Лекція 3

Групові політики

План

1. Групові політики. Об’єкти групової політики
2. Опрацювання групових політик
3. Інструмент *Group Policy Preferences*
4. Адміністративні шаблони

1. Групові політики. Об’єкти групової політики

Групові політики (*Group Policy*) забезпечують централізований спосіб керування налаштуваннями для користувачів та комп’ютерів.

Групові політики застосовуються до різних контейнерів (сайт, домен, організаційна одиниця), але **рекомендовано передусім застосовувати групові політики до організаційних одиниць (OUs)** - організаційні одиниці для цього й розроблялися.

Групові політики існують у формі **об’єктів групової політики** (Group Policy Objects, GPO).

Об’єкт групової політики складається з:

- **контейнера** групової політики (*Group Policy Container*, GPC)
- **шаблону** групової політики (*Group Policy Template*, GPT)

Шаблони, на основі яких створюються GPO, зберігаються у папці *SYSVOL* контролера домену.

Один GPO може бути пов’язаний з багатьма контейнерами.
Один контейнер може бути пов’язаний з багатьма GPO.

1. Групові політики. Об’єкти групової політики

Чого можуть стосуватися групові політики (деякі приклади)

- паролів (наприклад, термін дії, вимоги до складності, ...)
- аудиту
- мережних налаштувань
- налаштування принтерів
- автоматичного підключення мережного диску
- змінних середовища
- програм за замовчуванням
- інших налаштувань, які виконуються через *Панель керування*
- та багато чого іншого

Конкретні налаштування у межах GPO можуть стосуватися **користувачів і / або комп’ютерів**.

1. Групові політики. Об’єкти групової політики

Консоль ***Group Policy Management*** є базовим інструментом для роботи з груповими політиками (хоча задання групової політики можна ініціювати і з оснащення *Active Directory Users and Computers*, наприклад).

Консоль *Group Policy Management*:

- дає змогу бачити групові політики ієрархічно, в межах усього лісу;
- виводить відомості про те, як GPO різних рівнів пов’язані між собою;
- показує перелік всіх GPO домену окремим вузлом;
- дає змогу працювати з WMI-фільтрами;
- має окремий вузол *Starter GPO* для початківців;
- містить інструменти визначення результативного набору політик.

Нова групова політика створюється через створення нового GPO.

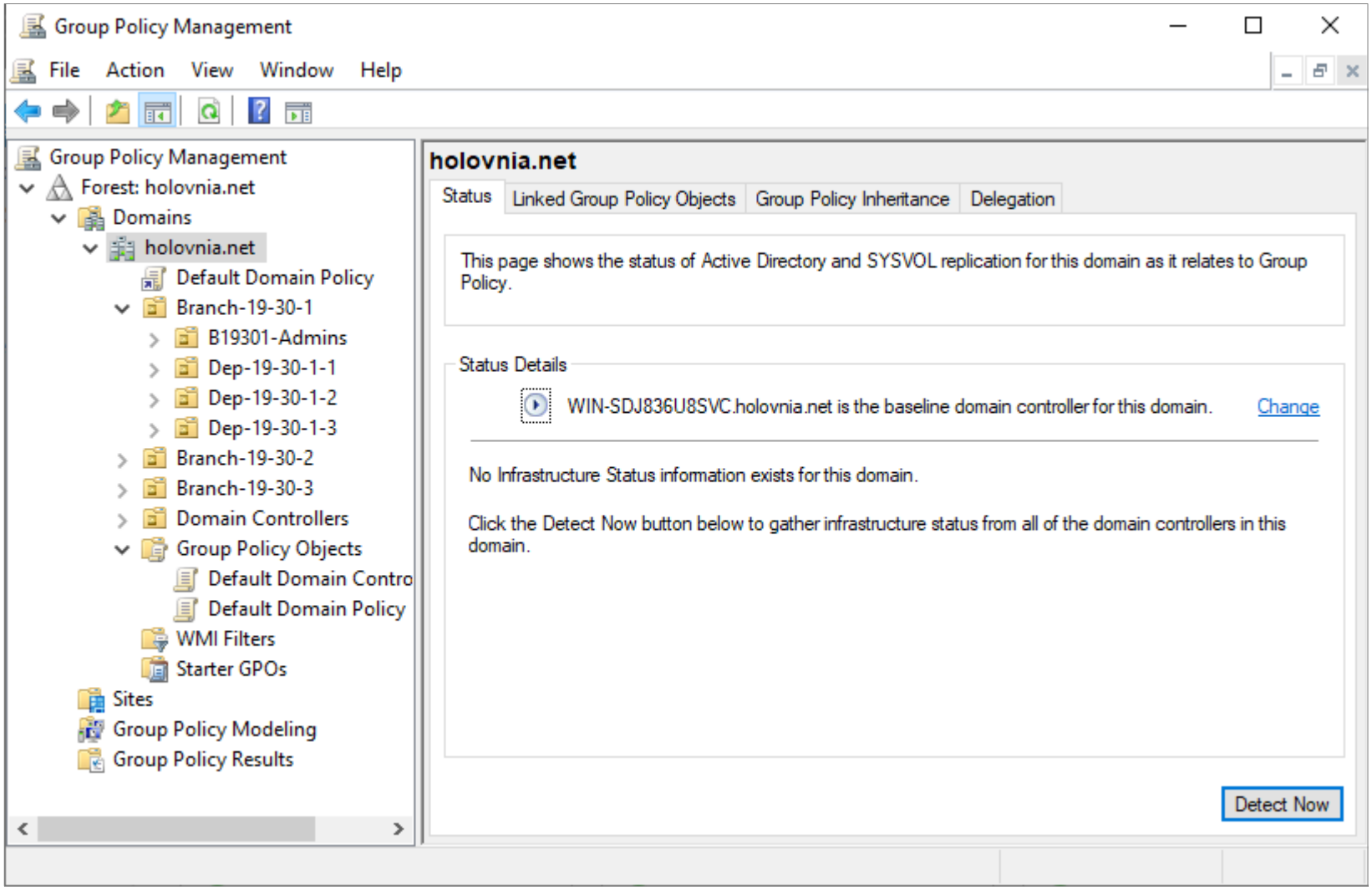
Під час **створення нового GPO:**

- спершу створюється GPO на основі стандартного шаблону (вказуються контейнери, яких буде стосуватися цей GPO),
- потім GPO доналаштовується для виконання необхідних задач.

Консоль Group Policy Management

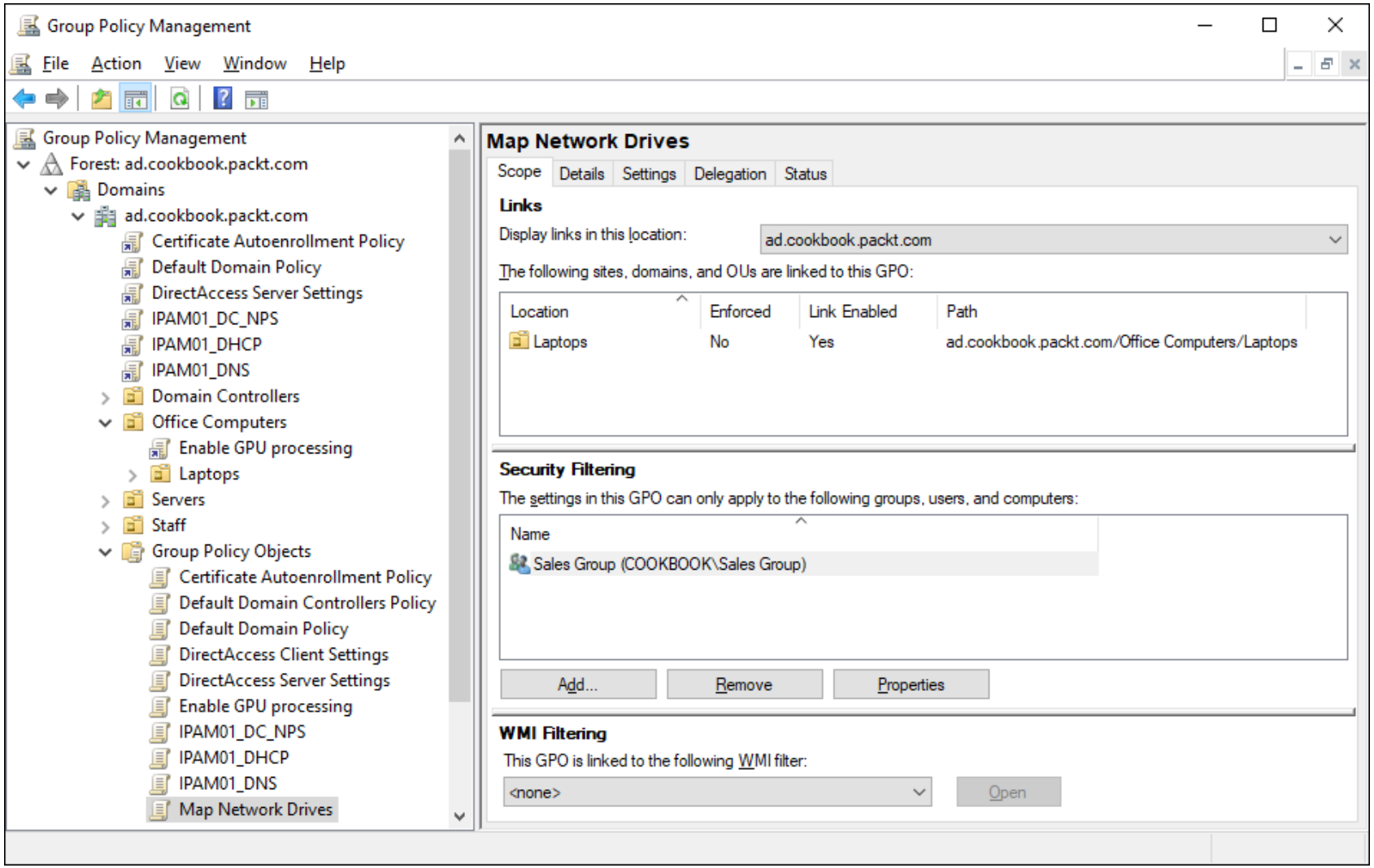
(Консоль керування груповими політиками)

у Windows Server 2019



Приклад групової політики. Крок 1:

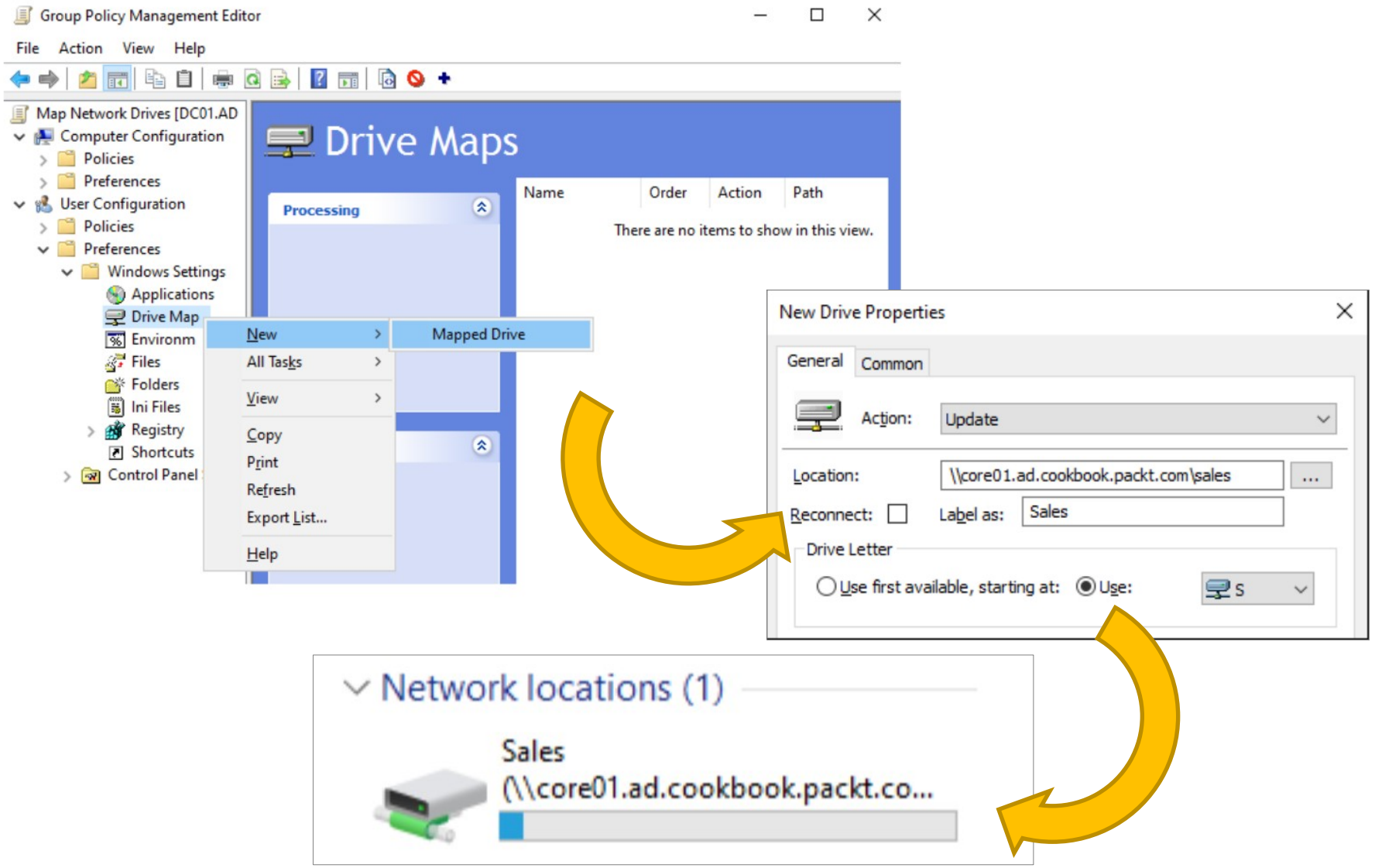
GPO має назву *Map Network Drives*,
застосовується до організаційної одиниці *Laptops* і групи *Sales Group*



Джерело прикладу: M. Henderson, J. Krause. Windows Server 2019 Cookbook Second Edition (Second Edition). Packt Publishing, 2020

Приклад групової політики. Крок 2:

GPO *Map Network Drives* тепер дозволяє автоматично підключати мережний диск відповідним користувачам



Джерело прикладу: M. Henderson, J. Krause. Windows Server 2019 Cookbook Second Edition (Second Edition). Packt Publishing, 2020

2. Опрацювання групових політик

Послідовність опрацювання групових політик:

1) Локальні політики (***L****ocal policy*)
2) Політики сайту (***S****ite policy*)
3) Політики домену (***D****omain policy*)
4) Політики організаційних одиниць (***OU*** *policy*)

У наведеній вище послідовності ↑
наступні політики (розташовані *пізніше* у цій послідовності),
мають перевагу над *попередніми політиками* (розташованими в ній *раніше*).

Приклад

Перша політика містить деяке налаштування на *рівні сайту (2)*.

Друга політики містить таке саме налаштування, але на *рівні OU (4)*.

Тоді щодо даного налаштування буде застосовуватися друга політика, бо вона розташована вище за першу (4 супроти 2).

2. Опрацювання групових політик

Виняток:

- Коли обрано опцію **Block Inheretance** (*Блокувати спадкування*)

  Опцію можна встановити для домену чи для OU.

  Фактично спадкування не блокується, а радше *фіксується*.

  Тоді починаючи від обраного рівня (цього домену чи цієї OU), наступні політики не будуть переважати над попередніми.

  (Тобто відбудеться *обов'язкове спадкування* налаштувань цього рівня наступними рівнями ієрархії)

  Виняток з винятка:

- Коли обрано опцію **No Override** (*Не замінятися*)

  Зупиняє дію опції *Block Inheretance* для окремих доменів або OU.

  (Зазвичай для тих, які потребують індивідуальних налаштувань, які не мають успадковуватися від попередніх рівнів)

  Опції *Block Inheretance* та *No Override* треба використовувати **дуже обережно** й лише за реальної потреби. У багатьох випадках достатньо стандартних налаштувань успадкування групових політик (як на попередньому слайді).

2. Опрацювання групових політик

Поширення групових політик

Якщо налаштування успадковування групових політик не змінено, то за замовчуванням:

- *GPO, застосовані до **сайту**,*
  застосовуються і до всіх користувачів та комп’ютерів цього сайту;
- *GPO, застосовані до **домену**,*
  застосовуються і до всіх користувачів та комп’ютерів домену,
  а також (шляхом успадковування) всіх користувачів та комп’ютерів організаційних одиниць, що містяться всередині цього домену;
- *GPO, застосовані до **організаційної одиниці**,*
  застосовуються і до всіх користувачів та комп’ютерів цієї організаційної одиниці, а також (шляхом успадковування)
  всіх користувачів та комп’ютерів в її дочірніх організаційних одиницях.

Як перевірити, чи правильно працюватимуть групові політики

Часто виникає потреба:

- зрозуміти, які політики застосовуються до конкретних об’єктів домену
- розібратися, чому групові політики не працюють так, як було задумано
- виявити та усунути конфлікти групових політик

Для вирішення подібних проблем використовують
результативний набір політик (*resultant set of policy*).

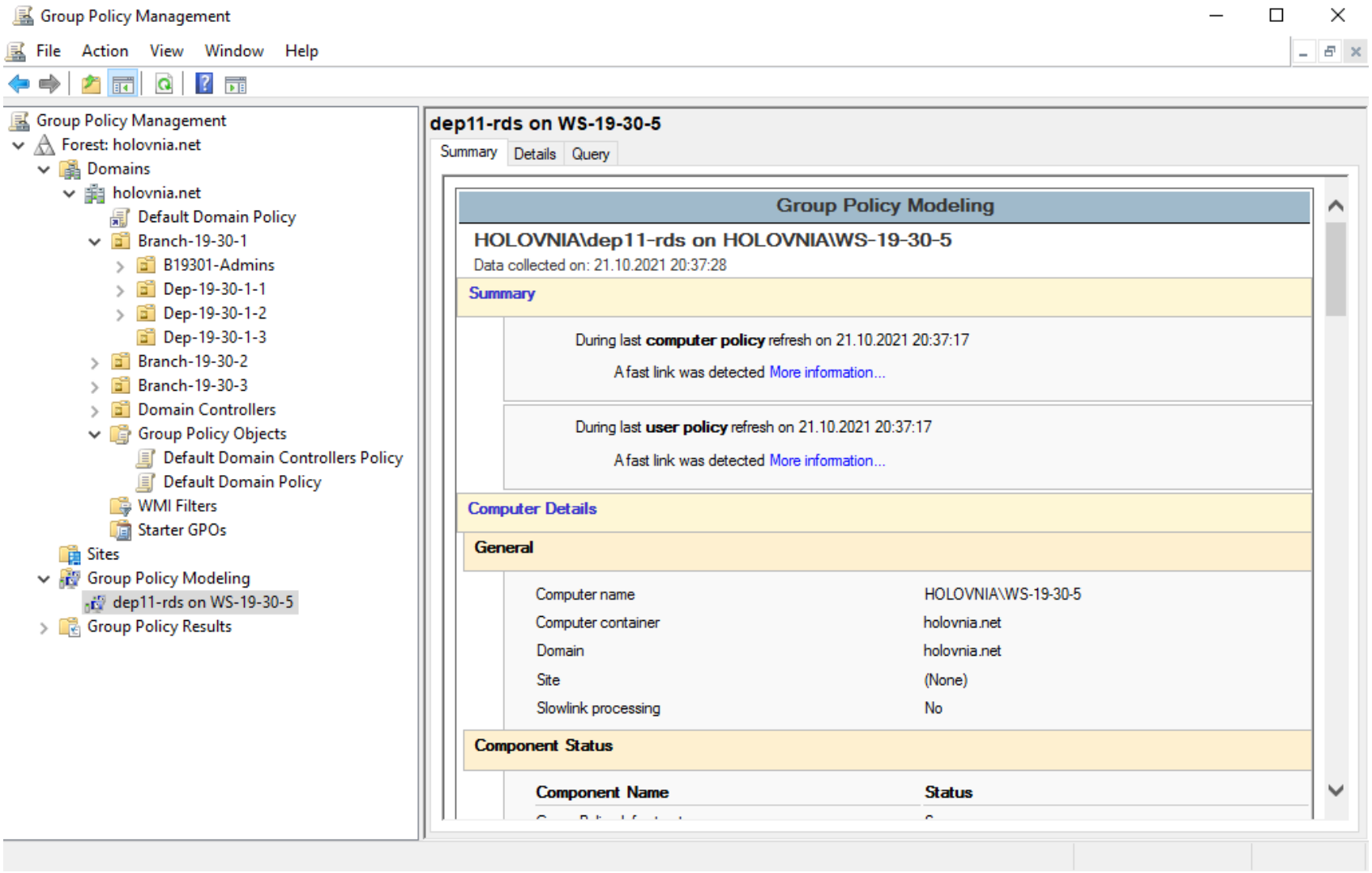
Інструменти для визначення результативного набору політик:

- **Group Policy Modeling** (Моделювання групових політик)
  Дозволяє побачити, як вплине зміна окремих налаштувань на застосування політик. *Приклади налаштувань, як можна дослідити:* переміщення облікових записів в іншу OU, зміна членства у групах тощо.

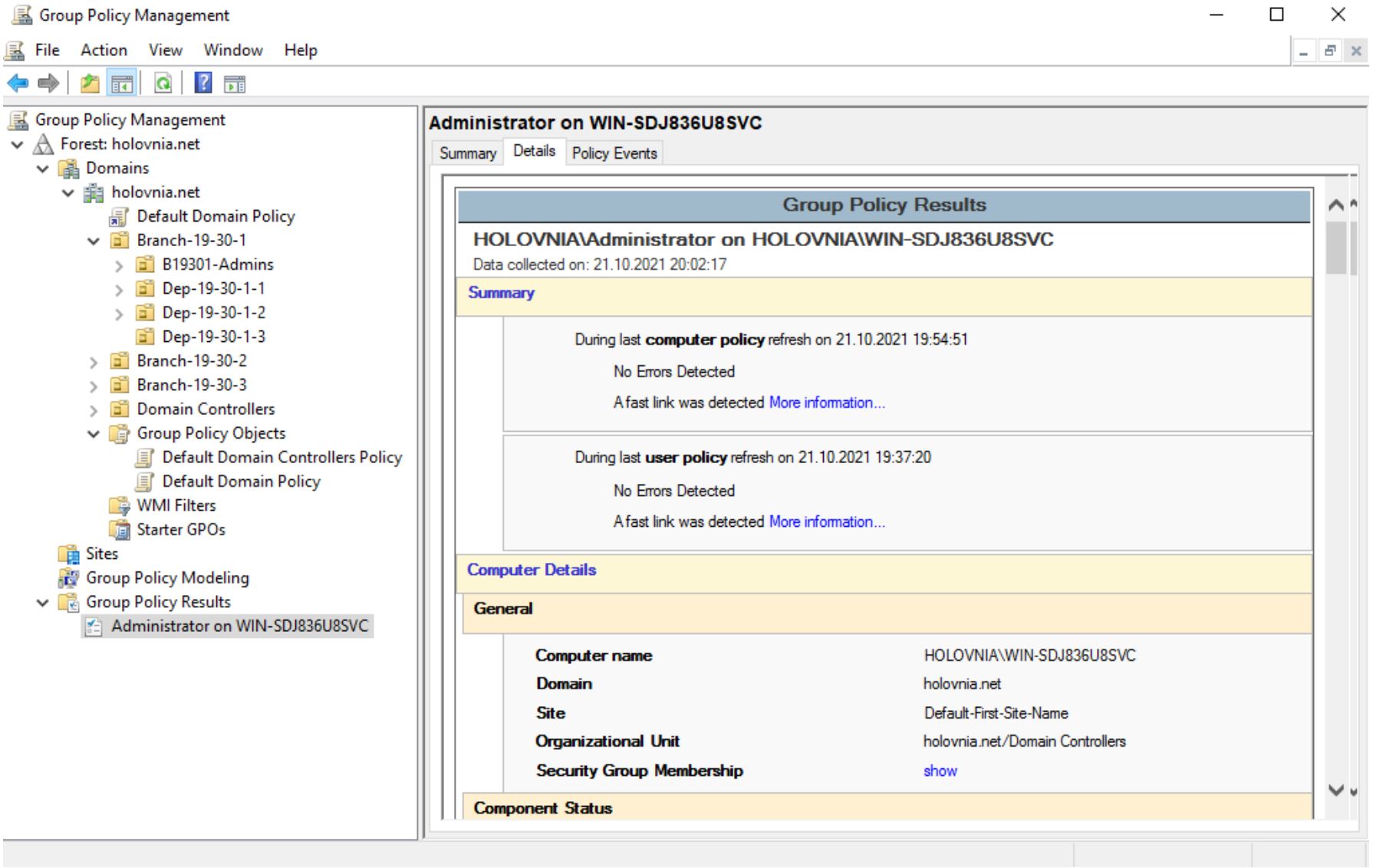
- **Group Policy Results** (Результати групових політик)
  Дає змогу вирішувати наявні проблеми з політиками, показуючи, які саме налаштування діють для конкретних користувачів та комп’ютерів.

  За замовчуванням, використовувати *Group Policy Modeling* та *Group Policy Results* можуть члени груп *Domain Admins* та *Enterprise Admins*. За потреби ці права можна делегувати.

Моделювання групових політик,
згереноване для випадку
додавання звичайного користувача домену у групу *Domain Admins*



Результати групових політик,
згереновані для адміністратора поточного контролера домену



2. Опрацювання групових політик

Фільтрування групових політик

Фільтрування дозволяє встановлювати окремі групові політики для об’єктів домену, не винесених в окрему організаційну одиницю.

Нудно, але важливо. Добре продумана структура домену часто дозволяє уникнути фільтрування групових політик.

Приклад ситуації, коли знадобиться фільтрування:

Потрібно встановити спеціальні групові політики для ноутбуків, під’єднаних до домену, й окремі - для ПК. Але ПК і ноутбуки не винесені в окремі OU.

Таке фільтрування можна зробити через WMI-запит.

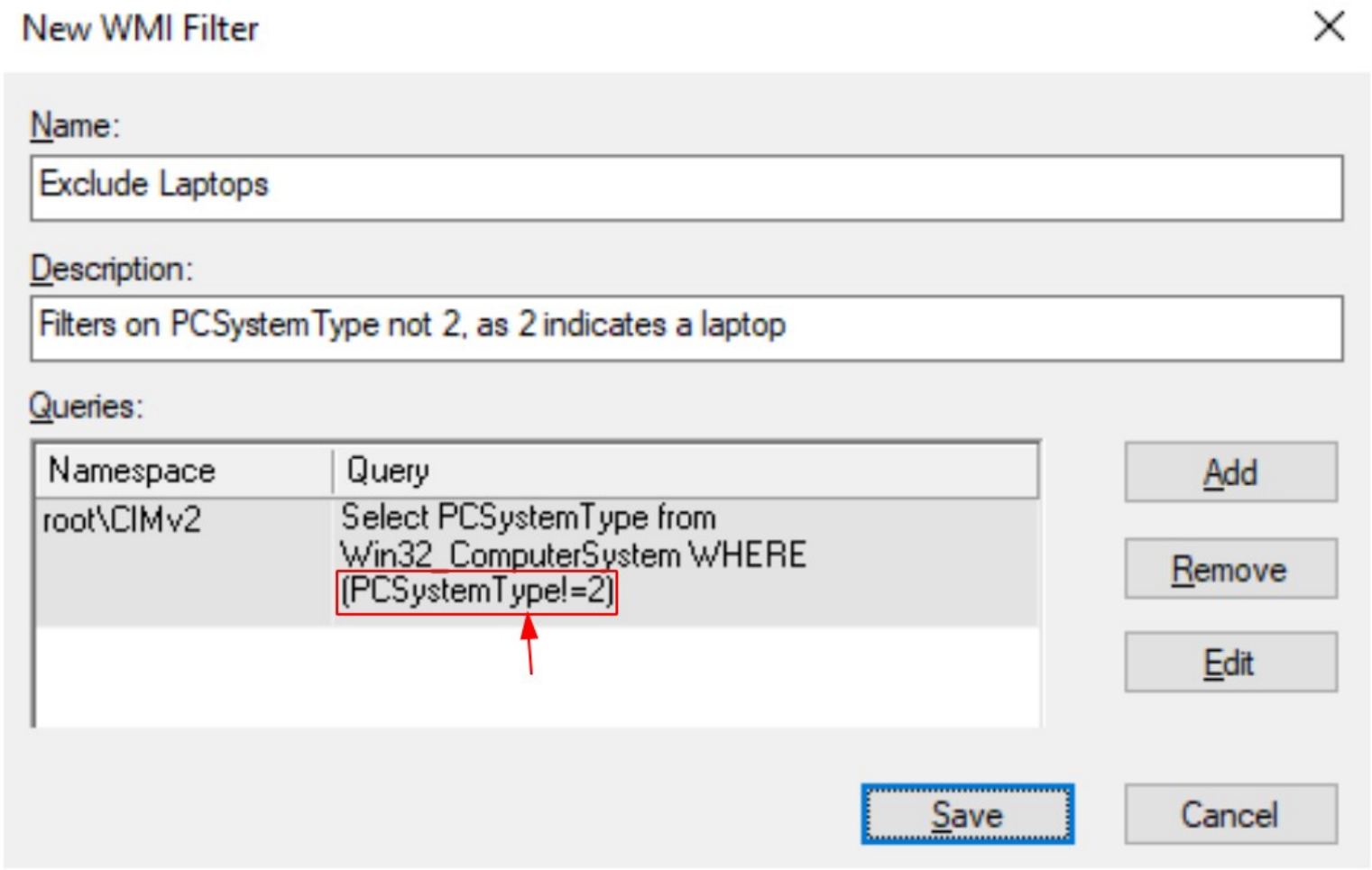
WMI (*Windows Management Instrumentation*) використовується для віддаленого адміністрування Windows систем. WMI-запити дозволяють одержувати різноманітну інформацію про систему.

Для фільтрування групових політик:

- спершу створюється фільтр, який відділяє потрібні об’єкти домену від решти;
- потім фільтр використовується для уточнення потрібного GPO.

Фільтрування групових політик. Крок 1:

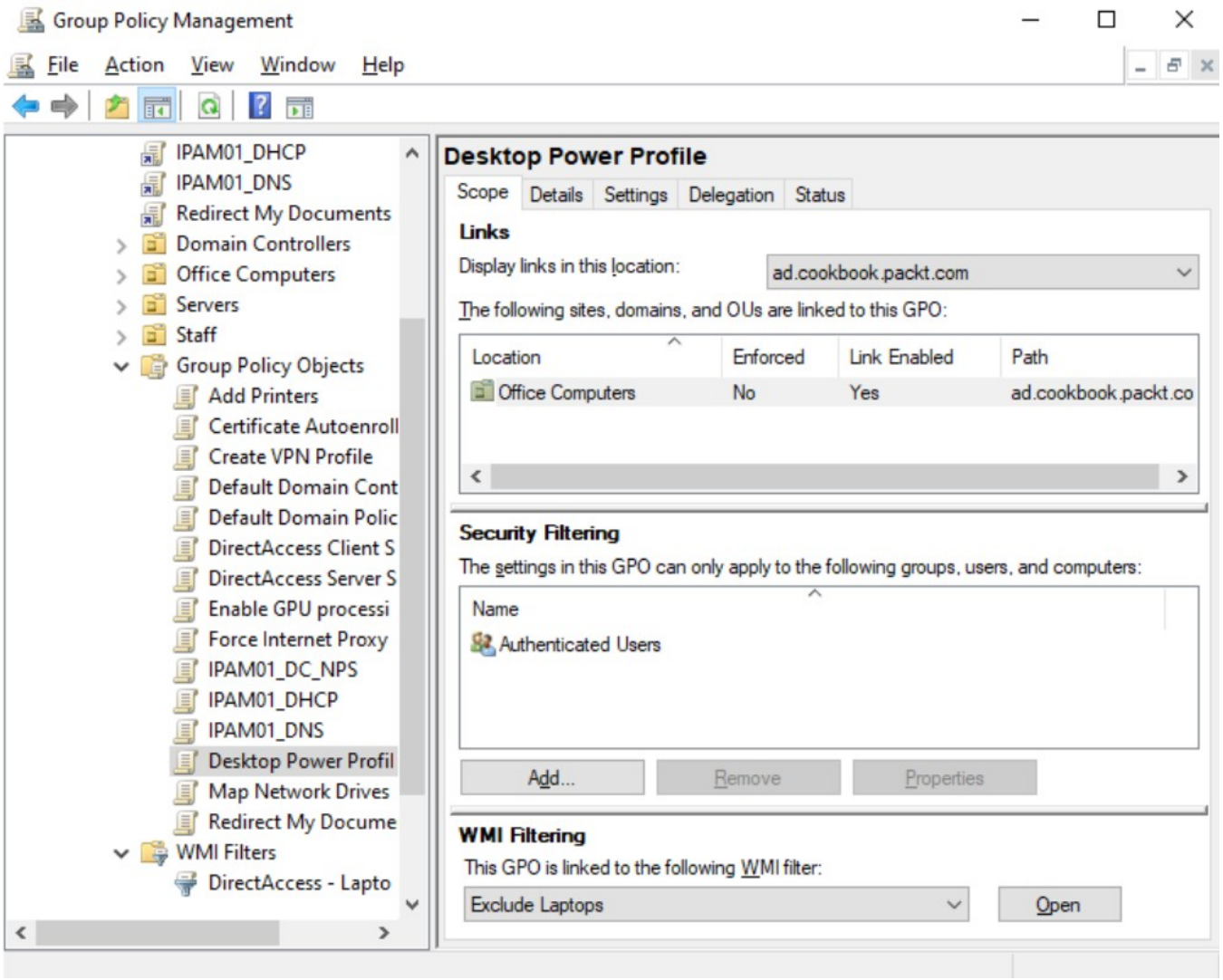
створення фільтру *Exclude Laptops*, який згодом дозволить виключати з об’єктів групової політики ноутбуки (PCSystemType!=2)



Джерело прикладу: M. Henderson, J. Krause. Windows Server 2019 Cookbook Second Edition (Second Edition). Packt Publishing, 2020

Фільтрування групових політик. Крок 2:

уточнення GPO *Desktop Power Profile* за допомогою фільтру *Exclude Laptops**



Джерело прикладу: M. Henderson, J. Krause. Windows Server 2019 Cookbook Second Edition (Second Edition). Packt Publishing, 2020

3. Інструмент *Group Policy Preferences*

Preferences (вподобання) у механізмі групових політик допомагають спростити традиційне налаштування користувацьких систем.

Group Policy Preferences виділені в окрему групу в оснащенні Group Policy Management Editor.

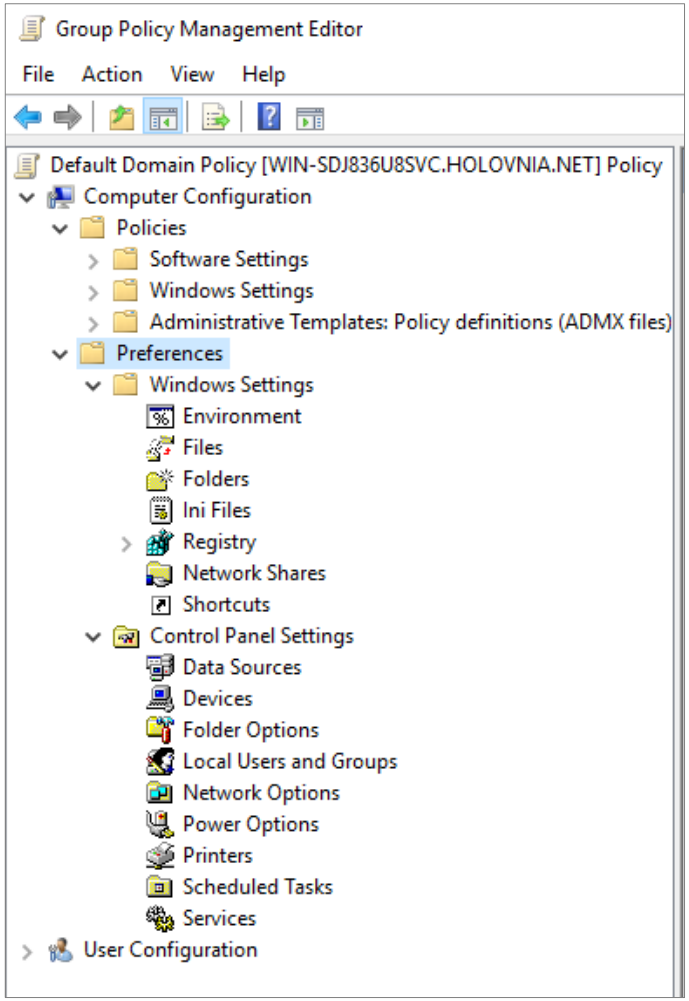
Іноді налаштування, доступне через *Group Policy Preferences*, можна встановити і через традиційні групові політики. Якщо те саме налаштування встановлене обома способами, перевагу матиме традиційне.

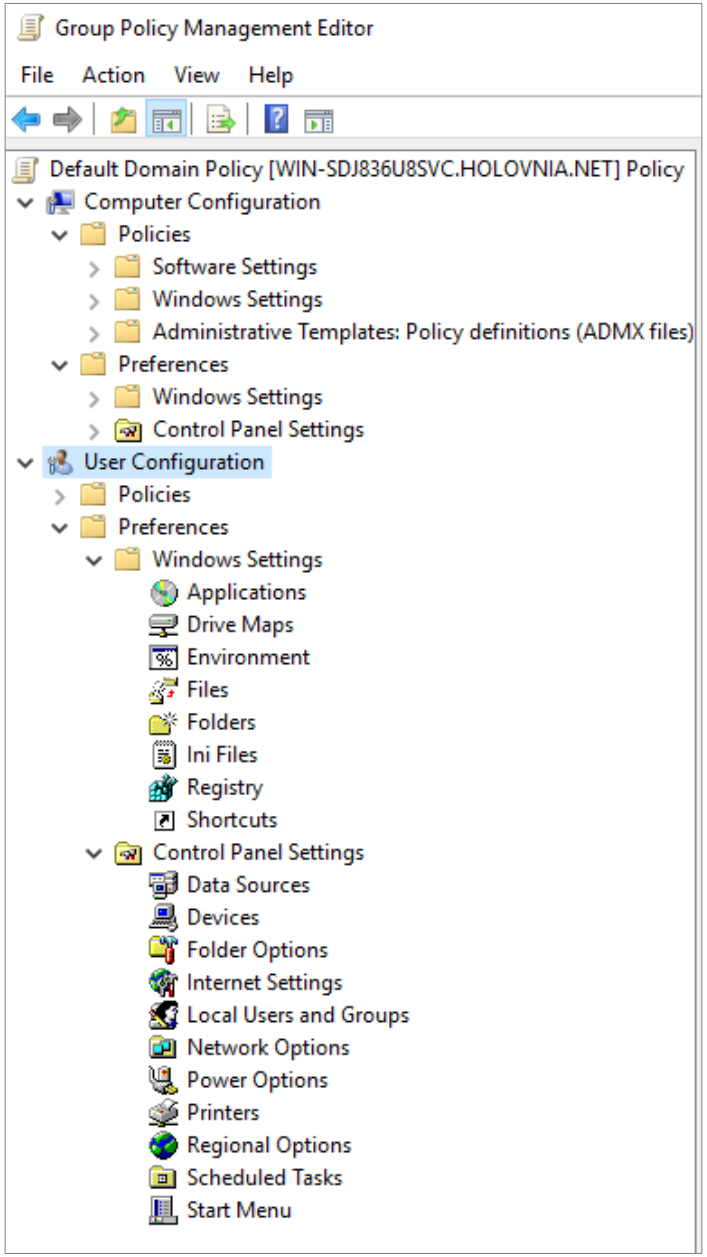
Основна відмінність *Group Policy Preferences* і традиційних групових політик: користувач може локально змінювати налаштування, задані через *Group Policy Preferences* (якщо має відповідні повноваження).

Group Policy Preferences ⟶ для користувачів

↓

для комп’ютерів





4. Адміністративні шаблони

Адміністративні шаблони (*Administrative Templates*) є механізмом розширення переліку стандартних налаштувань групових політик.

Шаблони можуть імпортуватися разом з певним програмним засобом чи технологією.

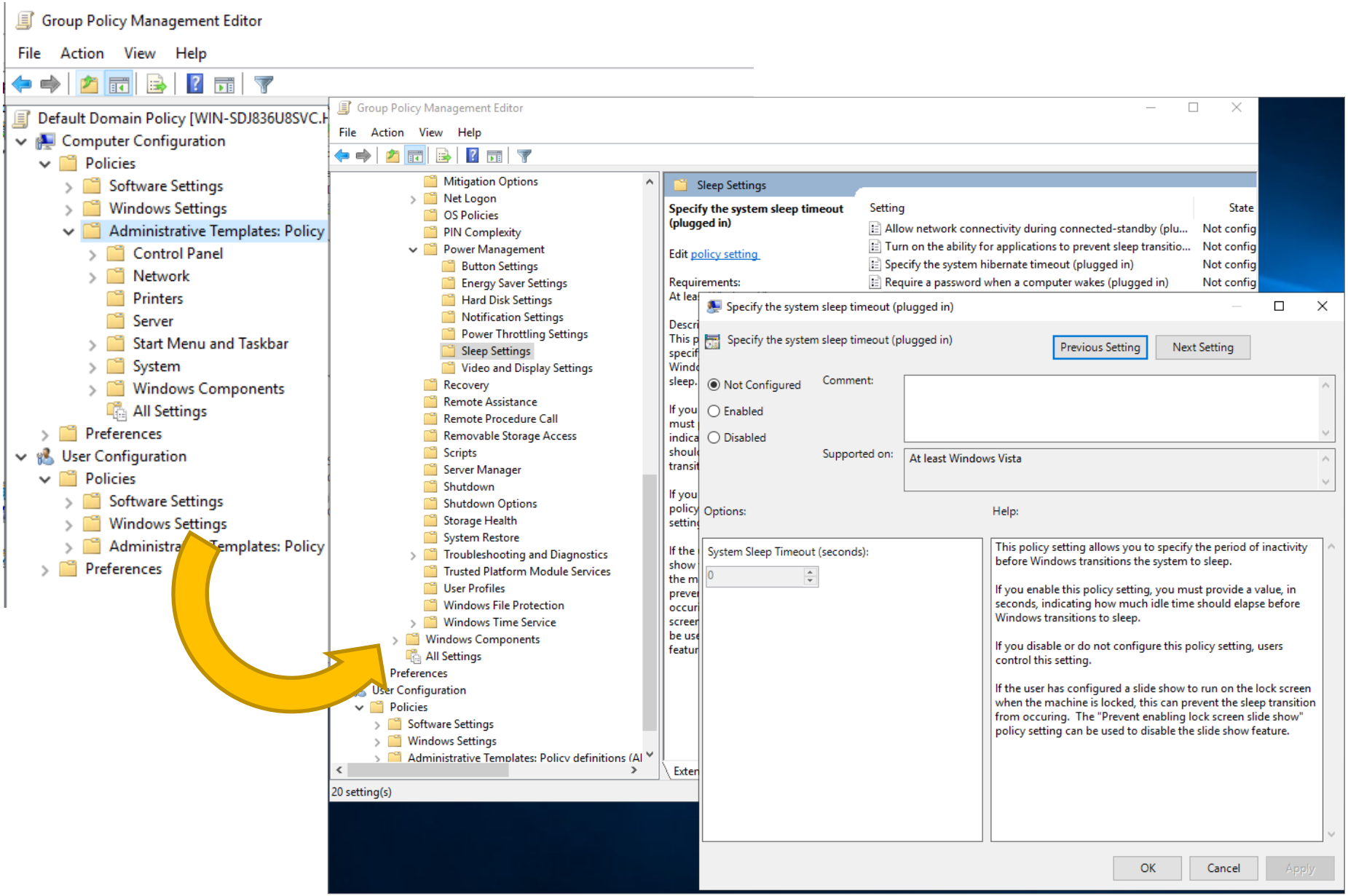
Адміністративний шаблон складається з двох файлів:

- ADMX-файл містить самі налаштування
- ADML-файл містить текст, який відповідає цим налаштуванням у вікнах консолі *Group Policy Management* (текст відображається мовою локалізації вашої системи)

Імпортувати адміністративні шаблони можна:

- через вузол *Administrative Templates*
  (пункт контекстного меню *Add/Remove Templates*)
- вручну, через відповідні папки на контролері домену.

Адміністративні шаблони для налаштування комп’ютерів
і приклад налаштування часу переходу в режим сну (неактивного)



4. Адміністративні шаблони

Приклад ситуації, коли може знадобитися підключити адміністративний шаблон:

під час налаштування GPO потрібної опції (наприклад, описаної у документації) не знайдено.

Для деяких технологій необхідні специфічні адміністративні шаблони.
Тоді ці шаблони треба імпортувати. Зазвичай ідеться про папки:

- C:\Windows\PolicyDefinitions (для ADMX-файлу)
- C:\Windows\PolicyDefinitions\en-US (для ADML-файлу, англомовна локалізація).