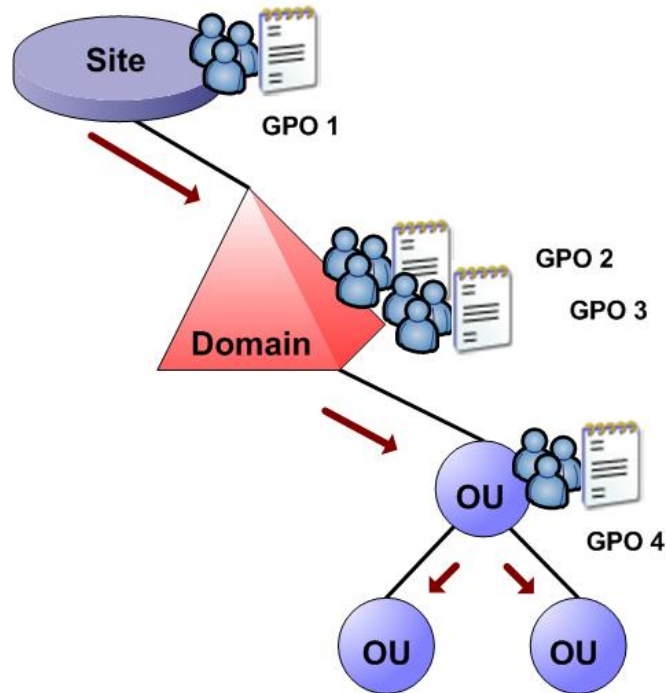


Windows Server 2003 Active Directory GPO – Zásady zabezpečení

Zásady zabezpečení (Group Policy Objects) slouží k centrální správě uživatelů a počítačů. Lze pomocí nich aplikovat jednotné nastavení platné pro skupiny počítačů nebo pro celou doménu.



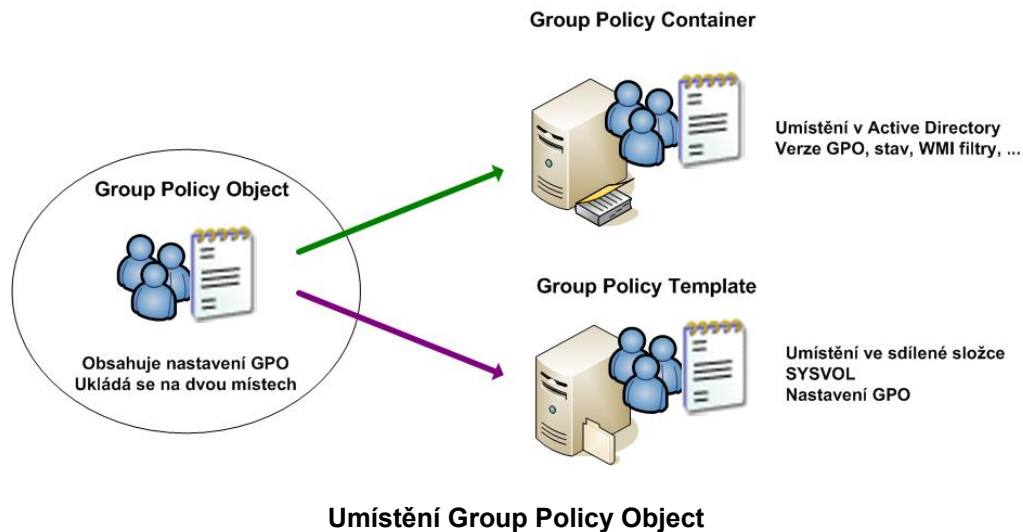
Zásady zabezpečení lze aplikovat na lokality (Sites), domény (Domains) a organizační jednotky (Organizational Units)

Použití zásad zabezpečení:

- Šablony pro správu
- Přihlašovací skripty
- Remote Installation Services
- Nastavení pro Internet Explorer
- Přesměrování adresářů
- Zabezpečení
- Instalace software

Zásady zabezpečení jsou aplikovány na všechny podřízené kontejnery (**Inheritance**). Nicméně je možné tuto výchozí vlastnost pro určité kontejnery zakázat. Dále je možné nastavením zabezpečení definovat skupinu uživatelů pro kterou budou dané zásady zabezpečení použity.

K definici GPO slouží - **Group Policy Object**. Ten je v Active Directory umístěn na dvou místech. Jedna část **Group Policy Container** je uložen přímo v databázi Active Directory. Druhá část obsahující vlastní nastavení je umístěna ve sdílené složce SYSVOL na doménovém řadiči.



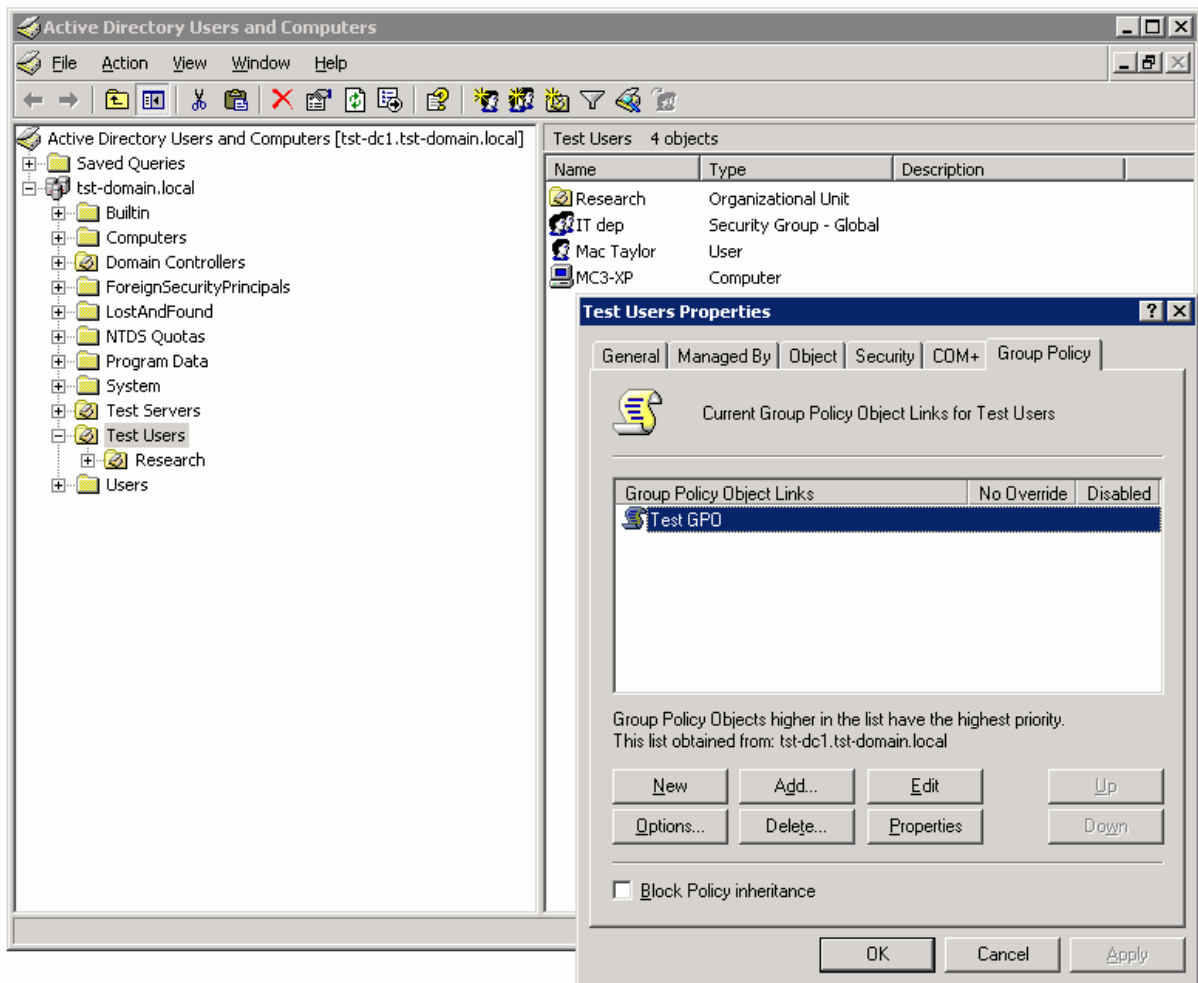
Zásady zabezpečení je možné aplikovat na:

- **Počítač** – použití pro takové zásady zabezpečení, které mají být stejné pro počítač/skupinu počítačů, bez ohledu na přihlášeného uživatele.
- **Uživatel** – zásady zabezpečení platné pro určitého uživatele/skupinu uživatelů, které platí bez ohledu na počítač, ke kterému se daný uživatel přihlásil

Po instalaci služby Active Directory jsou automaticky vytvořeny 2 objekty zásad zabezpečení:

- **Default Domain Policy** – aplikováno na celou doménu
- **Default Domain Controller Policy** – aplikováno na organizační jednotku Domain Controllers

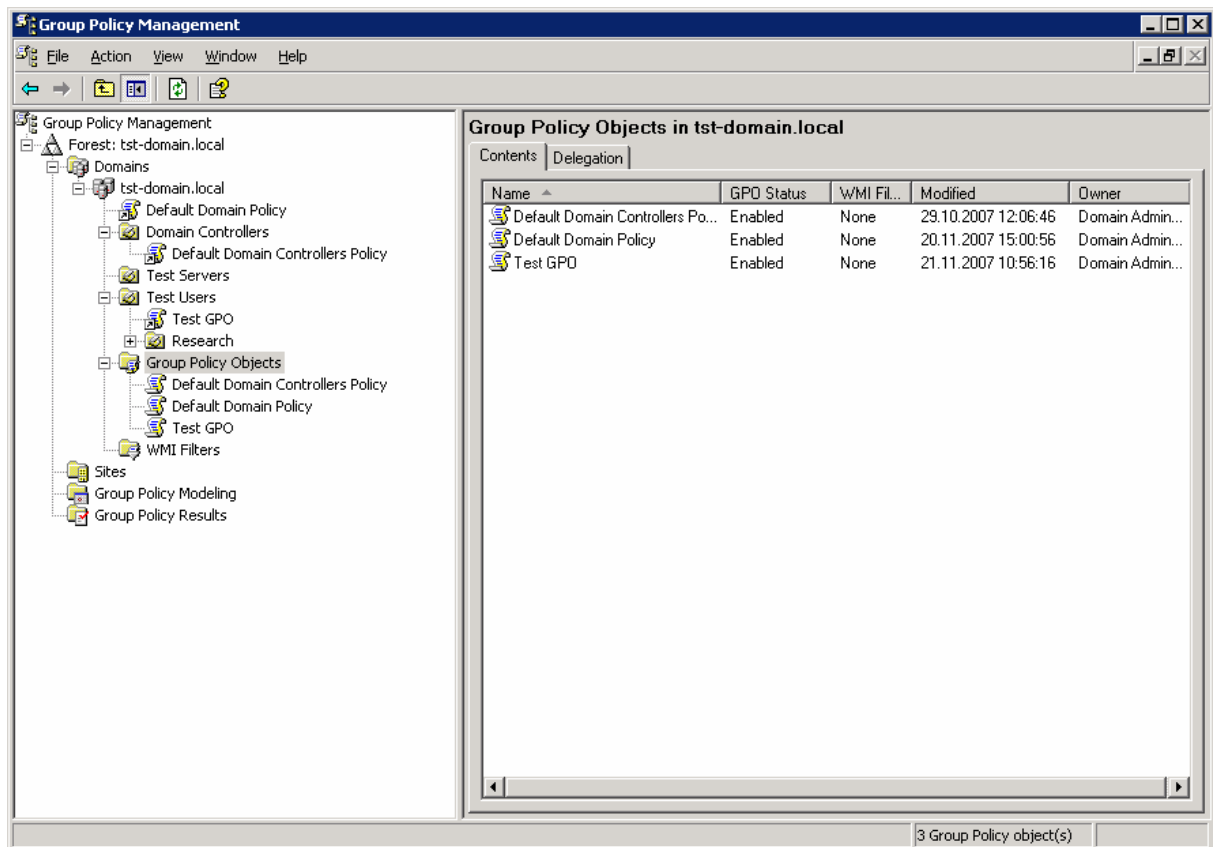
V těchto dvou zásadách zabezpečení jsou definovány zejména nastavení týkající se bezpečnosti. Jedná se o možnost přihlásit se k doménovému řadiči místně/vzdáleně, požadavky na hesla (komplexnost, platnost min. délka apod.)



Nastavení GPO se provádí z konzole Active Directory Users and Computers

Ke každé organizační jednotce je možné přiřadit více než jeden objekt GPO. Při aplikaci jednotlivých zásad zabezpečení na OU systém vygeneruje tzv. výslednou zásadu zabezpečení. Tato výsledná zásada zabezpečení obsahuje i nastavení aplikovaná na základě dědičnosti GPO z mateřských OU (domain, site). Pro prohlížení těchto výsledných zásad zabezpečení slouží příkaz GPreult.exe. Další možností je použití speciální MMC konzole pro správu zásad zabezpečení **Group Policy Management Console**. Tato konzole není standardní součástí operačního systému Windows 2003 a je zapotřebí ji instalovat. Je k dispozici na webových stránkách společnosti Microsoft.

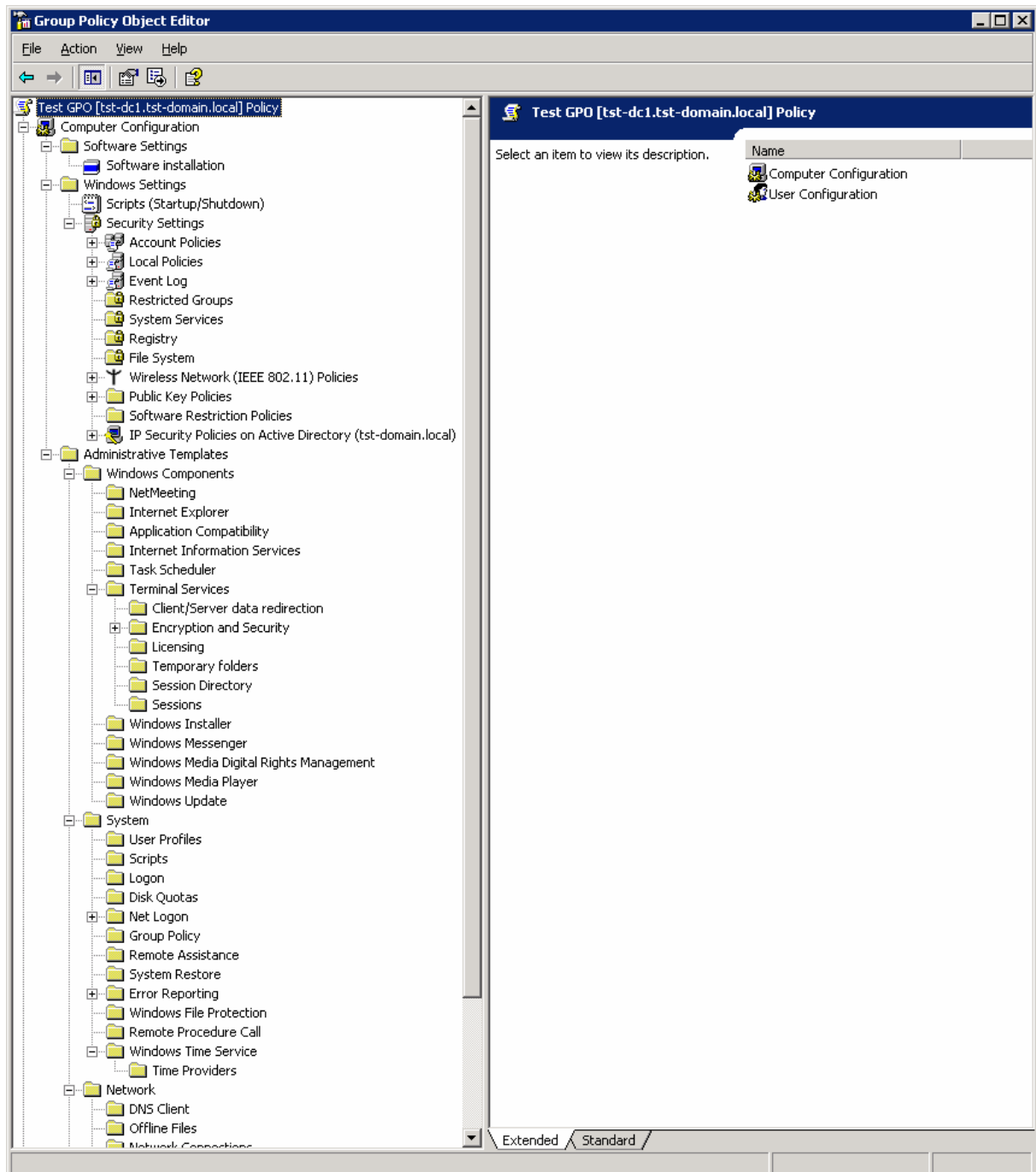
Dále je možné jeden objekt Group Policy aplikovat na více organizačních jednotek.



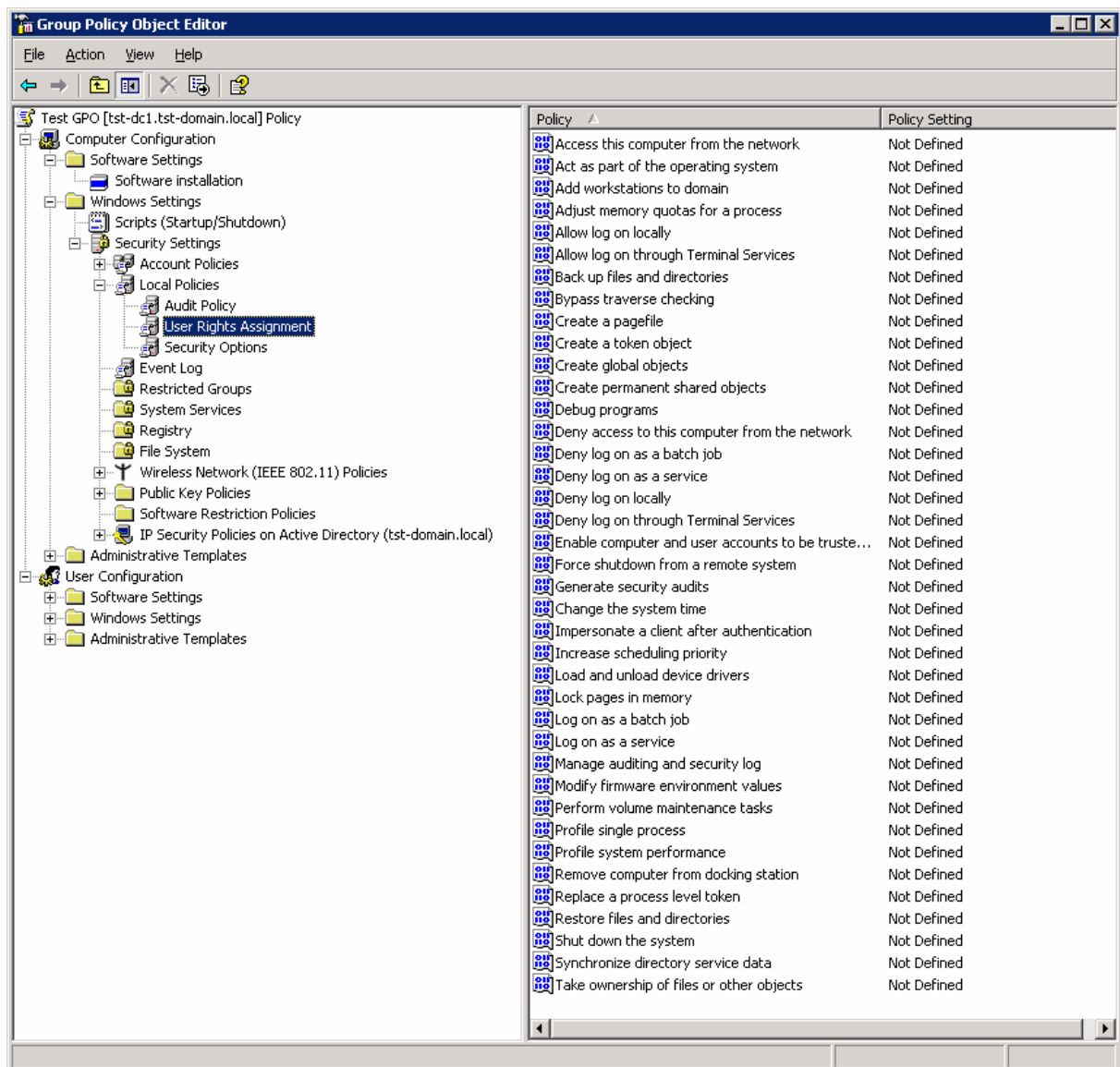
Konzole pro správu GPO

Výhodou této konzole je možnost správy zásad zabezpečení v celém lese. Dále je vidět, které zásady zabezpečení jsou přiřazeny příslušným OU. Seznam všech zásad zabezpečení je v kontejneru Group Policy Objects. U vlastních organizačních jednotek jsou zobrazeny zástupci (links) na příslušné objekty GPO.

Dále je zde možné spočítat výslednou sadu zásad a výsledek zobrazit v grafickém režimu. Případně použít průvodce pro modelování zásad zabezpečení.

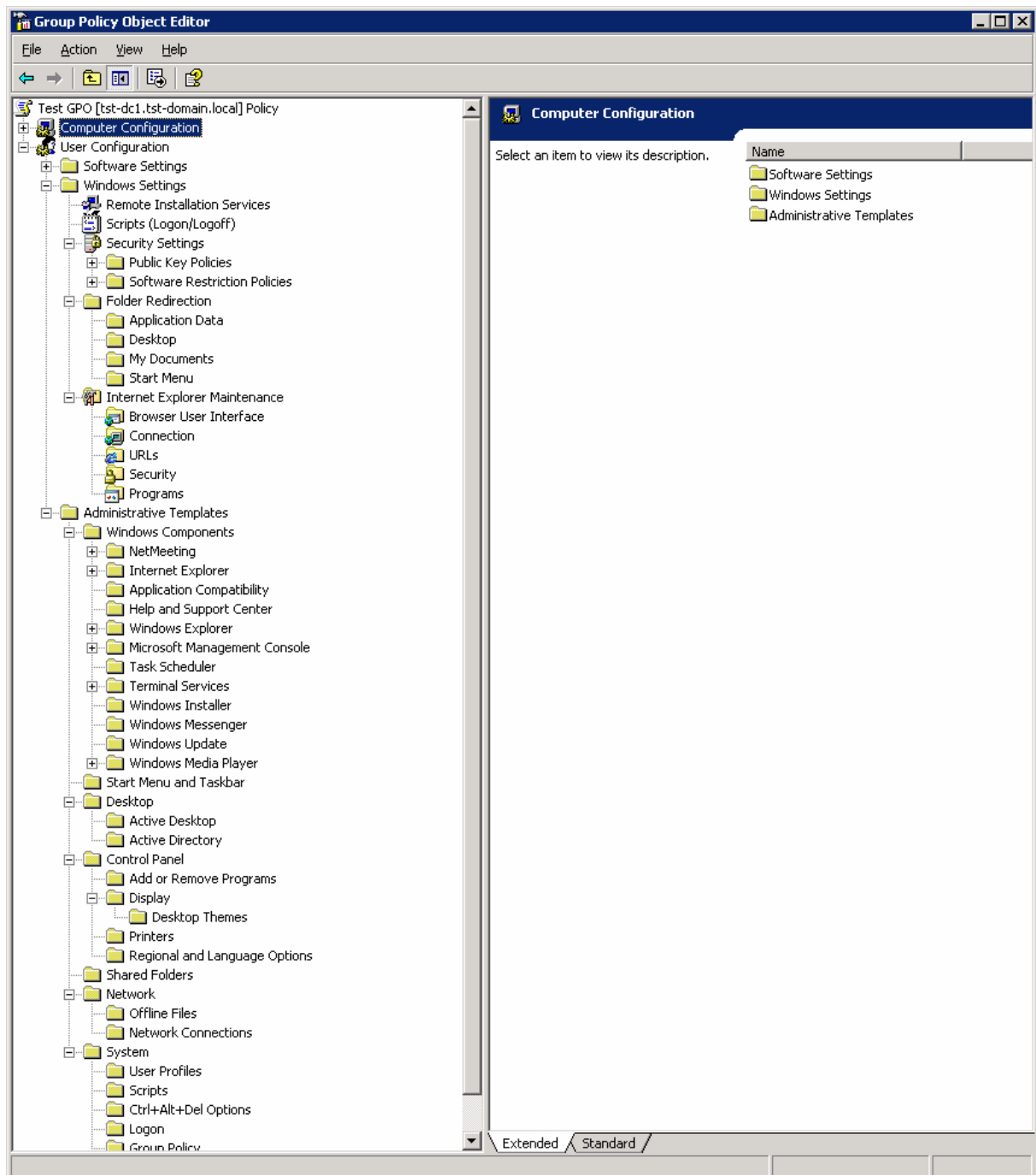


**K vlastní editaci objektu GPO slouží editor zásad zabezpečení.
Nastavení platná pro počítače.**



**K vlastní editaci objektu GPO slouží editor zásad zabezpečení.
Nastavení platná pro počítače.**

Mezi nejdůležitější nastavení v GPO platná pro počítač patří přiřazení uživatelských práv. Na základě těchto nastavení můžeme definovat, kteří uživatelé se mohou přihlásit k počítači. Kteří uživatelé ho mohou vypnout apod.



**K vlastní editaci objektu GPO slouží editor zásad zabezpečení.
Nastavení platná pro uživatele.**