12.4.11 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 includes registry settings, scripts, templates, and software-specific configuration values.

Keep in mind the following concerning GPOs:

- GPOs can be linked to Active Directory domains, organizational units (OUs), and containers.

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

- A GPO applied to an OU affects the objects in the OU and all sub-OUs.
- A GPO applied to a domain affects all objects within all OUs.
- A local GPO is stored on a local machine. Computers that are not part of a domain use the Local Group Policy settings to control security settings and other restrictions on the computer.
- GPOs are applied in the following order:
  1. The Local Group Policy on the computer.
  2. GPOs linked to the domain that contains the user or computer object.
  3. GPOs linked to the organizational unit(s) that contains the object (from the highest-level OU to the lowest-level OU).
- A specific setting in a GPO can be:
  - Not configured, meaning that the GPO has no value for that setting and does not change the current setting.
  - Enabled, meaning that the GPO identifies a value to enforce.
- 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.

  The Local Group Policy is applied only when there are no GPOs linked to a domain or an OU. GPOs linked to an OU override GPOs linked to a domain when both are applied.

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

GPO Category	Description
Computer Configuration	Computer policies (also called *machine policies*) are enforced for the entire computer and are 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 are initially applied as the computer boots and are enforced before any user logs on.
User Configuration	User policies are enforced for specific users. 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 user preferences.

GPOs contain hundreds of configuration settings that can be configured. The following table describes common settings you should be familiar with.

Setting Category	Description
Account Policies	Use Account Policies to control the following: ▪ Password settings ▪ Account lockout settings ▪ Kerberos settings

	Account policies are in effect only when configured in a GPO linked to a domain.
Local Policies/Audit Policy	Use Audit Policy settings to configure auditing for events such as log on, account management, or privilege use.
Local Policies/User Rights Assignment	Computer policies 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. Examples of user rights include: ▪ Access this computer from the network (the ability to access resources on the computer through a network connection) ▪ Load and unload device drivers ▪ Allow logon locally (the ability to log on to the computer console) ▪ Allow logon through Terminal Services (the ability to log on using a Remote Desktop connection) ▪ Back up files and directories (does not include restoring files and directories) ▪ Shut down the system ▪ Remove a computer from a docking station
Local Policies/Security Options	Security Options allow you to apply or disable rights for all users the Group Policy applies to. Examples of Security Options policies include: ▪ Computer shutdown when the Security event log reaches capacity ▪ Unsigned driver installation ▪ Ctrl+Alt+Del required for log on
Registry	You can use registry policies to: ▪ Configure specific registry keys and values. ▪ Specify if a user can view and/or change a registry value, view sub-keys, or modify key permissions.
File System	Use File System policies to configure file and folder permissions that apply to multiple computers. For example, you can limit access to specific files that appear on all client computers.
Software Restriction Policies	Use software restrictions policies to define the software permitted to run on any computer in the domain. These policies can be applied to specific users or all users. You can use software restrictions to: ▪ Identify allowed or blocked software. ▪ Allow users to run only the files you specify on multi-user computers. ▪ Determine who can add trusted publishers. ▪ Apply restrictions to specific users or all users.
Administrative Templates	Administrative templates are registry-based settings that can be configured within a GPO to control the computer and the overall user experience, such as: ▪ Use of Windows features such as BitLocker, Offline files and Parental Controls. ▪ Customize the Start menu, taskbar, or desktop environment. ▪ Control notifications. ▪ Restrict access to Control Panel features. ▪ Configure Internet Explorer features and options.