Короткі теоретичні відомості

Мистецтво адміністрування полягає в грамотному використанні всіх налаштувань операційної системи, а також у своєчасному поновленні системного програмного забезпечення.

Основною утилітою адміністрування є "Керування комп'ютером" ("Computer Management"), що містить три групи налаштувань:

1. "Службові програми" ("System Tools"), що, у свою чергу, складається із шести програм:
   - "Перегляд подій" ("Event Viewer") – перегляд системних журналів;
   - "Оповіщення і журнали продуктивності" ("Performance Logs and Alerts") – настроювання виду попереджень і повідомлень:
   - "Загальні папки" ("Shared Folders") – перегляд і адміністрування загальних ресурсів комп'ютера;
   - "Диспетчер пристроїв" ("Device Manager") – настроювання апаратної частини комп'ютера;
   - "Локальні користувачі і групи" ("Local Users and Groups") – адміністрування прав користувачів і груп.
2. "Запам'ятовуючі пристрої" ("Storage") – керування властивостями запам'ятовуючих пристроїв за допомогою розділів: «Зйомні ЗП», «Дефрагментація диска» і «Керування дисками».
3. "Служби і додатки" ("Services and Applications") – інформація про стан різних служб, наприклад, Plug and Play, DNS, DHCP і т.п. .

Другий по важливості в системі безпеки ОС WINDOWS є утиліта "Локальна політика безпеки" ("Local Security Policy"), призначена для адміністрування характеристик паролів, терміну їхньої дії, правил їхнього відновлення і т.д. .

Звичайно, настроювання рівня безпеки виключно індивідуально для кожної комп'ютерної системи і, у кінцевому рахунку, залежить від багатьох чинників. Однак, існують деякі рекомендовані стандарти, які реалізовані в шаблонах безпеки.

Шаблони безпеки для адміністратора WINDOWS

Шаблон безпеки являє собою звичайний текстовий файл із розширенням *.inf, що знаходиться в папці %WinRoot%\=security\templates і містить настройки наступних груп параметрів операційної системи.

- Account Policies: політика паролів, правила блокування облікових записів і настроювання протоколу Kerberos. Якщо дані політики застосовуються на рівні організаційного підрозділу (Organization Unit), то вони торкають тільки локальні бази облікових записів (SAM). Настроювання доменних облікових записів регулюються Default Domain Policy.

- Local Policies: система аудита, права користувачів і основних настроювань безпеки.
- Event Log Settings: настроювання трьох журналів аудита (System, Application, Security).
- Restricted Groups: обмеження членства в групах.
- System Services: режим запуску і контроль доступу до системних служб.
- Registry values: дозвіл на доступ до даних реєстру.
- File System: дозвіл на доступ до файлів і папок.

Стандартне постачання WINDOWS містить кілька шаблонів, яки зберігаються в папці %WinRoot%\inf, та використовуються для настроювання системи на різні рівні безпеки,

Додаткове прикладне програмне забезпечення:

- "*AUTORUNS.EXE*" – програма для відображення усіх процесів, що завантажені на даному комп'ютері. Ця програма *не потребує інсталяції.*
- "*FileMon.exe*" – програма - монітор процесів у реальній годині. *Не потребує інсталяції.*

Команда NET

Net accounts

Служить для оновлення бази облікових даних користувачів, зміни паролів і параметрів підключення для всіх користувачів.

Net computer

Служить для додавання або видалення імені комп'ютера з бази даних домену.

Net group

Додавання, відображення і зміна глобальних груп в доменах.

Net localgroup

Додавання, відображення і зміна локальних груп. Команда Net localgroup без параметрів виводить ім'я сервера і імена локальних груп комп'ютера.

Net share

Управління загальними ресурсами. При виклику команди Net share без параметрів виводяться відомості про всі загальних ресурсах локального комп'ютера.

Net view

Виводить список доменів, комп'ютерів або загальних ресурсів на даному комп'ютері. Викликана без параметрів, команда Net view виводить список комп'ютерів в поточному домені.