Top Ten Mistakes

Made While Managing Data Access on Windows Fileservers

Carsten Schaefer

"Can you please create a detailed report about which data Mr. Doe has access to?"

This type of request is common for management and data security officers, and is usually enough to prompt a cold sweat to break out on the foreheads of most IT administrators. This is especially true if the reason for the request is not because Mr. Doe is transferring to another department or leaving the company, but because there is a suspected breach of data privacy. In such scenarios, a reply stating "all sales data" is unacceptable.

Furthermore, the question "can you create a report outlining who has access to which data in sales?" usually throws the entire IT department into disarray.

In most of cases, generating such reports is not only extremely time intensive, but also interferes with the daily workflow. Therefore, many IT administrators refer to access issues as "naturally grown." This means that from the time the data storage structures and their access permissions were created they lacked a clean design, which allowed errors to creep in over time due to negligence.

Here are the 10 most common mistakes made during the conception and management of data storage structures on Windows fileservers:

Mistake 1

Lack of Planning

It is important to have an access authorization concept before the IT administrators create new data structures in the system, no matter whether those structures are for file data, web pages (Microsoft SharePoint), databases (MS SQL Server), applications, mailing lists, or folders (Micro- soft Exchange).

If this authorization concept is missing on all levels, especially for:

a. Use Cases, such as

- Permission assignments for users
- Withdrawal of permissions for individual users in individual access areas
- Simple reporting of access rights

b. And Business processes, such as

- Approval processes for data access
- Approval processes for the creation of new objects in the data structure

then, the tasks of day-to-day management and medium-term reporting can no longer be easily implemented. These tasks will grow increasingly time intensive as more uncertainties and secu- rity risks manifest. This is a nightmare for every IT administrator or security officer.

Mistake 2

Missing Responsibility of the Executive Board or Management

IT administrators manage IT objects, such as shares, folders, and printers. However, they are not responsible for data structures or processes, or granting access rights to data or other objects.

Often, there are no, few, or only poorly documented IT processes. Additionally, management will

Decisions on whether an employee can gain access to sales data cannot be properly deterred - mined in such a system.

For example,

if the "access rights applicant" is rhetorically superior to the IT employee or is on a differ- ent hierarchy level, it can create a conflict. If a service manager wants to grant one of his employees access to "sales", he should have to speak to the sales manager, who should be able to make the exclusive decision on the matter since it is his domain of authority.

Mistake 3

Missing Compliance with Business Processes and Requirements

Employees often try to circumvent the set processes. For example, sometime employees will call IT Operations to gain access without submitting the required documents or will request access rights without prior approval from management. Typical reasons for this behaviour are: "it's important/urgent" or "it was forgotten and the new employee needs access now" or "the manager said so" or "if I don't get access right now, I will..."

To complicate matters further, IT employees scarcely document granting access permissions. "Due to time constraints", documentation requirements concerning data structures and authori- zation concepts are often circumvented.

Take the following example:

A rule was established that the access rights to a file server are only granted on the folder level. A department manager then requests access to a certain file. To resolve the conflict, the IT administrator created a new folder and placed the file there. All permis- sions should be set and granted for this new folder. However, the administrator instead grants permission to the file "on the fly" to save time.

Mistake 4

Allocation of Individual Permissions

Often, non-department permissions are necessary for day-to-day operations. An HR employee, for example, needs access to the workforce planning spreadsheet located in the sales depart- ment's data.

The IT administrator cannot assign HR employees to the "Sales Group" and will, therefore, grant these employees individual access rights to the specific folder or file.

This has fatal consequences:

- A search, where a user has access rights, must now be performed at the file level on all servers.
- It becomes unclear which permissions need to be changed once an employee changes roles.
- If an employee retires or leaves and his/her ID is deleted, a "SSID Corpse" will be left in the ACL list for specific IT objects. This means that an ID will exist with access rights that can no longer be identified.

Mistake 5

Allocation of Additional Permissions to Deep Data Substructures

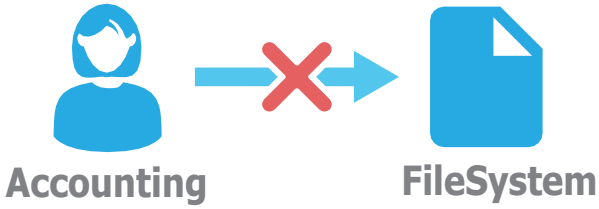
Management complexity increases exponentially if there is no limit to the depth of permissions nesting for data structures.

Suppose the average number of folders in a file system is 10. Thus, the complexity of the man- agement and documentation of the top-level folder is 10. If a second layer is added, the com- plexity will become 10 x 10 (or 100). If we further assume that the average depth of the folder is 10 as well and there is no restriction on granting permissions for folders, the complexity will skyrocket to 10 billion.

This means that an IT administrator must theoretically manage 10 billion permissions. This does not only impact documentation workflow, but also effects expenses.

Mistake 6

Assignment of Universal Security Groups for IT Objects



The typical, but incorrect way to set up data structure is as follows:

A set of permissions is granted for a specific department (sales). Parallel data areas are creat- ed, such as file services, SharePoint spaces, mailing lists, etc.

These data areas are then assigned to the "sales" group. This means that the group gains “write” access to the fileserver folder "sales", “read” access to the web server, and mail distribu- tion rights.

Next, the following requirements are introduced:

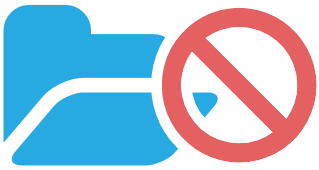
- If the Managing Director would like to access "sales", will he automatically be assigned to the "sales" group? What if he prefers not to receive mails from this group?
- An intern starts in the sales department. He/she should be in the mailing list and only have read access to the data areas. How will the permissions be set up for this intern?
- An HR employee must receive “read” permissions to sub-data areas, but not for the web space. How should one proceed in this case?

In all the above cases, the simple initial solution is no longer practical. This is due to the following problem:

The permission groups model the organization and do not follow the requirements of the data object.

Mistake 7

Application of "Deny" Rights

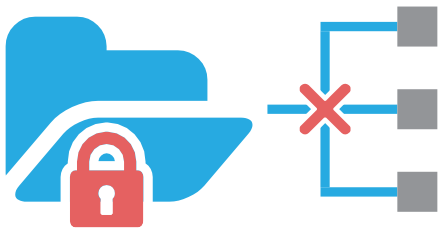


It is not advisable to implement access restrictions for users using "deny access" rights, which is a feature present in many permission systems.

Using “deny access” greatly increases the complexity of administration, documentation, and reporting. All deny groups in all parent data areas must be checked for each additional permission assignment.

Mistake 8

Assigning Share Permissions



When creating data share systems, it is possible to restrict general access to the share (using Share Permissions). However, doing so unnecessarily doubles the complexity of managing that share.

Instead, “write” access should be granted in such cases.

To avoid unwanted access attempts, you can hide the shares in question. Another option is to use "access-based enumeration", which exists on Windows Server 2012 (and later). Thus, a user will only be able to "see" a folder if he/she has the corresponding access rights.

Mistake 9

Insuficient Documentation

According to surveys, only half of all IT administrators document their activities. How access permissions are managed, who got access to what for which reason, and whose permissions were revoked by whom and for what reason are typically not documented.

In such cases, a data security breach or audit can have serious consequences even for adminis - trators.

Mistake 10

Inadequate Reporting and Access Permission Management Tools for Data Structures

The complexity of the IT field is constantly increasing. This is not only true for applications, networks, data volumes, and possibilities, but for the globalization and use of rented or non-lo- cal resources.

Administrators are increasingly challenged and often overwhelmed, when trying to cover their ever-expanding list of IT tasks. Therefore, it is imperative to use tools that make work easier, reduce expenses, and automatically record and comply with set processes.

The use of a simple reporting tool can help compile complete reports about granted and inherit- ed permissions for certain Windows folders. This tool can be made accessible to the owners of the data being protected (the project leader or department head), so that they themselves can generate the necessary reports at any time. This saves the IT administrator a lot of time and effort, because he/she can outsource stressful tasks to users.

On the other hand, a permissions management system can help company's comply with the established best practices for data and permission structures from the outset. Managing permissions for users can be reduced to a few clicks without even looking into the underlying group structure in the Active Directory or on the share.

Even the creation of new shares and new data folders is simplified, so that the CIO can outsource these tasks to the help desk or different departments (for self-management). There is no longer any need to directly rely on various tools such as the Server Manager or Active Direc- tory console. This is an elegant solution to grant orderly access to the management tool for certain user groups.