

Wcześniejsze ćwiczenia opatrzone były wskazówkami, których ilość zmniejszała się stopniowo. Miały na celu oswojenie ze środowiskiem i nabycie podstawowych umiejętności „uczenia się elementów systemu”.

Dwa kolejne ćwiczenia są typowo zadaniowe.

W ich ramach należy:

- zapoznać się z dokumentacją dotyczącą rozpatrywanego obszaru,
- ustalić scenariusz pokazania działania mechanizmów,
- zrealizować ww. scenariusz dokumentując kolejne kroki
- sporządzić raport/sprawozdanie

Raport powinien zawierać:

- część teoretyczną – opisującą zagadnienie w sposób wyczerpujący, przejrzysty, zwięzły.
- części praktycznej – opis przebiegu realizacji wspomnianego scenariusza ilustrowany zrzutami ekranów z newralgicznych kroków.

Raporty tylko w formie elektronicznej.

---

Zadanie 4a.

Zadanie dotyczy uprawnień w systemie.

To zadanie należy wykonać w grupie 2 osobowej. Jest to pewnym utrudnieniem, ale biorąc pod uwagę dostępne środki zadanie jest wykonalne.

W części teoretycznej należy zawrzeć:

- jakie są możliwe sposoby nadawania uprawnień i ich propagacji („exact”, „authorization list”, „user class”+ „special authorithies”, „primary group”....)
- predefiniowane klasy użytkowników – uprawnienia (\*USER, \*PGMR, \*SYSOPR...)
- rozwinięcie uprawnień (\*USE, \*CHANGE..., \*EXCLUDE) – na co pozwalają, co się pod nimi kryje
- co to jest „adopted authority” i jak działa
- hierarchia: które są ważniejsze
- \*PUBLIC
- własność i przejmowanie

Część praktyczna (niezbędne minimum):

1. Należy stworzyć obiekt (np. bibliotekę, Source Physical File w bibliotece)
2. Nadać uprawnienia bezpośrednio, pokazać działanie.
3. Stworzyć listę autoryzacji
4. Skojarzyć listę z pktu 3 z obiektem (1)
5. Nadać uprawnienia przez listę autoryzacji, pokazać działanie.

Sporządzić raport.

---

Zadanie 4b.

Journaling.

W części teoretycznej należy opisać mechanizm journalingu w systemie.

- jak działa,
- jakie obiekty są niezbędne, reguły,
- co możemy odnotowywać,
- które ze zmian są odwracalne automatycznie (komendą), a które tylko „do wiadomości”

W części praktycznej należy:

- utworzyć obiekt typu journal
  - utworzyć obiekt typu journal receiver
  - skonfigurować ochronę wybranego obiektu.
  - wprowadzić w chronionym obiekcie kilkukrotne zmiany.
  - pokazać, że zmiany zostały zapisane w kronice (zwrócić uwagę na filtrowanie wpisów)
  - odwrócić wybrane zmiany (zwrócić uwagę jak działa mechanizm odwracania)
- (tutaj należy uważnie zapoznać się komendami i ich opisami, APYJRNCHG nie służy do odwracania zmian – często sprawia to problem studentom)

„dobra rada”: jak chroniony obiekt warto wybrać sobie Source Physical File – zmiany/odwrócenie w (de facto) pliku tekstowym łatwo jest pokazać.

Sporządzić raport.