8.1.6 Group Policy Facts

A *policy* is a set of configuration settings applied to objects such as 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.

The following table identifies tasks for managing GPOs.

Task	Description
Managing Local Group Policy	Computers that are not part of a domain use local Group Policy settings to control security settings and other restrictions on the computer. Local Group Policy settings are also applied to domain-joined computers. However, domain Group Policy overrides local Group Policy if a particular policy setting is defined in both places. To manage local Group Policy, use Microsoft Management Console (MMC): ▪ Enter **mmc** at the command line to launch Microsoft Management Console. ▪ Add the **Group Policy Object Editor** snap-in from the File menu. By default, it will add the Local Computer Group Policy snap-in. ▪ Select **Users** to edit Local Group Policy for specific users on the computer. You can save the Group Policy Object Editor console to allow for easy access in the future. You can also access the local Group Policy snap-in directly by entering **gpedit** at the command line.

Managing Domain GPOs	Group Policy Objects (GPOs) can be linked to Active Directory sites, domains, and organizational units (OUs). Use the Group Policy Management console to link a GPO to one of these objects. Be aware of the following:
	
	▪ A GPO applied to an OU affects the objects in the OU and sub-OUs.
	▪ A GPO applied to a domain affects all objects in all OUs in the domain.
	
	Built-in containers, such as the Computers container, and folders cannot have GPOs linked to them.
	
	Once the GPO has been linked, you can edit various policy settings within it. When linking Group Policies:
	
	▪ The Default Domain Controllers policy is linked to the domain controllers OU by default.
	  ▪ This policy increases security of the domain controllers.
	  ▪ You can run the **dcgpofix** command to restore the original settings of the Default Domain Controllers Group Policy.
	▪ On the **Linked Group Policy Objects** tab, you can change the link order of Group Policies.
	▪ The **Group Policy Inheritance** tab lists the order in which Group Policies will be applied. The policies are listed in reverse order of precedence, meaning that the last policy on the list--the one with the highest precedence number--will be applied first.
	▪ To delete a Group Policy, you must delete it from the Group Policy Objects container.

Assigning GPO Permissions	Group Policy permissions control the operations that users can perform on the GPO as well as the application of the GPO to the user. ▪ To apply settings to a user, the user must have the **Allow Read** and **Apply Group Policy** permissions. ▪ By default, each GPO grants the Authenticated Users group (essentially, all network users) the **Allow Read** and **Apply Group Policy** permissions. This means that, by default, GPO settings apply to all users. ▪ Permissions also control who can edit Group Policy settings and manage the GPO.
Using Administrative Templates	You can use Administrative Templates to create Group Policies to manage Microsoft Office or in-house applications. File types for Administrative Templates use an XML-based file format that allows multi-language support and version control: ▪ .admx files are the Administrative Template files and require Windows Vista or later to edit. ▪ .adml files contain the language-specific Administrative Template files. .adm files are the pre-XML format used for Administrative Templates. This older format is still usable in current versions of Windows Server.

Using a Central Store	When you use Administrative Templates, the policy is stored locally, and the settings are saved to Group Policy on the domain controller. The central store allows Administrative Templates to be available to be edited by other domain administrators. ▪ Group Policies are kept in SYSVOL, a share that is created when you install Active Directory. All domain controllers in the domain have a replicated copy of SYSVOL. ▪ To create a central store: ▪ Create a folder named PolicyDefinitions in file:\\FQDN\SYSVOL\FQDN\. For example: **\\Northsim.com\SYSVOL\Northsim.com\PolicyDefinitions** ▪ Copy the contents of the local PolicyDefinitions folder to the PolicyDefinitions folder on SYSVOL. The path of the local PolicyDefinitions folder is typically: **C:/Windows/PolicyDefinitions**

Keep in mind the following about GPOs:

- If possible, combine multiple settings into one Group Policy. Reducing the number of Group Policies that require processing reduces boot and logon time.
- The Default Domain policy contains the only account and password policies that are going to take effect unless you create a password settings object (PSO).
- GPOs do not exist at the forest level. To enforce a GPO in multiple domains, create the GPO in one domain, export it, and then import it into other domains.

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

GPO Category	Description
Computer Configuration	Computer policies, or *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. They often customize Windows based on user preferences.

All computer policies run before any user policies run.