**Checklist: Tooling & Reporting**

**Carsten Schaefer**

**Managing Data Access on Windows Fileservers**

# **TOOLS, Quality CheCKS, AND REPORTING**

|  |  |
| --- | --- |
|  | Ensure you maintain the integrity of your IT infrastructure through deploying robust tools that check for security leaks. |
|  | Run frequent quality checks to ascertain the authenticity of the allowed permissions. |
|  | Use a professional folder management tool to generate reports listing all the users/groups together with their allowed level of access, enabling you to make informed decisions. |

# **SuPPORT USING SCRIPTS**

|  |  |
| --- | --- |
|  | Use scripts to save you the headache of managing folder permissions and ensuring their security. |
|  | Create a matrix in an Excel worksheet and use scripts to ease the administration of permissions. |
|  | Use scripts, such as a simple VBA or PowerShell script, to support you in automatically transferring permissions to the Active Directory. |
|  | Use scripts to easily take care of the requests requiring changes in the permission structure. |

# **SUPPORT USING TOOLS**

|  |  |
| --- | --- |
|  | Use professional tools to support you in the administration of permissions in your fileservers. |
|  | Use tools to easily manage permissions assignments in the NTFS file system, without requiring any scripting experience or sophisticated skills. |
|  | Avoid spending a lot of time manually administrating security groups in the Active Directory while there are tools that can save you the hassle. |

# **SECURITY ANALYSIS AND REPORTING**

|  |  |
| --- | --- |
|  | Use appropriate tools to carry out an analysis of the effective permission holders and ensure alignment with your permission management process. |
|  | Analyse members of access groups together with their assigned permissions to be sure that all rights are authorised. |
|  | Avoid nesting security groups because it makes analysis to be time-consuming and complicated. |
|  | Siphon the report generated after analysis and remove improper and excessive permissions. |

# **DOCUMENTATION**

|  |  |
| --- | --- |
|  | As an IT administrator, ensure you keep updated audited reports of folder permissions. |
|  | Properly document the administration of permissions; otherwise, the security consequences could be disastrous. |

# **NO TOOLS FOR MANAGING SECURITY RIGHTS**

|  |  |
| --- | --- |
|  | Use tools for managing security rights; otherwise, the challenges of the IT environment could overwhelm you. |
|  | Ensure you aptly manage security rights and maintain the control of your IT infrastructure by using the right tools. |
|  | Deploy robust tools to assist you cover the breadth of all your activities, reduce your workload, and maintain the integrity of all processes. |