

Linux Configuration and Security

Commands Documentation

Checking ACL Permissions:

- Command: `getfacl /mydir`
- Description: Uses `getfacl` to check the Access Control List (ACL) permissions for the directory `/mydir`.

Performing Long List on Directory with ACL Indicator:

- Command: `ls -ld /mydir/`
- Description: Performs a long listing using `ls -ld` on the directory `/mydir/`. The "+" sign indicates that ACL is set.

Setting No Permissions for Others in ACL:

- Command: `setfacl -m o:--- /mydir/`
- Description: Uses `setfacl` to set no permissions (---) for others in the ACL of the directory `/mydir/`.

Viewing Help for setfacl Command:

- Command: `setfacl -h`
- Description: Displays help and important keywords for the `setfacl` command.

Removing ACL Permission for a User:

- Command: `setfacl -x u:user3 /mydir/`
- Description: Removes ACL permission for the user `user3` from the directory `/mydir/`.

Checking ACL Permission Removed:

- Command: `getfacl /mydir`
- Description: Uses `getfacl` to verify that the ACL permission for `user3` has been successfully removed.

Removing All ACL Permissions:

- Command: `setfacl -b /mydir/`
- Description: Removes all ACL permissions from the directory `/mydir/`.

Setting Default ACL:

- Command: `setfacl -m d:u:user1:rwx /mydir/`
- Description: Sets default ACL permissions for the user `user1` with `rwx` on the directory `/mydir/`.

Checking the Manual for setfacl Command:

- Command: `man setfacl`
- Description: Uses `man` to check the manual for the `setfacl` command.

Creating a Directory:

- Command: `mkdir /dir1`
- Description: Creates a new directory named `/dir1`.

Changing User Owner of the Directory:

- Command: `chown vimal /dir1`
- Description: Changes the user owner of the directory `/dir1` to `ayush`.

Setting ACL Permission on User "vimal":

- Command: `setfacl -m u:vimal:rx /lwdir1/`
- Description: Sets ACL permissions (`rx`) for the user `ayush` on the directory `/lwdir1/`.

Checking POSIX and ACL Permissions:

- Description: Demonstrates the relationship between POSIX permissions (`rx` for user owner) and ACL permissions (`rx` for user `ayush`).

Logging in as User "jack" and Testing Permissions:

- Description: Describes the login as user `jack` and how the permissions (`r-x`) affect the ability to navigate, list, and create files.

Giving Dedicated Permission (ACL) to User "jack":

- Command: `setfacl -m u:jack:rx /dir1/`
- Description: Gives dedicated ACL permissions (`rx`) to the user `jack` on the directory `/dir1/`.

Setting Mask for Effective Permissions:

- Command: `setfacl -m mask:x /dir1/`
- Description: Sets a mask that allows only the execute (`x`) permission on the folder `/dir1/`, demonstrating effective permissions.

Umask and Default Permissions:

- Description: Explains the concept of `umask` and how it influences default permissions. Mentions the maximum permissions for directories (`777`) and files (`666`) and the default values.

Adding User to "wheel" Group:

- Command: `useradd -G wheel tom12333`
- Description: Adds the user `tom12333` to the "wheel" group.

Checking if "firewalld" is Installed:

- Command: `rpm -q firewalld`

- Description: Checks if the "firewalld" package is installed on the system.

Checking the Status of "firewalld":

- Command: `systemctl status firewalld`
- Description: Displays the status of the "firewalld" service.

Starting the "firewalld" Service:

- Command: `systemctl start firewalld`
- Description: Starts the "firewalld" service.

Checking if Firewall is Running:

- Command: `firewall-cmd --state`
- Description: Checks if the firewall is currently running.

Viewing Pre-created Zones:

- Command: `firewall-cmd --get-zones`
- Description: Displays the pre-created zones provided by Red Hat.

Checking Default Zone:

- Command: `firewall-cmd --get-default-zone`
- Description: Checks the default firewall zone.

Checking Active Zone:

- Command: `firewall-cmd --get-active-zones`
- Description: Checks the active zone for each network interface.

Listing All Pre-created Rules of the "public" Zone:

- Command: `firewall-cmd --list-all --zone=public`
- Description: Lists all pre-created rules for the "public" zone.

Listing All Zones:

- Command: `firewall-cmd --list-all-zones`
- Description: Lists all available zones, their targets, and services.

Setting Default Zone:

- Command: `firewall-cmd --set-default-zone=trusted`
- Description: Sets the default zone to "trusted".

Checking Active Zones:

- Command: `firewall-cmd --get-active-zones`
- Description: Checks the currently active zones.

Adding Service "http" to the "public" Zone:

- Command: `firewall-cmd --add-service=http --zone=public`
- Description: Adds the "http" service to the "public" zone.

Making a Rule Permanent:

- Command: `firewall-cmd --add-service=http --zone=public --permanent`
- Description: Adds the "http" service to the "public" zone permanently.

Removing Service "http":

- Command: `firewall-cmd --remove-service=http --zone=public`
- Description: Removes the "http" service from the "public" zone.

Adding Port 80:

- Command: `firewall-cmd --add-port=80/tcp --zone=public`
- Description: Adds port 80 to the "public" zone.

Viewing "rich rules" (Advanced Rules):

- Command: `firewall-cmd --list-rich-rules`
- Description: Displays the currently configured rich rules.

Adding "rich rule" to the "public" Zone:

- Command: `firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.1.12" port port="80" protocol="tcp" accept'`
- Description: Adds a rich rule allowing connections from source IP '192.168.1.12' to port 80 on TCP protocol in the "public" zone.