**Checklist: Assignment of Groups**

**Carsten Schaefer**

**Managing Data Access on Windows Fileservers**

# **ASSIGNMENT OF USERS TO FOLDERS**

|  |  |
| --- | --- |
|  | Assign permissions via Active Directory security groups, and not to individual users. |
|  | Construct the permission groups on the basis of the organisation’s structure, and not on the demands and requirements of the data objects. |
|  | Ensure that the access requirements for each folder in the file system is sufficiently defined. As such, to allow for the implicit inheritance of permissions, create at least one security group within the Active Directory for each folder. |
|  | Give the security groups succinct and intuitive names. |
|  | Where applicable, nest security groups to reduce the workload of assigning permissions to groups individually. |
|  | For each folder, create different security groups depending on the type of permissions to be awarded. |

# **ASSIGNMENT OF PERMISSIONS TO GROUPS**

|  |  |
| --- | --- |
|  | When assigning security groups permissions, begin with the folder that is highest in the hierarchy. |
|  | The first step in the process of allocation of folder permissions is to ensure that any existing inherited permissions are revoked. |
|  | The second step is to create the permissions for the administrator group. In the administrator group, give “Full Control” permissions to the built-in account system as well as the local group of administrators and operators. |
|  | The third step is to award permissions to the security groups created for each folder. |

# **BEST PRACTICES**

|  |  |
| --- | --- |
|  | Avoid setting the level for managed folders to go very deeply within your folder structure. Beyond the fifth level, the complexity of administration increases exponentially. |
|  | Avoid creating security groups with “Deny” permissions. |
|  | Avoid using the “Share” permissions when creating shares within a file system. |
|  | Frequently audit the actions of the security groups to ensure that all activities are authorised. |
|  | Make every confidential share hidden by including a dollar sign ($) to the end of every share name. |
|  | You can create scripts to allow you easily manage the security groups with folder permissions. |