BEST PRACTICES FOR PLANNING AND IMPLEMENTING NTFS PERMISSIONS FOR RECERTIFICATION

Background

Microsoft's Recommendations for an NTFS Permission Structure

In the Windows 2000 era, Microsoft developed best practices for permission design using a hierarchical, role-based access control model. This model, which includes Active Directory, is commonly known as AGLP (accounts, global groups, local groups and permissions). Still commonly used, AGLP's objective is to assign folder-level permissions on a file system using domain local groups that contain domain global security groups. Unlike domain local groups which manage file system permissions, domain global security groups contain a logical group of users with the same business role or job function.

Since the advent of AGLP, businesses were globalized, regulations were developed (PCI, SOX, PII, etc.) and data complexity has increased. As a result, many organizations are facing significant challenges because AGLP practices do not offer sufficient granularity to support data protection and regulatory requirements. For example, cross-departmental data, usually shared by a small subset of users from multiple business groups, should only be accessible to selected users from multiple business roles. In many cases, compliance regulations, such as HIPPA and SOX, require recertification of the permissions that allow access to this data. AGLP practices limit the ability to perform recertification; this is due to its incapability of applying permissions to only a selected number of people from multiple business roles. Numerous approaches have been adopted to resolve this issue, however with little success. In most cases, the attempts to work around AGLP's insufficient granularity leave the file system's permission in a state of over-permissive access, rendering it impossible to maintain and recertify.

The following sections describe common problems that are encountered when analyzing the state of customer permissions. In addition, a proposed solution is provided to aid customers with the design and implementation in facilitating recertification.

Software version N/A Document version 1 Publication date August 6, 2015

Common Permission Implementation Issues

Over-Permissive Access to Sensitive Data is Caused by Using Functional Groups

A common practice is to grant an entire functional group, business role, or global access group, permissions to a data share. Because Microsoft requires that permissions be granted through Active Directory groups, this method is widely used to provide access. Although this approach ensures that users who require access have sufficient rights, it also poses a security risk. Many unauthorized users are also granted permission to sensitive data, mainly because they are included as a member of a specific role.

User and Non-Group Permissions are Directly Assigned on an ACL

Another way to manage permissions on sensitive data is to directly grant user accounts permissions on the folder instead of using security groups. This ensures that only authorized users have access; however, it also makes permission recertification a very complicated and tedious process. Granting direct permission makes it difficult to effectively manage access across the file system, especially when a user, whose role was changed or employment was terminated, no longer requires access.

Ordinary Users are Intentionally Assigned Full Control Permissions

In many cases, administrators intentionally grant Full Control permissions to ordinary business users. This approach poses a security risk; in the event of a security breach, a malware or cyber- attack, Full Control permissions could be leveraged to perform nefarious activities. For example, these nefarious activities can include removing all permissions from other groups, deleting all data within the folder, and other harmful activities. Business users with Full Control permissions may also inadvertently change folder permission settings, resulting in the loss of access or deletion of data.

Ordinary Users are Unintentionally Assigned Full Control Permissions

IT administrators may unintentionally grant Full Control permissions to ordinary business users by failing to limit default *Owner* rights. While unintentional, this approach also poses a security risk for the same reason identified earlier.

It is important to note that Owner rights should be explicitly defined on the ACL with Modify permissions and *not* Full Control permissions. Additionally, attempts to remove Owner rights will only remove the visual display of the permission and revert the Owner rights to Full Control.

IT Administrators are Unnecessarily Granted Full Control Permissions

IT administrators are usually granted Full Control permissions to all data, including sensitive data. Although this practice may be acceptable in tightly controlled organizations, the prevalence of IT outsourcing has caused the governance of administrative groups to become careless and negligent.

Failure to Audit and Recertify Access

In most environments, there is no clear definition of what data is considered sensitive. In cases where sensitive data is identified, having both multiple functional security groups and direct permissions can cause auditing access and permission recertification to be a complicated and time-consuming task for organizations. Data owners who fail to audit and recertify access to sensitive data risk its unexpected exposure.

A Proposed Solution to Meet the Requirements of Recertification

Identify Actively Accessed Sensitive Data

Because home drives and public group shares usually do not require permission recertification, they can be managed through role-based access using MSFT AGLP and identity management tools. For data that requires more granular protection, such as folders containing sensitive data, permission management should be based on the content of the data and not the functional role of the users requiring access. Data-specific security groups should be created for these folders and direct permissions should be avoided.

For example, a services firm may have sensitive customer data that should only be accessible to specific individuals. Once the folders that contain this data are identified, permissions should be granted only to individuals in a content-specific group. Departmental groups should not be assigned permissions on the folder.

Identify and Utilize Data Owners in the Recertification Process

The owners of sensitive and protected data should be identified and involved, not only in the permission authorization process but also in the recertification process. Owner-to-data mapping should be managed and maintained to ensure proper execution of both the authorization and recertification processes.

Define Standards for Access Permissions

Many customers utilize many different types of permissions, including Read, Write, Modify, Full, and so on. It is recommended that customers adopt a least privilege permission model and minimize the permissions used to grant access. In most cases, Read and Modify permissions are the only permissions required by business users. These permissions should be assigned through directory-specific security groups and not role-based groups. Using directory-specific security groups to govern access to sensitive data reduces the risk of direct permissions and ensures proper execution of recertification.

For example, a manufacturing company may have legacy permissions which allow Read, Write, List, Modify, Execute and special permissions for allowing role-based access to sensitive information. The consumers of this data could include users from Product Management, company executives, Project Management, and Engineering teams. In most cases, only a few key members from each team should be modifying the data. Enforcing an access standard, where there is only one folder-specific Read group and one folder-specific Modify group, reduces complexity, facilitates recertification and ensures that only privileged users can modify data.

Define the Authorization and Recertification Process

Once data owners have been identified and permissions have been granted according to the defined permission standards, it is critical to develop an ongoing authorization and recertification process. This will ensure that data permission integrity is controlled and maintained. The failure to develop and maintain an authorization and recertification process will cause the permissions to revert to their previously chaotic state.

Define Audit and Exception Reporting

From an operational stand point, building a proper permission structure, defining an access provisioning process and

developing a recertification process are not sufficient. Continuous monitoring of permission granting and revocation is required to identify exceptions and to ensure the integrity of designed permission structure.

Ensure That There Are No Exceptions to the New Access Provisioning Authorization and Recertification Process

Once the authorization and recertification process is developed and deployed, it is imperative that all access provisioning occurs through the accepted process. Failing to do so will cause permissions to revert to their previously chaotic state. All stakeholders must take this into account when developing the process.

Ensure Strict Control of Administrative Group Membership to Meet Least Privilege Administrative Access

It is important to identify IT personnel that are responsible for managing access to data and grant them (and only them) full NTFS rights on the folders. IT administrators who do not manage access to data, such as Exchange administrators, Windows administrators, and storage administrators, should not be granted rights on the folders.

Other Recommended Best Practices

Utilizing Share and NTFS Permissions

When accessing data over a network, the most restrictive share or NTFS permissions will govern user accessibility. It is recommended to leave Share access open to Everyone and manage access via NTFS permissions. The proper use of the NTFS inheritance setting provides more granular security settings than Share permissions.

The Use of Global Access Groups

Global access groups should only be used to grant users access to public information. Some organizations may choose to grant List permissions to their entire share structure, thus making it easier for employees to navigate within the share. Other organizations choose to restrict List permissions to Everyone due to the naming convention of their folders and files. If folder or file names reveal sensitive information (i.e., client or project names), List permissions should *not* be granted to Global Access Groups on the share.

The Use of Functional Security Groups

For departmental folders, information is usually made available to all users within the same business unit. In this case, functional security groups should be used. By using Identify and Access Management applications, users with a specific function are granted access to all the relevant information. However, with protected and sensitive data, NTFS inheritance should be restricted and data-specific security groups should be used to govern user access.

The Use of NTFS Inheritance

NTFS inheritance should be used whenever possible so that permission control and recertification are manageable. Inheritance should be restricted only when the data set is accessible to a smaller set of users than the parent folder. When inheritance is restricted, permissions should be managed differently and data owners should be identified in order to facilitate a proper provisioning and recertification process.

Defining an Appropriate Folder and Permission Structure

It is highly recommended to design a folder structure in which protected folders (folders on which inheritance is restricted) are placed at the top of the structure. Data should be grouped within folders so that inheritance can be used throughout the many levels of the folder structure; this can keep the number of protected folders manageable and helps to facilitate the recertification process. Folders that are available to a common set of users and which are configured in multiple diverse folder trees can create redundant provisioning and recertification processes. Folders that are configured to restrict NTFS inheritance need to be managed as independent permission entities.

Sensitive Data Identification and Ongoing Monitoring

The classification and identification of sensitive data are critical to proper governance. These practices ensure that sensitive information remains unavailable to users in global access groups or general departmental groups. It is highly recommended to continuously monitor sensitive data in order to minimize its exposure to the wrong parties.

Summary

Preparing for permission recertification requires a comprehensive understanding of access provisioning methodologies and processes. By applying the practices identified in this document, companies can reduce unnecessary risk through a scalable, controlled and auditable access control process.