AXIS COMMUNICATIONS

TECHNICAL NOTES

NETWORK STORAGE SERVERS **AXIS STORPOINT SERVERS**

Security Emulation in Windows NT Servers

Created: January 5, 2001
Last updated: January 5, 2001
Rev: 1.0

TABLE OF CONTENTS

INTRODUCTION 2

1 WINDOWS NT SERVER STANDARDS 3

1.1 WINDOWS NT'S NATIVE TOOLS 3
1.1.1 SETTING PERMISSIONS 4
1.2 NT FILE SYSTEM SECURITY POLICY 6
1.2.1 NTFS ENCODING STRUCTURE 6
1.2.2 IMPLEMENTATION IN AXIS STORPOINT SERVERS 6
1.3 PASS-THROUGH AUTHENTICATION 7
1.3.1 IMPLEMENTATION IN AXIS STORPOINT SERVERS 7
1.4 USER- LEVEL SECURITY 8
1.4.1 IMPLEMENTATION IN AXIS STORPOINT SERVERS 8
1.5 SHARE-LEVEL SECURITY 8
1.5.1 IMPLEMENTATION IN AXIS STORPOINT SERVERS 8

The AXIS StorPoint servers act as Windows NT 4 member servers on Windows NT (CIFS) Domain Networks.
This means that the AXIS StorPoint servers process user authentication and file security according to Windows NT server standards.

The AXIS StorPoint server is automatically identified as an NT Server and authentication is performed. The AXIS StorPoint server adheres to the stringent roles governed by the NT Server and ensures in this manner maximum security and integrity of the data stored on the storage server.

The Administrator can assign rights and permissions to the AXIS StorPoint server directly on the domain server or on any NT workstation attached to the domain using well-known NT native tools.

1 Windows NT Server Standards

In short, AXIS StorPoint servers fully support the following:

- Windows NT's native tools
- NT file system security policy
- Pass–through authentication and multiple domain authentication
- User–level security
- Share–level security

1.1 Windows NT's Native Tools

The AXIS StorPoint server uses Windows NT's native tools to set Volume, Directory and File permissions.

> **Notes:**
> - AXIS StorPoint CD servers support Volume permissions.

The Administrator does not need any additional client software or Web-based tools in order to perform these tasks from any NT workstation or server connected to the network.

The Axis StorPoint server allows the Administrator to work with NT's well-known tools. Thus, the Administrator can complete the given tasks easily, swiftly and with confidence.

The Administrator has convenient and full access to user and group lists, provided by the domain controllers when logged-in as an administrator on any NT workstation on the network. The Administrator can grant permissions for specific users or groups to access explicit Volumes, Directories or Files on the AXIS StorPoint server.

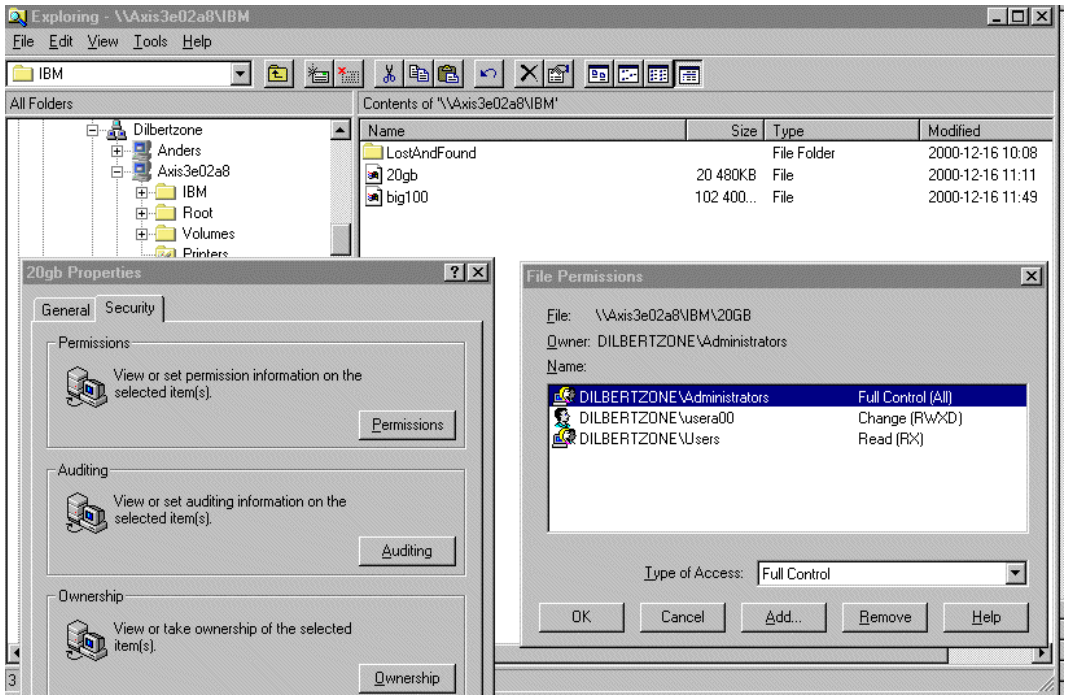
In user-level security, a variety of permissions can be granted:

Volume Directory	No Access	Read	Write	Full Control	List
File	No Access	Read Only	Write	Full Control	

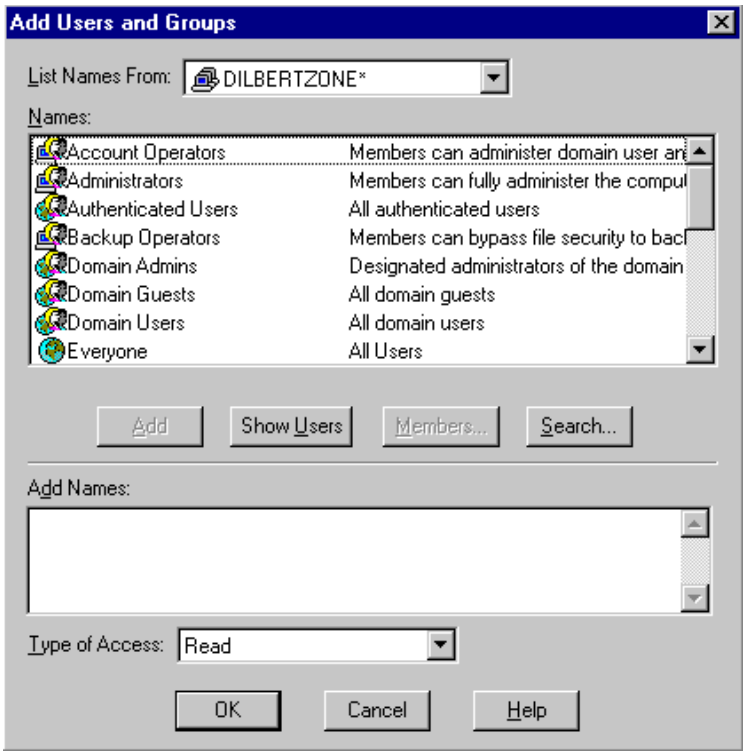
1.1.1 Setting Permissions

To set permission to a file or directory, follow these steps:

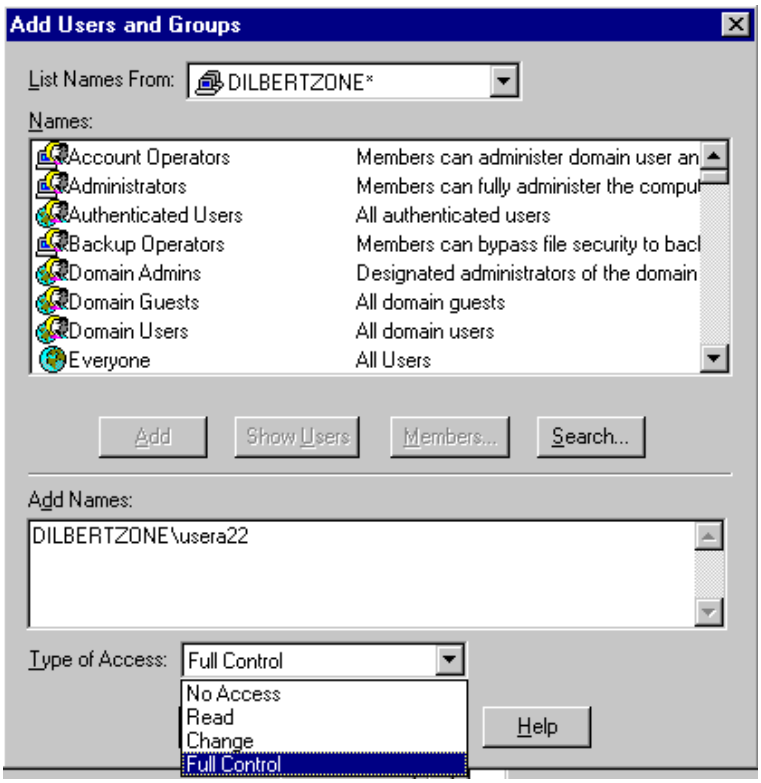
1. Logon to the network as Administrator.
2. Open **Windows Explorer**.
3. Locate the AXIS StorPoint server within **Network Neighbourhood**.
4. Right-click the desired file (or directory) for which you want to set permissions.
5. Select **PROPERTIES** | **SECURITY** and click the **PERMISSION** button.



6. The **FILE PERMISSIONS** dialog box appears. The dialog displays the current users and groups that are assigned permissions to the file and the type of permissions. To add users or groups, click the **ADD** button.



7. The **ADD USERS AND GROUPS** dialog appears. This dialog displays the list of accounts in the domain. This list is imported from the domain controller servers. Different domains can be chosen. To view users, click the **SHOW USERS** button.
8. To add permissions to a specific user, select the user from the list and click the **ADD** button.



9. Select the type of access you want the selected user to have. Click **OK** to save your changes.

1.2 NT File System Security Policy

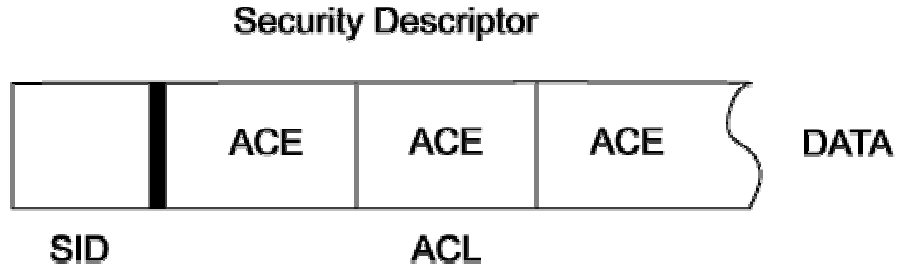
The Windows NT Server file system, NTFS, is the only file system that allows full and extended Directory and File permission settings. Identification of groups and users as well as specific access permissions for these groups and users are appended to the file itself and stored with the file.

1.2.1 NTFS Encoding Structure

The security information for directories and files is encoded in a specific data structure, named the *Security Descriptor (SD).* The SD contains the following components:

- Owner *Security ID (SID)* – The SID is a unique identifier of users and groups. Users and groups that are granted permissions to directories and files are identified by their specific SID.

- *Access Control List (ACL)* - The ACL is a list of users and groups and their individual permissions. Each user or group is represented as a separate entry in the ACL and is called the *Access Control Element (ACE).*



1.2.2 Implementation in AXIS StorPoint Servers

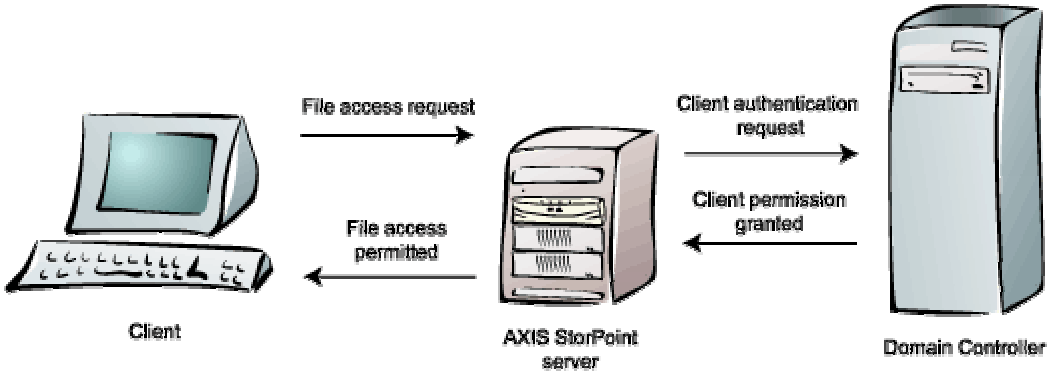
The AXIS StorPoint servers are not using NTFS, but follow this file system security policy closely and append extended attributes according to NTFS standards. Using a different file system and storing the permission attributes in a unique format on the actual AXIS StorPoint server ensures extremely high security.

1.3 Pass-Through Authentication

Pass-through authentication is used in Windows NT domains when a user account must be validated but the local server cannot validate the account. The AXIS StorPoint servers are using the Windows NT pass-through authentication method.

The user will not notice any difference whether accessing a file from an NT server or from the AXIS StorPoint server. The process is completely transparent to the user.

1.3.1 Implementation in AXIS StorPoint Servers



When a user wants to access a file on the AXIS StorPoint server, the user account and password information supplied by the user are passed from the AXIS StorPoint server to the Windows NT Server acting as Domain Controller (DC). The DC performs the validation and the information is returned to the AXIS StorPoint server and stored locally in a Security Access Token. The user is then permitted (or denied) access to requested file.

Any further requests are validated locally in AXIS StorPoint server since authentication had already taken place. However, the Security Access Token might expire within the given period of time. In this case, new pass-through authentication must take place in order to validate the user.

Pass-through authentication can be used over domain borders. Users from different domains can be validated upon request.

1.4 User- Level Security

User-level security will grant specific users and groups access to specific resources. By default, no permissions are granted to the system files. Thus, these resources are protected from unauthorized access. However, the Administrator must actively limit access to the other network resources, i.e. Volumes, Directories and Files.

The Administrator can assign access permissions to users and groups. Each Volume, Directory or File is accessible only by the permitted users and groups. In addition, access permissions are divided in access elements enabling specific types of access such as No Access, Read Only, Write or Full Control.

The Administrator using standard tools and the access list from the Domain Controller easily manages permissions. The Administrator can easily grant specific access to individual users and/or groups.

1.4.1 Implementation in AXIS StorPoint Servers

AXIS StorPoint servers fully support user-level security, which ensures easy and convenient administration of permissions. Above all, it guarantees maximum level of integrity and security of all Volumes, Directories or Files located on the StorPoint Server.

1.5 Share-Level Security

Share-level security allows a password to be assigned to each shared resource. If a password has been set, the users will be prompted to supply this password before they are allowed access the shared resource.

This way, data resources can be partially protected. However, the passwords must be communicated to all authorized users. For security reasons, the passwords should be altered regularly. This procedure is cumbersome and unmanageable in larger networks. However, in very small networks, a reasonable security level could be maintained by the acting Administrator.

By default, shared Volumes, Directories or Files are fully accessible by everyone. This approach simplifies peer-to-peer networking for small networks and eliminates the need for a dedicated Network Administrator. However, it creates potential security hazards as files could be accidentally deleted.

1.5.1 Implementation in AXIS StorPoint Servers

AXIS StorPoint servers are true ready-to-operate servers as they use share-level security as the default setting. No configuration is needed in order to have the system up and running. The users gain instant access to the data stored on the AXIS StorPoint server.