netwrix

File Analysis Best Practices

Short File Analysis Best Practice Guide

"File analysis enables storage managers, legal and security professionals, and business analysts to understand and manage unstructured data stores to reduce costs and risk, increase efficiency of business-critical data, and make better information management decisions for unstructured data." — Gartner

Best Practices for File Share Data Management

- Create a file server usage policy that defines how users should manage their folders and files. Be sure to specify what types of files they should store on file server and what they shouldn't; how new folders should be created and how access should be assigned to them; and the penalties for not following the policy.
- Use centralized data folders to better manage your data and simplify backup.
- Segregate your file shares by department. Create one global folder where users can share files across departments, and create a script that cleans up that folder automatically every day.
- Regularly review the contents of your file servers. Pay special attention to the largest files, and look for duplicate files and empty folders. Analyze the results to identify any files and folders that do not comply with your file server policy, and work with the data owners to either delete them or bring them into compliance.
- Try to classify files by type storing the same file types in one folder.
- Regularly report on file extension statistics so you know which types of files you have the most of.
- Deploy e-discovery tools that enable advanced searches of your file shares for legal and other business purposes.
- Identify files that have not been accessed for a very long period of time (six months or a year) and work with the data owners to archive or delete them, as appropriate.
- Protect your file share with regular backups — at least one full backup every month and one incremental backup every day.

Best Practices for File Server Permissions

- Have users log on using domain user accounts rather than local accounts. This approach centralizes the administration of share permissions.
- Create a file server permission policy that clearly defines your permission management process.
- Remove 'Everyone' permissions from every resource except the global folder designated for file exchanges.
- Assign permissions to groups, not user accounts. This approach enables you to add users to or remove them from groups without having to reassign permissions, simplifying management and improving accuracy.
- Give each group a succinct yet descriptive name to avoid errors.
- Define sets of permissions that reflect the access needs of a particular department or a specific role in the organization.
- Assign the most restrictive permissions that still allow users to perform their jobs. For example, if users need only to read information in a folder and not to change, delete or create files, assign the Read permission only.
- Organize your resources so that objects with the same security requirements are located in the same folder. For example, if users require the Read permission for several application folders, store those folders in the same parent folder. Then give Read permissions to the parent folder, rather than sharing each individual application folder separately.
- Avoid denying permissions to a shared resource explicitly. It is usually necessary to explicitly deny permissions only when you want to override specific permissions that are already assigned; this can indicate that either permissions were assigned directly rather than via group membership, or that a user is a member of the wrong group.
- Assign Full Control permission only to the Administrators group and strictly limit membership in this group. This permission enables a user to manage application software and control user rights.
- Create a "global deny" group so that when employees leave the company, you can quickly remove all their file server access by making them members of the group.
- Audit every change to permissions on your file servers and always check whether those changes were authorized.

Corporate Headquarters:
300 Center Drive, Suite 1100, Irvine, CA 92618

Phone: 1-949-407-5125
Toll-free: 888-638-9749

Int'l: 1-949-407-5125
EMEA: 44 (0) 203-318-0261

netwrix.com/social