

Re: Please help refresh my memory on AD DC

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2008-11/msg00567

- *From:* Joe <Joe@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 12 Nov 2008 06:14:04 -0800
-

Hello Meinolf,

Thanks for your reply. I am getting very clear on this now.

"WEB308\administrator" does not longer exist, because DC's have no local administrator.

This is great I can now purge this from my thought process.

I have two scenarios that I am wondering how to tackle?

By saying that using local accounts would defeat the use of the Domain I can see why. The whole idea is to controll the environment PC and User.

So here is a question/Scenario
Using my Laptop as an example:

When I boot my Laptop I reach the Logon screen for XP Laptop and here I am presented with
Domain Logon or
This Computer

Ok the Local user for my Laptop is Joseph
However if i wanted to Logon to the domain I have to use the DC's administrator account. There is no other domain user at this time on the DC.

This presents an entirely new desktop on the XPLaptop. Which is normal.

So I guess I would need to create a Domain User for this Laptop NOT an admin account to be able to Login so I can control it from the DC. Is this correct?

Second Scenario:

Re: Please help refresh my memory on AD DC

A Server has websites already hosted on it in a Workgroup and now I join it to the domain. What happens to the permissions of the anonymous account (or any account) IUSR_MACHINNAME if I needed to add this permission on a folder for write permissions? Or similar situation?

Would I login to the DC and do it from there? If I can recall this is how I did a few years back.

Present FTP users would they change Logons?

That is all I think that narrows it to the core.
I deeply appreciate your time Mr. Weber

Thanks You,

Joseph

"Meinolf Weber" wrote:

Hello Joe,

"WEB308\administrator" does not longer exist, because DC's have no local administrator.

"However this does not mean that there is a user from that added machine in the domain users." Correct, they still are locally.

"It is just on the Domain network...?" The computer is now member of the domain, if you mean this and still has the local user account.

"in order to add the server or pc I would have to have a user on the domain to logon to the domain . This would be added by the Domain admin account on the DC." Correct

"1. logon Locally 2. Logon to the domain. To Logon locally I would use the admin account of the Server 2003 machine. To Logon to the domain I would use the AD DC Domain admin account to logon to the domain." Correct

"Unless there was a user specified for this server added to the Domain User accounts." No, do not longer use local users. In a domain only use domain user accounts. Over that accounts you have full control in Active directory users and computers. If you configure local users you have to control them allways on that special machine and you have to change passwords/settings/etc. allways on the machines. You kick out the advantage of a domain.

Best regards

Re: Please help refresh my memory on AD DC

Re: Please help refresh my memory on AD DC

Meinolf Weber

Disclaimer: This posting is provided "AS IS" with no warranties, and confers no rights.

** Please do NOT email, only reply to Newsgroups

** HELP us help YOU!!! http://www.blakjak.demon.co.uk/mul_crss.htm

Hello Mr. Weber,

Thanks for the update. That is some awesome info. Yes I have worked with AD before but not for a long time and not in a large environment. When I did work with it. It was when Server 2003 came out and I was using it on a small scale. Even then I was a little confused on the naming conventions. That is the reason I posted so I could get human intervention. I am very familiar with DNS as the 9 servers are a small hosting company. We have a few DNS servers serving zones for public sites –but not an AD DC setup. We are looking to host MS Dynamics CRM and this is feature requires AD.

You clarified a lot for me. Thank you very much!!.

I realize that the DC controls the entire network except that I will only be using one Master DC. I do think that you are correct I need to do a little more reading on the permissions sections as there is a domain user and then there is the local machine user.

Also when I promoted this Server 2008 box it did something that was not normal.

It made me change the password from the old

Let me explain. I had a saved Icon on my Desktop of my Laptop for WEB308 and it was set to RDP in automatically. Ok fine. When I did this I got the prompt for

WEB308\administrator

password

my old password did not work however as you mentioned since this is now a DC would the only logon be a Domain logon or would the option to logon locally still exist in this DC?

However after realizing out of the blue that the netbios was changed for me. I then approached the logon as such:

WE3080\administrator
old password

Re: Please help refresh my memory on AD DC

and it made me change the password Don't know why but I got passed that part.

I then saw the WEB3080 as an option to logon to with my Laptop so I am getting my memory back on this. Correct me please if I am wrong...

The Domain administrator has the rights to add a PC or workstation/server to the domain. However this does not mean that there is a user from that added machine in the domain users. It is just on the Domain network...?

in order to add the server or pc I would have to have a user on the domain to logon to the domain . This would be added by the Domain admin account on the DC.

Example: Server 2003 box as a user administrator and a password this is now a workstation. Then it is added to the Domain by the domain admin. When it is rebooted the newly added Server 2003 machine would have the option to either

1. logon Locally 2. Logon to the domain.

to Logon locally I would use the admin account of the Server 2003 machine.

to Logon to the domain I would use the AD DC Domain admin account to logon

to the domain. Unless there was a user specified for this server added to the

Domain User accounts.

Yes I will read up a bit on this.

Thanks for ALL you help!!

Joseph

"Meinolf Weber" wrote:

Hello Joe,

See inline.

Best regards

Meinolf Weber

Disclaimer: This posting is provided "AS IS" with no warranties, and

confers

no rights.

** Please do NOT email, only reply to Newsgroups

** HELP us help YOU!!!

Re: Please help refresh my memory on AD DC

http://www.blakjak.demon.co.uk/mul_crss.htm

Hello,

I am currently using a workgroup infrastructure with 9 servers and I am in need of changing it to a AD DC Domain infrastructure. However I am a little rusty in some areas. I have 4 Server 2003 Enterprise machines and 4 Server 2008 Standard machines. One Linux but that doesn't matter.

1. When I created the domain I used the same name as the server and this caused the installation wizard to change the NetBIOS name from WEB308 to WEB3080 The Original name for this server was web308.mydomainname.com and when I was asked for the FQDN I entered the same thing. This is what prompted the NetBIOS change as it told me to avoid conflict with the DC.

If you promote a server to Domain controller, there is no renaming of the computer. As you said you have to specify on the first install the full qualified domain name (FQDN) you like to use. In your case you choose web308.mydomain.com, after that it pops up with the Netbios name which you can choose your own, the suggestion is always a part from the FQDN in your case it uses "web3080".

2.Ok so when I rebooted the server and it rebooted as a DC I could no longer access the server by the old administrator password as it was as so Administratator

Re: Please help refresh my memory on AD DC

password1

I now had to change the password but not for
WEB308 it now was
WEB3080.

As said before the name of the computer is not changed during promotion to a DC. I assume you mean the logon window with USERNAME, PASSWORD and the "LOGON TO" which now shows only "web30380", the Netbios name of the domain, this is NOT longer the computer name as on a workgroup server. On a member server of a domain for example, you have two options under "LOGON TO", the "NetBios name" of the domain and the "computername(this computer)".

What I am struggling with is there are so many names that I am unsure which is the DC and which is just the NetBIOS.

On a domain controller you have ONLY the Netbios name displayed, in your case "web3080". You can NOT logon locally, like on a member server.

On a member machine, either server or client, you have "web3080" AND "computername(this computer)". With "web3080" you are able to logon to the domain with a domain user account and with "computername(this computer)" you have to use user account, created on the local machine.

I kinda figured that out as I tried to access old shares that still had WEB308 as the label . But when prompted I had to use the new WEB3080 and the new password for access.

See above the description about domain logon and local logon.

Re: Please help refresh my memory on AD DC

Part two:

Now I have always been confused about what SHOULD you use as a DC FQDN? I looked in the DNS of the DC and now the full computer name is web308.web308.mdomainname.com

This is correct, your servername is still "web308" as before and is now working/providing/serving for the domain "web308.mdomainname.com". The FQDN is now correctly "web308.web308.mdomainname.com"

The domain is specified as web308.mdomainname.com. So when joining the other servers and boxes the name that I should enter is this one correct?

If you join other machines to the domain, you can choose either the netbios domain name "web3080" or as you said the FQDN, both should work.

Now that the AD DC was created successfully I wanted to test the "joining ability" with my XP Pro Laptop. I used the network ID method on the myComputer Properties Computer Name Tab. Here is where I get lost.

Correct place for joining, here choose the CHANGE button and on the next window, you have the option domain and workgroup. Choose domain and enter either the netbios or FQDN.

Re: Please help refresh my memory on AD DC

I joined the domain successfully however I joined the domain using the administrator and password of the AD DC Server (which I understand is correct for the correct rights to add) and it successfully joined but it asked to add this user which was me on this XP Pro Laptop. My username and password for this Laptop. It failed when I said yes.

For joining to the domain you have to use an account that has the right to join computers to the domain, the Domain Administrator in your case is the correct one. A username/password from the local computer will not work, because this is local and not known from the domain.

I rebooted the XP Laptop and then when I went to join the domain it paused and looked for a list of domain controllers. It found WEB3080.

Don't know what you mean with "paused" but after reboot you have on the "LOGON TO" option NOT a domain controller to connect to, it is the domain where you have to connect to and this is shown with the netbios name of the domain "web3080", so this is complete correct. Additionally you have the option to logon locally to "computername(this computer)".

That confused me as I thought that the DC was now

Re: Please help refresh my memory on AD DC

web308.mydomainname.com

Correct, the DC is still having the computername "web308", but as said before, you do not logon to the domain controller, you logon to the domain and a domain can have multiple domain controllers which share one database that is stored on all DC's and updates itself automatically.

However I logged on as the administrator of the domain controller and that was it.

OK fine.

So the real questions lie in the user part of this. thanks for you patience.

When I go to add the other servers what do I add them as? Do I join the domain for the other servers with just the administrator of the DC?

As said above, it must be an account that has the right to join computers to the domain. The Administrator of the first installed domain controller is now shared on all domain controllers and different from the local administrator on member servers and workstations.

When you built a domain you have a domain administrator which is on all Domain controllers the same. That is different from member servers and workstations, they still have the local computer administrator.

Or do I create a user for each server and then log them on?

No, if you have a domain, you make it normally to use only domain

Re: Please help refresh my memory on AD DC

user accounts centralized managed from the domain controllers. There is no longer a need for local user accounts on servers or workstations.

Did you read about building a domain structure before? Do you have any experience with it? Anyway, it sounds that not, so start reading about Domain controllers and active directory and DNS to find some basics. Managing a domain is not as easy as to install it. If you configure it not correct you have lot's of problems.

I would strongly recommend that you built a domain for testing with Virtual server, so that you can learn about, before using it. Also you should think about joining a basic course for Active directory or read some books and test with them.

Thanks very much for this wordy question.

Joseph