8.12.4 Group Policy Facts

A *policy* is a set of configuration settings applied to users or computers. Group policies allow the administrator to apply multiple settings to multiple objects within the Active Directory domain at one time. Collections of policy settings are stored in a Group Policy object (GPO). The GPO is a collection of files that includes registry settings, scripts, templates, and software-specific configuration values.

Each GPO has a common structure, with hundreds of configuration settings that can be enabled and configured. Settings are divided into two categories:

GPO Category	Description
Computer Configuration	Computer policies are enforced for the entire computer and are initially applied when the computer boots. Computer policies are in effect regardless of the user logging into the computer. Computer policies include: ▪ Software that should be installed on a specific computer. ▪ Scripts that should run at startup or shutdown. ▪ Password restrictions that must be met for all user accounts. ▪ Network communication security settings. ▪ Registry settings that apply to the computer (the HKEY_LOCAL_MACHINE subtree). Computer policies also include a special category of policies called *user rights*. User rights identify system maintenance tasks and the users or groups who can perform these actions. Actions include: ▪ Changing the system time ▪ Loading and unloading device drivers ▪ Removing a computer from a docking station ▪ Shutting down the system Computer policies are initially applied as the computer boots and are enforced before any user logs on.
User Configuration	User policies are enforced for specific users and are applied when the user logs on. User policy settings include: ▪ Software that should be installed for a specific user. ▪ Scripts that should run at logon or logoff. ▪ Internet Explorer user settings (such as favorites and security settings). ▪ Registry settings that apply to the current user (the HKEY_CURRENT_USER subtree). User policies are initially applied as the user logs on and often customize Windows based on user preferences.

GPOs apply to objects when they are linked to containers and configured with specific settings.

- GPOs can be linked to Active Directory domains or organizational units (OUs).

  Built-in containers (such as the Computers container) and folders cannot have GPOs linked to them.

- A GPO applied to an OU affects only the users and computers in the OU and OUs.
- A GPO applied to a domain affects all users and computers in all OUs in the domain.
- A local GPO is stored on a local machine. It can be used to define settings even if the computer is not connected to a network.
- A specific setting in a GPO can be:
  - Undefined, meaning that the GPO has no value for that setting and does not change the current setting.
  - Defined, meaning that the GPO identifies a value to enforce.
- GPOs are applied in the following order:
  1. The Local Group Policy on the computer.
  2. GPOs linked to the site.
  3. GPOs linked to the domain that contains the User or Computer object.
  4. GPOs linked to the organizational unit(s) that contain(s) the User or Computer object (from the highest-level OU to the lowest-level OU).

  Use the acronym LSDOU (Local, Site, Domain, and OU) to help you remember the order that GPOs are applied. The local policy is always applied, but it may get overwritten by a policy from Active Directory.

- Individual settings within all GPOs are combined to form the effective Group Policy setting as follows:
  - If a setting is defined in one GPO and undefined in another, the defined setting will be enforced (regardless of the position of the GPO in the application order).
  - If a setting is configured in two GPOs, the setting in the last-applied GPO will be used.