

# Re: GC Question

---

*Source:*

[http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active\\_directory/2006-04/msg00115.html](http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2006-04/msg00115.html)

---

- *From:* "GIG" <gig@xxxxxxxxxxxx>
  - *Date:* Mon, 10 Apr 2006 02:47:13 +0100
- 

Hello Herb

To confirm this i seted up the Following Scenario:

- 1 Site (1 subnet)
- 2 Domains
- 1 Dc in Each Domain (Both Run Windows 2003 Enterprise Edition)
- Domain01.root and Child.domain01.root
- The Domain01 has 1 Dc and is a GC
- The Child has 1 Dc and is not a GC
- The Domain and Forest Level are in 2003
- 1 WindowsXp Workstation (Workgroup-No Domain)

After creation of the 2 domains I disconnected both servers.  
Then i started up only the Dc for Child domain (isn't Gc)  
Then I started up the WindowsXP

1st Test

objective: (I read in a article that when no GC is available for a domain that isn't a Root Domain (First Domain to be Created) no one is able to logon on that domain including in the Domain Controller for that Domain, that article also states that in this type of situations only Domain Admins or Enterprise Admins of the Root Domain are able to logon on "lower" domains to be able to fix something or to make the "lower" domain controllers Global Catalogs.

Results:

– Well it looks that is not truth – I was Able to logon with Administrator Account.

Conclusion:

We're able to logon on dc even if no GCs are available, it doesn't matter if the account belongs to the top root domain or not.

2nd Test

objective: See if it's possible to add computers and users to a domain with no Dc available. Process: Add The computer account to the Domain, and create a User Account in the Child Domain with the Gc turned off.

## Re: GC Question

### Results:

- I was able to add the computer account to the Child Domain with no problems.
- When I try to create the user account "User01" I received the following message:

"Windows cannot verify that the user name is unique because the following error occurred while contacting the global catalog:

The server is not operational.

Windows will create this user account, but the user can logon only after the user name is verified to be unique. Make sure the global catalog is available."

After this message i was able to finish creating the user account.

(Personal note: this message seems strange to me because it stats that needs a Gc to verify if the User is UNIQUE??? Were in the Domain? In the Forest? – Well let us see – every domain Contains 4 Partitions:

Schema: Contains All objects and the Attrib that those objects can have – This Partion is common to all domains in the Forest.

Configuration: Contains Information about Logical Structure or replicationtopology – This Partion is common to all domains in the Forest.

Domain: Contains Information of all objects in a domain. This is domain especific and is replicate to every domain controller in that domain.

Application Stores dynamic data application–especific, except security principals (users, groups, computers). I'm not sure but I believe that is here were ForestDnsZone and DomainDnsZone are created... And I also read that when we create new App in this partition they can't be created in Gcs, i'm not sure if this is true....

Partial Replica Containing commonly used attributes for all directory objects in the forest (replicated between GCs Servers only)

Well the reason why that message sounds strange to me is that every Dc has Domain Partition (Full Replica) that Contains all the Objects For that Domain!!! – And I know that if I create a User Account Object Named "User01" in this Domain (Child), I can also Create a user account named "User01" in other domains because all objects have a Unique SID, and the Security ID consists of the domain security ID (That is the same for all security IDs created in the Domain) and a relative ID that is unique for each security ID created in the domain. Master Role Responsible for doing this is the RID

## Re: GC Question

master role server and this server olds that rule as any other rules (PDC and Infrastructure) for the Child domain .So according to this why the hell does the Dc needs the Gc. The Dc knows the SIDS, knows all Objects for his domain right? Well maybe not Please someone clarify me please.)<<<

- I restarted the WXP – Wkst, and I tried to logon with the User account "User01" Guess what ... I wasn't able to logon hehehe....
- But then I try to logon with Administrator Account for the Child Domain, and I was able to logon with no problems.

### Conclusion:

The Administrator account for the local domain can logon in any machine for that domain, including Dcs.

To create user accounts we need an available Gc. (I don't know understand why...)

### 3rd Test

objective: Turn On Both Dcs for both domains. Create User account named (User02) in child domain , and create User account (User02) in Domain01.(confirms the creation of two "equal" user account objects.

Turn Off all machines, Turn On only the Child Dc and The WXP machine, then try to logon with "User02" with no Gc available. If the User isn't able to logon then start up the Gc and try again.

### Results:

- I was able to create both user accounts "User02" one in each domain.
- I wasn't able to logon with the "User02" or with "User01", when i tried to do that i received the message:

"The system could not log you on. Make Sure your user name and domain are correct, then type your password again. Letters in passwords must be typed using the correct case."

(Personal note: This is a strange message isn't it? At the first time I believed that I was doing something wrong like typing the wrong password or wrong user name.... – Then i went to the dc and confirmed the user account and I reseted the password and tried again but with no success. But it seems a strange message any way because is telling me that I'm typing something wrong, and doesn't tell me that there isn't at least one valid server to process the logon. I understand that this message couldn't say something like No Gc available to process logon, because the

## Re: GC Question

users wouldn't understand that, but in the other hand telling the user that they are typing something wrong can lead bad understanding of the objective of the message in itself, and the users may try for some time retyping their passwords or user accounts, and this could lead for example to a account lockout if GPO has Security settings defined to lockout accounts, and, after the account has been locked out, then the user will call to the IT Depart. MS Should review this message, don't you agree???) (When I first posted the question on this news group, all my doubts has to do it with this kind of situation: In this case this user doesn't belong to any external group, he only belongs to the Domain Users Group, is this group considered an external group?? If no why a Gc is need – The Gc should only be need when a user from a different domain tries to logon on a domain controller that doesn't belong to his User Account Domain?? No? Well it seems not please someone explains that to me)<<<

– After I turned On the Gc, I was able to logon on the Child Domain.

### Conclusion:

- We can create User accounts with the same name in different domains.
- We can't logon with user accounts (not the administrator account for the domain) if no Gc is available

### 4th Test

Objective: When we try to logon using the format of: username@xxxxxxxxxxxx for example, the combobox for the available domains graysout, this tell us that the logon process doesn't use the information provided in that combobox that list all domains that exists in a forest. So in this case If we could create 2 "igual" user accounts named "User02" one in each domain, and if that user accounts are using the same Upn Suffix, how the domain controller knows which user of which doamin is trying to logon???

Create additional Upn Sufixes on ADDT. (Upn = test.com)

Change the User Account Upn suffix "User02" for the Domain01 to test.com = User02@xxxxxxx – Password = \*#DOMAIN01

Change the User Account Upn suffix "User02" for the CHILD to test.com =

Re: GC Question

User02@xxxxxxx – Password = \*#DOMAIN02

Results:

– Well when we try to change the second account to the same Upn has the first one, we can't and a message appears stating that: "The specified user logon name already exists in the enterprise. Specify a new one, either by changing the prefix or selecting a different suffix from the list."

Conclusion:

"Iqual" User Accounts in different domains always must have different Upn Suffixes.

I expect that some one could read this series of tests and answer to some questions in it.

Have a nice day, and thank you again for your time.

Regards.

---

"Herb Martin" <news@xxxxxxxxxxxxxx> wrote in message  
[news:u6kgI NCXGHA.2356@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:u6kgI NCXGHA.2356@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

"GIG" <gig@xxxxxxxxxxxxxx> wrote in message  
[news:uJMMtYAXGHA.2356@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:uJMMtYAXGHA.2356@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Hi Everyone

I know that is needed at least one GC per forest.

Better is at least one GC per Site. More for fault tolerance and in extreme situations more for performance.

The GC enables finding directory information regardless of which domain in the forest contains the data, and provides Universal Group Membership

Re: GC Question

Information.

Yes.

Applications also use the first (any object in the forest);  
Exchange is the prototypical example of this.

I read somewhere that a Gc is always needed to process the logons, and if no Gc was available then the users would only be allowed to logon locally.

Technically this is in Native(+) modes.

Now, if the Gc provides Universal Group Membership Information, and for example, the user that is trying to logon isn't member of any group outside of his domain and the domain controller for his domain is available but isn't a Gc and there isn't any Gc on the site were his in, and the wan link that connects to site were the Gc is in isn't available.

The only way to no the user is in no Universal Groups is to query the GC (if in native+ modes where Universal security groups are allowed.)

The user Can or can't logon?

Cannot logon in native+ modes.

And if there is only one domain? Why do I need a Gc?

Native mode effectively requires the GC and in a single Domain forest there is NO reason not to make every DC a GC.

In a single domain forest, every DC ALREADY holds ALL of the info so making a DC a GC costs practically nothing.

The above is also true in a SMALL forest with multiple domains.

As forest size increases the penalty for creating a GC (increase replication, increased storage) increases.

Re: GC Question

And if the user that I was talking about every time that he or she logs-on they must need a Gc all times ?

In Native+ modes.

I know that Xp caches logon Inf in cache, how long does the cache is enabled.

It's a long time (forever I think but I could easily be wrong about this)

I'm just trying to understand I do i need a Gc, for example if i have different Domains in one forest but the users only access to their domains and don't belong to other groups in other domains and they don't access to resources in other domains.

Yes.

Unless the forest is large there is no reason NOT to make (enough) GCs and if the forest is small or single domain it is entirely reasonable to make EVERY DC into a GC.

--

Herb Martin, MCSE, MVP  
Accelerated MCSE  
<http://www.LearnQuick.Com>  
[phone number on web site]

Tank you for your time