

Wnioski z ćwiczenia dotyczącego zarządzania ACL w systemie Linux

1. Precyzyjne zarządzanie uprawnieniami

Uczniowie nauczyli się, że dzięki ACL można bardzo dokładnie określić, kto ma dostęp do plików i katalogów – niezależnie od tradycyjnych uprawnień właściciela, grupy i innych użytkowników. ACL pozwala przypisać indywidualne prawa dostępu dla wielu użytkowników i grup.

2. Różnice między plikami z ACL a bez ACL

- Pliki z ustawionymi ACL są oznaczone znakiem „+” w wynikach polecenia `ls -l`.
- Pliki bez ACL mają tylko standardowe uprawnienia (rwx dla właściciela, grupy i innych).
- ACL umożliwia nadanie uprawnień użytkownikom, którzy nie są właścicielami ani członkami grupy przypisanej do pliku.

3. Znaczenie narzędzi

- `getfacl` – pozwala sprawdzić aktualne ustawienia ACL.
- `setfacl` – umożliwia dodawanie, modyfikowanie i usuwanie ACL.
- `chacl` – alternatywne narzędzie do zarządzania ACL (w niektórych systemach).

4. Domyślne ACL

- Ustawienie domyślnych ACL dla katalogu powoduje, że nowe pliki i katalogi dziedziczą te uprawnienia.
- To bardzo przydatne w środowiskach współdzielonych, gdzie wiele osób pracuje w jednym katalogu.

5. Usuwanie ACL

- Można usunąć konkretne wpisy ACL lub wszystkie jednocześnie (`setfacl -b`).
- Po usunięciu ACL plik wraca do standardowego modelu uprawnień.

6. Podsumowanie praktyczne

Ćwiczenie pokazało, że:

- ACL to potężne narzędzie do zarządzania dostępem.
- Pozwala ono na większą elastyczność niż tradycyjny system uprawnień w Linuxie.
- Uczniowie zdobyli praktyczne umiejętności w tworzeniu użytkowników, grup, przypisywaniu uprawnień i analizie ich działania.