Temat: Prawa dostępu i prawa własności do plików w Linux.

Listy kontroli dostępu (ACL)

Komendy omówione w poprzednim ćwiczeniu nie pozwalają na nadawanie uprawnień na danym pliku więcej niż jednemu użytkownikowi lub grupie.

Umożliwiają to listy kontroli dostępu (ACL – Access Control List), które zapewniają możliwość ustawienia na plikach i katalogach rozszerzonej grupy uprawnień.

Pozwalają administratorom ustawiać w taki sposób uprawnienia, że różnią się one na poszczególnych katalogach.

Aby możliwe było użycie ACL system plików musi być podmontowany z włączonym wsparciem dla ACL, opcja acl musi być dodana do montowanego systemu plików w pliku /etc/fstab.

W systemie plików XFS takie wsparcie jest domyślnie włączone, w systemach plików EXT wsparcie ACL musi być aktywowane.

Listy kontroli dostępu mogą być także używane w systemach plików NFS i CIFS.

ACL podzielone są na dwie kategorie:

access ACL – dostępowe listy kontroli dostępu, ustawiane na plikach i katalogach.

default ACL – domyślne listy kontroli dostępu, ustawiane tylko na poziomie katalogu.

Pliki i podkatalogi wchodzące w skład katalogu z ustawionymi domyślnymi ACL dziedziczą domyślne ACL katalogu nadrzędnego.

Komendy zarządzania ACL

Komenda	Opis
# getfacl	Wyświetla ustawienia ACL dla pliku i katalogu.
# setfacl	Ustawia, modyfikuje i kasuje ACL dla pliku lub katalogu.
# chacl	Zmienia ustawienia ACL na pliku lub katalogu. Komenda z systemu IRIX UNIX.

Jeżeli będziemy chcieli zrobić backup plików lub katalogów z ACL musimy zwrócić uwagę na fakt, że tar nie wspiera ACL. W takim wypadku należy użyć star, który pracuje z tymi samymi opcjami co tar a dodatkowo wspiera ACL.

Można także wykonać backup ACL używając polecenia getfacl:

```
getfacl -R /directory &gt; plik.acls
```

Przywracanie ACL:

```
setfacl --restore=plik.acl
```

Przykład:

```
pwd /root

touch plik1

ll plik1
```

-rw-r--r-- 1 root root 0 03-14 19:28 plik1

```
getfacl plik1
```

file: plik1

owner: root

group: root

user::rw-

group::r--

other::r--

Zwróć uwagę na wiersze związane z uprawnieniami i dwukropki.

W przypadku użycia ACL pomiędzy tymi dwukropkami znajdą się rozszerzone uprawnienia.

Np. ACL: user:1000:r-- na pliku oznacza, że użytkownik user z UID 1000, który nie jest właścicielem pliku ani członkiem grupy, która jest jego właścicielem, ma uprawnienia tylko do odczytu tego pliku.

Podobnie ACL: group: ngrupa:rw- przyzna grupie ngrupa prawo odczytu i zapisu pliku.

Komenda setfacl zawiera wiele opcji:

Opcja	Opis
-m	Ustawia lub modyfikuje ACL

-x	Usuwa konkretne ACL
-d	Ustawia domyślne ACL
-k	Usuwa wszystkie domyślne ACL
-b	Usuwa wszystkie ACL
-R	Ustawia ACL rekursywnie na wszystkich plikach i podkatalogach

Zasada ACL	Opis
u[ser]:UID:perms	Uprawnienia przypisywane do konkretnego użytkownika (nazwa użytkownika lub UID). Użytkownik musi się znajdować w pliku /etc/passwd.
g[roup]:GID:perms	Uprawnienia przypisywane do konkretnej grupy (nazwa użytkownika lub GID). Użytkownik musi się znajdować w pliku /etc/group.
m[ask]:perms	Maksymalne uprawnienia jakie konkretny użytkownik lub grupa może mieć mieć na pliku lub katalogu. Np. rw- oznacza, że żaden użytkownik lub grupa nie będzie miał większych uprawnień niż odczyt i zapis.
o[ther]:perms	Uprawnienia przypisane użytkownikom nie należącym do grupy będącej właścicielem.

Znaczenie maski w ACL

Maska ACL determinuje maksymalne możliwe uprawnienia przyznane konkretnemu użytkownikowi bądź grupie do pliku lub folderu. Jeżeli maska na przykład ustawiona jest na rw to żaden użytkownik czy grupa nie przekroczy tych uprawnień. Opcja –c powoduje, że getfacl nie wyświetla nagłówka:

getfacl –c plik1

user::rw

group::r--

other::r--

Jeżeli przyznamy użytkownikowi u1 prawo do zapisu i odczytu i zmienimy maskę na tylko do odczytu w tym samym czasie to efektywnymi uprawnieniami dla u1 będzie tylko odczyt:

setfacl –m u:u1:rw,m:r plik1

getfacl –c plik1

user::rw

user:u1:rw- #effective:r--

group::r--

mask::r--

other::r--

Czyli użytkownik u1 nie będzie mógł modyfikować tego pliku, mimo że wydaje się, że ma uprawnienia do zapisu. Po zmianie maski jak poniżej użytkownik u1 będzie mógł modyfikować plik plik1.

setfacl –m m:rw plik1

getfacl –c plik1

user::rw

user:u1:rw

group::r--

mask::rw

other::r--

Domyślne ACL

Czasami zachodzi potrzeba, aby wielu użytkowników, którzy należą do różnych grup, współdzieliło jeden katalog.

Potrzebują oni tak ustawionych uprawnień, aby pliki i podkatalogi utworzone w katalogu nadrzędnym dziedziczyły te uprawnienia.

W taki sposób użytkownicy nie muszą ustawiać uprawnień, które ustawili na katalogu nadrzędnym, na każdym pliku i podkatalogu z osobna. Takie wymaganie spełnia domyślne ACL.

ACL	Opis
d[efault]:u:perms	Domyślne standardowe uprawnienia dla właściciela.
d[efault]:u:UID:perms	Domyślne uprawnienia dla konkretnego użytkownika (jego nazwa lub UID).
d[efault]:g:perms	Domyślne standardowe uprawnienia dla grupy.

d[efault]:g:GID:perms	Domyślne uprawnienia dla konkretnej grupy (jego nazwa lub GID).
d[efault]:o:perms	Domyślne uprawnienia dla innych.
d[efault]:m:perms	Domyślne maksymalne uprawnienia, które może mieć użytkownik lub grupa, gdy tworzy plik lub katalog z domyślnymi ACL.