Who can add workstation to the domain

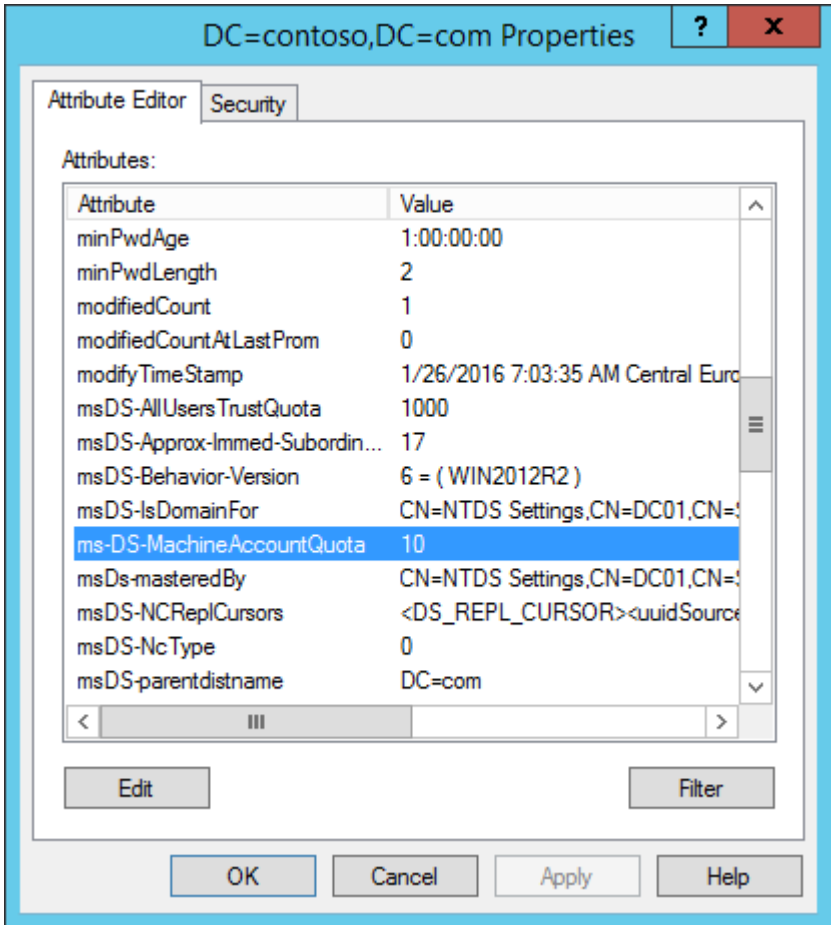
Article02/01/2016

Hello

It's Rafal Sosnowski from Microsoft **Dubai Security PFE Team**. During my numerous Security Audits and Assessments I deliver to customers, I usually discover too wide permissions and user rights configured in Active Directory. One of them is "Add Workstation to the Domain". There are 3 items that might influence who can add computer to the domain:

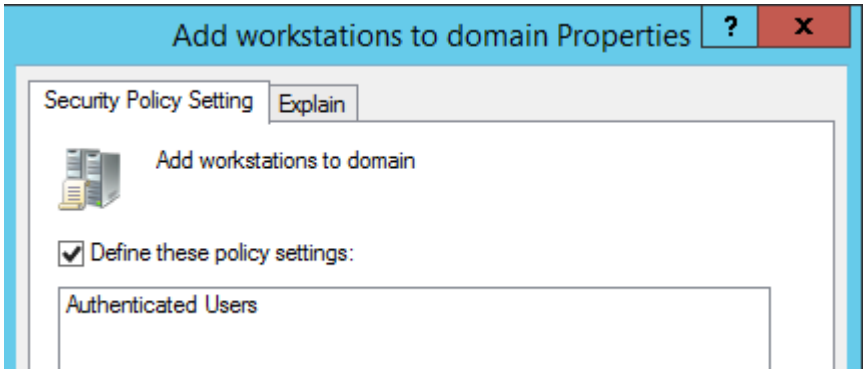
ms-DS-MachineAccountQuota

It is an attribute on Domain Naming Context object. This attribute specifies how many computers can be added by single user to the domain. **Default value is 10**. This value can be modified using different tools including ADSIEdit.msc



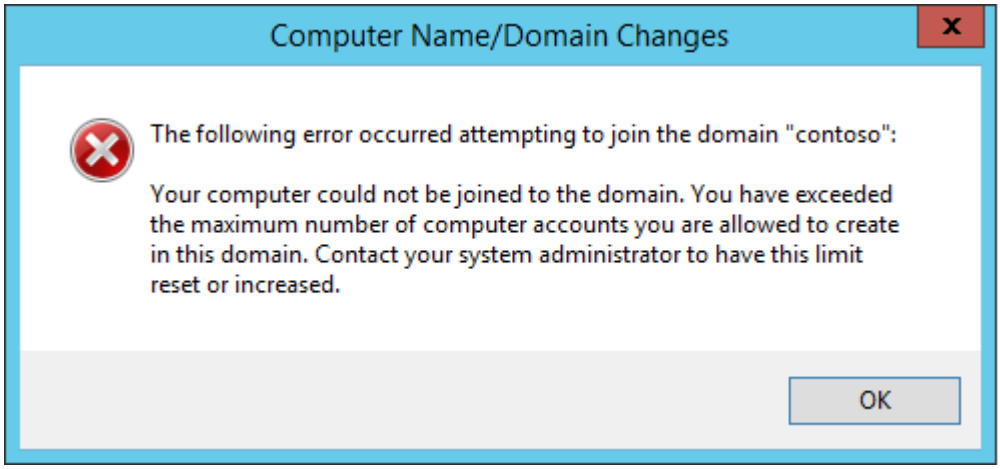
Add workstation to the Domain

This User Right configured via Default Domain Controller Policy or via local policies on Domain Controllers specifies who can join computer to the domain. Default value is **Authenticated Users**.



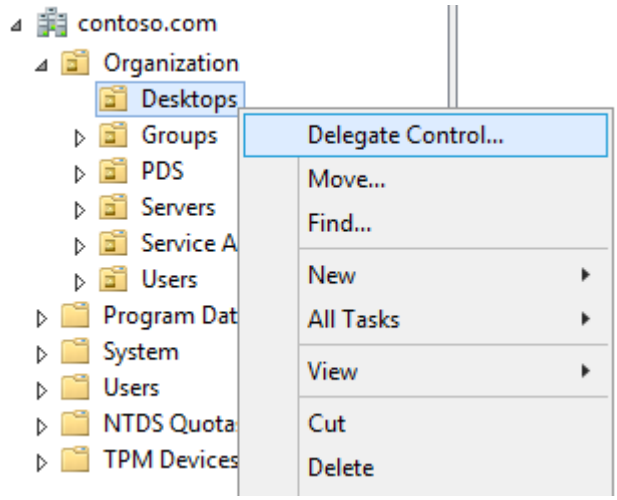
So taking into consideration above 2 items, **by default any authenticated user can join up to 10 machines to the domain**. This is because "Authenticated Users" are added to the "Add workstation to the Domain" User Right and ms-DS-MachineAccountQuota is 10.

Now if you replace Authenticated Users with your domain, custom HelpDesk group and leave ms-DS-MachineAccountQuota untouched don't be surprised if helpdesk users join only up 10 computers. After exceeding this number, they will get following error:

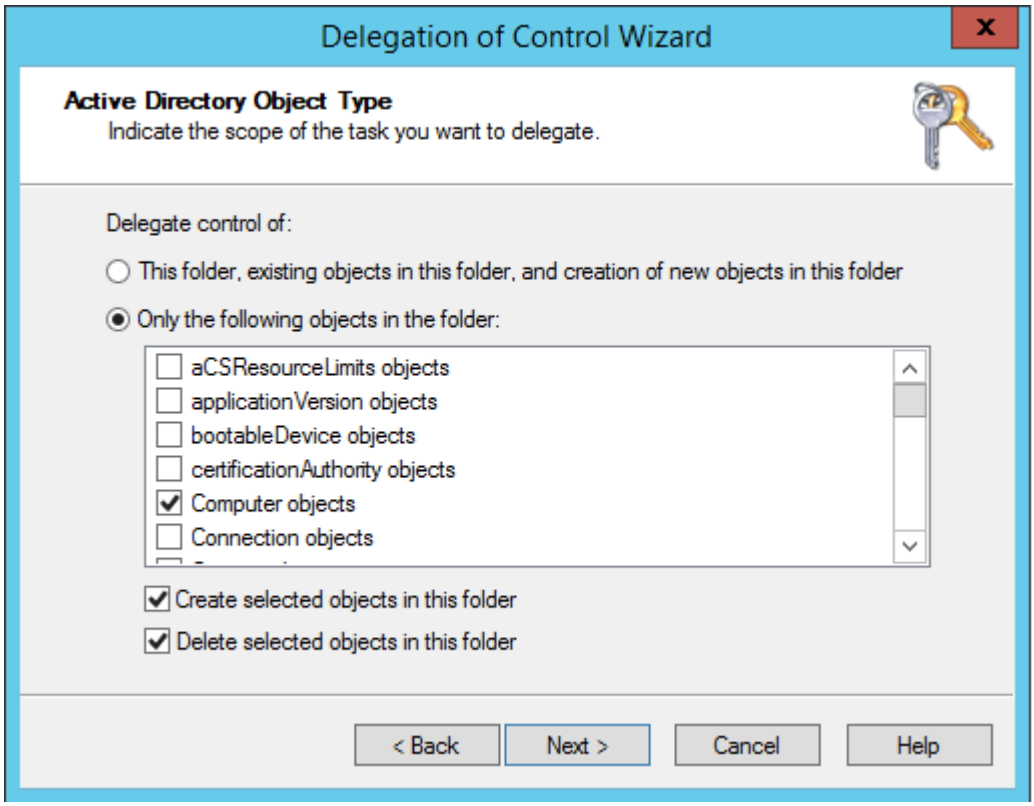


Delegation

Here comes the right method of granting permissions to your domain: **AD Delegation**. You can granularly control who can do what in your domain including domain join. Designing proper delegation model is quite time consuming because you need to define administrative roles, develop proper OU structure, create security groups and finally configure permissions and auditing.



Delegation can be configured using **Delegation Wizard** (right click on OU > Delegate Control…) or by applying ACLs directly on the OU or domain level. ACLs on Active Directory containers define what objects can be created and how those objects are managed. Delegation of rights involves basic operations on objects, such as the ability to view an object, create a child object of a specified class, or even deleting an object.

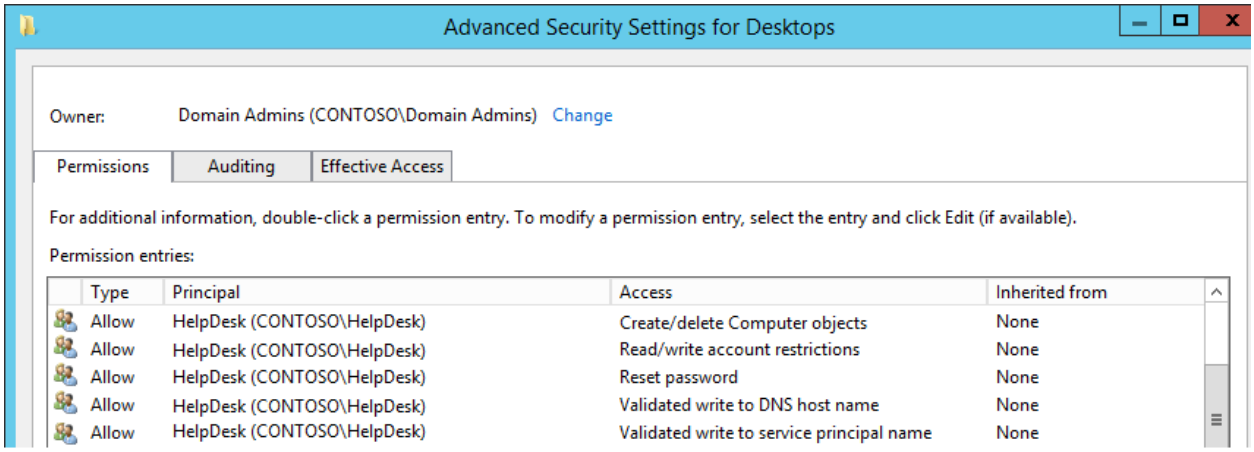


Adding computer to the domain requires only singe, delegated permission:

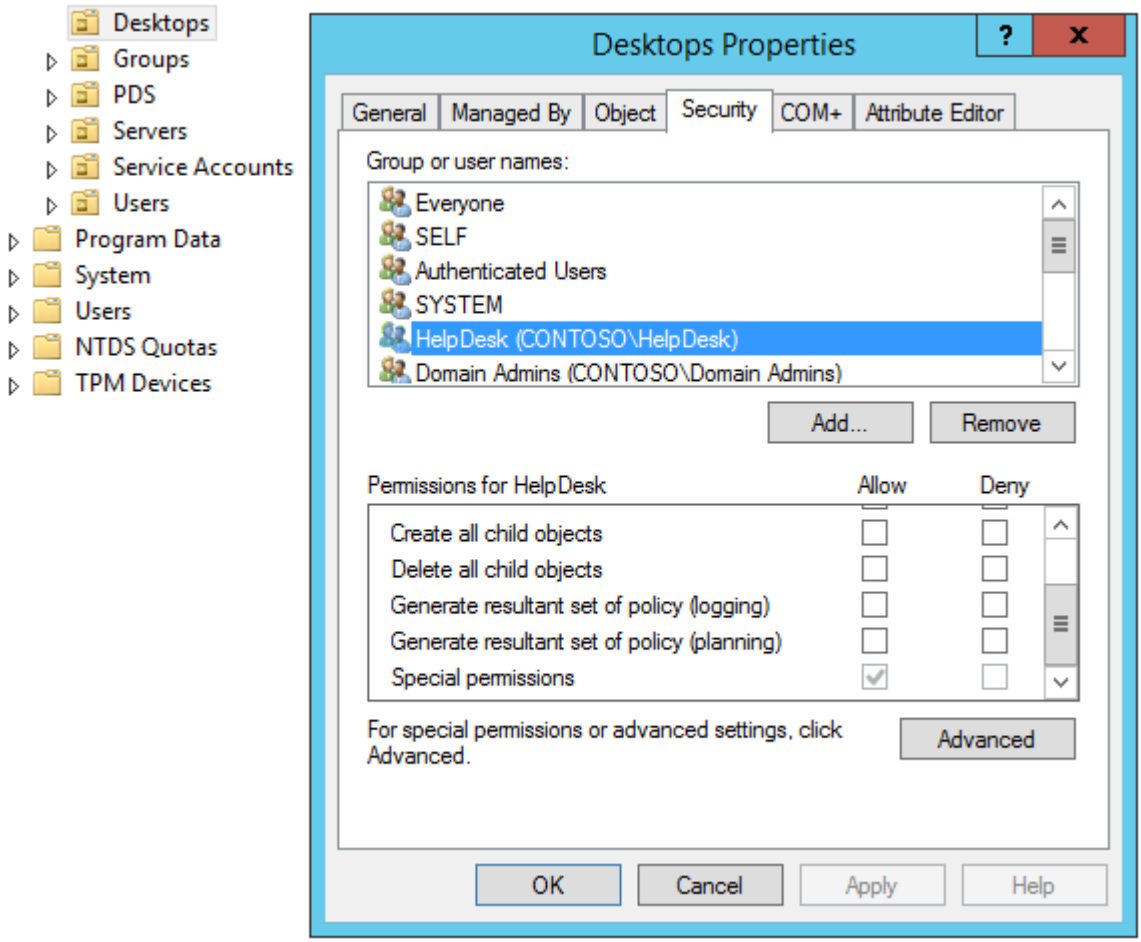
1. **Create computer object**

Active Directory however allows you to delegate permissions to other computer related tasks:

1. Delete computer object
2. Reset Password (of computer object)
3. Read and write Account Restrictions (used to enable / disable computer object)
4. Validated write to DNS host name
5. Validated write to service principal name (used to set SPN) and many, many more...



To check if permissions are ok, just right click on the OU or Domain name and investigate “Special” permissions for your Group/User by clicking Advanced.



At least "Create computer object" should be there.

Remember to redirect your default Computer container to the specific OU using **redircmp** command, otherwise you will need to configure delegation on default “Computers” container.

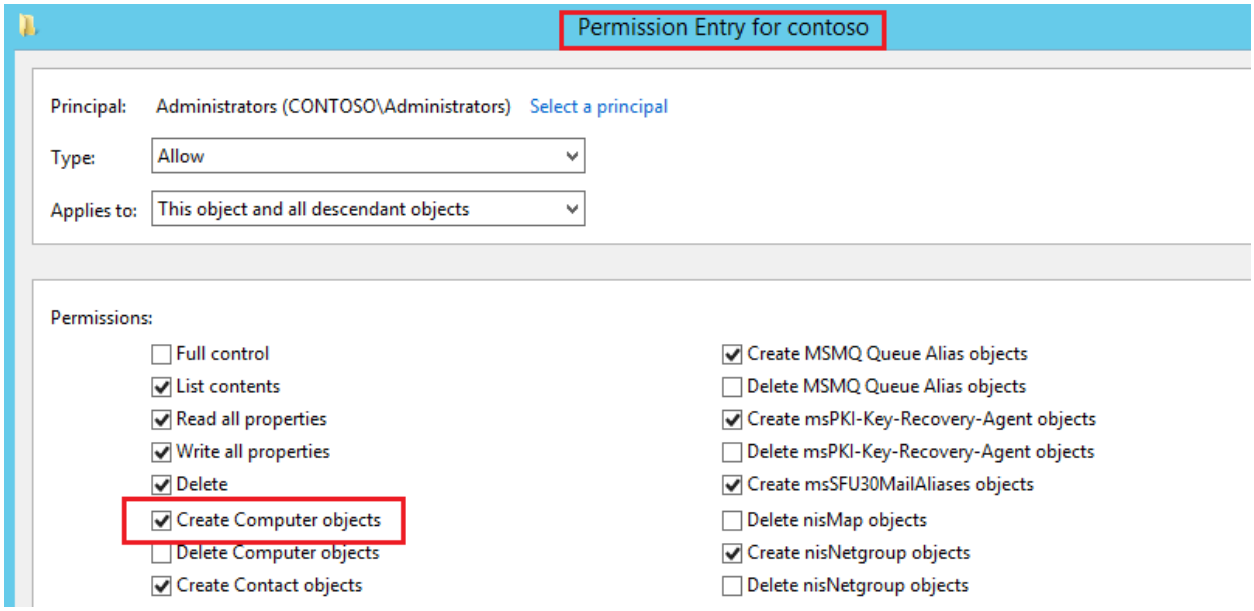
```
redircmp CONTAINER-DN

    where CONTAINER-DN is the distinguished name of the container
    that will become the default location for newly created computer objects

    Note: The domain functional level must be at least Windows Server 2003


C:\Windows\system32>redircmp OU=Desktops,OU=Organization,DC=contoso,DC=com
Redirection was successful.
```

Delegation will completely ignore threshold in the ms-DS-MachineAccountQuota meaning **user can add unlimited number of computers to the domain**. On other hand "Add workstation to the Domain" user right will bypass any ACLs on the OU.

Now if you have in place: Delegation for Group1 and “Add workstation to the domain” for Group 2– both will be able to add computers to the domain.

So you might ask: although I configure delegation only on specific OU, and “Add workstation to the domain” is empty why **Domain Admins can still add machines to the domain**?

This is because “Administrators” group (containing Domain Admins) has direct and explicit ACL permissions to create Computer objects. This permission is assigned on the domain level with propagation enabled.



As a side note there is also Active directory group called "**Account Operators**" – however I don't recommend using it as it has too wide permissions over AD: it can create/delete users, computers and other AD objects.

It is important to control who can add new machines to our AD environment. Although we can enforce various security settings via GPO on newly added machines, user could join machine which is not configured according to our security standards and at the same time having ownership of various objects in the system (local admin account, ACLs on file system etc.).

I do recommend using delegation and remove all users from "Add workstation to the Domain" from Default Domain Controller Policy except Administrators (as contingency plan). Also you can reduce ms-DS-MachineAccountQuota value to 0.

Moreover, I am not big fan of allowing standard users to join their workstations to the domain, as they become Owner of the computer object in AD (from ACL perspective) and additionally have ACCESS_CONTROLL flag which means they can read confidential attributes for that object (for example LAPS passwords). This is another argument for using delegation.

You can find more info here: https://support.microsoft.com/en-us/kb/251335

Comments

- **Steve Morley**

January 8, 2017

Hello, This is a great article, although I am seeing a different outcome in my LAB. I have redirected my computer OU. I have set my 'ms-DS-MachineAccountQuota' attribute to '0'. I have created my own security group and added it to 'Add workstation to the Domain'. My test account is a member of the above group. Now if I try and join a computer to the domain, I get an error telling me I have added too many computer accounts. Even though I am a member of the group to allows me to join computers. If I then delegate control on the OU for the same security group, I can add machines to the domain. I just don't understand what role the 'Add workstation to the Domain' is playing here as it appears I don't need to configure this, just delegate instead. Can you help clear up my confusion? ;-)

- **Steve Morley**

January 8, 2017

After some more testing, is it correct in saying: 1) If you have delegated rights on the OU, you can join unlimited computers to the domain. Regardless of what is in the DDC policy. 2) If you do not have delegated rights on the OU, but are listed within the DDC

policy, then you can add machines up to the limit of the "ms-DS-MachineAccountQuota" attribute.

- **Rafal Sosnowski [MSTF]**

January 10, 2017

@ Steve - yes this is what I have explained in my article: Delegation will completely ignore threshold in the ms-DS-MachineAccountQuota meaning user can add unlimited number of computers to the domain. On other hand “Add workstation to the Domain” user right will bypass any ACLs on the OU.