

Re: providing backup for other domains

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2006-12/msg00457.html>

- *From:* steve@xxxxxxxxxxxxxxxx <stevemcmillaninccom@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 22 Dec 2006 06:34:00 -0800
-

Ace,

Thank you so much.

I did open tcp & udp 53 on the routers. I also set security in DNS to allow zone transfers and, it all seems to be working.

I appreciate the thorough response!

Steve

"Ace Fekay [MVP]" wrote:

In news:468F8C78-3362-439D-94EC-2CA40835E546@xxxxxxxxxxxxxxxx, steve@xxxxxxxxxxxxxxxx <stevemcmillaninccom@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> stated, which I commented on below:

We are a consulting firm who helps small to medium businesses set up Windows 2003 servers. Most have a local domain name with 10 to 50 workstations. Some have small business server running and some just have a single server running DNS, AD, print services, file services.

Because they only have a single server, im looking at finding ways to make some things redundant, including DNS.

My question is, in my office, on my Windows AD server that is running DNS, can i create a DNS Zone or Domain that is a replica of one of the other businesses zone?

If you mean of one of your clients for a backup, yes. But it will be a secondary zone of the client's zone. You will have to also allow the appropriate ports from the clients' firewalls to your firewall to allow access for zone transfers (TCP & UDP 53).

If the source zone, say it is on another DC that belongs to a totally different forest/domain, yes as well,. You can do the same with zone

Re: providing backup for other domains

transfers.

Your machine can also host the zone for any domain that is not in it's forest too, but it won't be able to reap the features of AD Integrated zones.

When updates occur, will my replica zone be updated?

With zone transfers, yes, sort of. It just copies over changes using IXFR (incremental zone transfer), from the Master (the Primary zone, or the source) to your copy of the zone (the Secondary zone).

Or...is Windows DNS not a full fledged fully functional DNS server?

Yes, it SURE IS, and much much more. It's a full RFC compliant DNS service with additional features.

Can I also have a replica of a Zone from a Unix run DNS server that is an authoritative name server for some xyz.com zone?

YEP. See above about Primary/Secondary zones.

Thanks for the help.

Steve

You are welcome.

Zone transfers allow you to put a read only copy (Secondary zone) elsewhere from a read/write copy (Primary zone). Primary and Secondary zones store their data as text files. On a Windows machine, the files can be found in the \system32\dns folder with a file name such as "domain.com.dns". You can have numerous read only copies, but there can only be one read/write of that zone.

And also keep in mind, the authoritative DNS server listed in the registrar say for a public domain zone) does not have to be a Primary, it's just the nameserver listed as authoritative. It can get it;s data from a Primary that is not listed, hence protected from public view.

AD Integrated zones are similar to Primary zones, however their data is

Re: providing backup for other domains

stored as binary data in the actual AD database and not as a text file. The specific place in the AD database depends on the type of operating system and replication scope and would take a deeper understanding of AD to explain.

Additional security of AD integrated zones, is one of the numerous additional feature of AD integrated zones, as well as the fact that there can be more than one Primary zone copy of it. This is because all DNS servers that host the zone in a domain or forest has the ability to be a writable copies and becomes the actual "start of authority" (SOA) of that zone when that occurs. That is why you can watch the SOA name on AD integrated zones change. The data is replicated automatically as part of the AD replication process because it is stored in the AD database. If you install DNS on another DC, the zone data will *automatically* appear because DNS will recognize the data in the AD database. AD integrated zones can also act as a Primary zone for secondaries, whether they are on Windows machines, BIND (on Unix) or any other name brand.

Remember, AD integrated zones still follow the RFCs, but have more features.

Learn Active Directory Design and Administration in 15 Minutes a Week:

Microsoft DNS – Part 3

<http://www.serverwatch.com/tutorials/article.php/2226201>

Understanding zones and zone transfer

<http://technet2.microsoft.com/WindowsServer/en/Library/940cdf9b-8e43-4b08-9a53-9fc2152644031033.ms>

--

Ace

Innovative IT Concepts, Inc (IITCI)

Willow Grove, PA

This posting is provided "AS-IS" with no warranties or guarantees and confers no rights.

Ace Fekay, MCSE 2003 & 2000, MCSA 2003 & 2000, MCSE+I, MCT, MVP

Microsoft MVP – Directory Services

Microsoft Certified Trainer

Having difficulty reading or finding responses to your post?

Instead of the website you're using, I suggest to use OEx (Outlook Express or any other newsreader), and configure a news account, pointing to news.microsoft.com. This is a direct link to the Microsoft Public Newsgroups. It is FREE and requires NO ISP's Usenet account. OEx allows you to easily find, track threads, cross-post, sort by date, poster's name, watched threads or subject.

It's easy:

How to Configure OEx for Internet News

<http://support.microsoft.com/?id=171164>

Re: providing backup for other domains

Infinite Diversities in Infinite Combinations
Assimilation Imminent. Resistance is Futile
"Very funny Scotty. Now, beam down my clothes."

The only constant in life is change...