UNIX servers more often than Windows Servers because the UNIX support management made the decisions separate from the Windows support management. No reboots might be a goal for some but again, there is nothing inherently bad in a reboot.

Domain Controllers and the domain structure is specifically designed to be as non-intrusive during reboots as possible. This is why there is such an intense domain resource location capability and clients have such great failover capability. Machines going down is a fact of life until such a time that they can supply their own power and guarantee connectivity beyond anything else can impact. Failure to plan for that is very shortsighted.

Every design or environment I work on I always think in the direction of how do things work if a given DC is unavailable for whatever reason up to and including having to reboot hourly for some issue. This enforces the idea of building for transparent fail-over which is something you really want to do.

Regardless, this has little to do with a company with three DCs other than the fact that it is even more unlikely that such a small company will have protected datacenters and redundant power generators to maintain a server through external issues so reboots are fact of life.

- > If the DS team laughs quite a while, they are laughing from
- > them selves, and the mess that they do in the developed systems
- > provided by them. IMO
- > a STABLE system SHOULD be set to never be rebooted. Of course
- > unfortunately that's not the case, so they can continue to laugh of
- > yheir own products.

This is a shortsighted and uninformed comment. Any system now running, will be rebooted. I don't care what OS or RTS it is running. Failure to plan for and design for that is silly – even in the mainframe world which truly are the most stable machines out there and I built systems like that as well and interestingly that is where serious clustering started getting built which is an acknowledgment that systems do indeed reboot and become unavailable.

Believing that good systems won't be rebooted is even more silly. What the DS team has put together is one of the more fault tolerant environments available for authentication/authorization. As an example, when the NE portion of the United States had its power failure, my group, the AD Admins, was the only group not scrambling trying to get resources working. Everyone who could get on the network could log on to the North America domains even though 80% of the DCs of one NA domain and 60% of the DCs of the other NA domain were without power. These machines being down was no fault of the machines, completely external. But since no one involved believed that a DC should never be rebooted, the design accounted for that and everything worked.

joe

Joe Richards Microsoft MVP Windows Server Directory Services
Author of O'Reilly Active Directory Third Edition
www.joeware.net

---O'Reilly Active Directory Third Edition now available---

Re: Should DC's with DNS point to self first?

Re: Should DC's with DNS point to self first?

<http://www.joeware.net/win/ad3e.htm>

Jorge Silva wrote:

Hi again Joe

There are good reasons to use itself. Regardless, a DC DOES NOT have to point at itself for primary.

It's not mandatory to do so. But a good practice. If you've problems then that's another situation, but the poster is asking for where should the DNS pointing to (IMO: to itself). And the shutdown/restart reason stated before is definitely not a good reason to do so IMO.

Several reasons, DCs aren't the only machines that need to use DNS.

Agree. But Gonzo has DNS on his 3 servers, so that's why I said if you don't plan to use it why install.

However DCs are some of the worst impacted when DNS is not functioning properly.

Agree, never said something that would suggest otherwise.

Maybe DNS is installed just to increase the number of DNS servers to handle all of the clients but you still want DCs to still use a specific set of DNS servers. This was also a common config with WINS.

Agree.

While this may not be required in the OP's specific case, it certainly is an option and you shouldn't outright say it MUST be configured in a specific way.

Again, the shutdown/restart reason stated before is definitely not a good reason to do so IMO.

The OP should be fine doing it EITHER way.

IMO: No. There's no reason (in common scenario) to use other DNS server when you have all locally, by doing so IMO you're wasting server resources and network traffic just for fun (Bad configuration)

however if the OP has experienced replication issues, I would be quicker to point him to NOT pointing the DC at itself for DNS. I fix screwed up and

Re: Should DC's with DNS point to self first?

underperforming AD deployments for a living, far more instances have been cases where I ran into issues due to DCs pointing at themselves than pointing at other DNS servers.

The poster didn't stated anything about replication issues or something like that, if it was that would be a different story.

BTW: And if the server that he was pointing had missing DNS records or bad DNS replication.... The story would be the same, it doesn't matter, if no specific scenario IMO the DNS should always point to itself otherwise it's just a waste of resources.

This was in regards to the comment of "DCs weren't made to be rebooted" which is absolutely incorrect. If you read it somewhere, I need to get it corrected. If you came up with it on your own, you should probably refrain from such guesses. If you presented that comment to anyone on the DS team they would probably laugh quite a while.

Note: I never said that the DCs never do reboots, but the purpose should be that one. If the DS team laughs quite a while, they are laughing from them selves, and the mess that they do in the developed systems provided by them. IMO a STABLE system SHOULD be set to never be rebooted. Of course unfortunately that's not the case, so they can continue to laugh of yheir own products.

Again, your opinion, again I don't agree with it. Even the best practice documentation doesn't state it this strongly, it presents several options including pointing at self, pointing at another DNS server, and a combination strategy. None of them are listed as incorrect and none of them are incorrect. It depends entirely on the configuration and DESIRES of the administrators.

Again, in this scenario, i don't think of any reason to do otherwise. You don't win nothing at all, you just loose. (in this scenario of course).