Controlling Access to NFS Shares

LPIC-2: Linux Engineer (202-450)

Objectives:

At the end of this episode, I will be able to:

1. Describe NFS mount options and how they control user access.
2. Describe and implement TCP wrappers to limit user access.

> Additional resources used during the episode can be obtained using the download link on the overview episode.

- NFS Access Controls
    - Understanding NFS Authentication
    - Limiting User Permissions with Export Options
    - Restricting Client Access with Export Options
    - Restricting Client Access with TCP Wrappers
- Understanding NFS Authentication
    - NFS4
        - Supports Generic Security Service API (GSS-API)
        - Allows for granular user/group access controls
        - Many clients are incompatible
    - Not directly supported by NFS 2/3
    - NFSv3 Assumptions
        - Another system is providing user IDs
            - OpenLDAP
            - FreeIPA
        - User ID matches on client and server
        - File system permissions are configured
- Limiting User Permissions
    - `rw` and `ro`
        - **rw**: Allow read and write access
        - **ro**: Allow read-only access
    - `squash`
        - **root_squash**: Treat root users as anonymous.
        - **no_root_squash**: Allow root users to connect with elevated privileges.
        - **all_squash**: Treat all users as anonymous.
- Restricting Client Access with Export Options
  - Restricts which clients can connect
  - Supports hostname, IP, and ranges
  - Examples
  + `10.0.222.50(sync,no_subtree_check)`
  + `10.0.222.0/24(sync,no_subtree_check)`
  + `DonsLaptop(sync,no_subtree_check)`
  + `*.itpro.tv(sync,no_subtree_check)`
- Restricting Client Access with TCP Wrappers
    - `rpcbind` includes `libwrap.so`
    - Allows controlling TCP connections
    - TCP Wrapper Lists
        - `/etc/hosts.allow`
        - `/etc/hosts.deny`
    - Allow is applied first
    - Configuring

- /etc/hosts.allow
    - rpcbind: 10.0.222.*
- /etc/hosts.deny
    - rpcbind: ALL