

Re: replication between sites

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2009-04/msg00387

- *From:* Garry Starck – MCITP <vjsparx@xx>
 - *Date:* Wed, 8 Apr 2009 19:20:01 -0700
-

Yes, implement Change Notification, then site boundaries are there for the localisation purposes of apps, etc, but the scheduled repl in AD Sites and Services is ignored. Try to remember to not perform bulk changes during hours, like changing everyone's phone number etc or deleting DLT objects, I have however never looked to see if FRS maintains repl from AD settings and therefore replicates SYSVOL changes as to the set schedule, or if it still follows the AD Notify Based Updates.

You know that MS BestPractice is to not snag SYSVOL with files larger than 10MB, but FRS 2003 unlike AD 2000 will keep on replicating a large file even if the replication window closes, therefore not causing the same file to try in an endless loop

FYI: Have you tried this at all, simple fast and faultless and much faster dcpromo's in remote regions
<http://support.microsoft.com/kb/813338>

—
Garry Starck
MCITP, MCTS AD, MCSE 2003 Messaging, MCDBA

"Gabor" wrote:

Thanks for both your and Marcin's response. I believe it would make sense to go into a bit more details.
I understand what you wrote below about the way replication works. I think I want to bend it a little.

I have an application which provides data updates to another application. The ideal location for this data would be a TXT record in a DNS zone, for several reasons not detailed here. I want this application to be able to dynamically update this DNS record. Therefore, as I want to do it securely, I must go with a directory integrated zone. I have this zone, it's working well.
Up to this point everything is cool and everything is done.

At the same time, I have 3 distinct sites in 3 separate locations in the

Re: replication between sites

directory. The bandwidth between them is, let's say, enormous. The amount of changes in this txt record is minor. Therefore, I am certain my domain controllers could handle even hundreds of updates per second.

My problem is that if I do an update to this DNS zone on one domain controller, it takes several minutes to propagate that change to the domain controllers at the other sites.

Do you guys see any way to achieve a fast update of this integrated DNS zone across the sites?

I do know that I could go with non directory integrated DNS but then I lose ability to do dynamic updates which is a must.

Any suggestions?

Thanks again
Gabor

"Garry Starck – MCITP" <vjspax@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:B9F55630-421E-44F8-BAED-F2AE267ABF78@xxxxxxxxxxxxxxxxxxxx

Hi Gabor

Configure site link replication availability ---
<http://technet.microsoft.com/en-us/library/cc779337.aspx> and then
Set Ignore replication schedules ----
<http://technet.microsoft.com/en-us/library/cc778048.aspx>

15 Minutes is minimum, and the 15 mins is a cycle. It waits 15mins and then updates, then the clock resets to another 15, so If admin created an account at 10H00 and the last replication occurred at 09H46, this account will replicate to the outbound replication partner (bridgehead) which then updates all other DC's within its site 15sec's + 3 for all site-local DC's. Every DC in the forest cycle at different times, so AD is not consistently updating during the 15 min's, just at the turn of the clock.

Now remember, If you have 4 sites, 1 but, 2 branch offices and one satellite branch that has a WAN connection hanging off one of the branch offices, then then MAX repl cycle can be 30mins provided the cycle repl partners are unluckily timed, the upside to this is that an indirect sites may all cycle with the upper tier office just after that office has replicated at with the hub site, only seconds to effectively converge (complete) the object addition/mod/deletion/update.

Re: replication between sites

If you really need to ensure immediate update of other sites, use a feature manually modified on DC's to ignore site link replication schedules and repl windows.

Try typing in repadmin /replsum and look at the elapsed times since each dc replicated and you will get a clear understanding.

Also, Are your DNS zones supporting each to the domains in the forest set to replicate via AD, and if so which of the 3 options is selected. I like each domain to replicate is DNS ZONE via the DNS servers in the domain only, stored in the NC=DomainDNSZones,CHILDDOM.EXAMPLEDOMAIN.LOCAL (AD Partition) which all DC's in the CHILDDOM.EXAMPLEDOMAIN.LOCAL domain replicate. I then setup DNS delegation for every child domain if they exist (Remembering the critical glue record entries to in effect reverse down to the child DC's IP address for that domains specific records. Remember the DNS servers will cache the records so does not generate a blip on the network monitors. Set DNS Forwarders upward through the hierarchy from lowest domain up to the SCHEMA/ROOT Domain DNS Servers.

THE _msdcs.exampledomain.local zone should be replicated forest wide and this usually has minimal update, stored in the NC=ForestDNSZones,EXAMPLEDOMAIN.LOCAL (AD Partition) which all DC's forestwide replicate this NC

Also set DNS scavenging, whilst doing this, evaluate your lease periods in DHCP scopes and then set the No-Refresh interval calculated to the DHCP scopes lease duration. The No refresh Interval under the properties of each zone stops unnecessary frequent client record updates. You can also set a GPO to set all DC's to register DNS every 24 hours (Default is hourly (stand to be corrected), but lockdown the Forest/Domain related zones security to such an extent that not even individual domain admins can edit, or delete records. The DNS refresh interval is when an existing record becomes enabled to itself a record update, which will either be new timestamp updates to negotiation from DHCP, or IP address changes. If during the Refresh Interval, no update is made, that record becomes scavengable.

Re: replication between sites

TTL values are to advise any DNS server that has cache a record, when to drop it out of cache. It's has nothing to do with replication speed.

remember

that the forwarding hierarchy thought the forest should if forward orderly moving to the root, I understand now that you may want to change the

target

hosts DNS record

in a hurry, then you should set the TLL/expirey to suit the criteria.

You could also creat stubzones, weigh up your differences/needs, if this zone if say for an important portal than changes physical location often

or

you want to be able to in them event of an issue,

In Short, Intra-site based repl takes +- 15 sec's till originating DC

pushes

the change, + 15 sec's extra per DC per at site locally. The Bridge Head

in

AD 2K3 are usually auto-selected via info from each sites ISTG (Intersite Topology Generator)/Kwnoledge Consistency Checker (auto assignend to a dc

local to each site that replicates it's sites data with IntER-site Repl

Partners (IE Bridgeheads). It is Best practice to leave the ISTG/KCC

running

and the BridgeHead set to auto selection for resilience.

Your AD is prefect replication at 15 min cycles, in fact, the more

consistent the convergence of objects updates the better. Password changes get secure channel immeadiate update from other DC's to the PDC emulator

to

ensure the password is very consistent. All DC's look against the PDC to

evauluate the password to check if their may be a new password

--

Garry Starck

MCITP, MCTS AD, MCSE 2003 Messaging, MCDBA

"Gabor" wrote:

I have fairly good bandwidth between 3 sites in 3 separate locations. the

current replication interval is 15 minutes, I checked this at the site

settings.

I believe these 15 minutes apply to DNS changes as well.

And it seems to

be

the case - when I change a record on one domain controller,

Re: replication between sites

I see the
serial
increase, etc just fine on the other DC in the same site, but
other sites
receive these updates several minutes later.
So I have a real business need to speed up DNS replication
and take it
down
to even a minute if possible.

Can I just lower that site replication interval to 1 minute? I
am fairly
certain my domain controllers and the bandwidth can handle
it, and I
would
obviously do it in steps – but so is this the right way to
approach the
DNS
replication? or is it enough to approach it the DNS way and
play with the
refresh/TTL values? we're talking about an integrated zone
of course, but
one that is actually not used by the directory itself.

thanks
Gabor