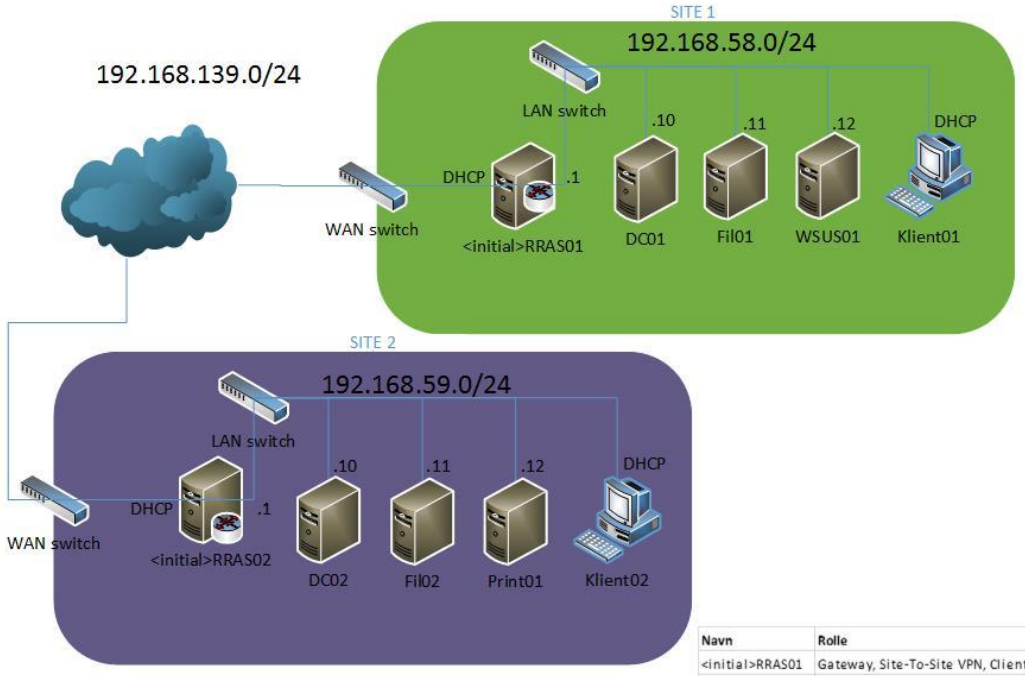
John Have Jensen

Access Management med NTFS og shares

In this guide we will configure access management with NTFS and shares following Microsoft best practice.

We will create shares on Fil01, we will be using existing Active Directory global groups and create new Active Directory domain local groups.



Navn	Rolle	Operativsystem
<initial>RRAS01	Gateway, Site-To-Site VPN, Client/server VPN	Server 2012 Standard
DC01	Domain Controller, DNS, DHCP, PKI	Server 2012 Standard
Fil01	Filserver	Server 2012 Standard
WSUS01	Windows Server Update Services Server	Server 2012 Standard
<initial>RRAS02	Gateway, Site-To-Site VPN, Client/server VPN	Server 2012 Standard
DC02	Domain Controller, DNS, DHCP	Server 2012 Standard
Fil02	Filserver	Server 2012 Standard
Print01	Printserver	Server 2012 Standard
Klient01	Workstation	Windows 8 Enterprise
Klient02	Workstation	Windows 8 Enterprise

	Shares		
Employees in global groups	Administra-tion	Management	Production
Administration	Read and write – delete own files	Read	Read
Management	Read and write – delete own files	Read and write – delete own files	
Production	Read	Read	Read and write – delete own files

To make an efficient Access Management structure, Microsoft recommends the following approach: **A**ccounts are made member of **G**lobal groups that are made member of **d**omain **l**ocal groups which are added to a **A**ccess Control List with a certain permission. You can try to remember the rhyme AGDLA.

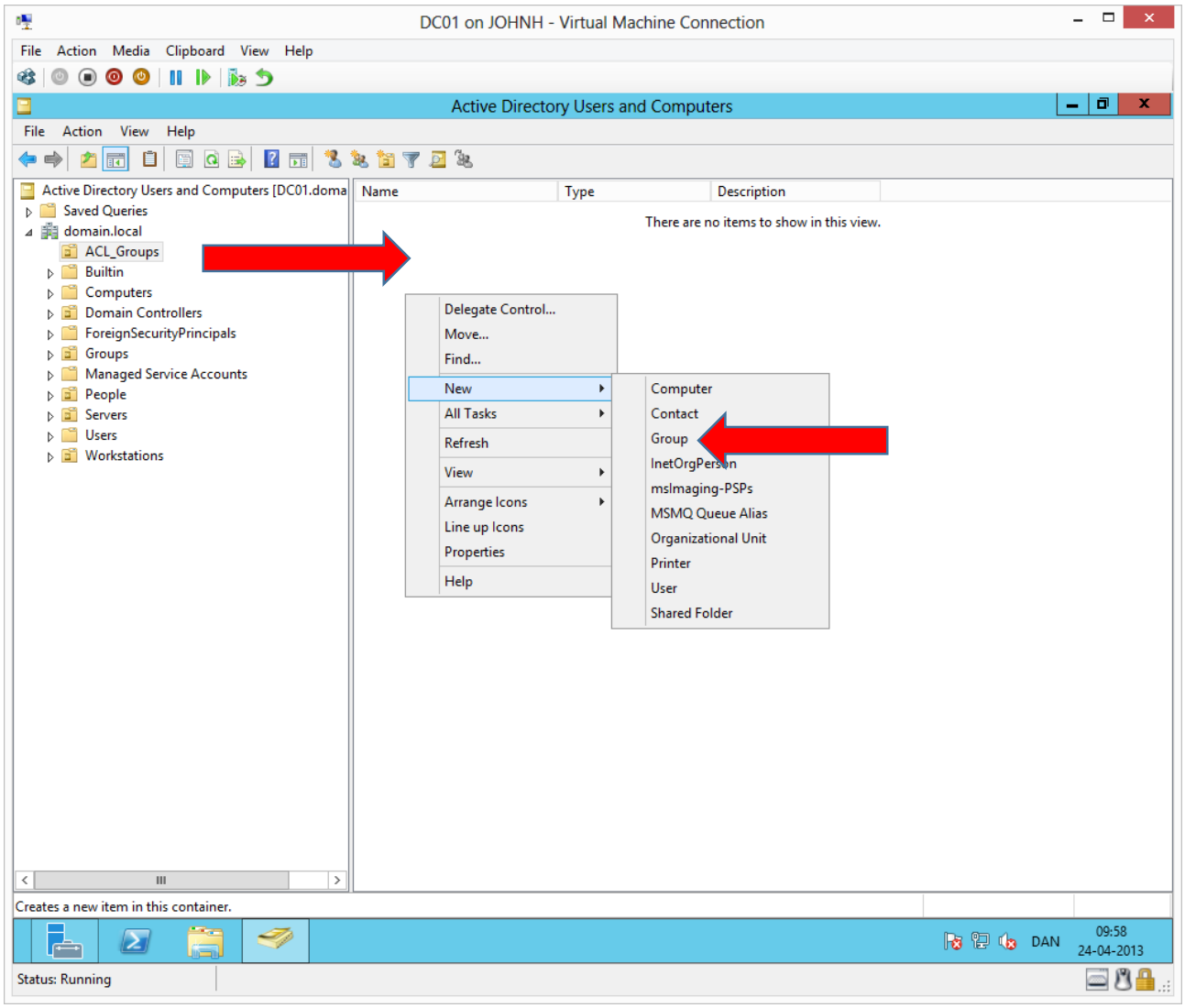
We have already created the global groups **administration**, **ledelse (management)** and **Produktion (Production)** in Active Directory and made the correct users member of the groups (Global groups represents the different departments). Therefore, we will start by creating the domain local groups, which each represent a certain level of permissions.

For the administration share (Look at the above scheme), we will need two types of permissions: Read and write – delete own files and Read. For this purpose, we will create two domain local groups, one for each level of permissions.

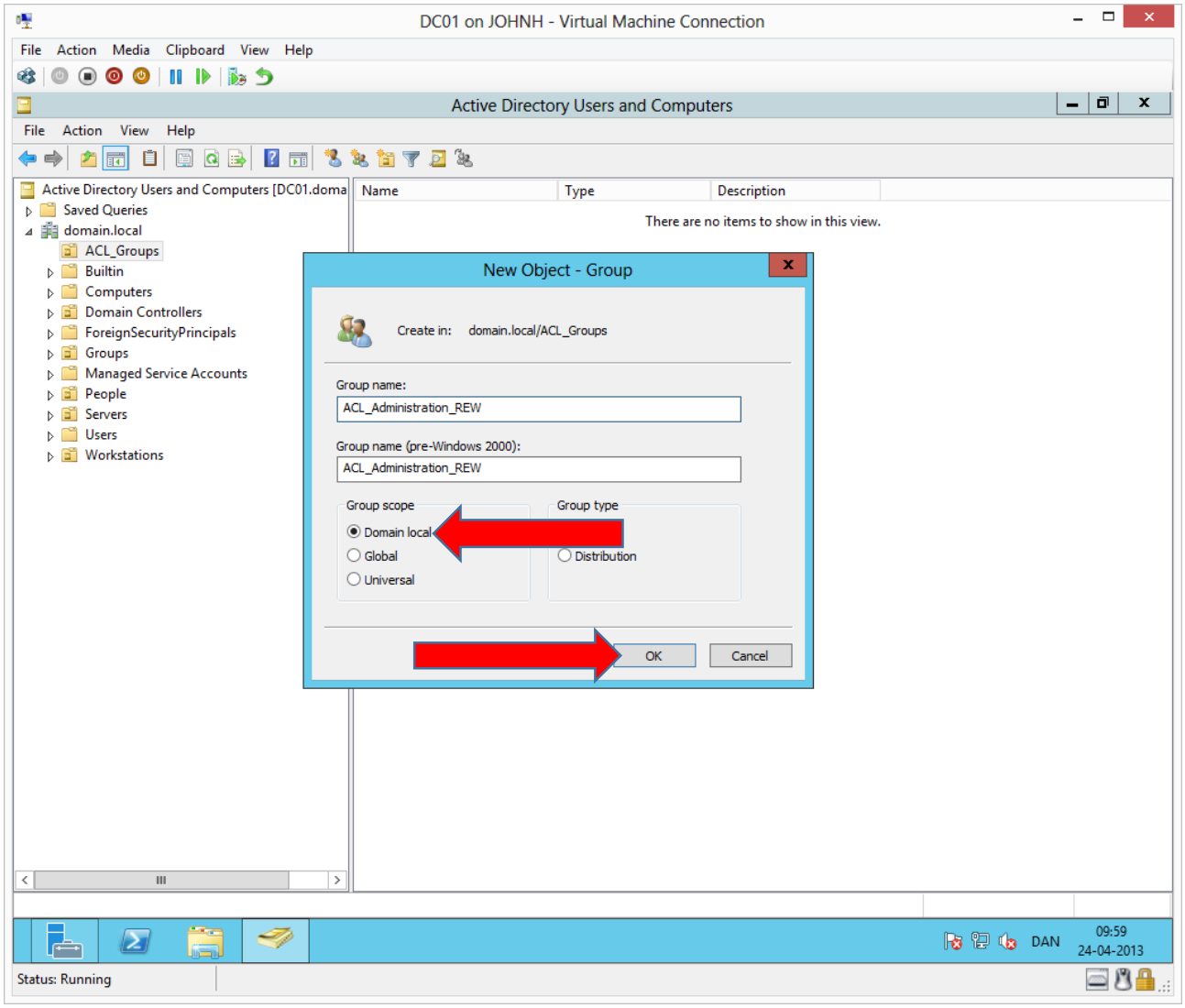
This is actually the case for all three shares: Following the scheme, each share only needs two different types of permissions

John Have Jensen

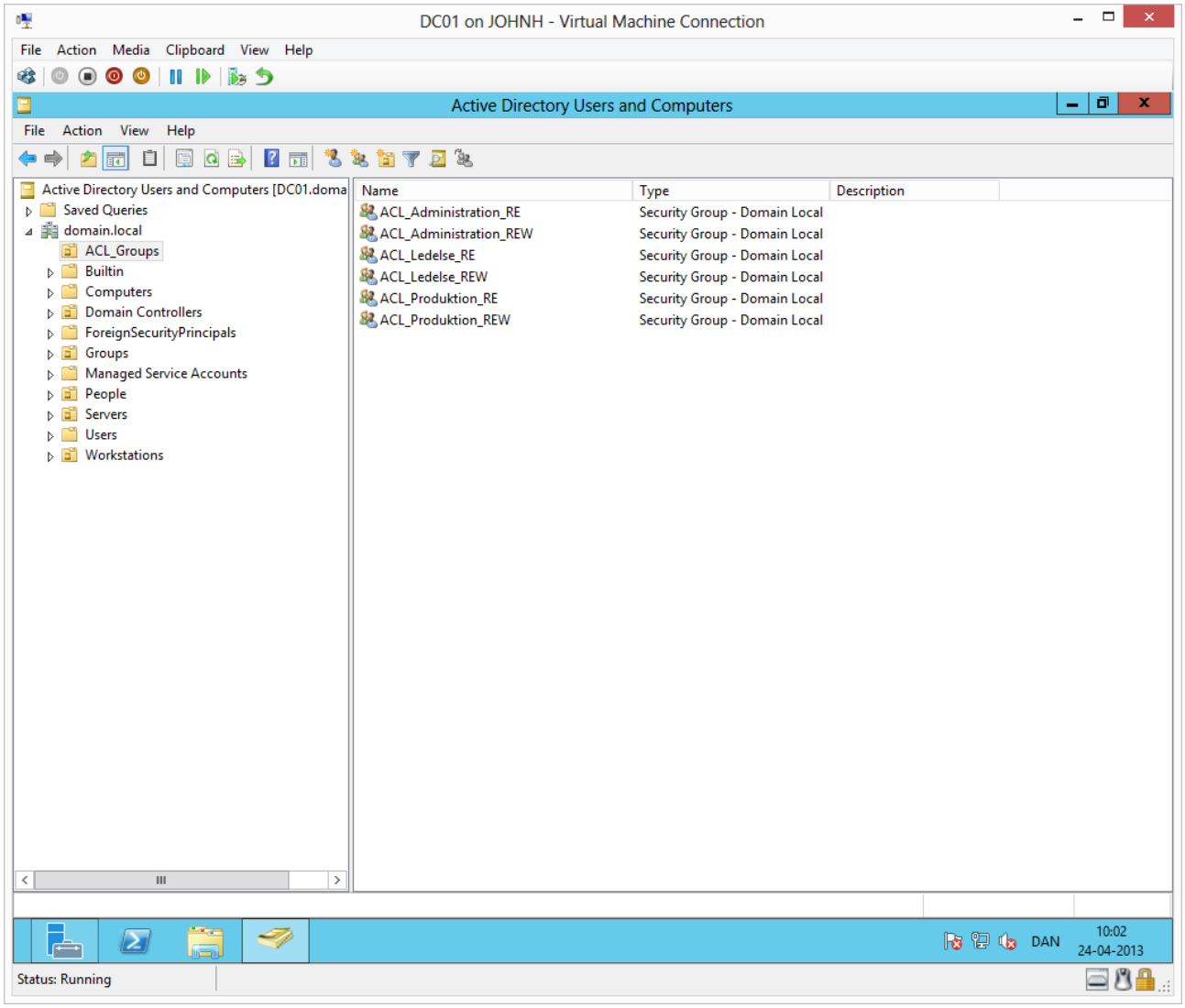
Creating and configuring groups



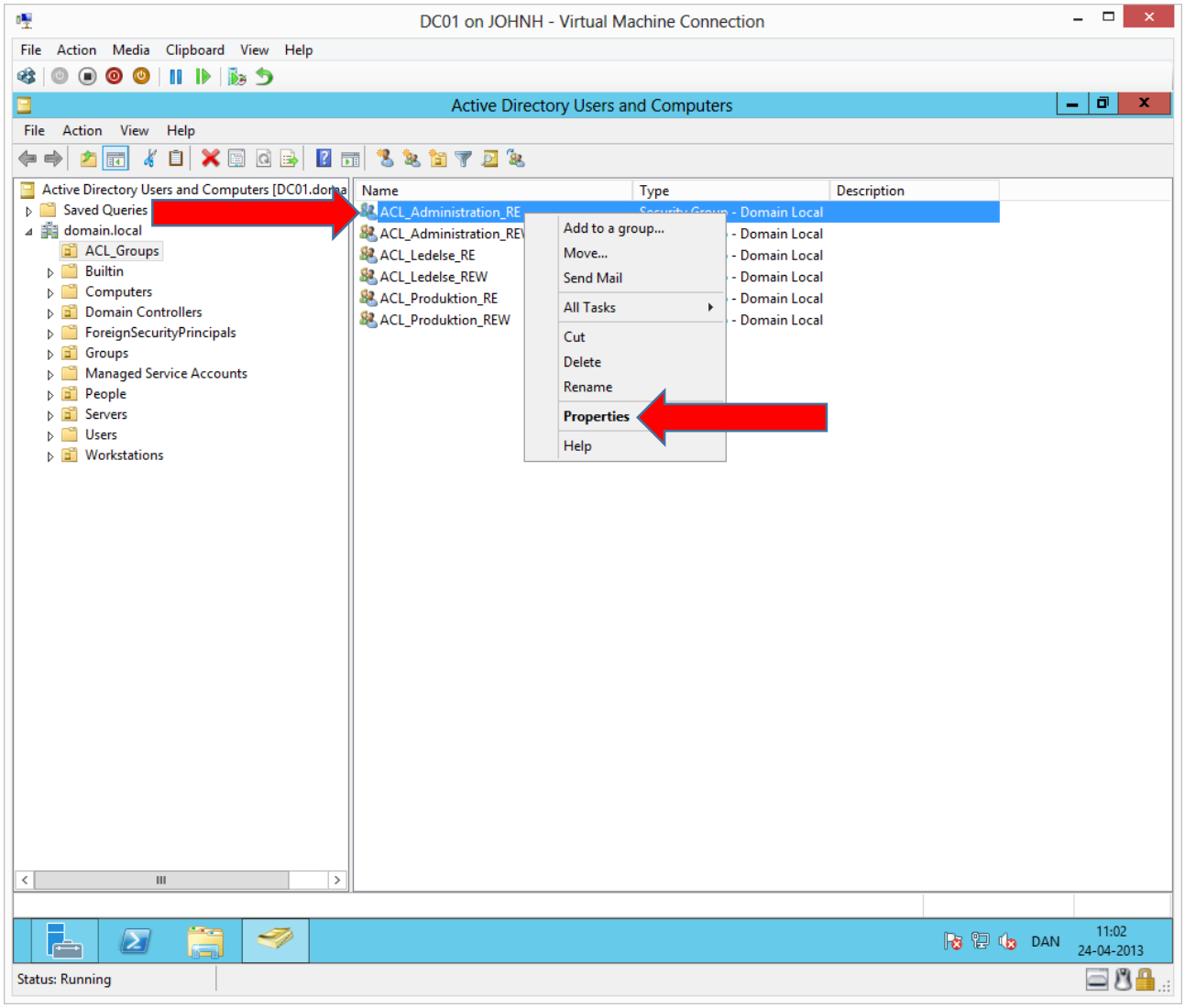
On DC01 in the Active Directory Users and Computers snap in, we will create a new group under the ACL_Groups OU by right clicking the OU or in the empty space and choosing **New→Group**



By naming the group as above, it is easily searched throughout the Active Directory forest and easy to understand the purpose of the group. This is a group that is added to an **A**ccess **C**ontrol **L**ist in a share called **Administration** and the group will provide **R**ead **E**xecute and **W**rite permissions on this share.



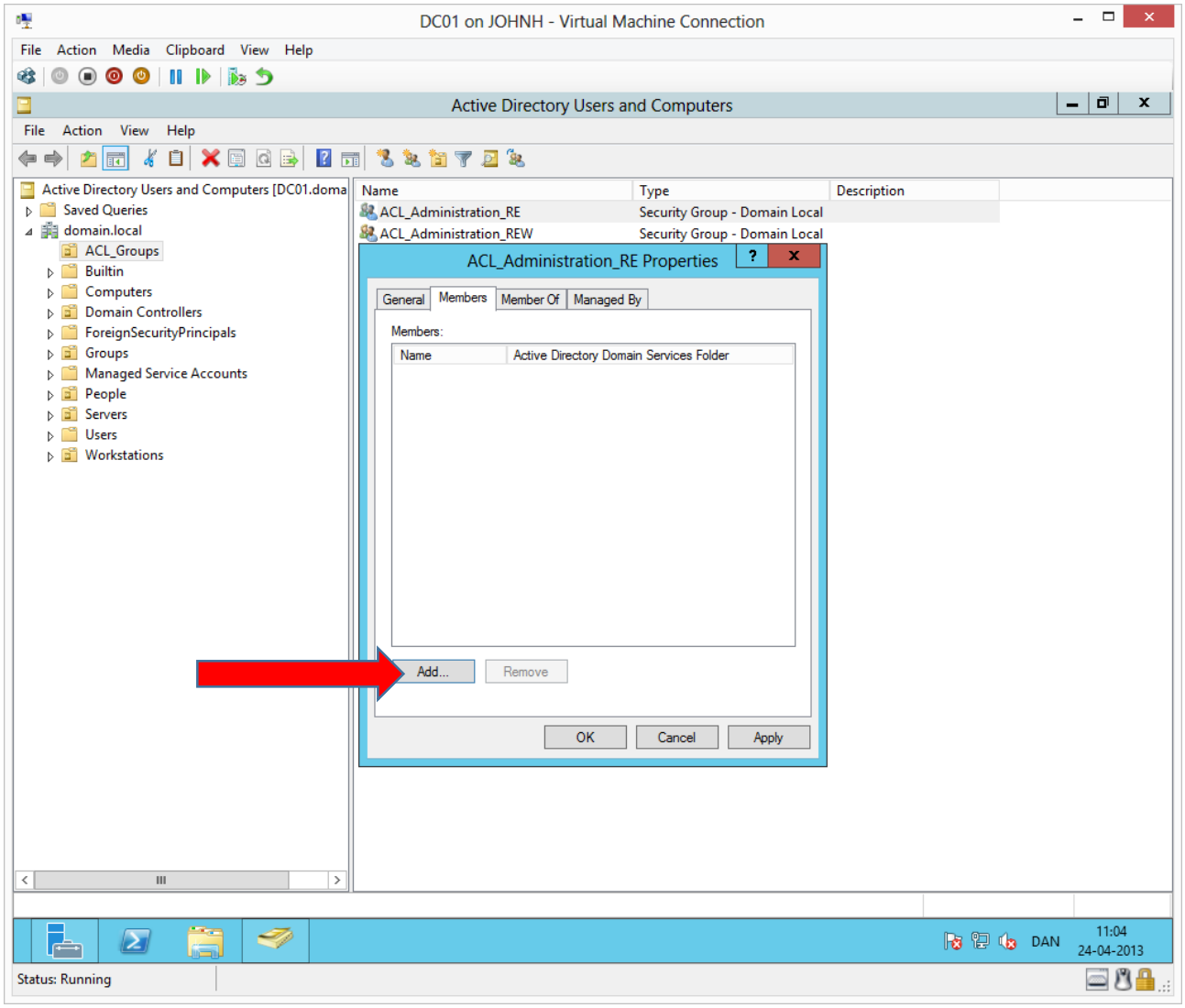
Create the remaining groups following the scheme – two groups per share.

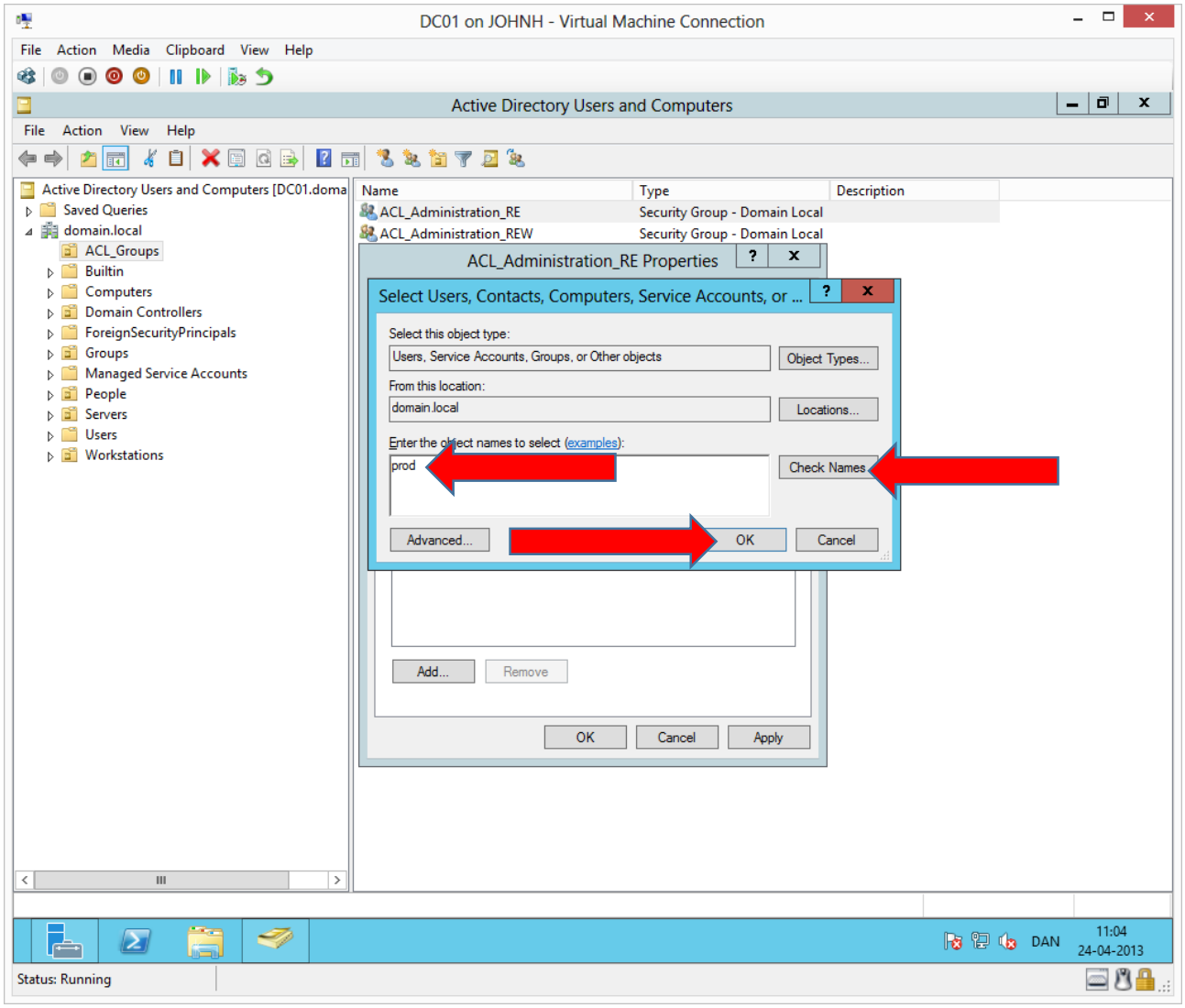


Our ACL groups are empty meaning no one has any permissions yet. Now we will connect our global groups to the correct domain local groups. We must look at the scheme to decide, which global groups must be member of which domain local groups. For example, if we start with the first group **ACL_Administration_RE**, we can see in the scheme that only production must have read permissions on the administration share.

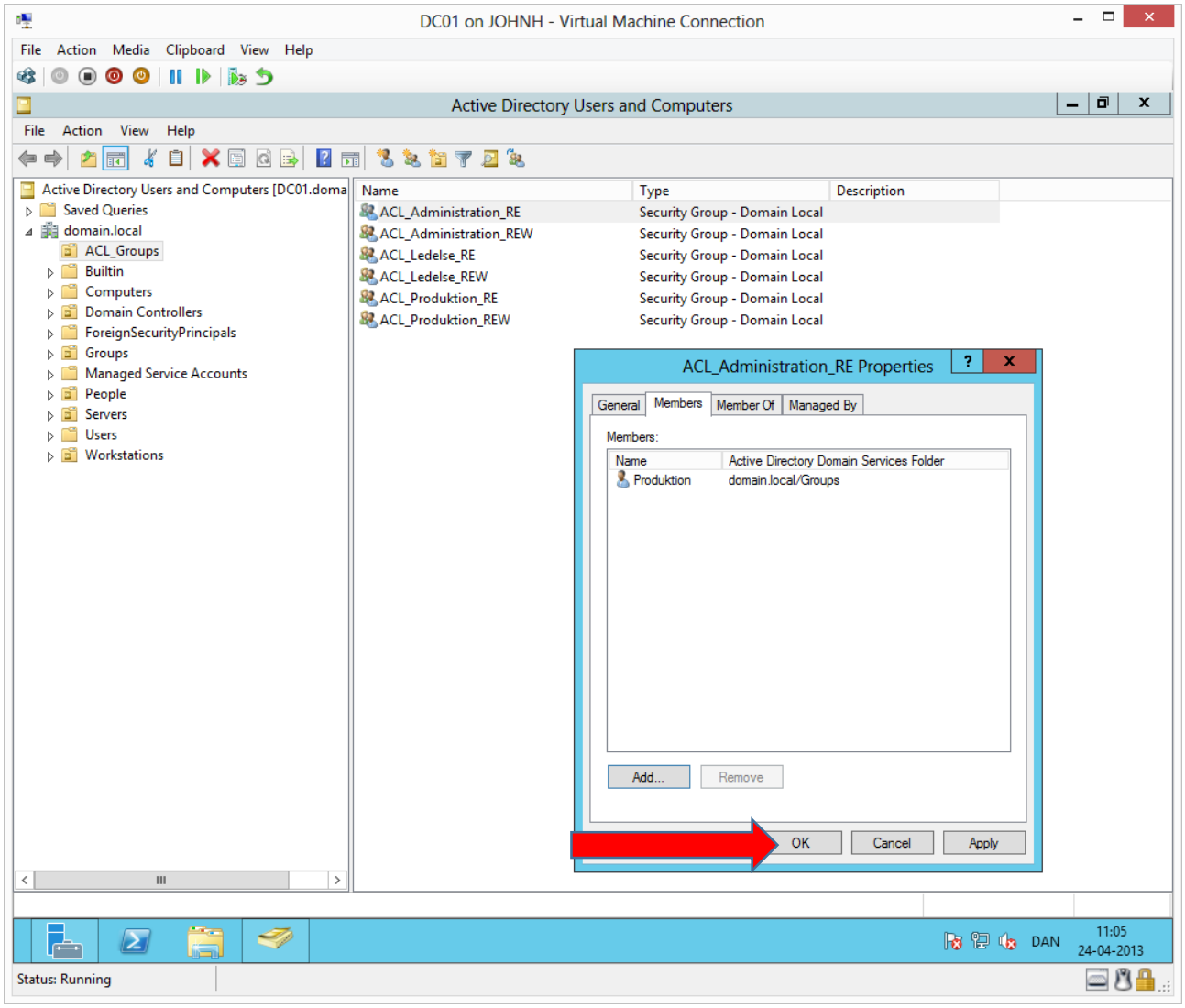
Therefore, we will add the production global group to the domain local group representing the level of permissions needed. Right click **ACL_Administration_RE→Properties**

John Have Jensen

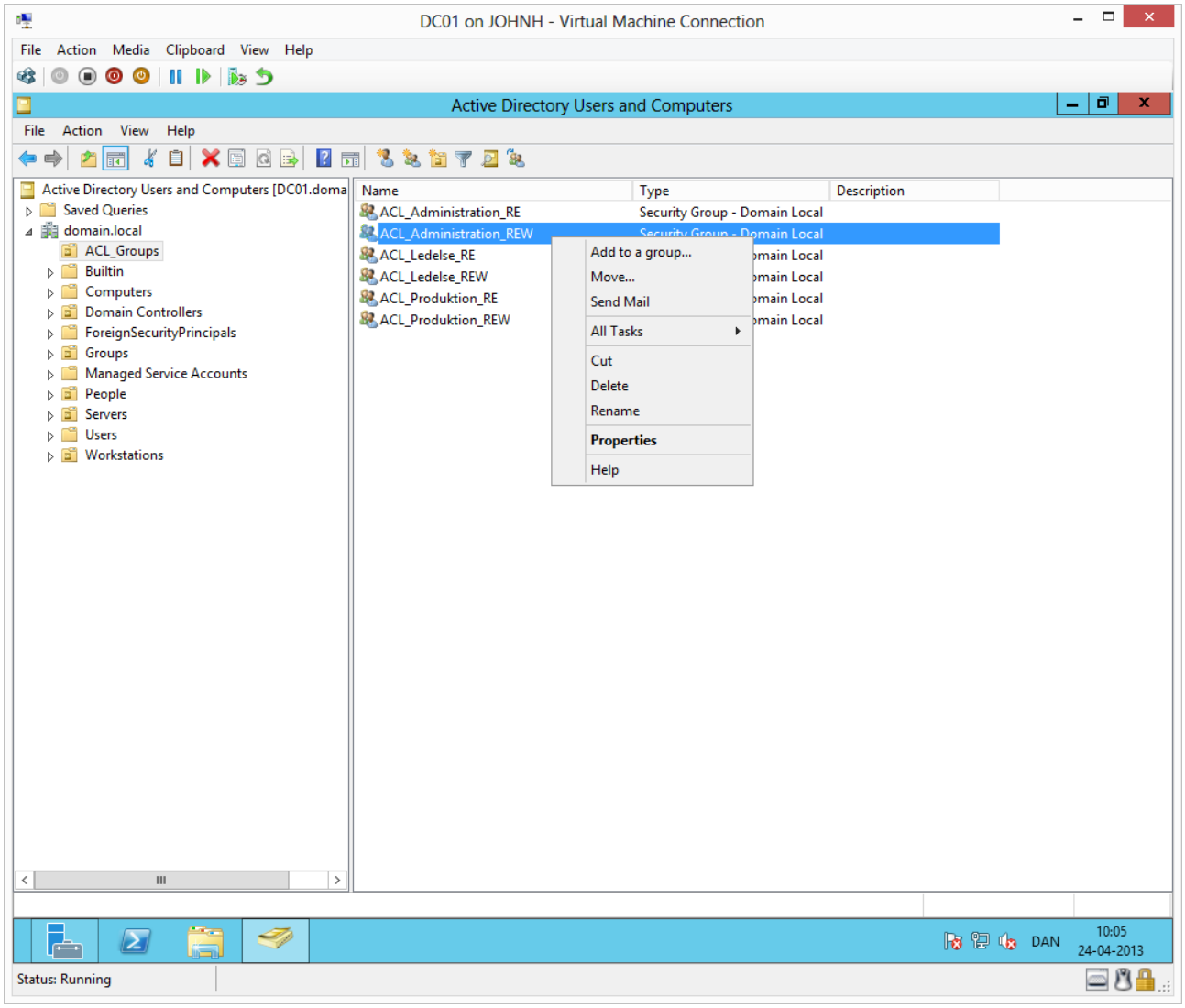




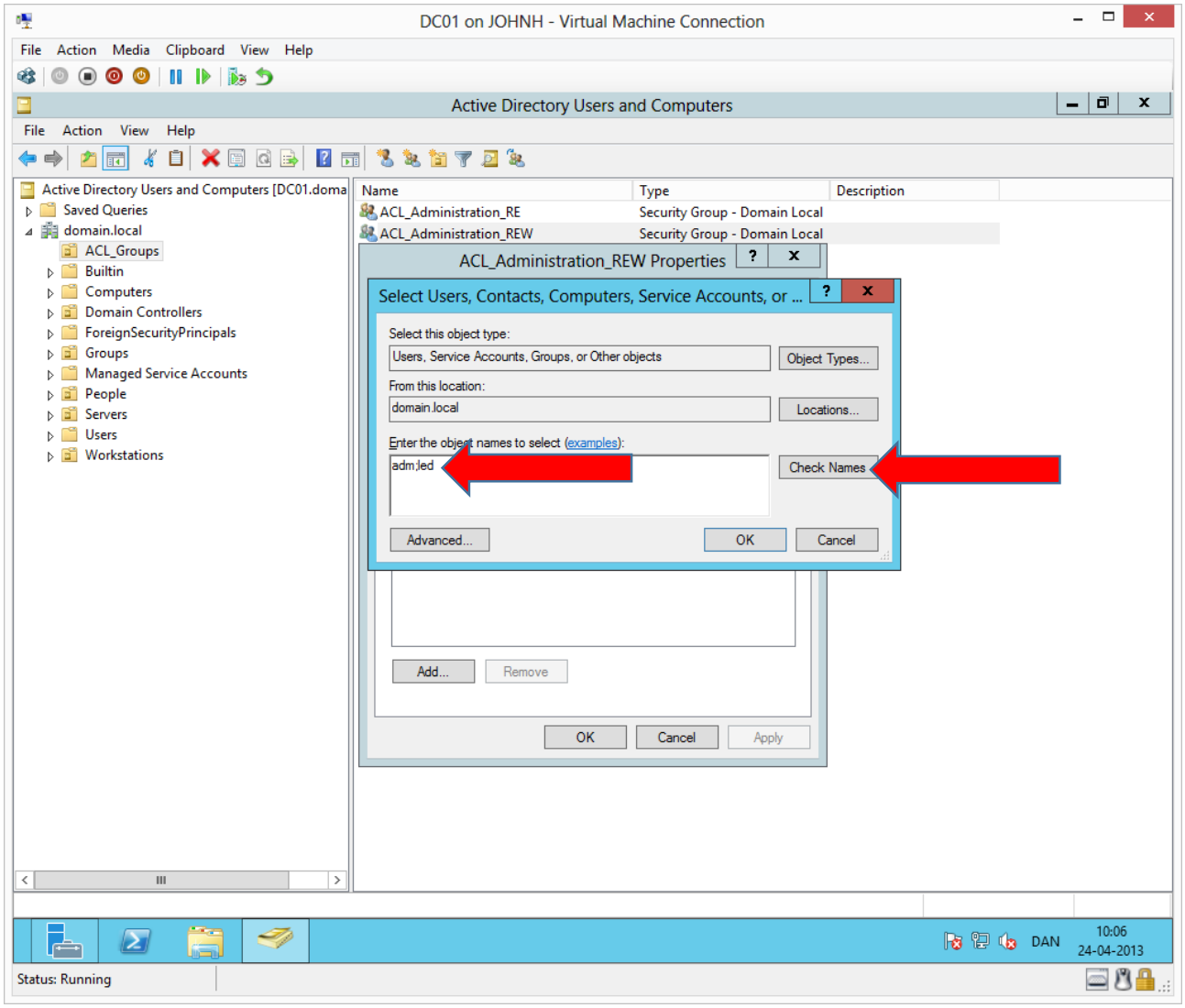
Type the whole or some of the name, of the global group and press **Check names** then **OK**.



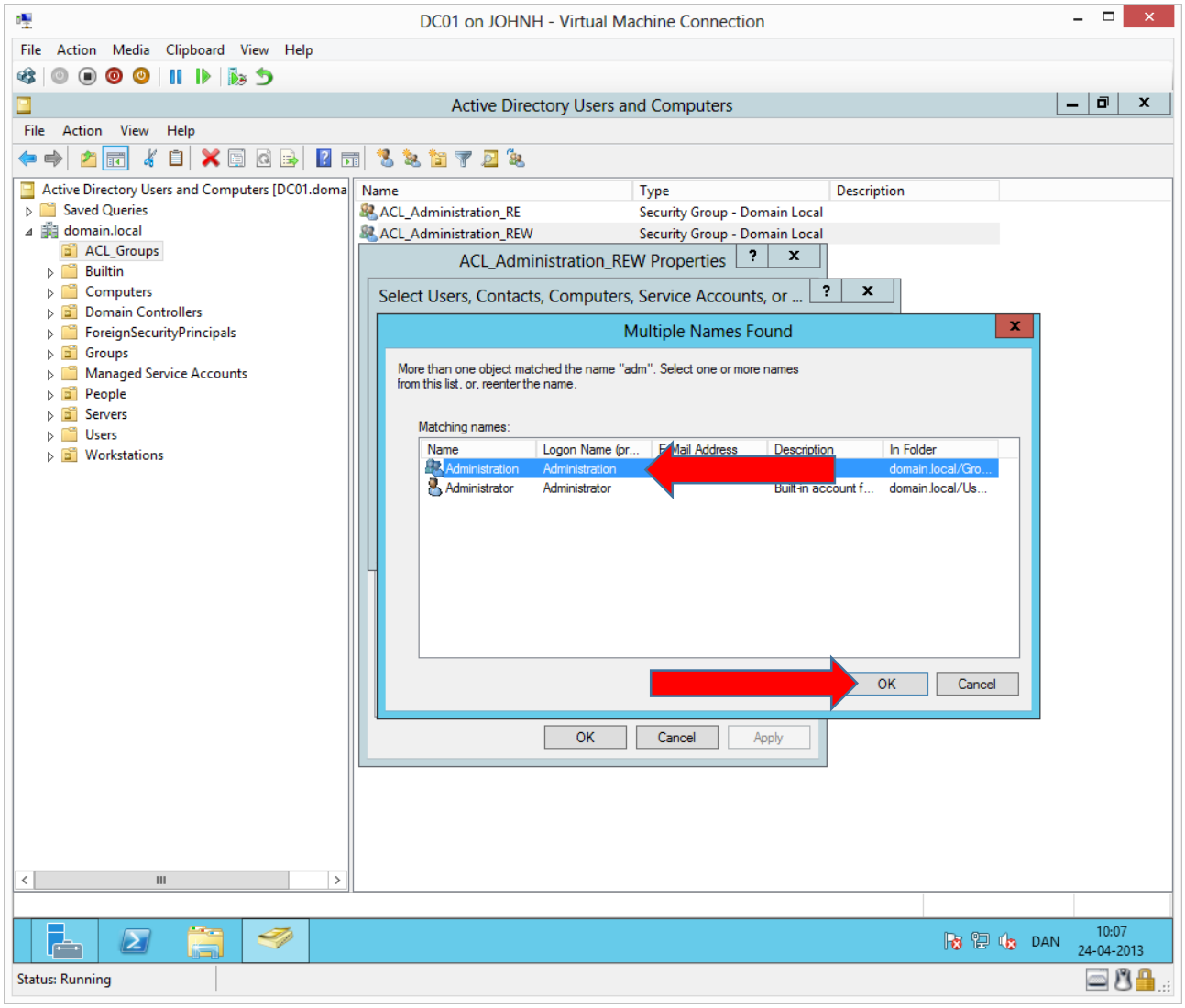
Now we have connected the global group (The production department) with the level of permissions needed on the administration share.



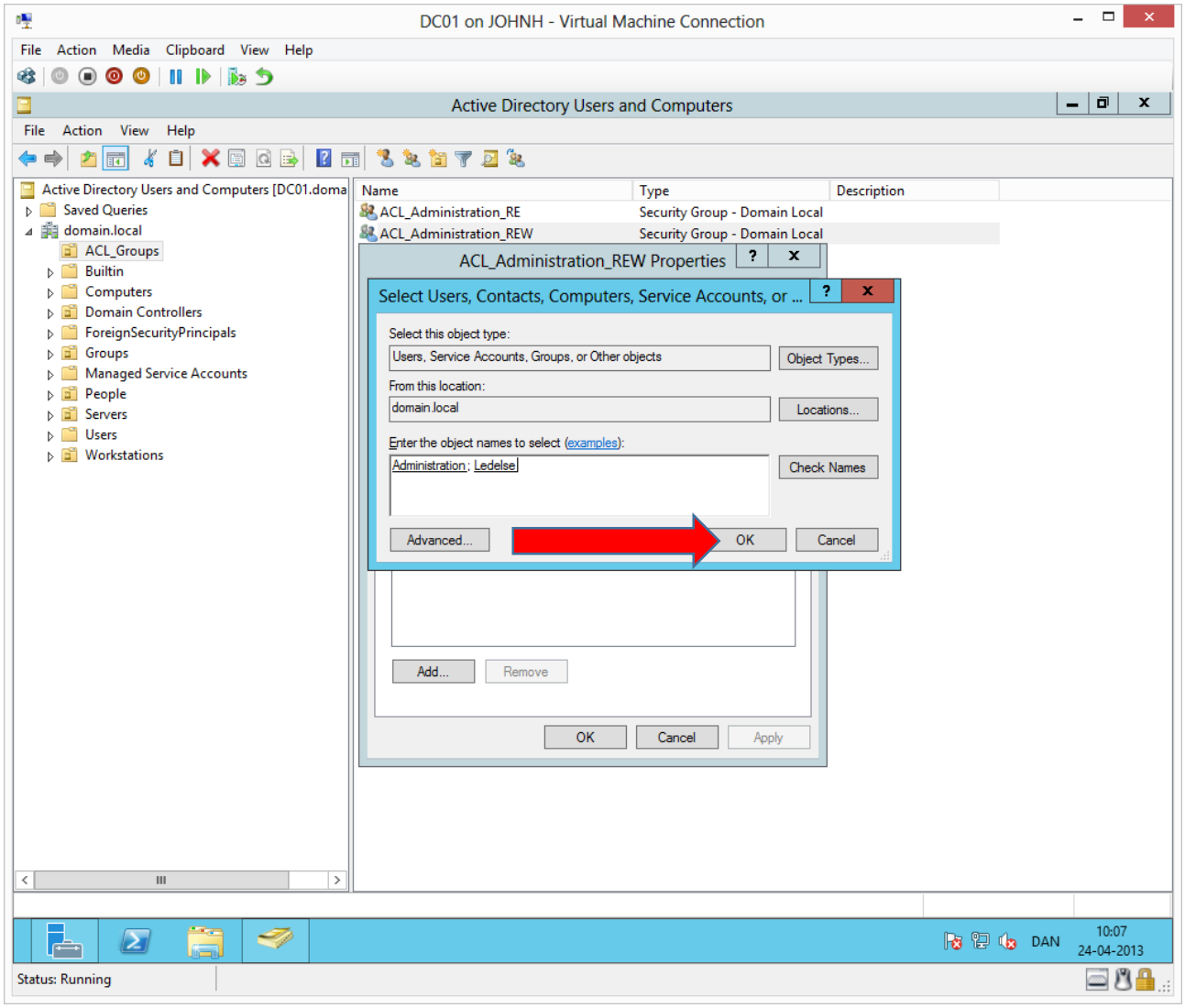
If we move on to **ACL_Administration_REW**, we can see on the scheme, that both administration and management (Ledelse) must have read and write access to the administration share. We will add the global groups in the same way.



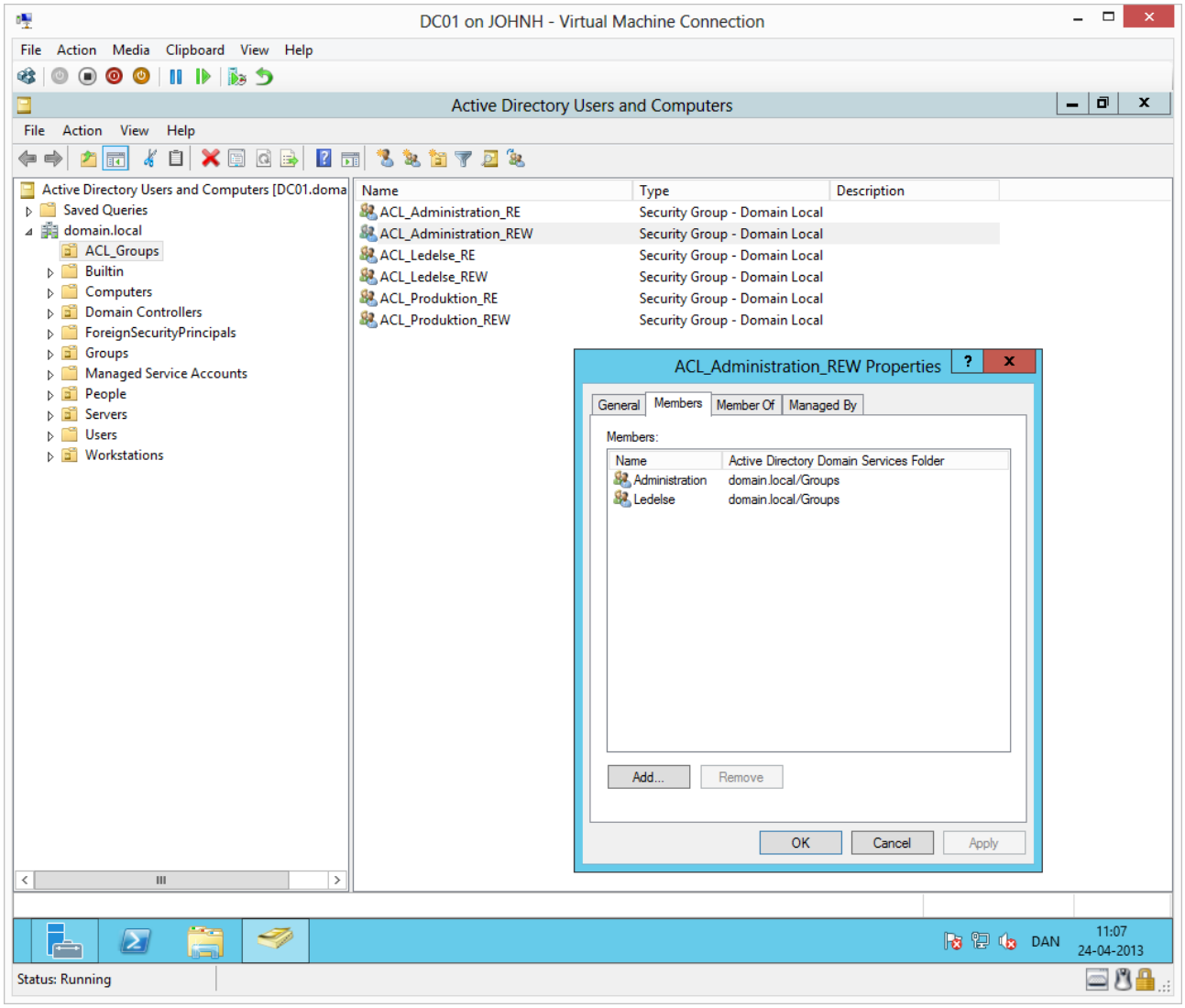
When adding several groups, you can type the whole or some of the group names separated by a semicolon, like above. To check that Active Directory recognizes the names, click **Check names**.



Several names start with adm, we select the global group **Administration**.



When all names have been underlined (found), press **OK**.



We have finished connecting the Administration and Management (Ledelse) departments with the level of permissions required on the share administration.

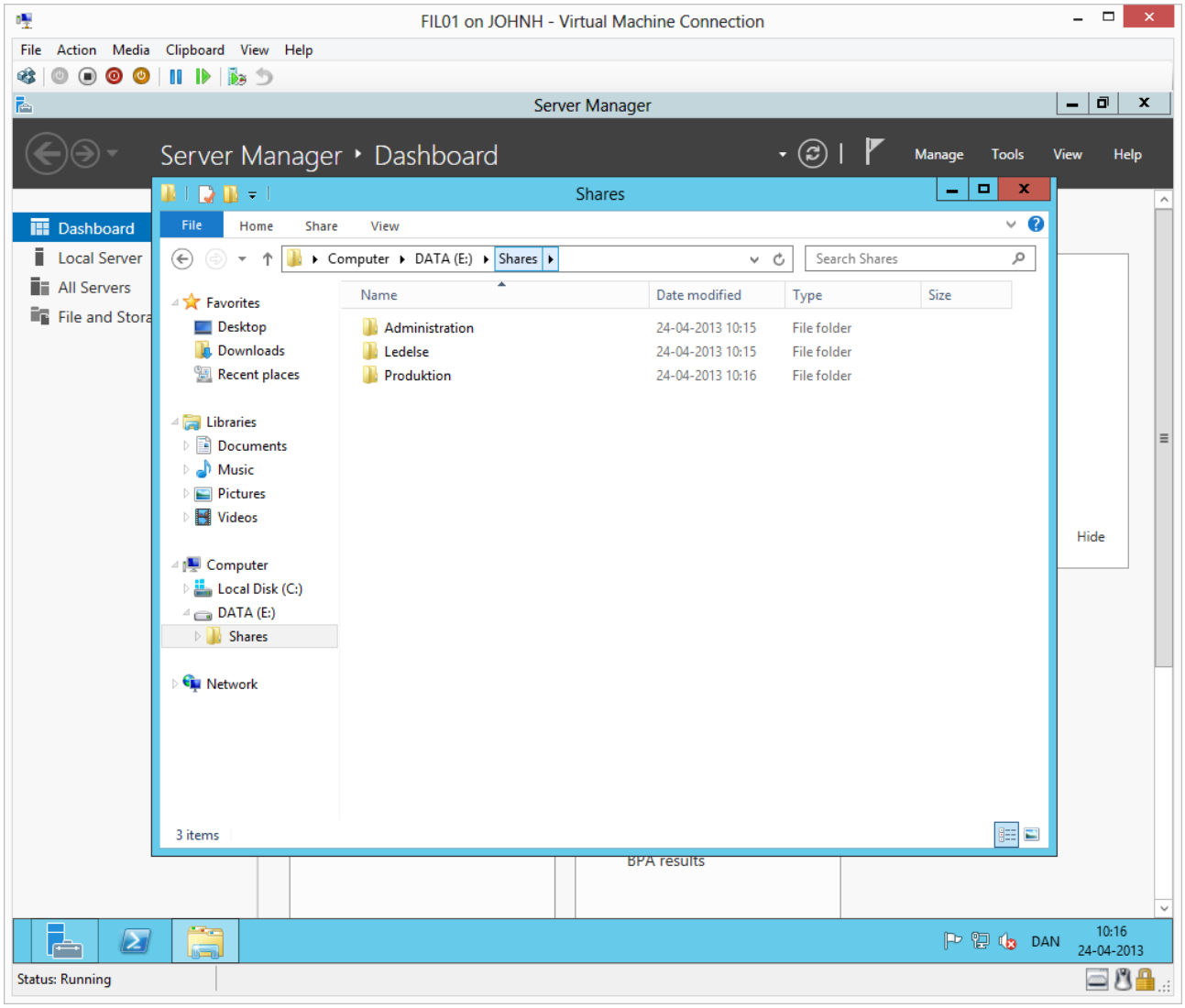
Continue adding the correct global groups to the correct remaining domain local groups.

Adding domain local groups to Access Control Lists

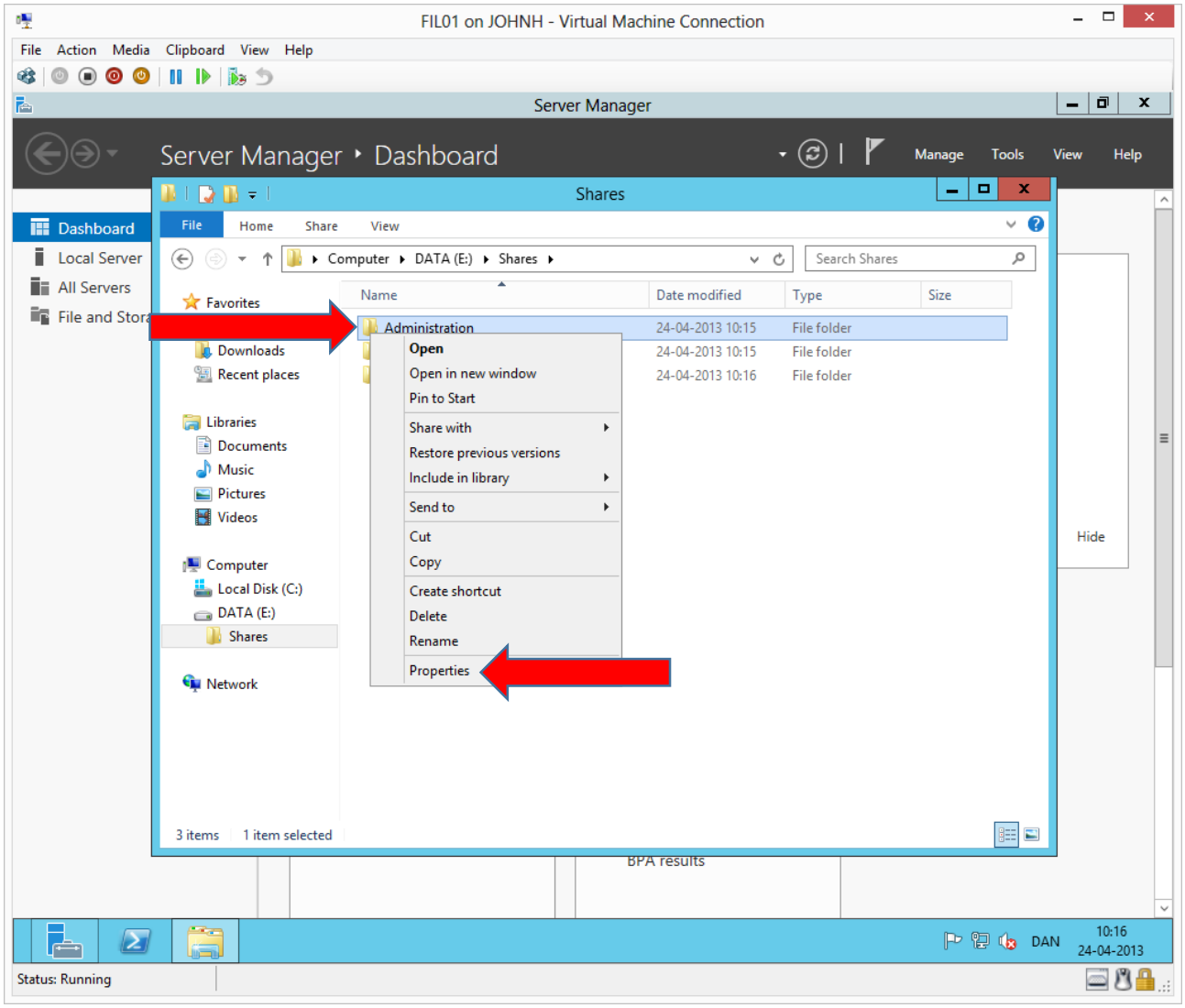
We have completed the AGDL part of AGDLA. **A**ccounts are member of **G**lobal groups that are now member of **D**omain **L**ocal groups.

The global groups (each representing a department) have been made member of several domain local groups, which each specify a level of permission needed for the department on a share.

We are missing the last part, **A**ccess List, where we will link the correct domain local groups to the Access List on each share.

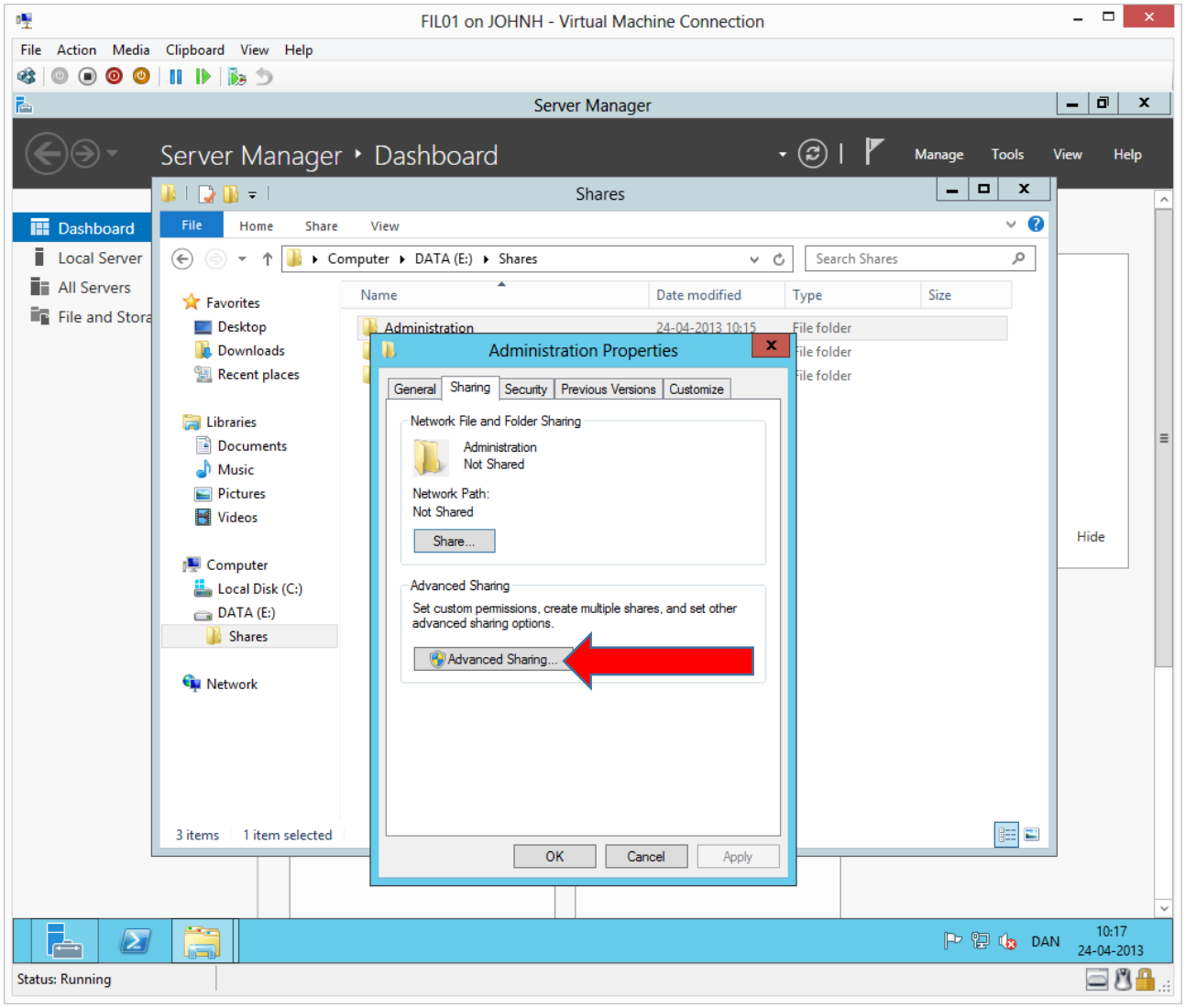


On Fil01 on the extra disk, create a folder per share. It is a good idea to create a root folder for the shares (like above)

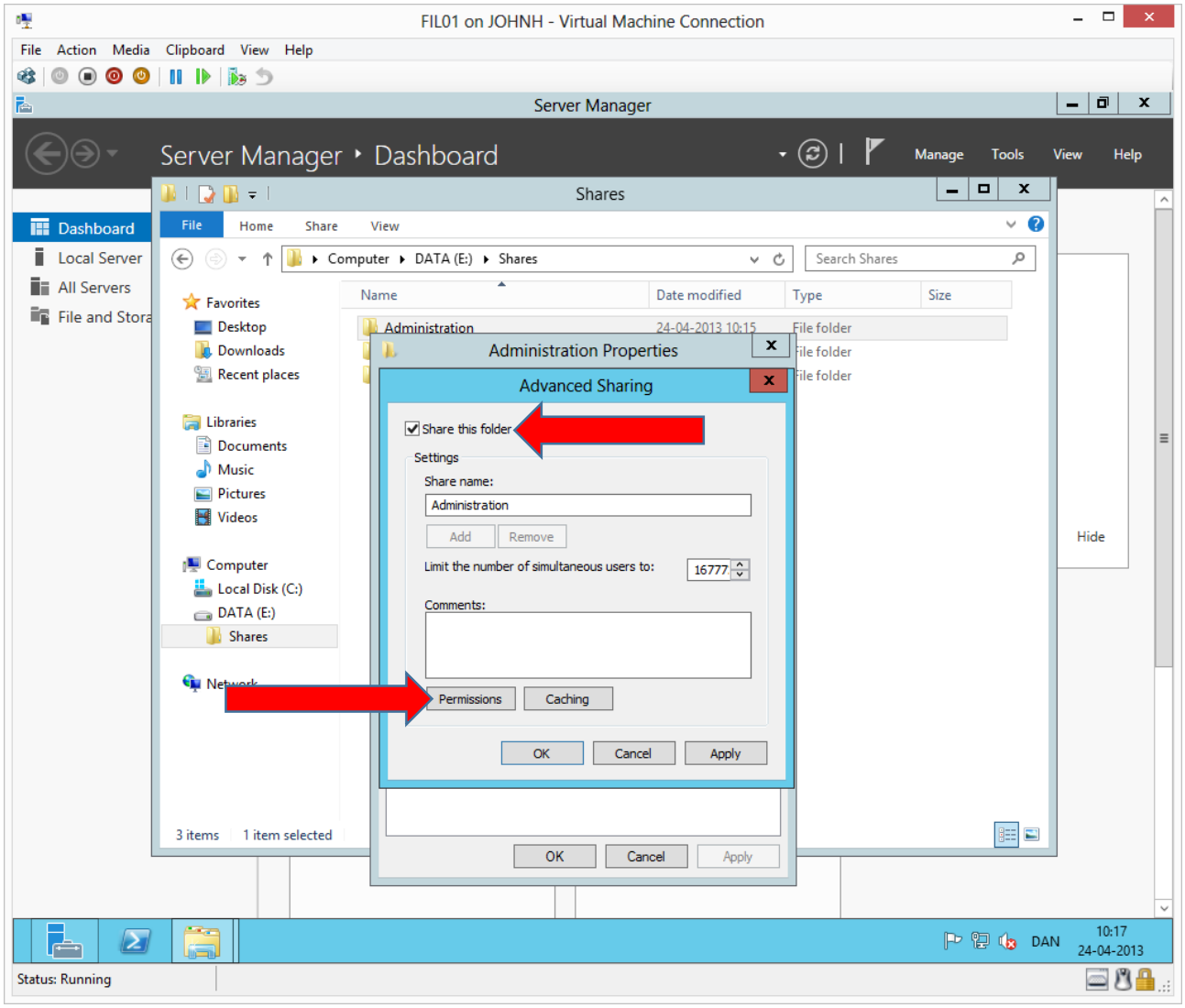


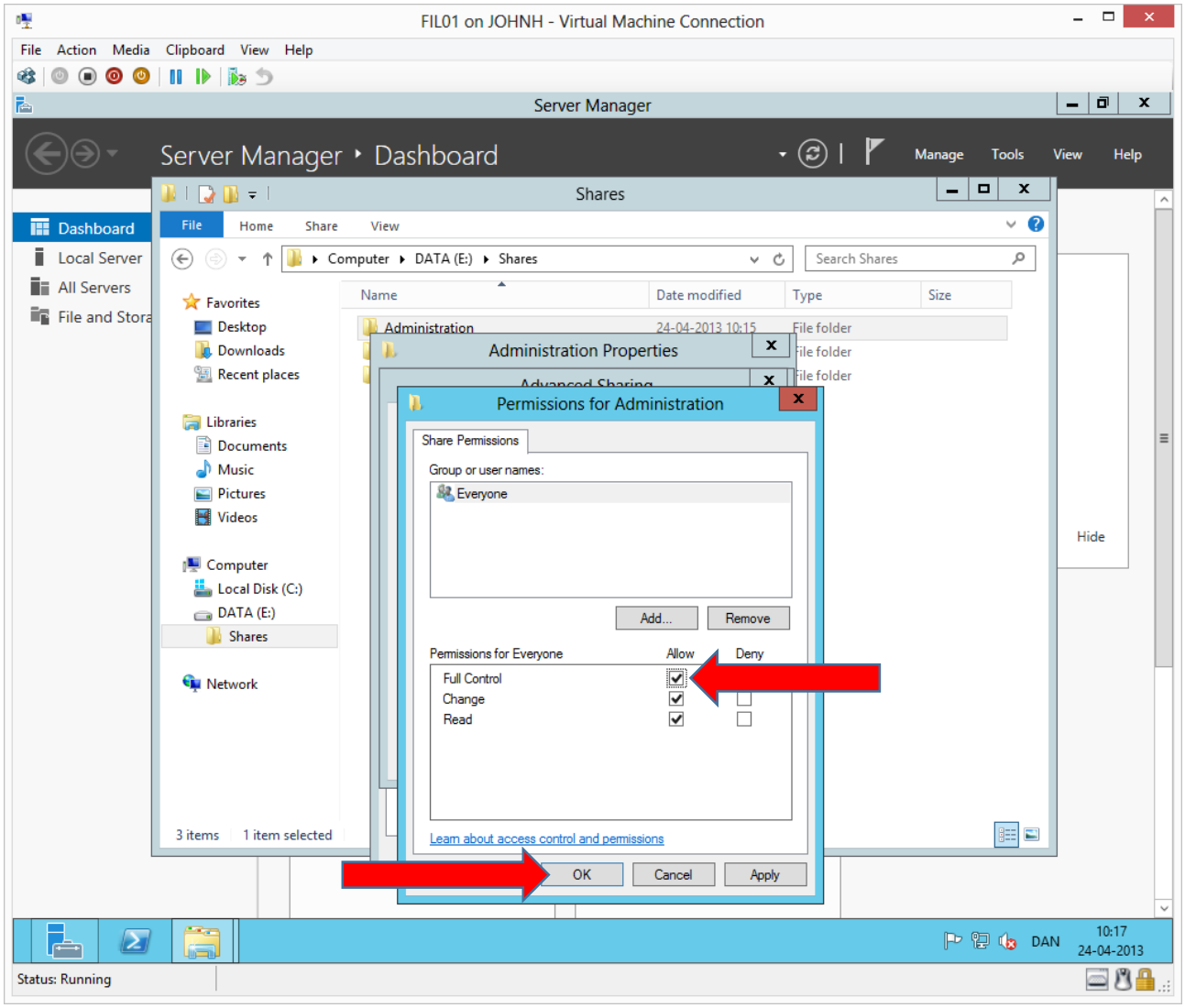
Right click the folder **Administration** and choose **Properties**

John Have Jensen

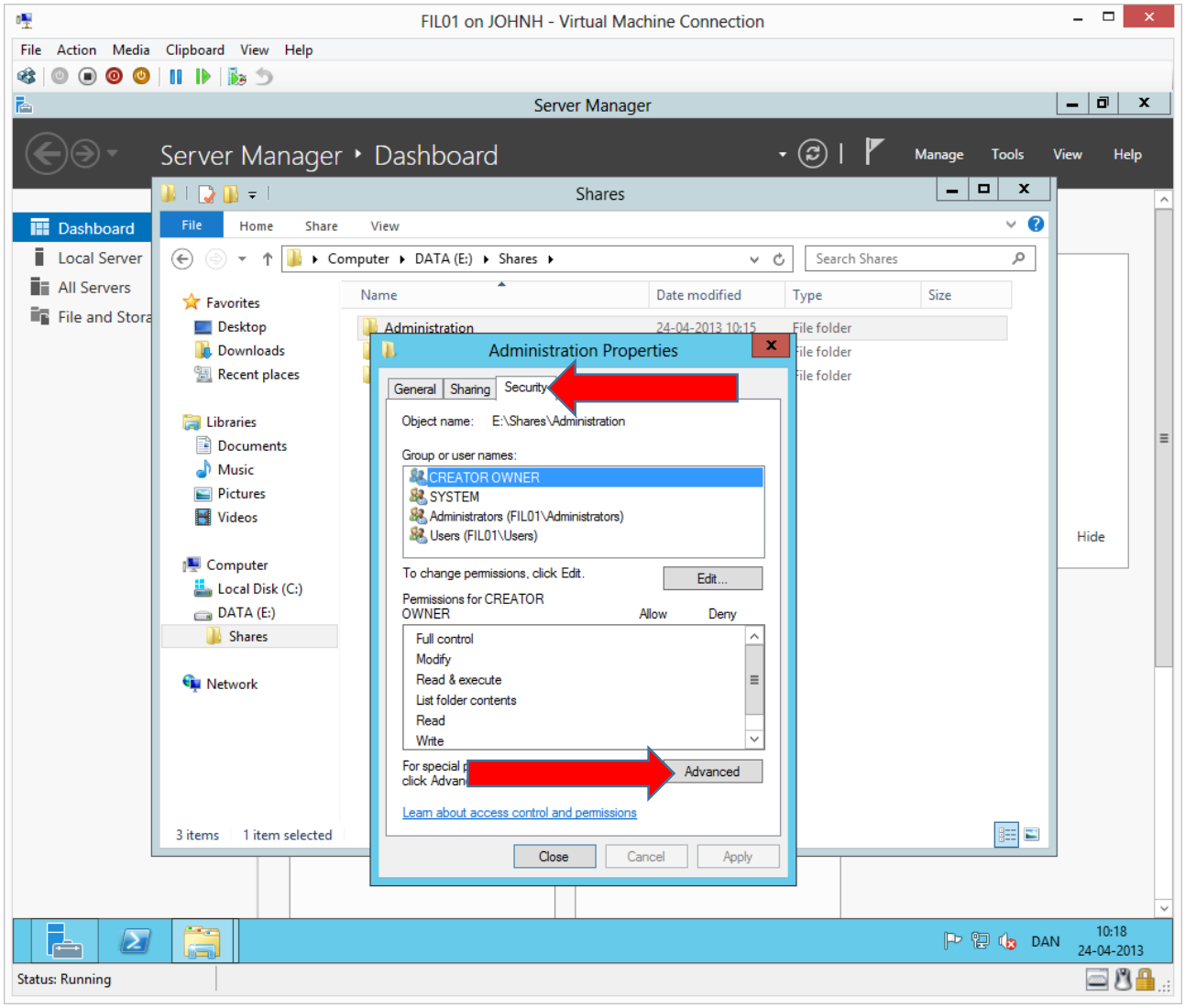


John Have Jensen



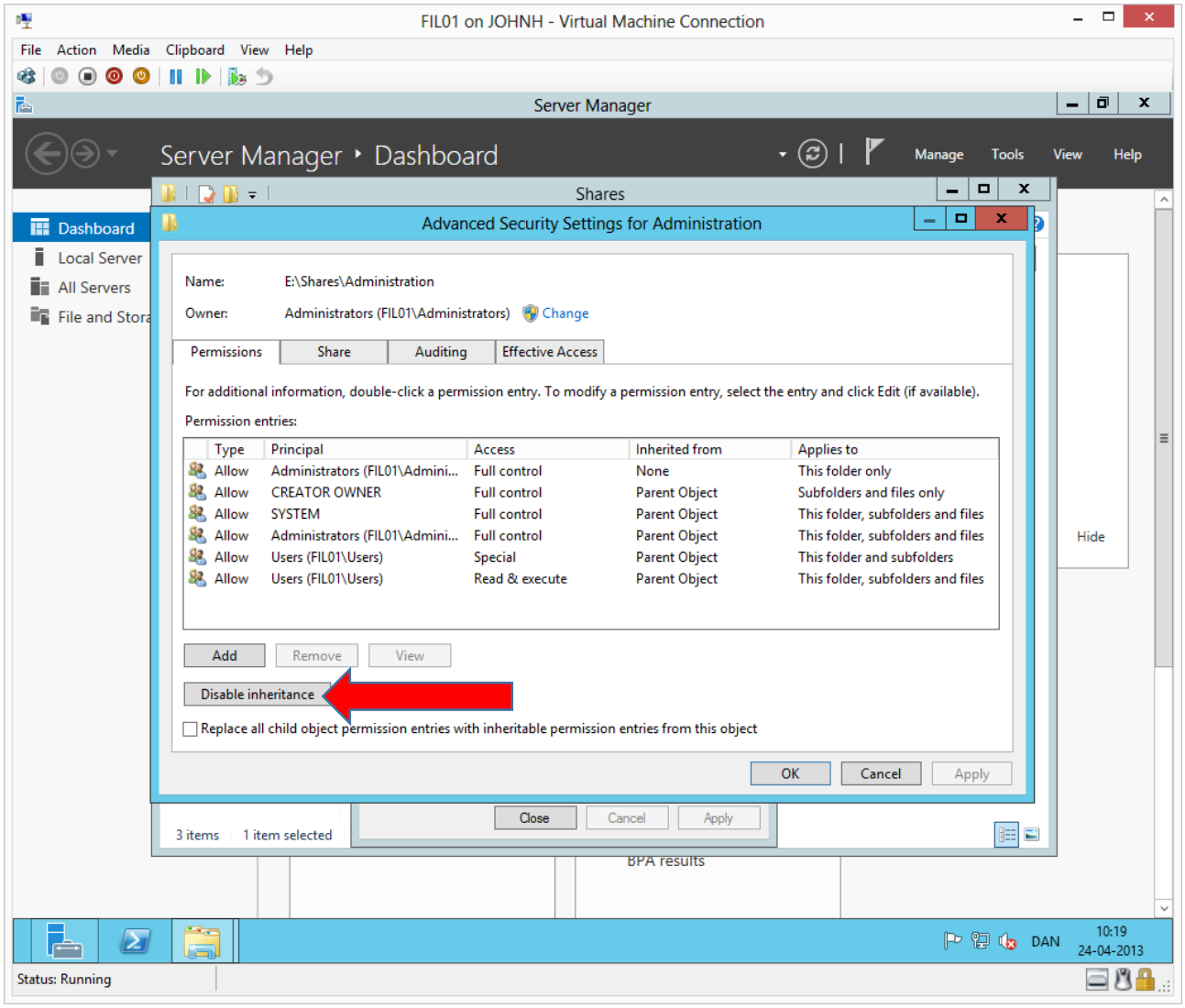


When accessing a share (making network access to a folder) the account must go through two Access Control Lists: A share ACL and an NTFS ACL. The most restrictive ACL will decide the level of access. Therefore, it is OK to make **Full Control** permissions to all accounts on the share ACL, because the account will meet the NTFS ACL afterwards and will be restricted by the level of access here. Click **OK** two times.

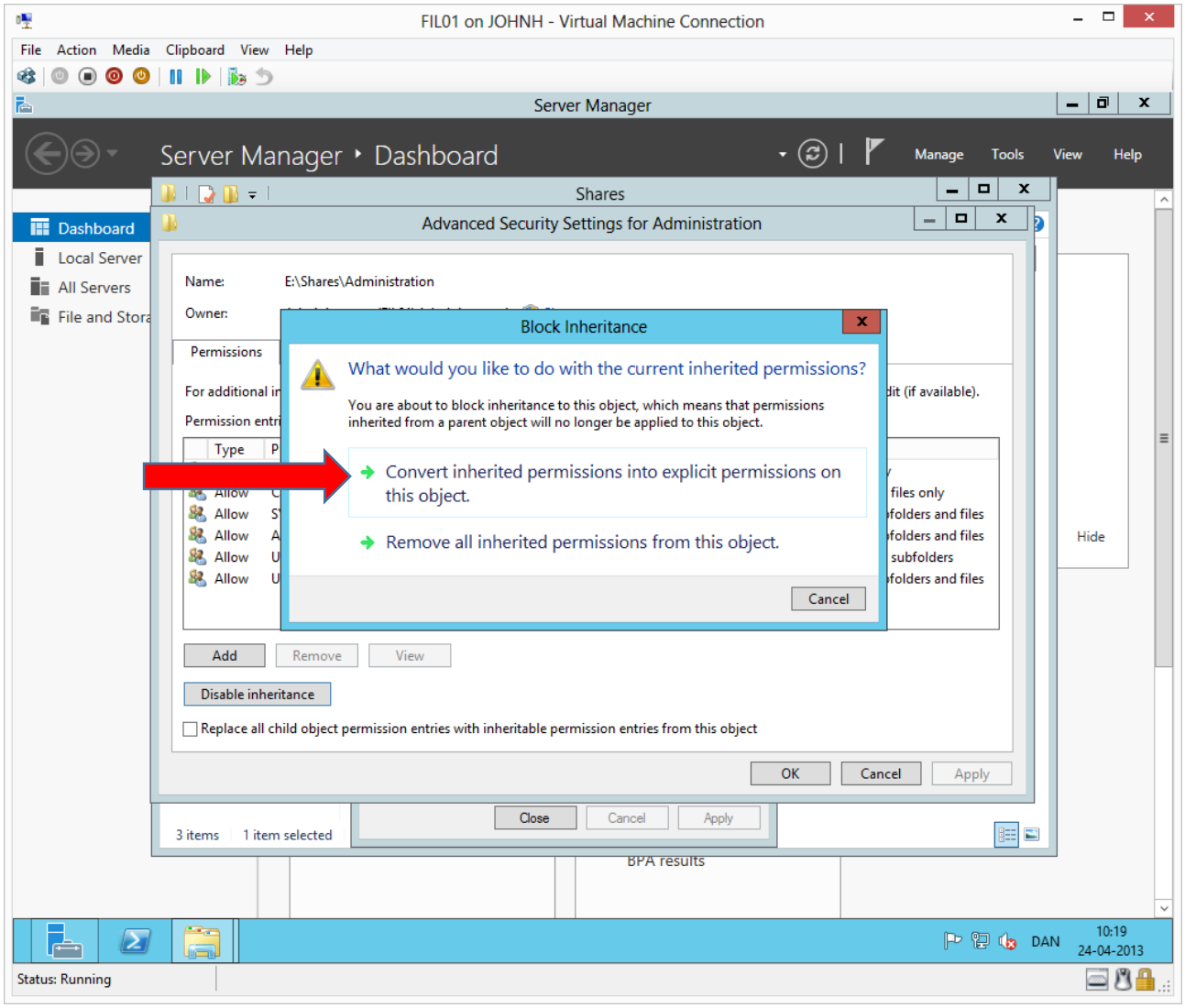


We will configure the NTFS ACL, which is located under the **Security** tab.

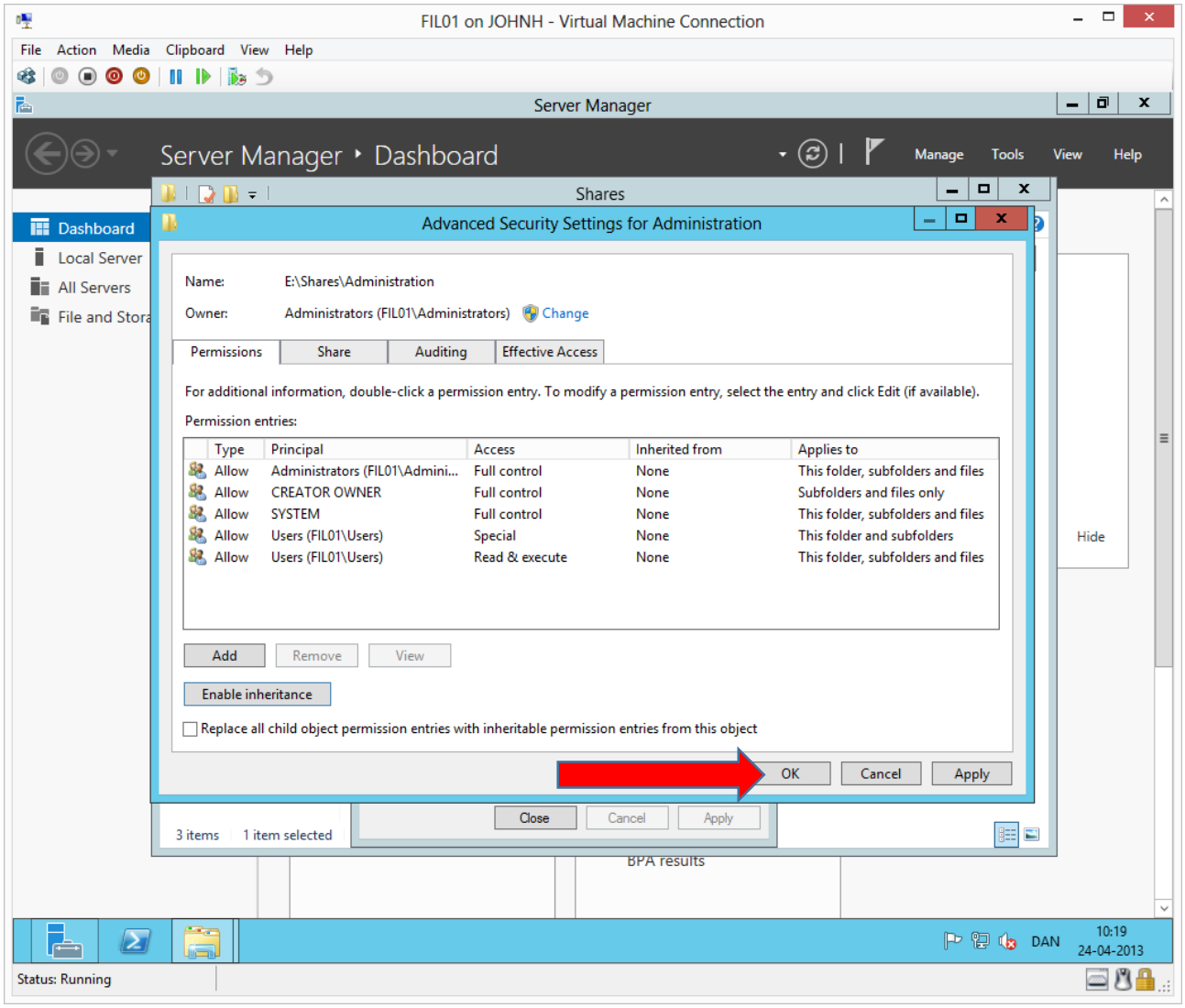
John Have Jensen



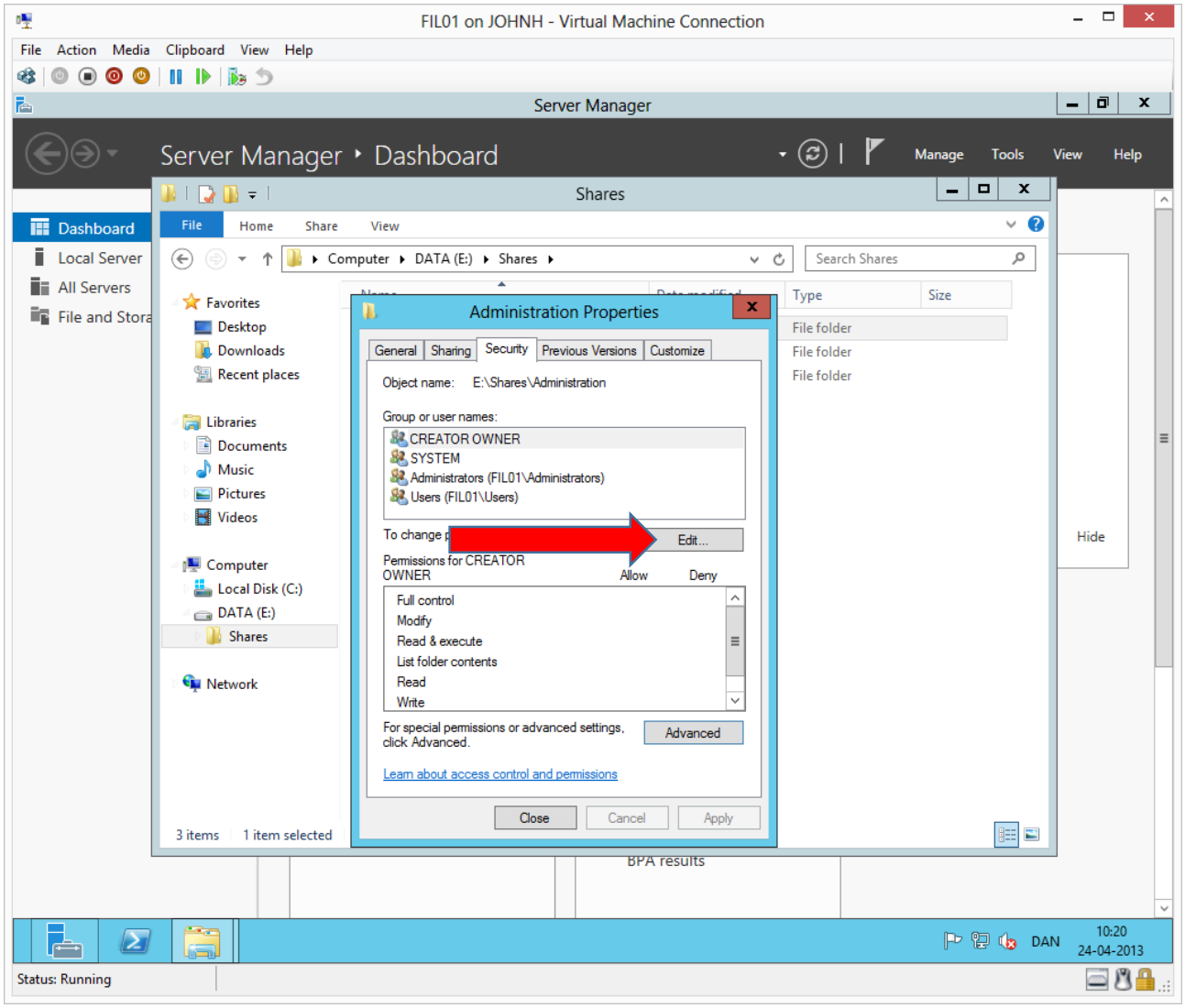
John Have Jensen

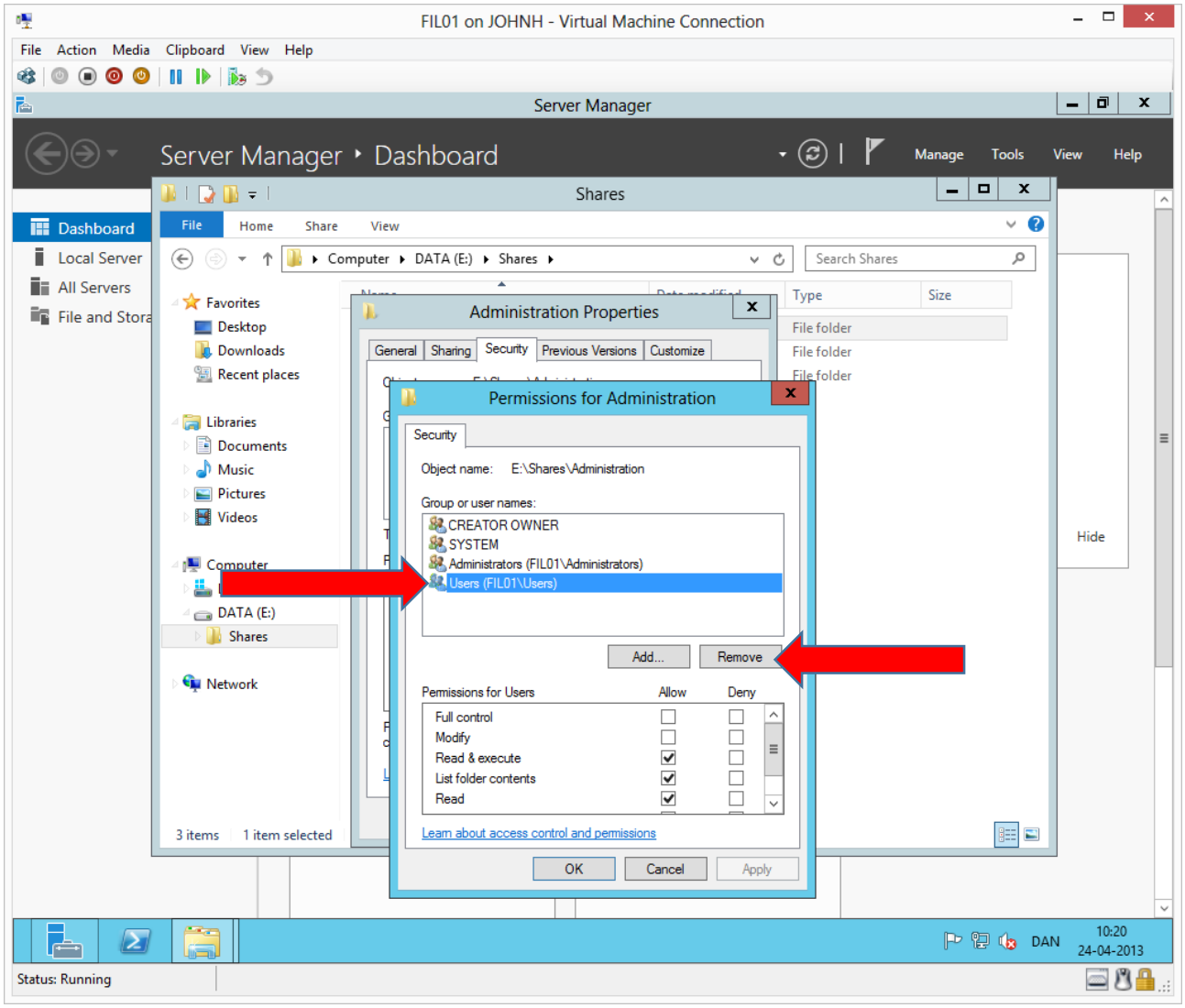


John Have Jensen

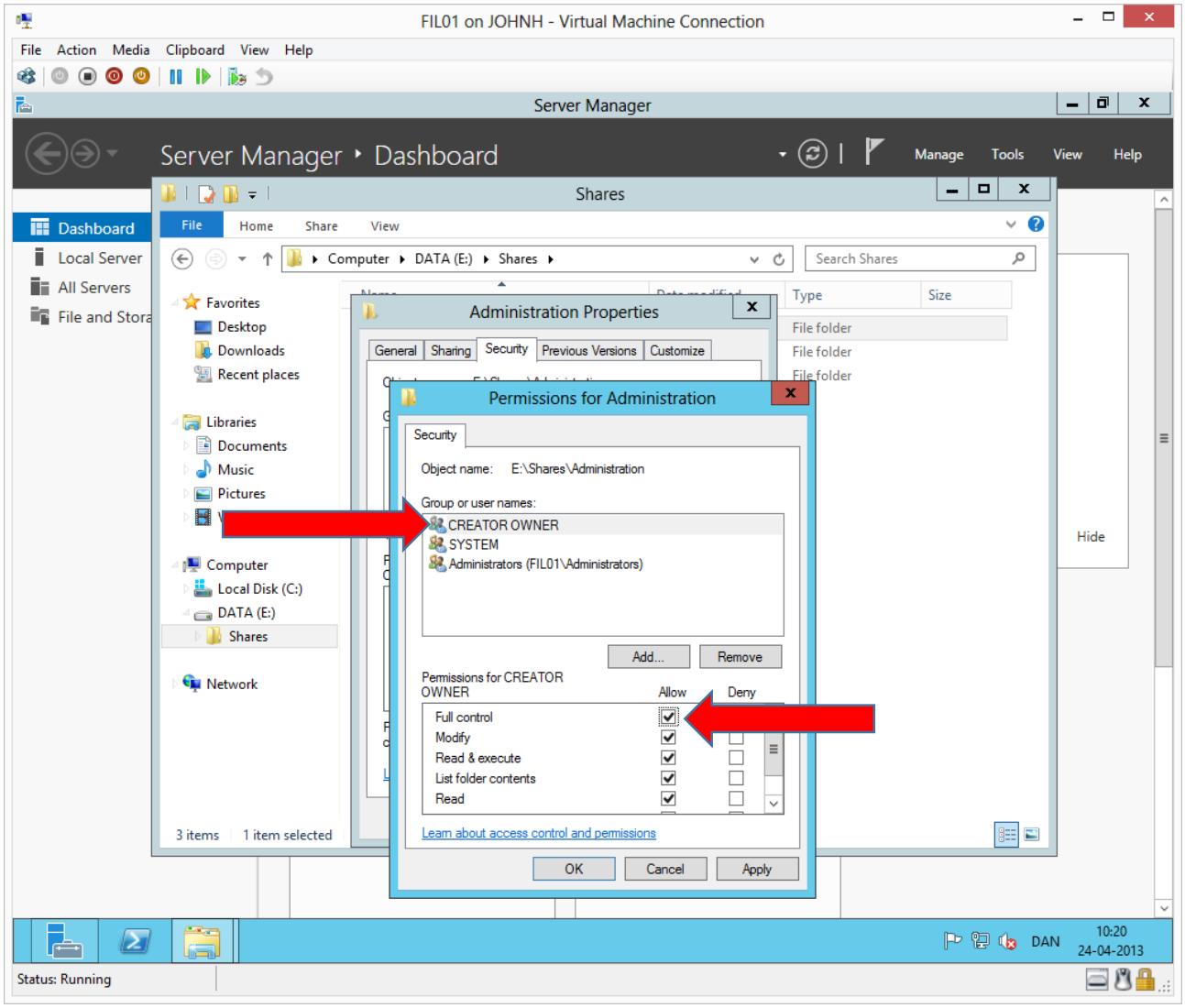


John Have Jensen



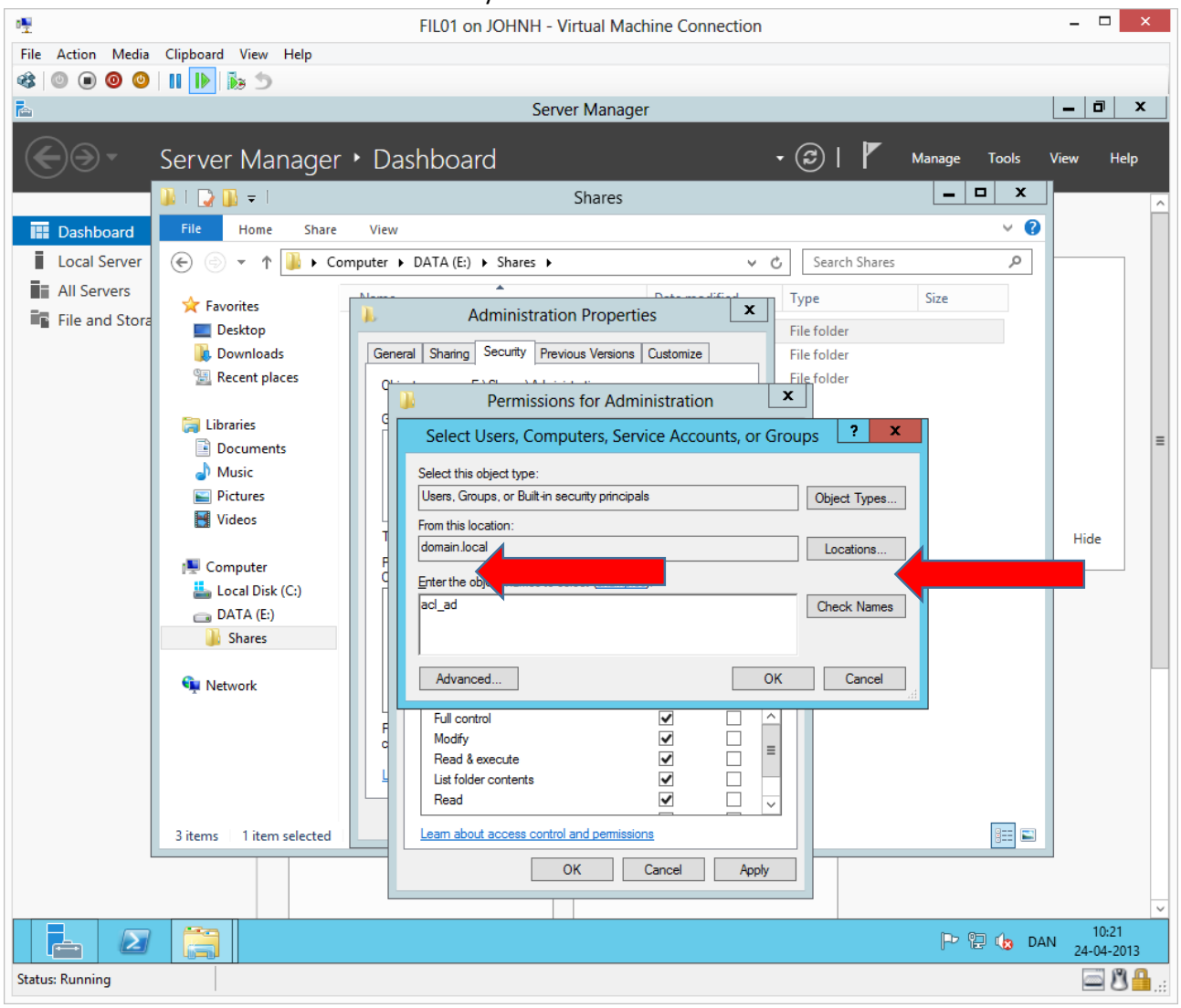


Default all users have read access. We will remove this.

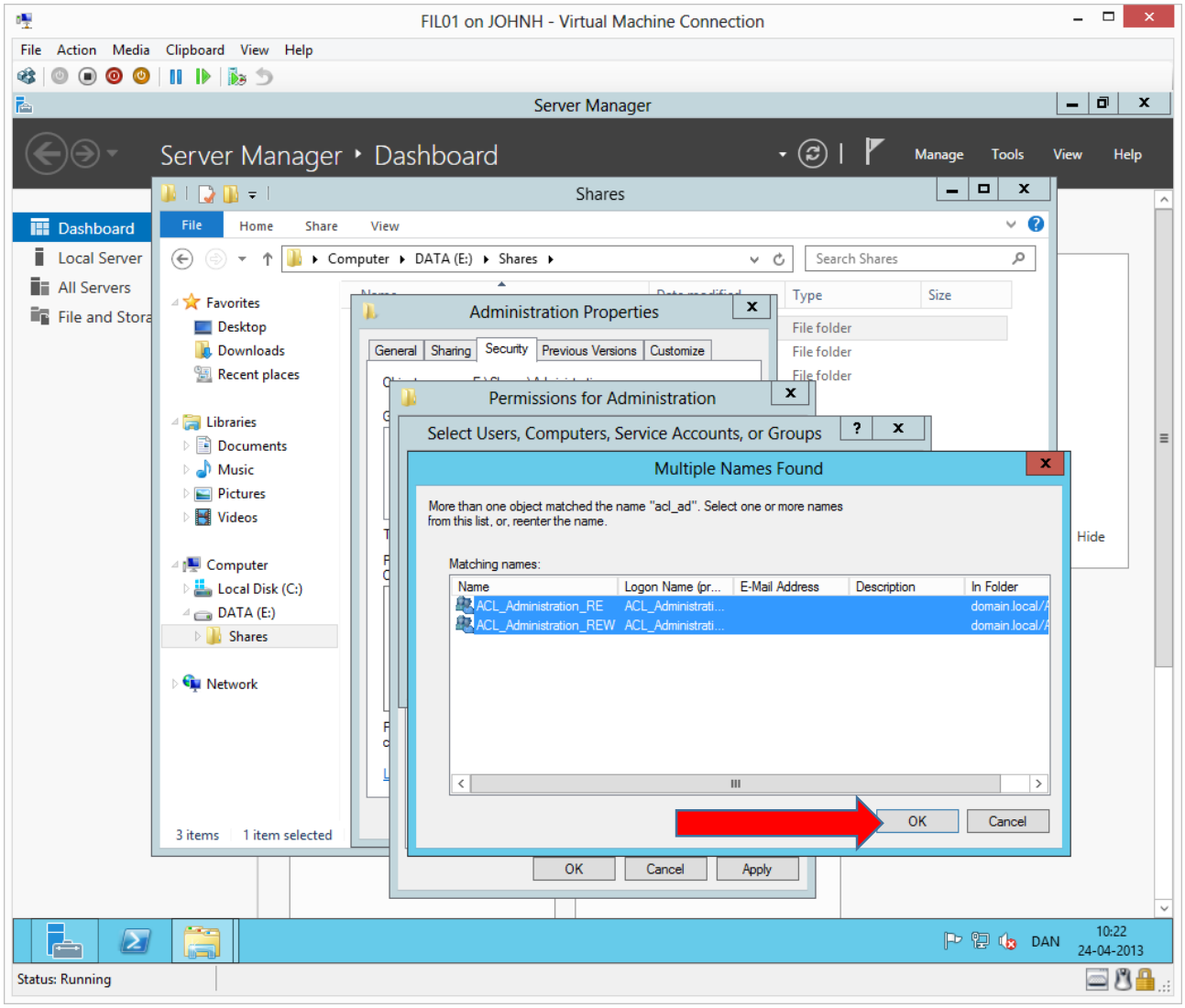


The buildin group **Creator Owner** is a special group that represents accounts that have created an object (In this case: A file or folder). If you create a new folder, only you will be Creator Owner of the folder. Therefore, we can safely give **Full Control** to the Creator Owner group, which (among other things) means

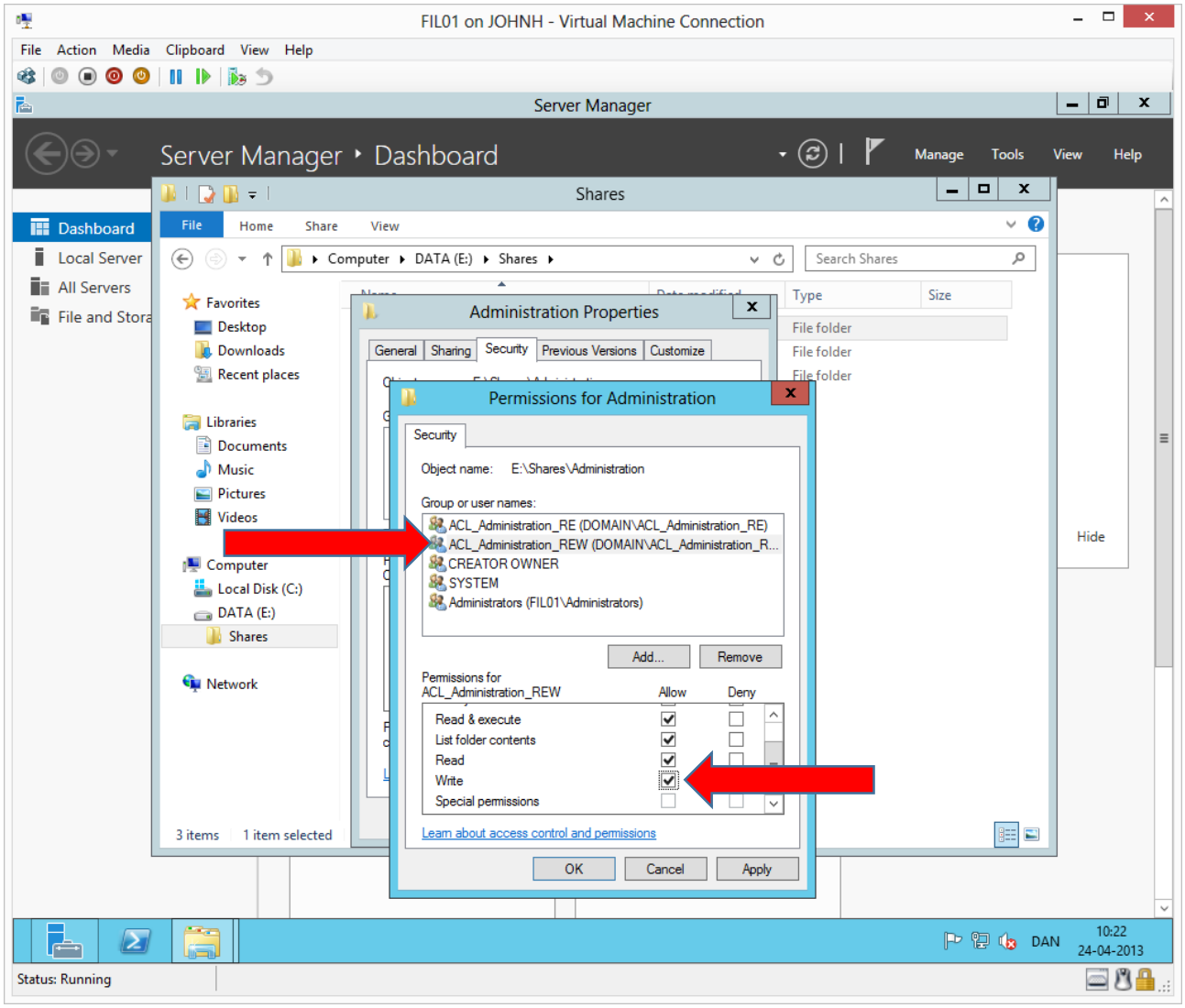
that accounts can delete files and folder they have created.



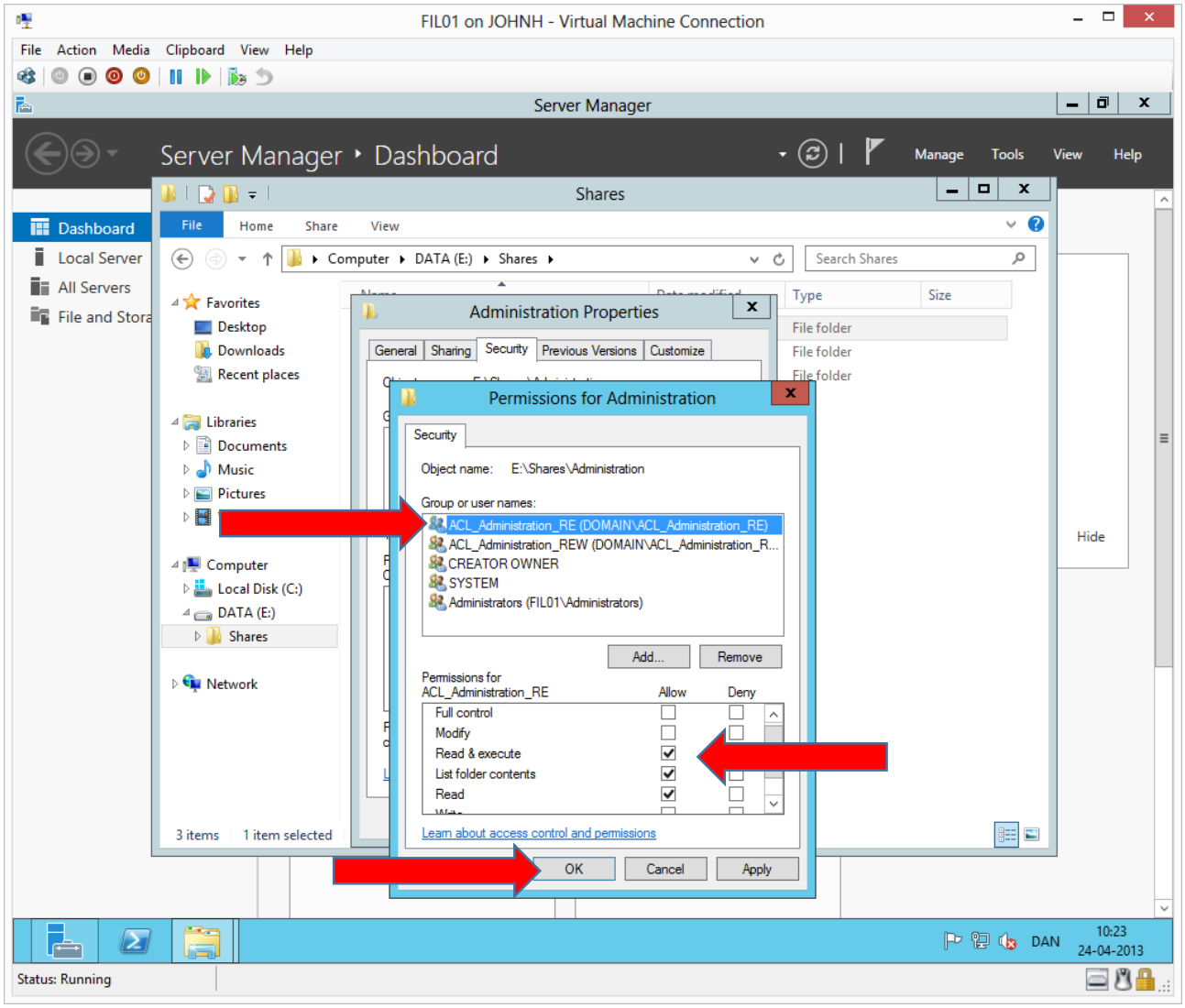
We are searching for ACL groups for the administration share.



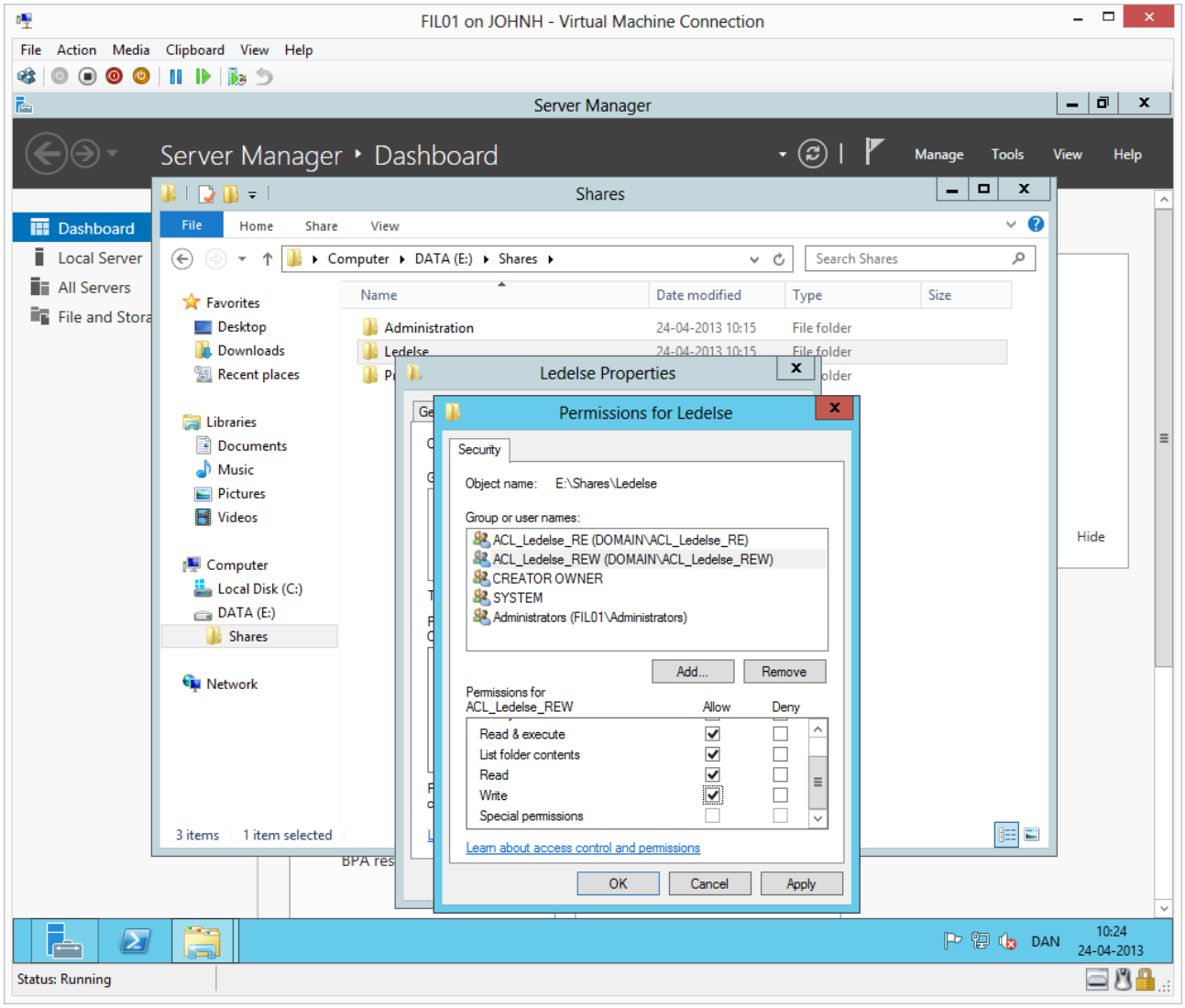
There are two ACL groups for the Administration share. Mark both and click **OK** twice.



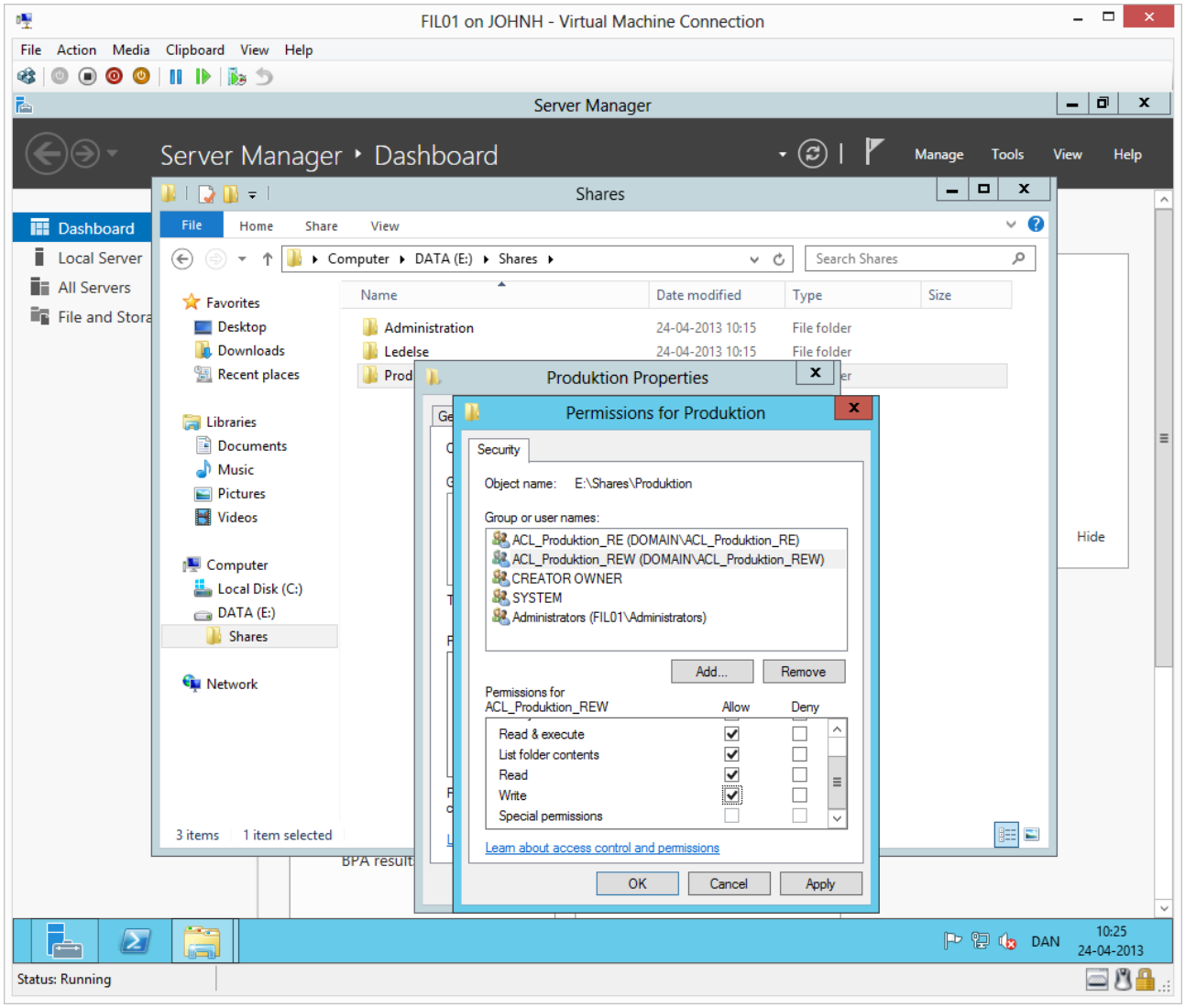
Mark the REW group and check the permissions needed as specified by the group name.



The RE group need no changes, as Read & Execute is default. **List folder contents** and **Read** is a part of Read & execute.



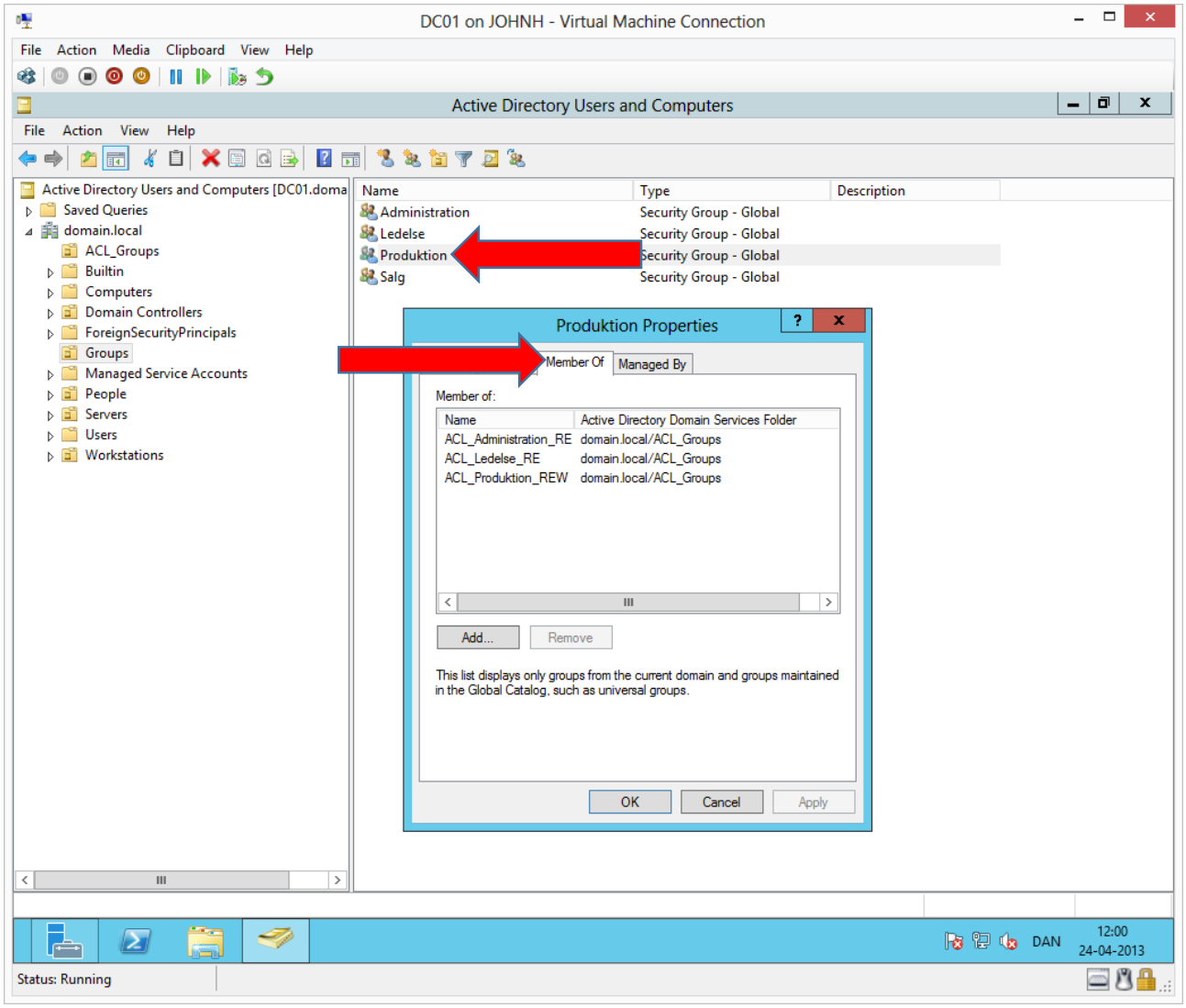
Share the last two folders; add the correct groups and the correct level of permissions. **Ledelse (Management)** NTFS ACL is shown above.



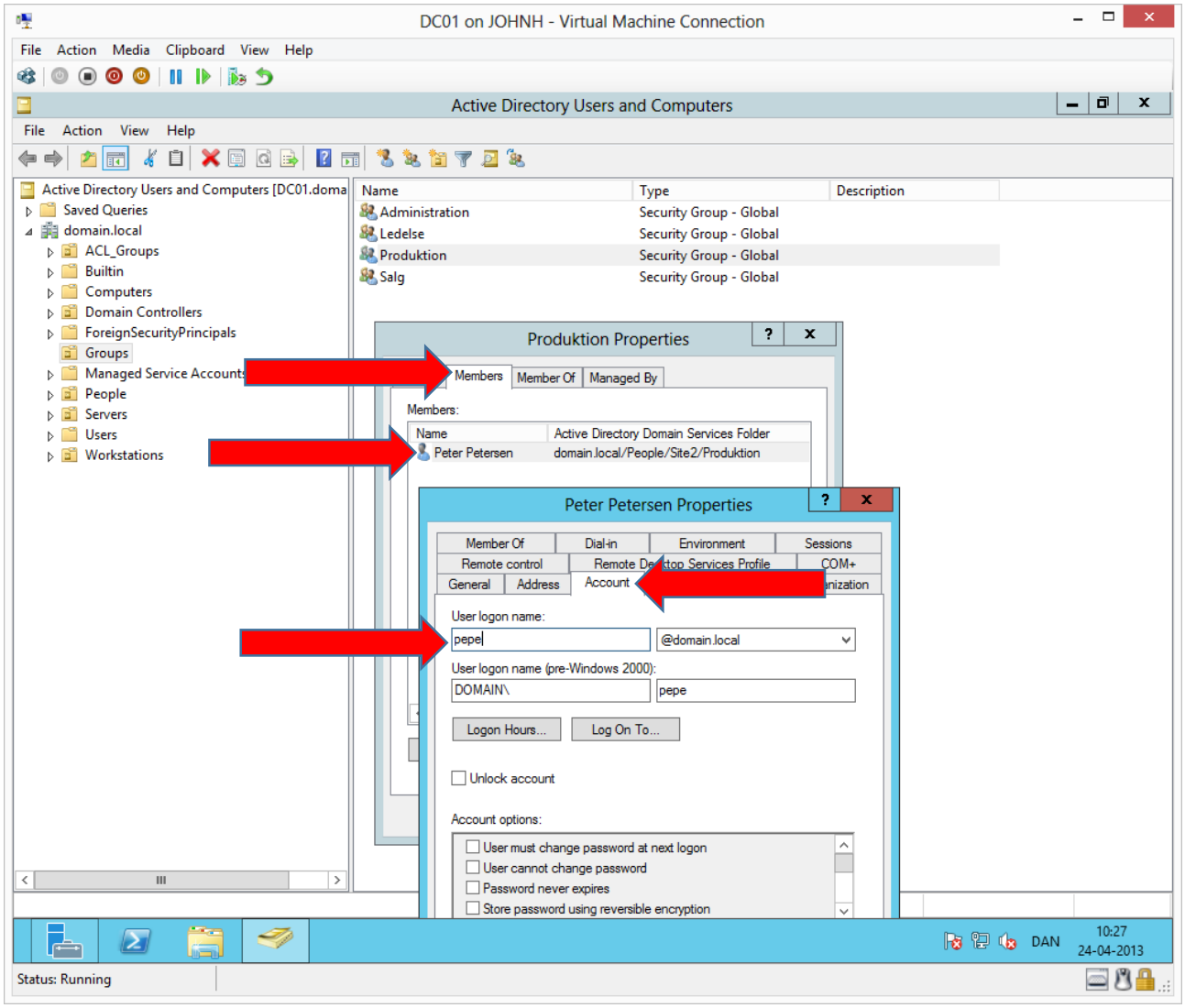
This is the **Produktion (Production)** NTFS ACL.

Verify the permissions

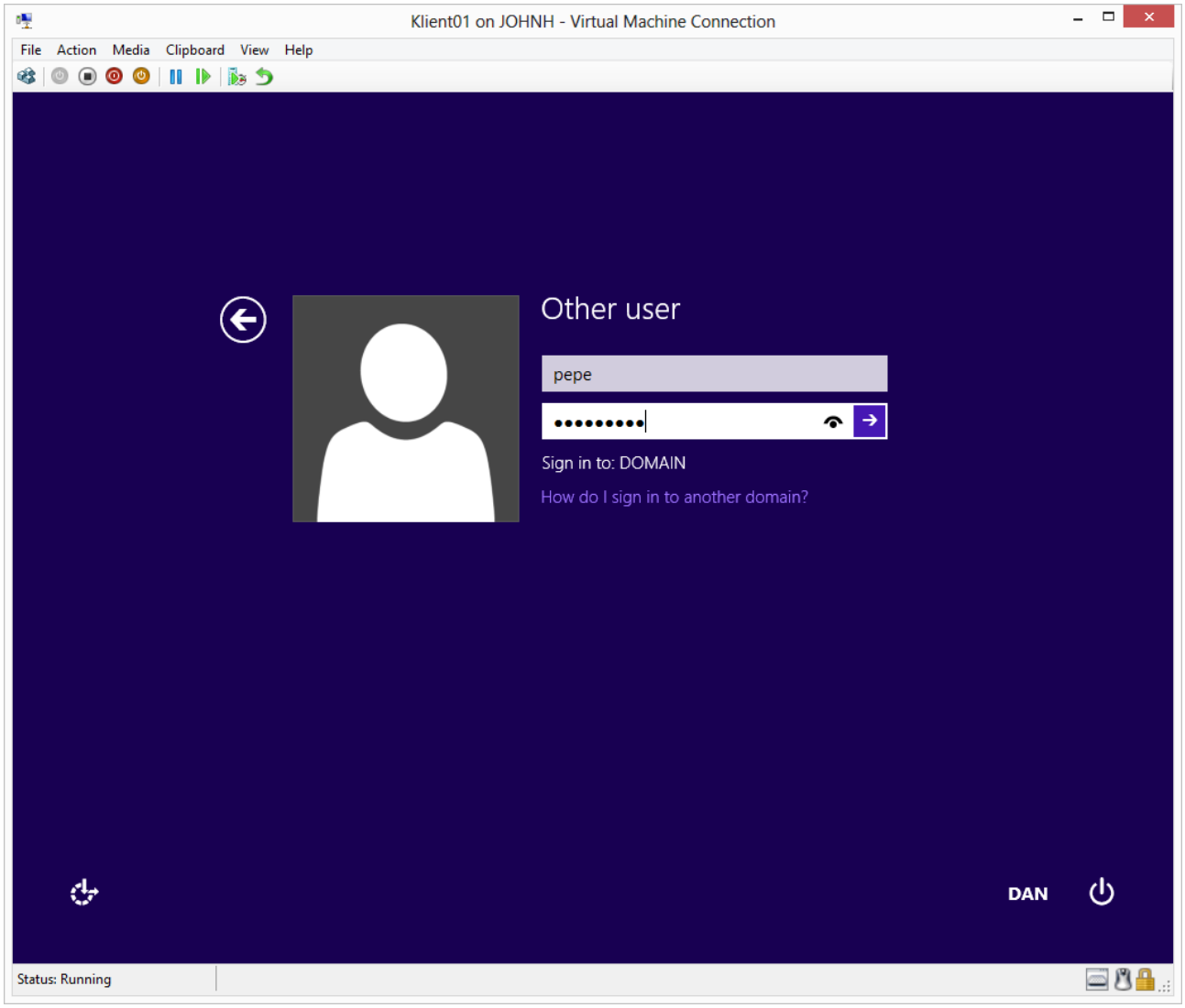
If Access Management has been configured correctly, the users should now have access to the three shares in relation to the scheme.



Under properties of the global group **Produktion (Production)** and under the **Member Of** tab we can easily see which permissions the department has. This method for Access Management is self-documenting.

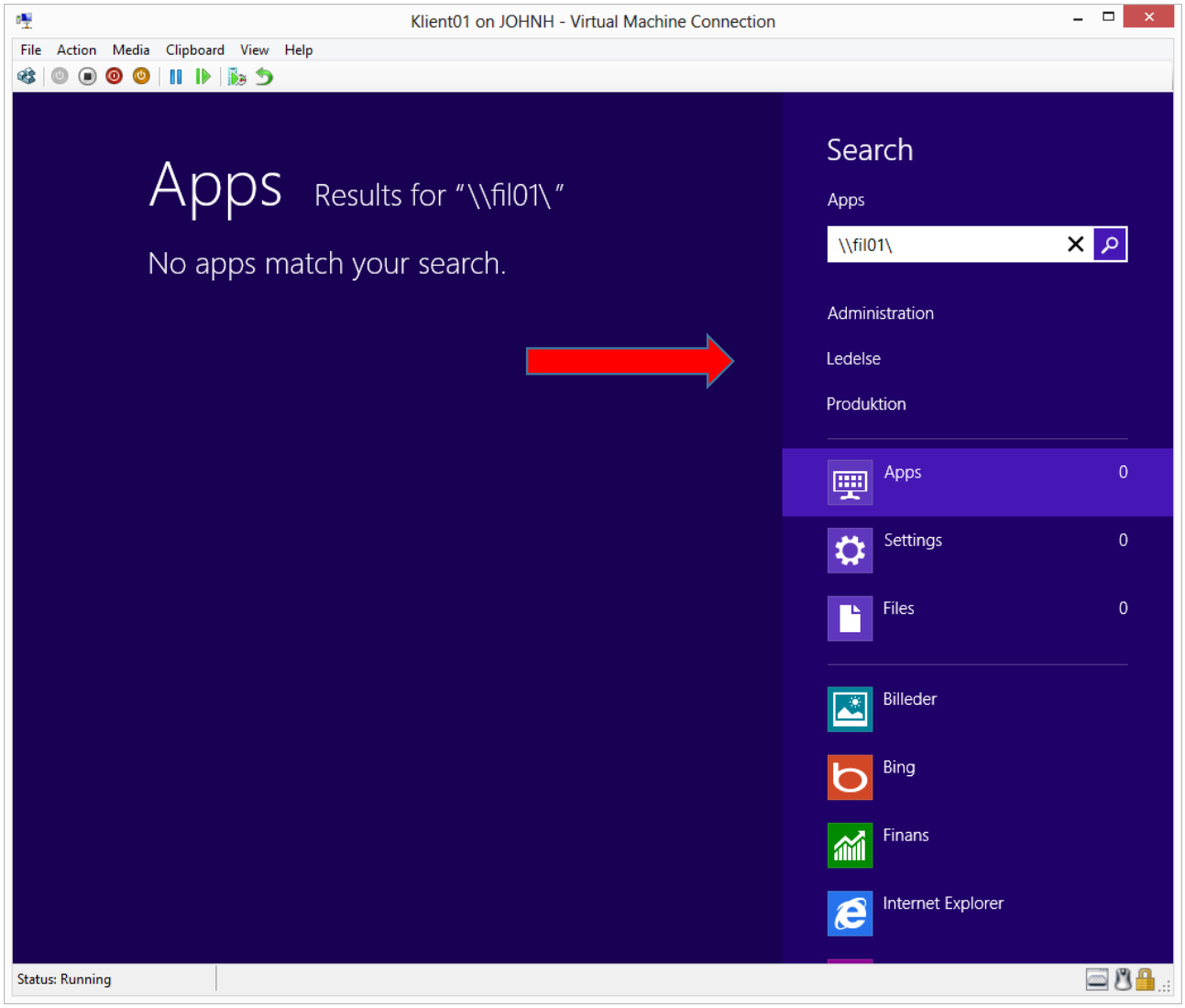


Under the **Members** tab, we can see which users are member of the global group (The department). If we double click on **Peter** and go to the tab **Account,** we can see the user logon name: **pepe**.



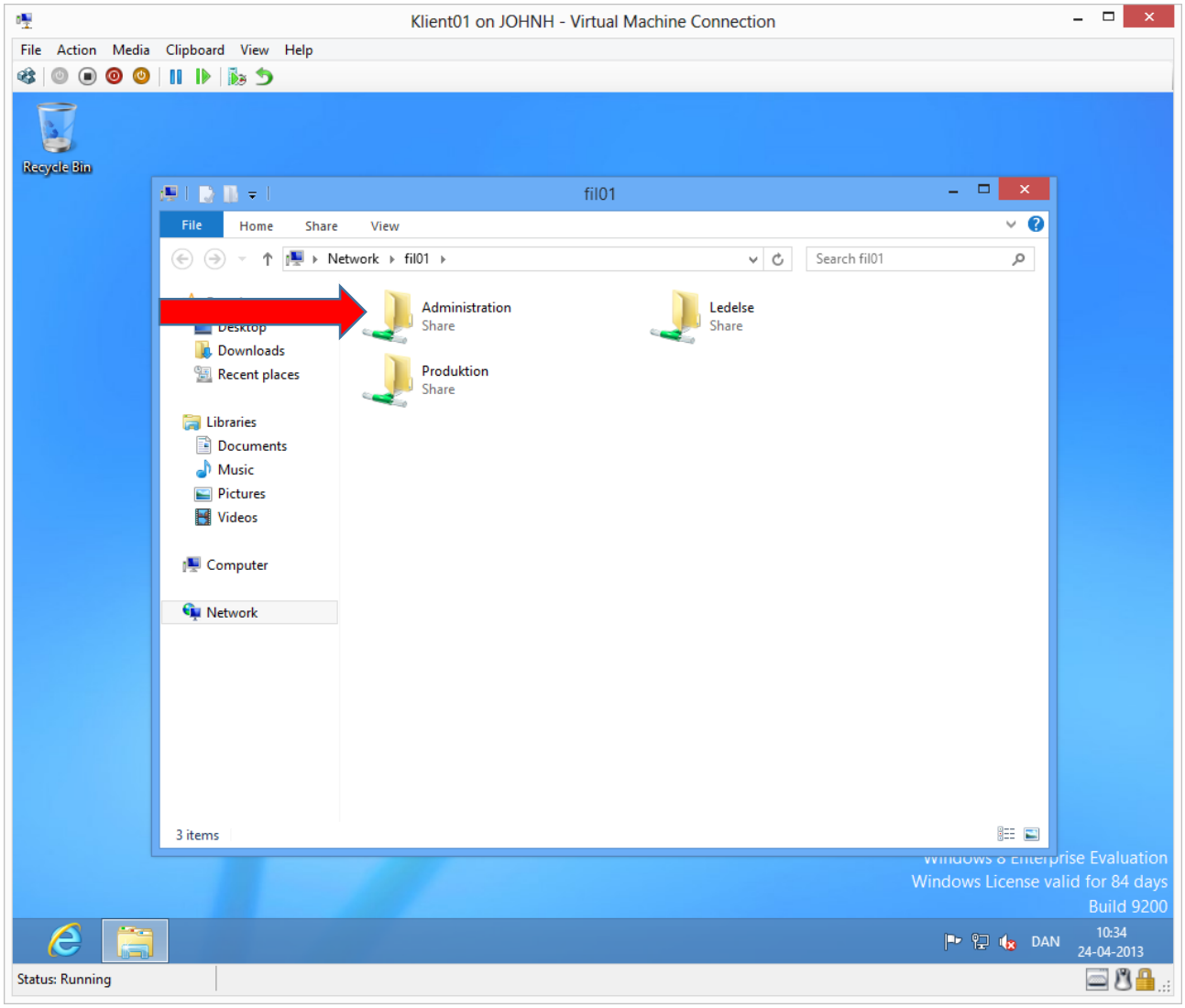
We will test the permissions by logging onto Klient01 with Peter.

John Have Jensen

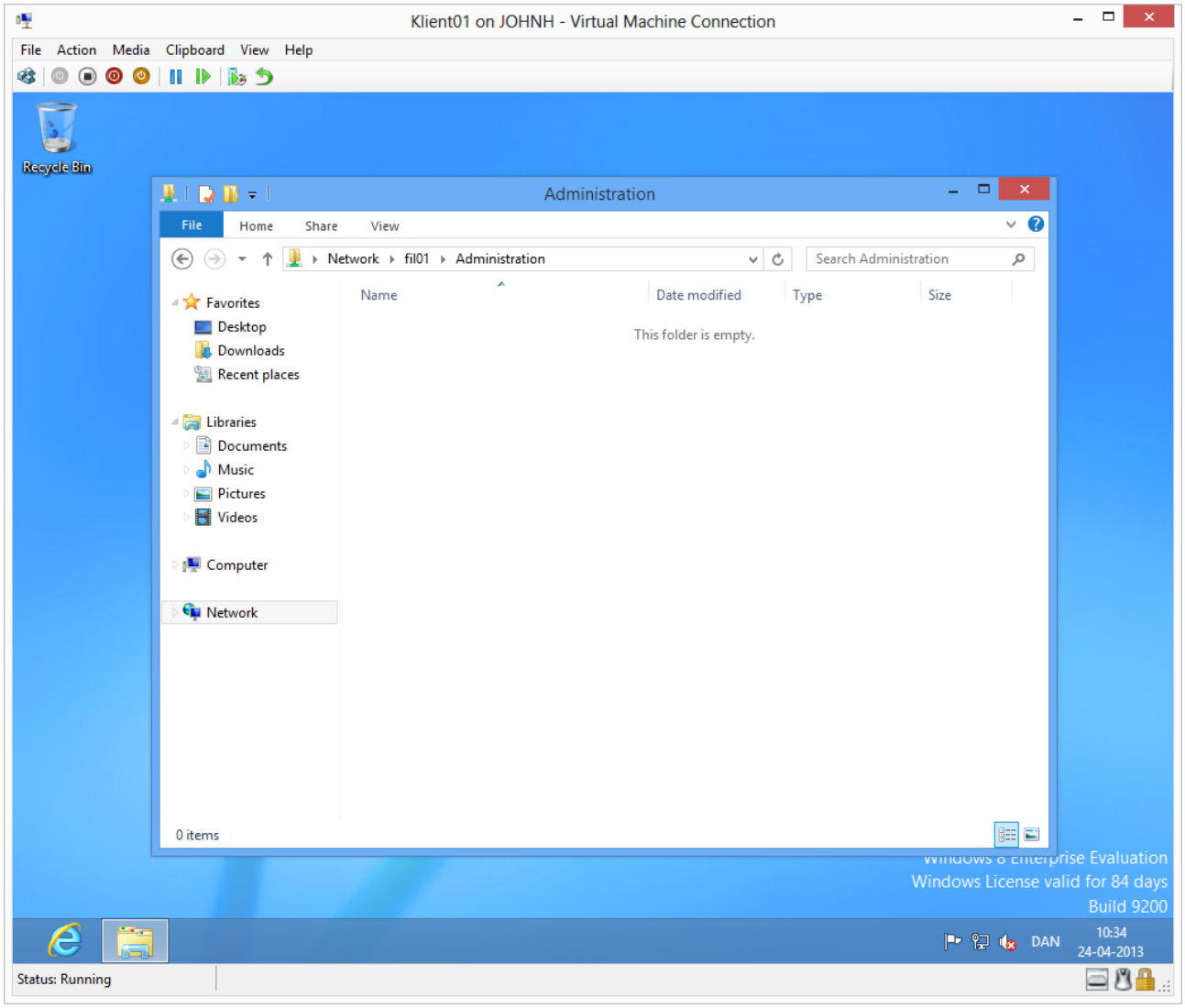


At the Windows 8 start screen type: **\\fil01** and the computer will list the shares on Fil01 as shown above.

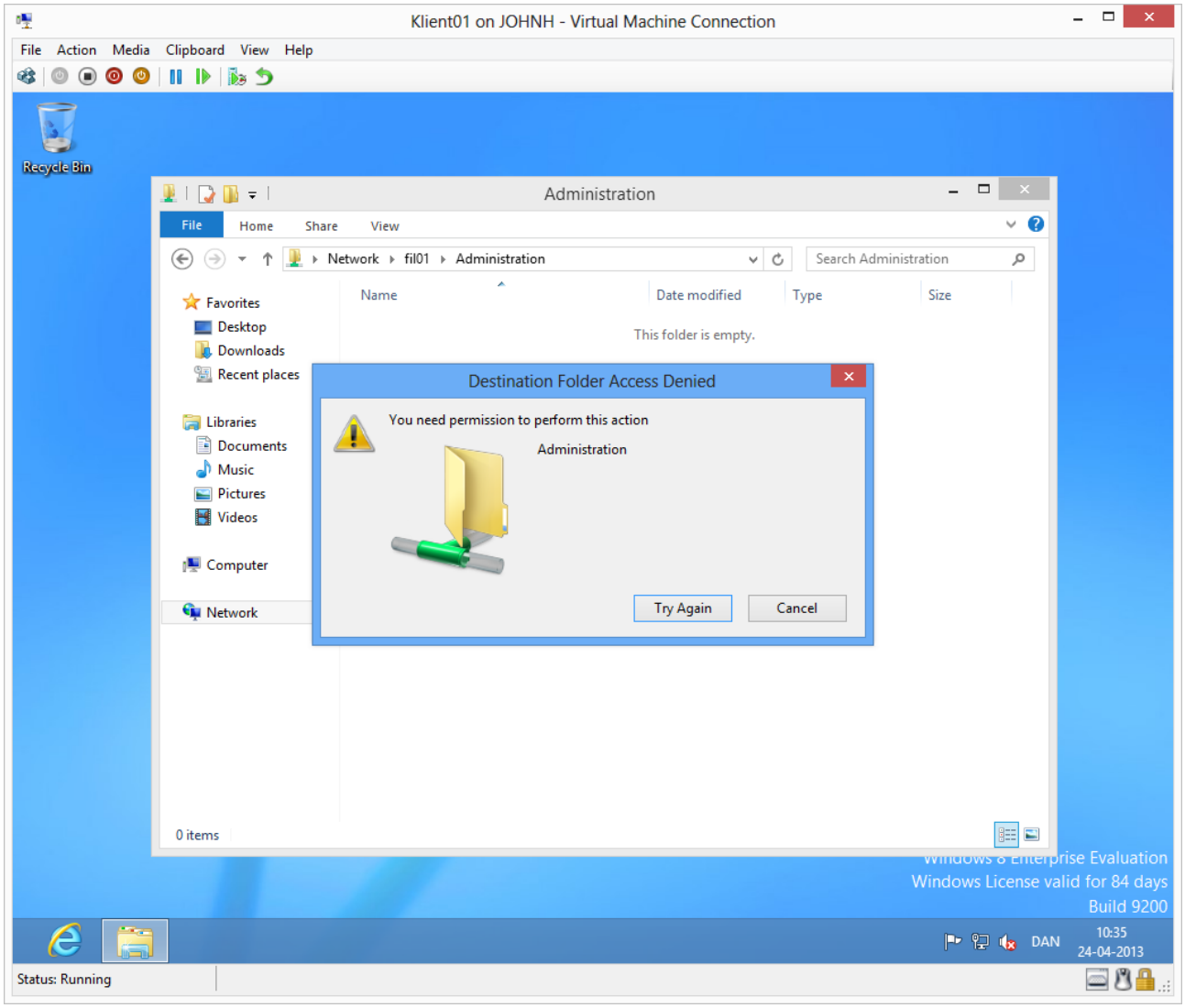
Press **enter** to open Windows Explorer.



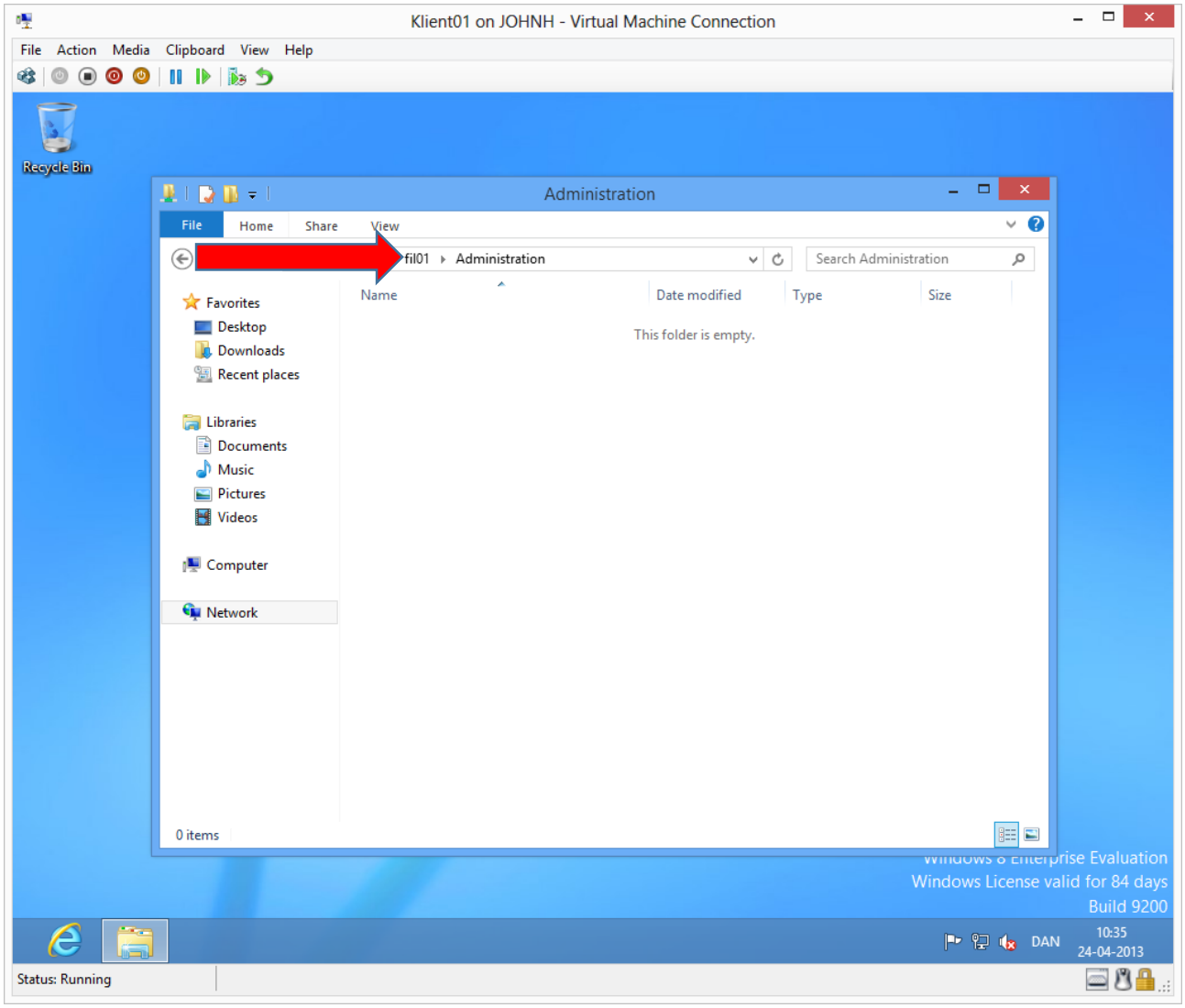
Open the **Administration** share.



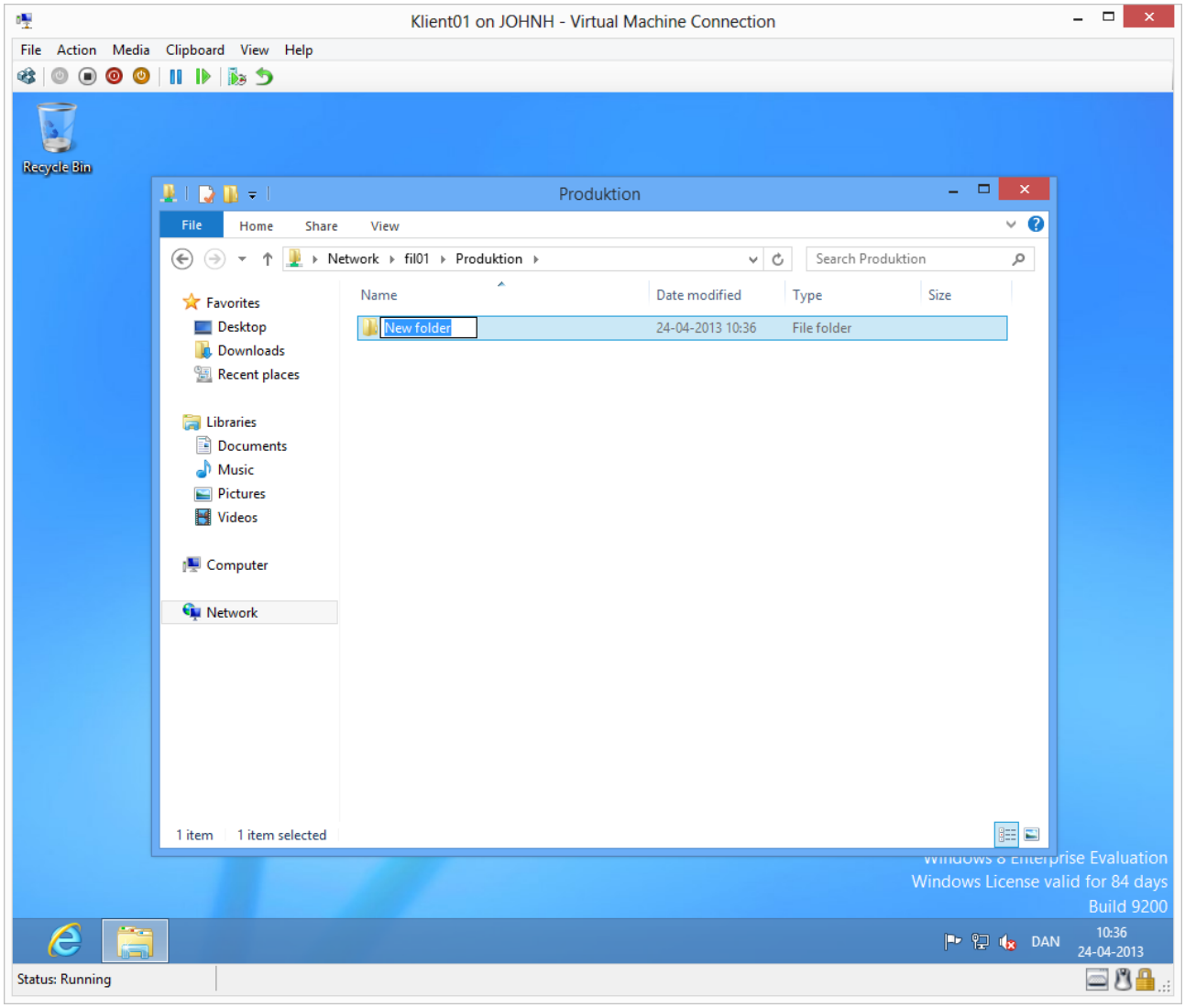
If the folder opens, Peter has read access, otherwise an access denied message would appear.



Try to create a folder or file. The above message should appear because the Production department should not have write access to the administration share.

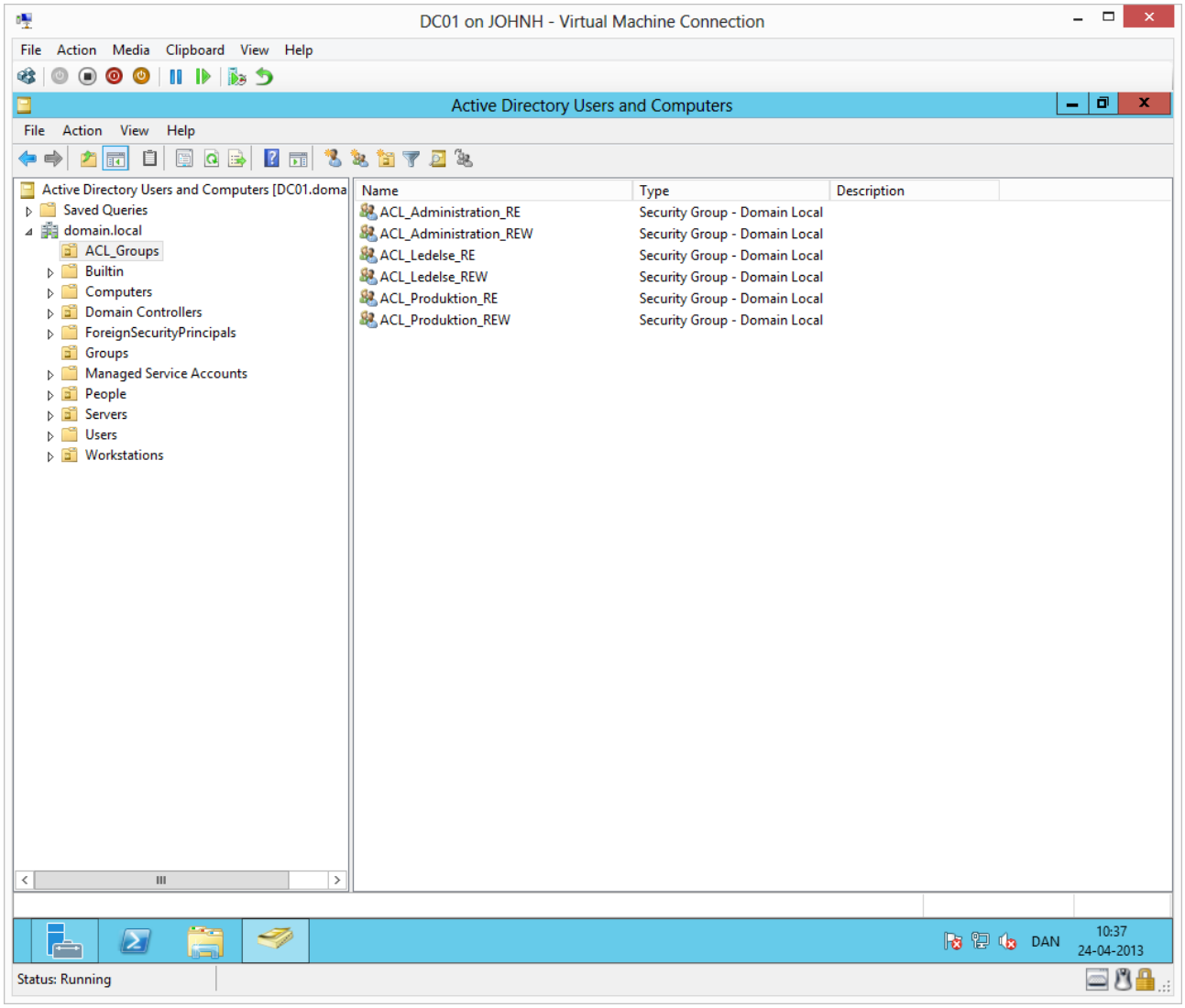


Jump back by clicking **fil01** and open the Produktion (Production) share.



You should be able to create a file or folder her, as the Production department has write access to the production share.

As the write permission does not allow deletion of objects, Peter will get this permission from his membership of the system group Creator Owner, which has Full Control.



If other users need any of the above permissions, this can be controlled from Active Directory Users and Computers solely, by managing group memberships. No changes are necessary on Fil01.

If later, the need arises, for other types of permissions, new ACL groups must be created and one would have to go through the process again with global group membership of ACL groups (domain local) and adding the ACL groups to the ACL on the fileserver.