Best Practice Security - Windows file sharing Lab

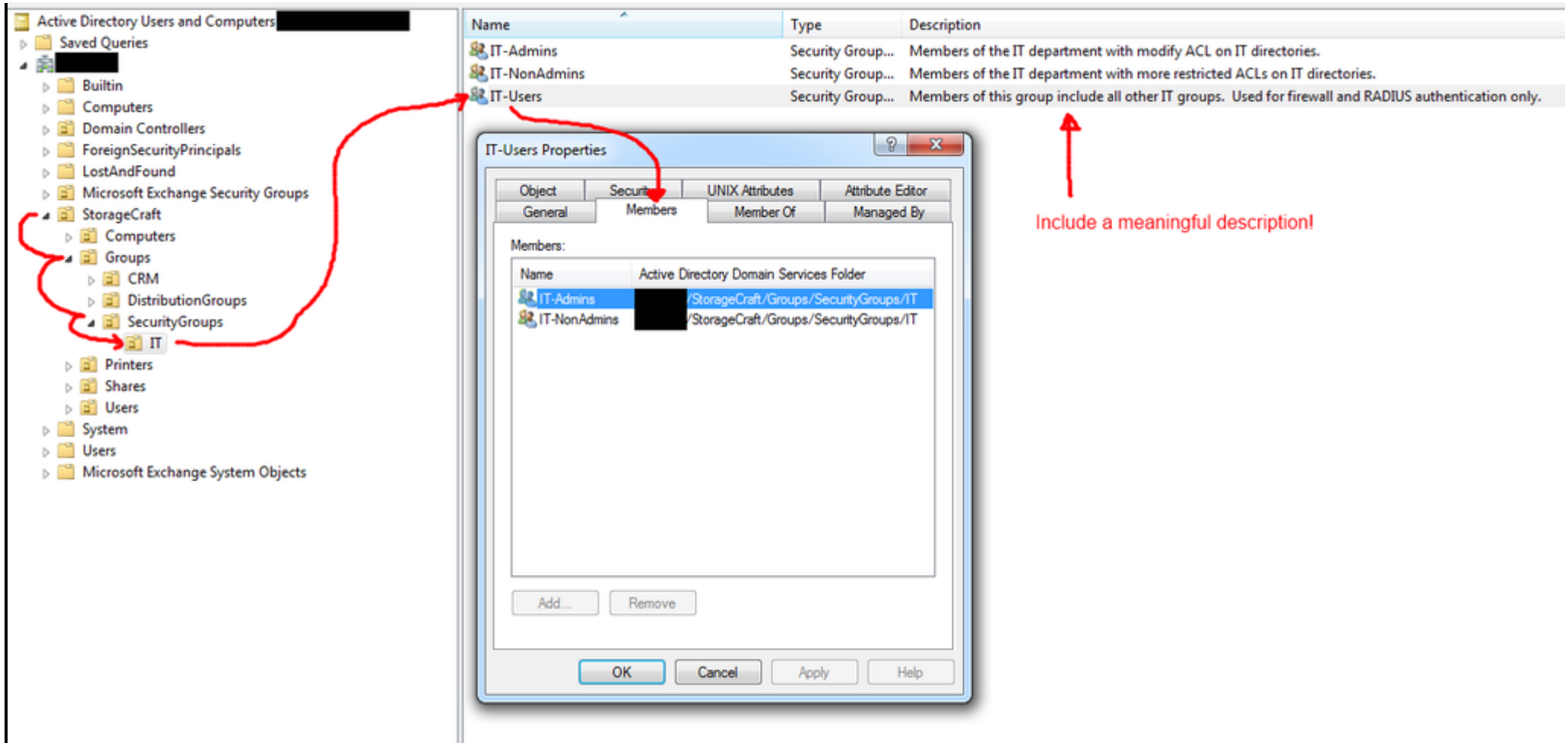
Introduction

I will be outlining several best practice techniques I have used and bettered over the years with the goal of giving least privilege access to file shares on a Windows Server 2008R2 Domain. Microsoft has given it's list of file sharing best practices (see References) without any implementation guide. This guide addresses several of those listed best practices (namely the ones that are security centered) and walks you though how to implement and audit them.

Steps (7 total)

1

User and Group Organization



You cannot effectively implement network shares according to any best practices without organized Active Directory groups. Because I work here, let's use StorageCraft as an example. StorageCraft is creating a share for its IT users. Their Active Directory groups OU structure looks like so:

StorageCraft (Top Level) > Groups > IT

Within the IT OU, there are three groups:

1) IT-Users
2) IT-Admins
3) IT-NonAdmins

The IT-Users group contains two members only: IT-Admins and IT-NonAdmins. The other two groups contain the user objects. The reasoning behind this is, if you want to use other network authentication services like RADIUS/TACACS or SSO, they often allow you to authenticate by group membership. There's often no reason to be extremely granular with these services, so just add the top level group whose members are the lower level groups.

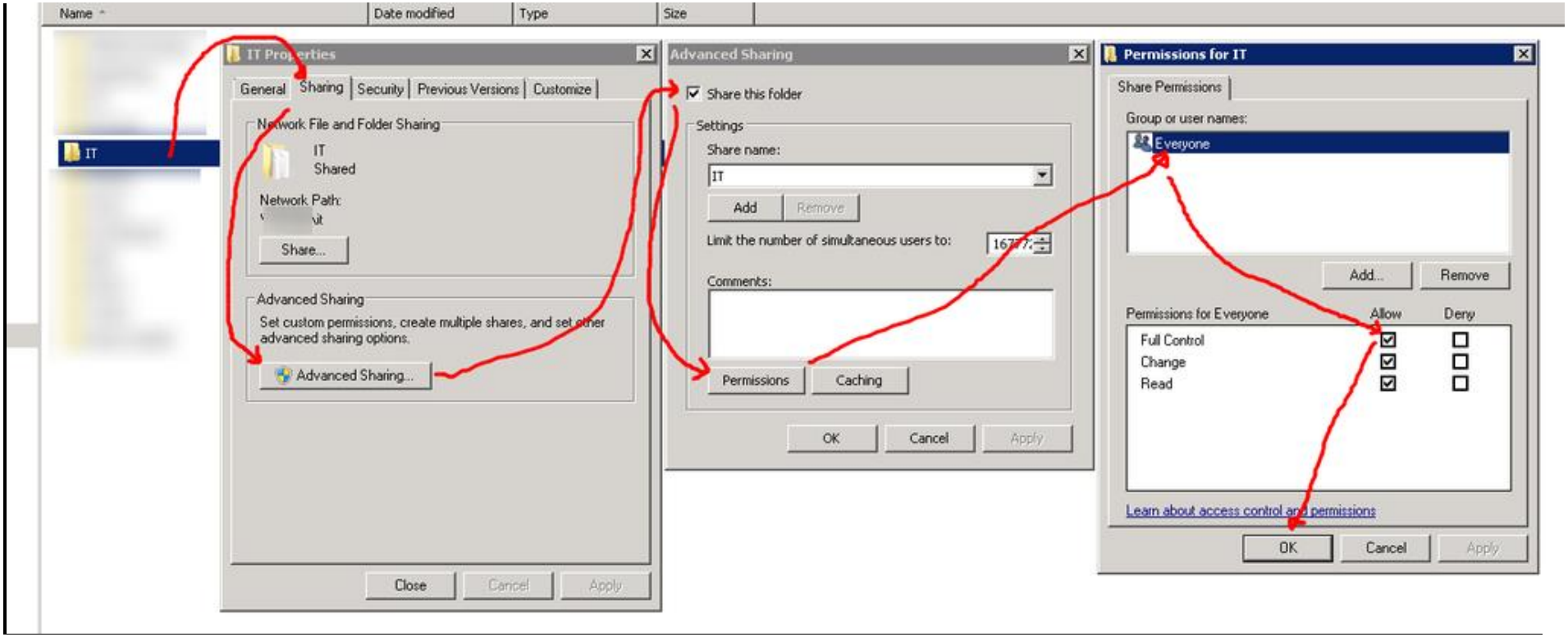
The IT-Admins group will contain members who need full or modify NTFS permissions on the IT share (which we will create in step 2).

The IT-NonAdmins group will contain members who only get read access (and in some cases write/modify) permissions to designated directories within the IT share.

You may need to create additional groups based on the type of access you will grant (read&write but no delete, or no copy, etc...). Read through this article, then decide if that's something you need.

2

Create the folder and share it



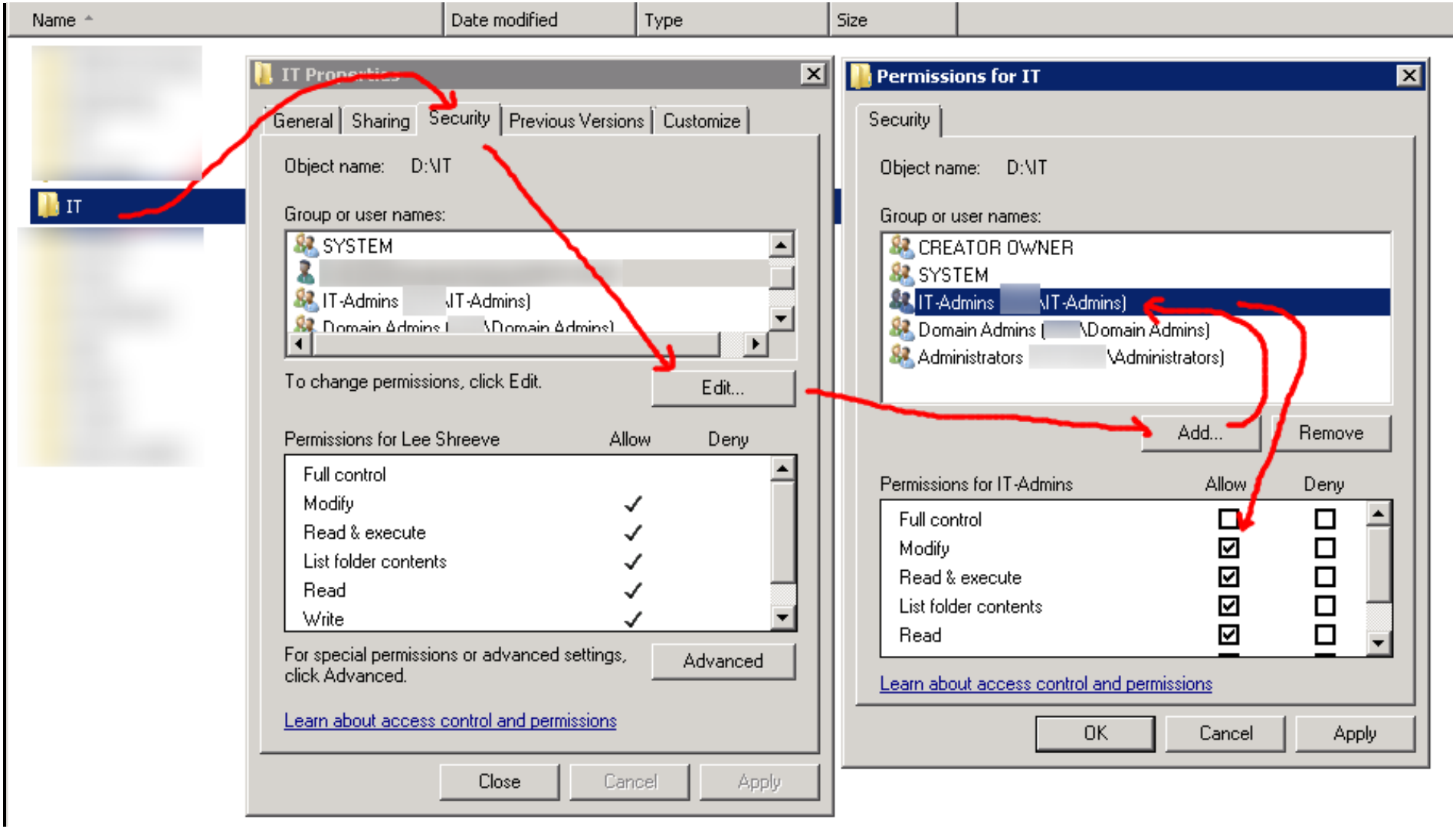
Echoing some of the best practices set forth by Microsoft:

1) Use centralized data folders.
2) Use intuitive, short labels for shared resources.
3) If users log on locally to access shared resources, such as on a terminal server, set permissions by using NTFS file system permissions or access control.

Create a folder and share it. We will restrict users at the NTFS permission level in step 3.

3

Set NTFS permissions



Echoing some of the best practices set forth by Microsoft:

1) Assign permissions to groups, not user accounts.
2) Assign the most restrictive permissions that still allow users to perform required tasks.
3) Limit membership in, and assign the Full Control permission to, the Administrators group.
4) In most cases, do not change the default permission (Read) for the Everyone group.
5) Grant access to users by using domain accounts (rather than local).

Move to the Security tab. In most cases the default permissions set are okay to leave. Add the IT-Admins group, and grant Modify permission.

4

Sub folders and sub shares

Everything within the IT share is now Readable, Writable, and Modifiable by members of the IT-Admins group. What about other IT users like humble IT help-desk technician? Surely they need access to some of the files within that folder at some point? Do we just create a second share for them, separate from the IT share? Well, yes and no.

Everything within the IT folder is modifiable by IT-Admins, including all sub-folders and files. Somewhere within this folder we want to create a sub-folder that members of the IT-NonAdmins can READ ONLY. Then, within that sub-folder will be a sob-folder that members of the IT-NonAdmins can read/write (or modify). For example, let's say we have the following folder structure:

IT
.|
._Folder 1
.|
._Folder 2
....|
...._Folder 3
....|
...._Folder 4
......|
......_Folder 5

Folder IT is our top level folder, shared to IT-Admins. They have modify permissions on all it's contents, including folders 1-5.

Folder 2 we share (same as in steps 2 & 3) to the IT-NonAdmins group. We give them Read NTFS permissions only. All sub-folders (including folders 3-5) inherit those permissions. Folder 4 however, gives the IT-NonAdmins additional modify or write permissions. Everything within folder 4 (including folder 5) IT-NonAdmins can create and modify.

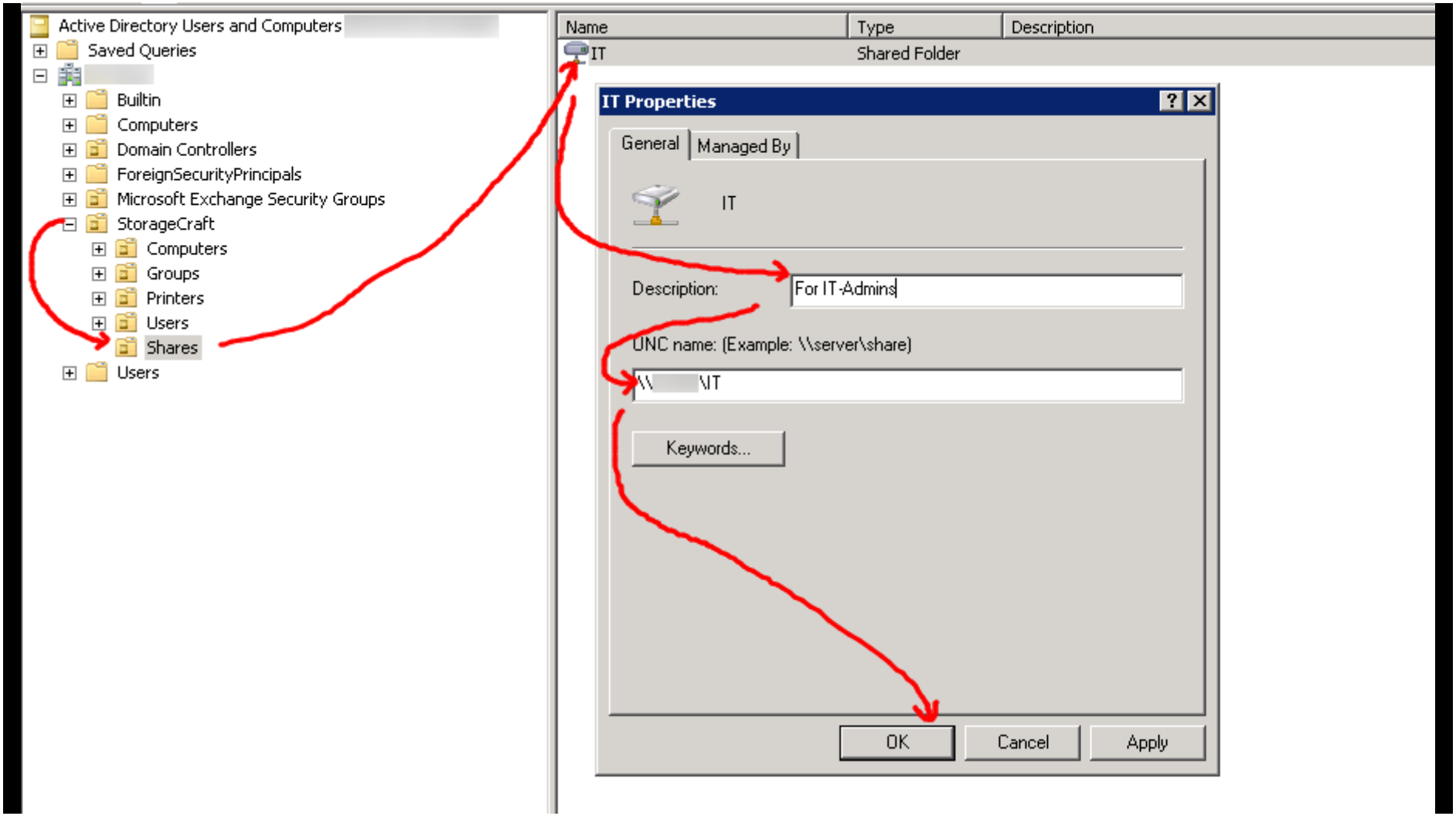
A more realistic example:

IT <---- Shared to IT-Admins (modify)
.|
._Vendors <---- Not visible to IT-NonAdmins
.|
._Network Documentation <---- Shared to IT-NonAdmins (read only)
....|
...._Switch Configuration Files <---- read only to IT-NonAdmins, they only need to access this for reference.
....|
...._Workstation Drivers <---- modifiable to IT-NonAdmins, they can create and modify folders under this folder
......|
......_DELL Latitude E6430U

You may need to add write/modify permissions for the IT-NonAdmins to other folders within Folder 2. That's ok. As long as they have everything they need, and nothing more.

5

Publish Share in Active Directory



Echoing some of the best practices set forth by Microsoft:

1) Turn off Network Discovery in a domain environment, as it can generate excessive network traffic that can interfere with normal network activities.
2) Publish shared folders in Active Directory so that users can search for them in the directory and access them instead of having to browse the network to find them.

This is pretty straightforward. In Active Directory, create a Shares OU structure like so:

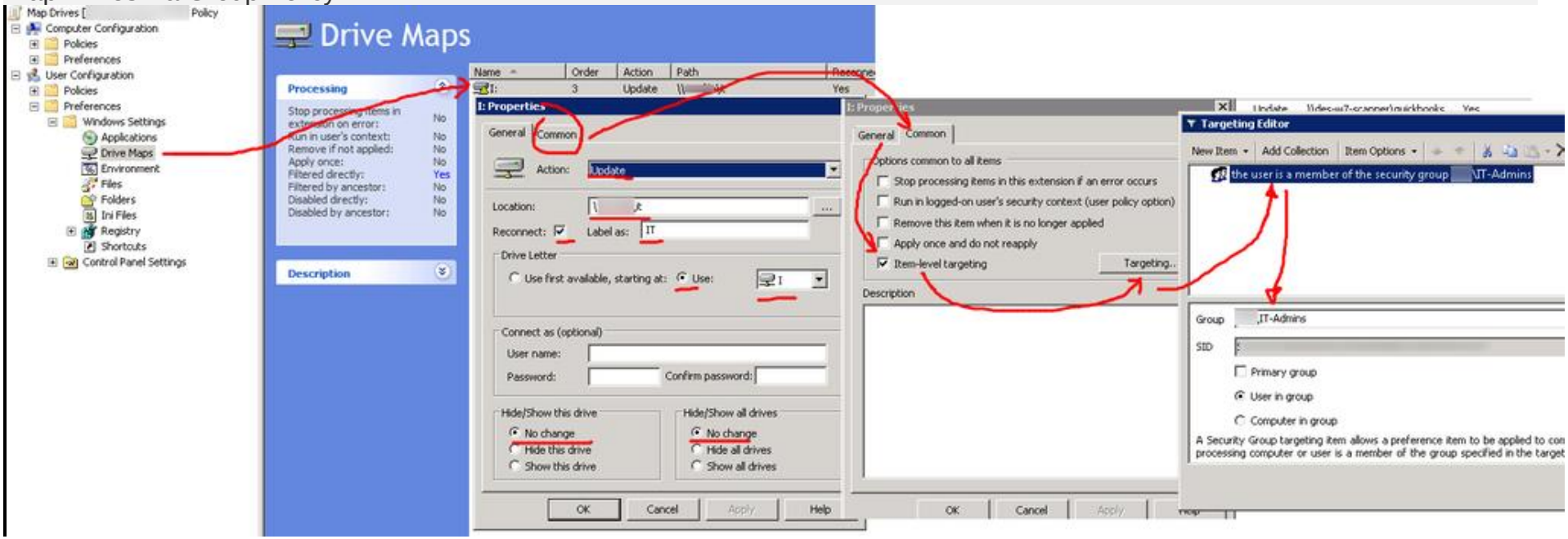
StorageCraft > Shares

Right click somewhere on the right > New > Shared Folder. Give it a name and the UNC network path. Continuing with our example above, I will name it "IT", and give it a network path of \\file-server\IT. Click OK.

Create a second share, pointed to the sub-folder, "Network Documentation" (\\file-server\network documentation).

6

Map Drives via Group Policy



There's really no best practices for this. Either it's setup correctly and users get their drive maps, or it's not...and they don't. I guess if there were a best practice, it would be to have your Active Directory user structure organized in an efficient manner. But with Group Policy Preferences (which we will be using) even that doesn't matter too much.

We want to attach this group policy on the OU that contains all Employee user objects (no service accounts). Looking at StorageCraft's OU structure, we see:

StorageCraft (top level OU) > Users > Draper. Right click that OU and select "Create a GPO in this domain, and Link it here..." (not sure why L is capitalized...). Navigate to User Configuration > Preferences > Windows Settings > Drive Maps > New > Mapped Drive.

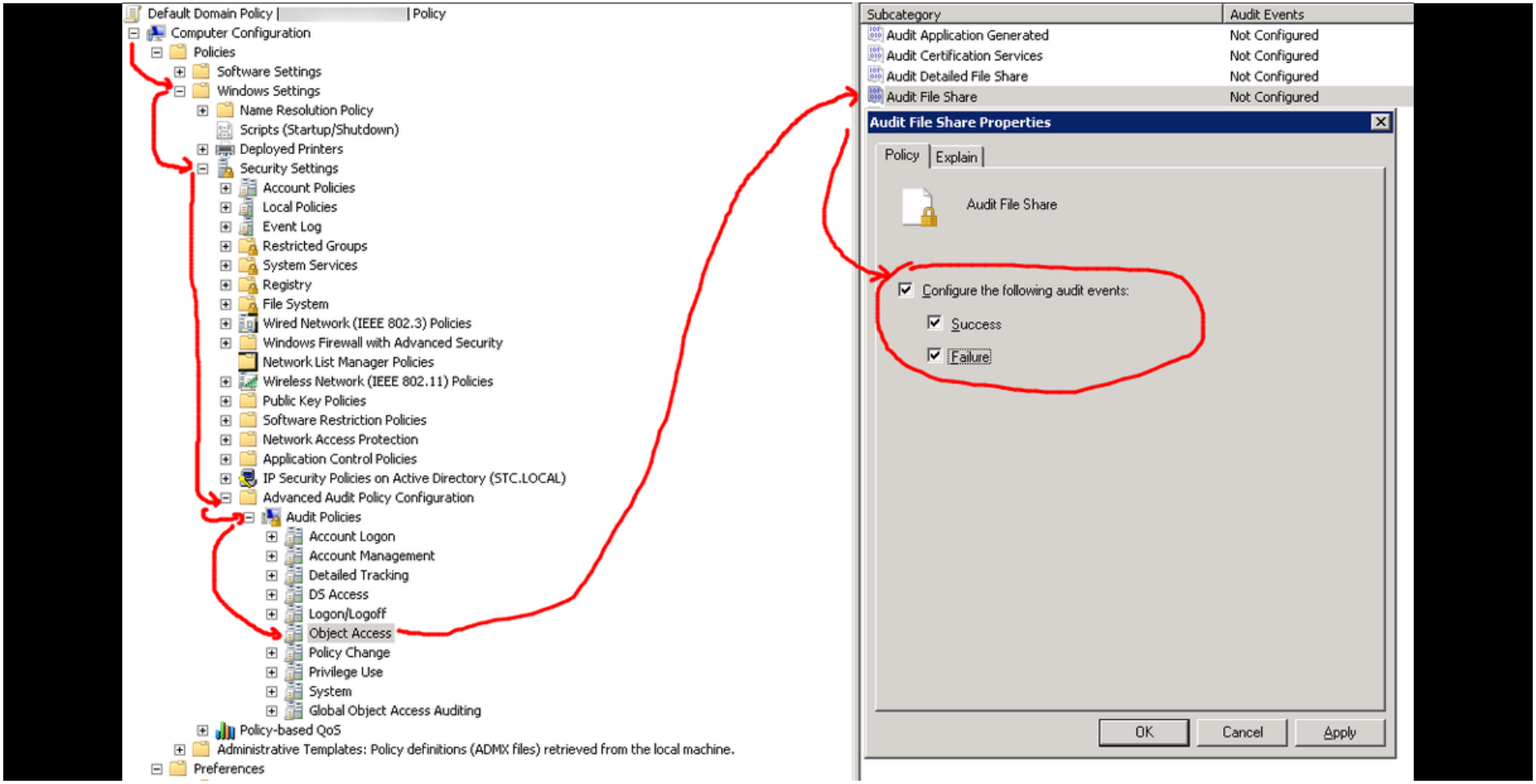
Leave action on Update (this will update users drive mappings if you change it in the future).
Select the location in UNC format = \\file-server\IT
Select the Common tab > check Item level targeting
Targeting button > New Item > Security Group > IT-Admins > Hit OK.

The next time group policy refreshes and an IT-Admin logs in, they should have an I drive.

Do the same thing for the IT-NonAdmins group. Create a new map pointing to the shared sub-folder within the IT folder. Item level target IT-NonAdmins.

7

Auditing



This step really depends on your organizations requirement for auditing. If you don't need it, don't do it. But how else will you know who deletes a particular file?

Most auditing is done in Group Policy at Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Config > Audit Policies. For this particular guide, we will look at Object Access > Audit File Share.

Please note, there are no system access control lists (SACLs) for shares; therefore, once this setting is enabled, access to all shares on the system will be audited. Combined with File System auditing, File Share auditing allows you to track what content was accessed, the source (IP address and port) of the request, and the user account used for the access. Once enabled, you can track events in your Event Viewer. The following event IDs will be generated:

5140 - A network share object was accessed.
5142 - A network share object was added.
5143 - A network share object was modified.
5144 - A network share object was deleted.
5168 - SPN check for SMB/SMB2 failed.

Note - Auditing Success and Failure is recommended in a high security environment (if your share is source code!) and will generate a lot of data. It may be best to forward events to an event collector, which is outside the scope of this article, but easy enough to setup.