

# کتاب رنگ آمیزی **SELINUX**

"این باران سک ها و کر به ها است!"

با رنگ  
آمیزی  
یاد بگیرید!



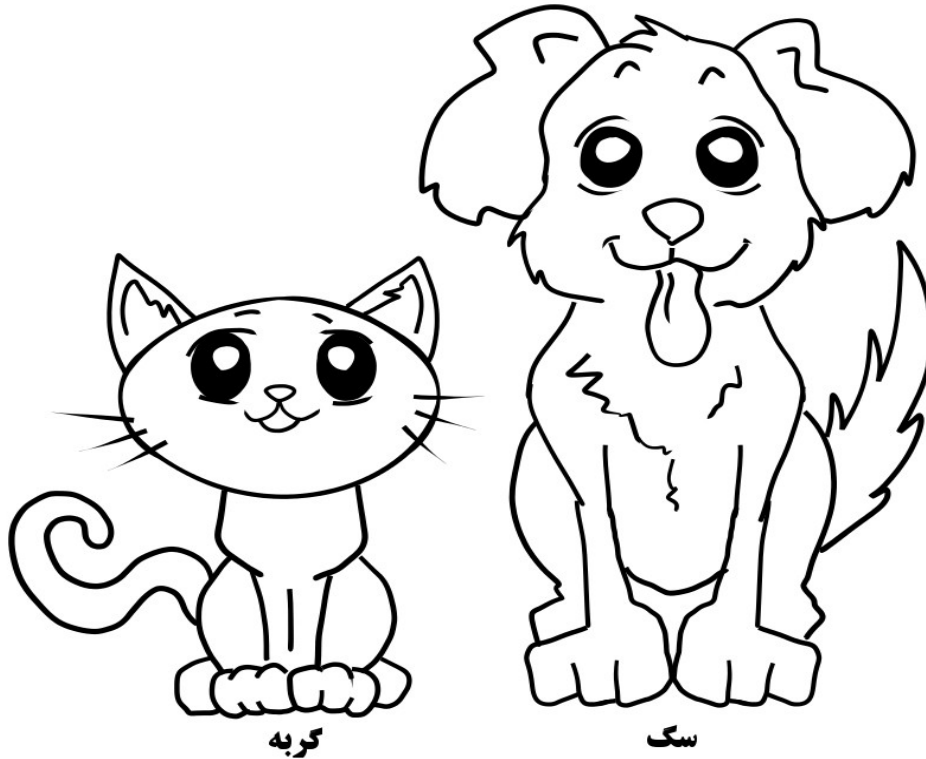
نوشته شده توسط: **DAN WALSH**

تصویر سازی توسط: **MÁIRÍN DUFFY**

Translated by :  
Mohsen Mostafa Jokar  
mohsenjokar@gmail.com

## نوع Enforcement انواع رونر

مدل اصلی Selinux یا اجرا نوع enforcement نامیده می شود. در واقع این بدان معناست که ما یک برچسب را بر روی یک فرایند مبتنی بر این نوع تعریف کرده ایم و برچسب بر روی یک شی سیستم فایل مبتنی بر این نوع است. یک سیستم را تصور کنید که در آن ما انواع را بر روی اشیائی شبیه به گربه و سگ تعریف می کنیم.



## انواع شی

ما یک کلاس از اشیا، داریم که آن‌ها می‌خواهند با چیزی که ما غذا می‌نامیم ارتباط برقرار کنند. و من می‌خواهم انواع را به غذا با نام های cat\_chow و dog\_chow اضافه کنم.



CAT\_CHOW



DOG\_CHOW

## قوانین سیاست

به عنوان یک نویسنده سیاست، من باید بگویم که یک سگ اجازه خوردن dog\_chow را دارد و این قانون را در سیاست همانطور که در زیر نشان داده شده است می‌نویسم.



اجازه دادن



گربه



اجازه دادن



سگ



غذا و یک گربه مجوز خوردن غذای cat\_chow را دارند. در Selinux ما باید

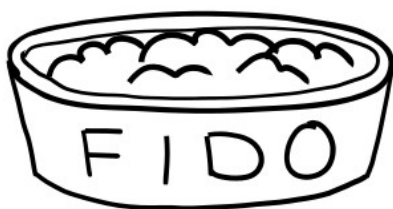


+



CAT\_CHOW:FOOD

خوردن



+



DOG\_CHOW:FOOD

خوردن

با این قوانین هسته باید به فرایند گربه اجازه خوردن غذا با پرچسب cat\_chow و به سگ اجازه خوردن غذا با پرچسب dog\_chow را بدهد.



CAT\_CHOW:FOOD



اما در یک سیستم **Selinux** به طور پیش فرض همه چیز رد شده است. این به این معنی است که اگر فرایند **سگ** سعی به خوردن **cat\_chow** کند، هسته جلوی آن را می گیرد.

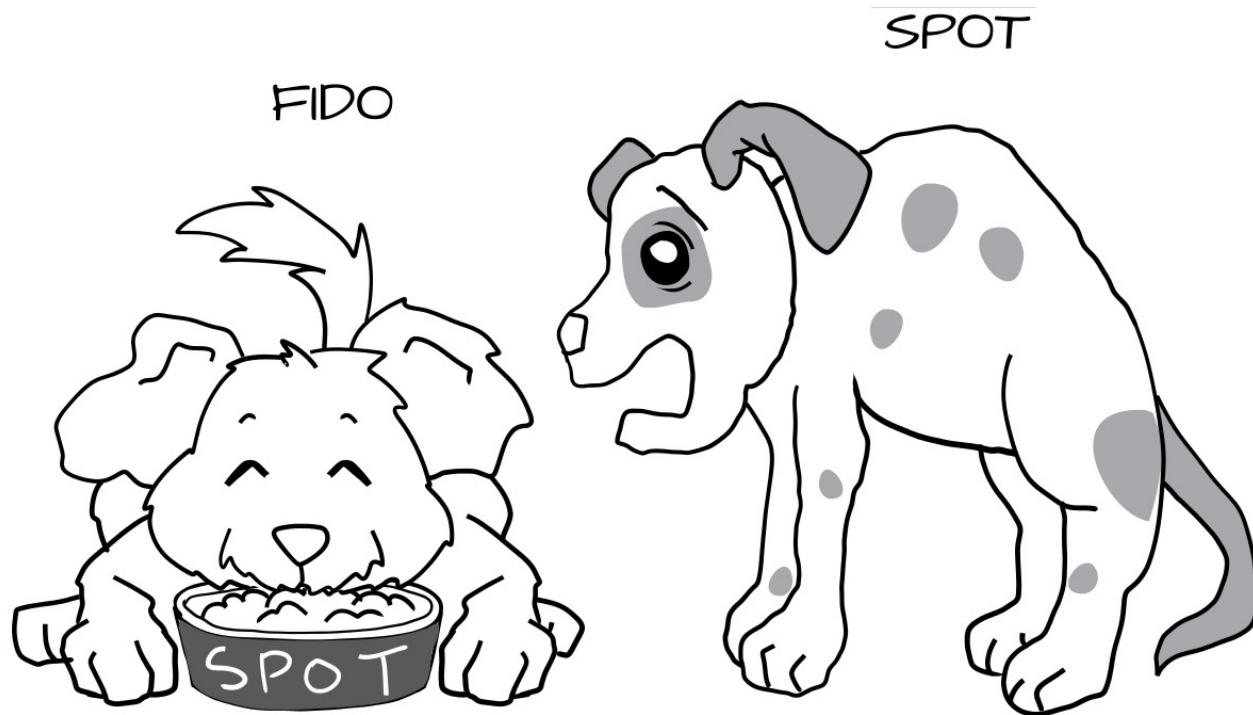


به همین ترتیب گربه نیز اجازه لمس کردن غذای سگ را ندارد.



## MCS Enforcement

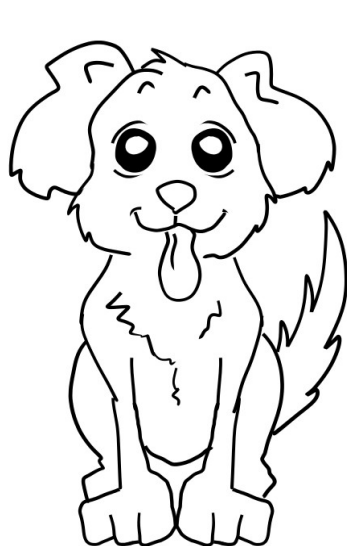
ما فرایند سگ و گربه را داریم، اما اگر شما چند فرایند سگ را داشته باشید چه اتفاقی می افتد: Spot و Fido. شما می خواهید جلوی Fido را از خوردن dog\_chow که مربوط به Spot است بگیرید.



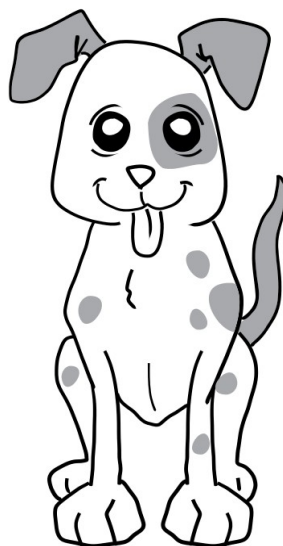
یک راه حل ایجاد تعداد زیادی از انواع جدید شبیه Fido\_dog\_chow و Fido\_dog خواهد بود. اما این به سرعت به یک مشکل تبدیل می‌شود زیرا تمام سگ‌ها تقریباً مجوز یکسان دارند.

برای رسیدگی به آن ما یک شکل جدید از اجرای قانون را توسعه داده‌ایم، که ما آن را امنیت چند رده (MCS) می‌نامیم. در MCS، ما یک بخش دیگر از برچسب را اضافه کرده‌ایم که می‌توانیم آن را به فرایند سگ و غذای dog\_chow اعمال کنیم. حالا ما فرایند سگ را به صورت dog:random1 (Fido) و dog:random2 (Spot) برچسب گذاری می‌کنیم.

ما غذای سگ را به صورت dog\_chow:random1 (Fido) و dog\_chow:random2 (Spot) برچسب گذاری می‌کنیم.



DOG:RANDOM1



DOG:RANDOM2



DOG\_CHOW:  
RANDOM1



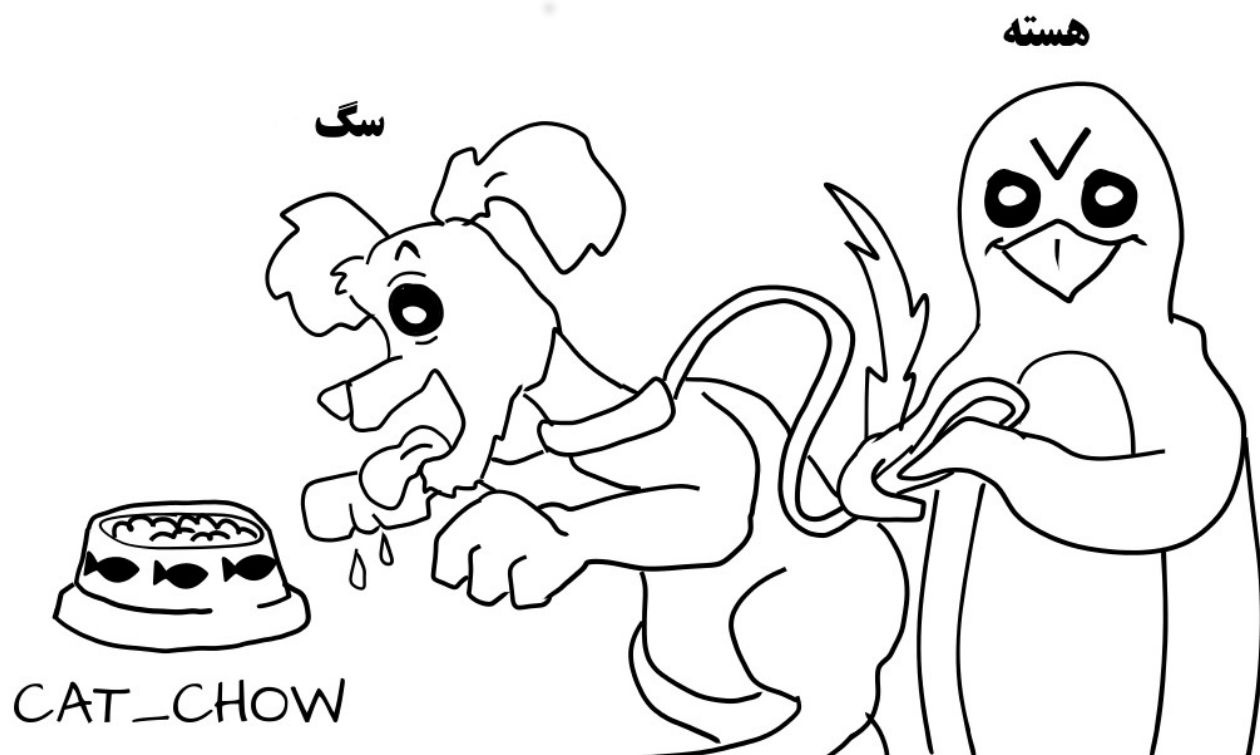
DOG\_CHOW:  
RANDOM2



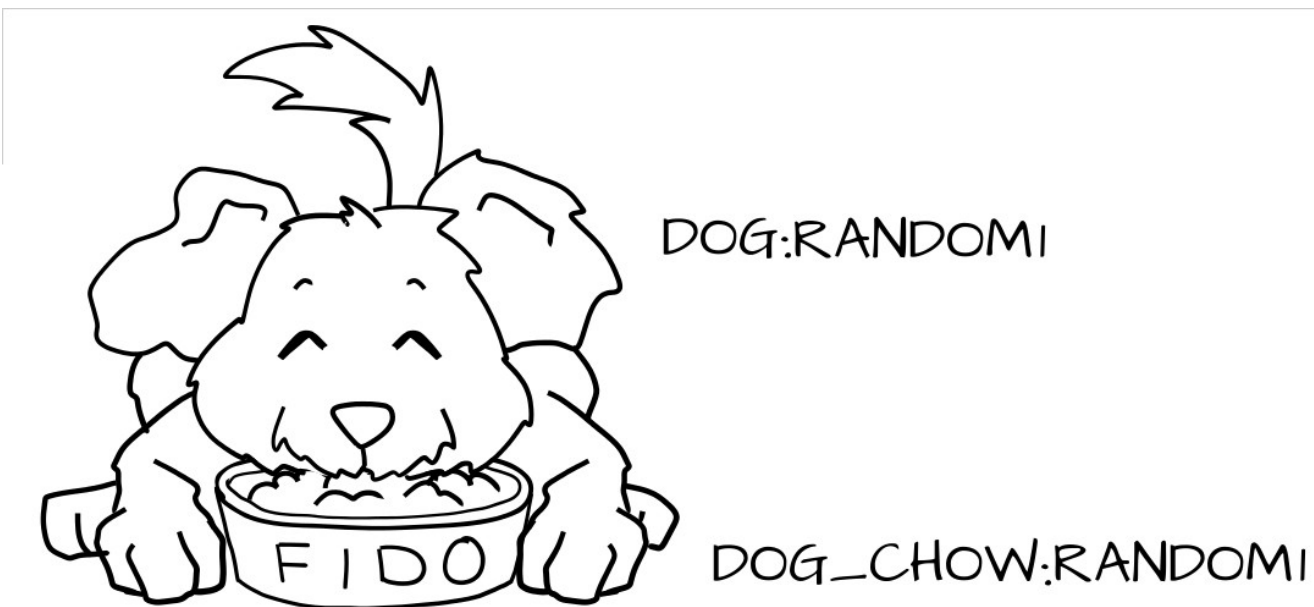
قوانین MCS می‌گویند که اگر قوانین از نوع enforcement درست هستند و برچسب‌های تصادفی MCS دقیقاً مطابقت دارند، آن وقت دسترس مجاز است و در غیر این صورت آن را رد می‌کنند.

## نوع ENFORCEMENT

Fido (dog:random1) تلاش می‌کند تا cat\_chow:food که توسط نوع enforcement رد شده است را بخورد.

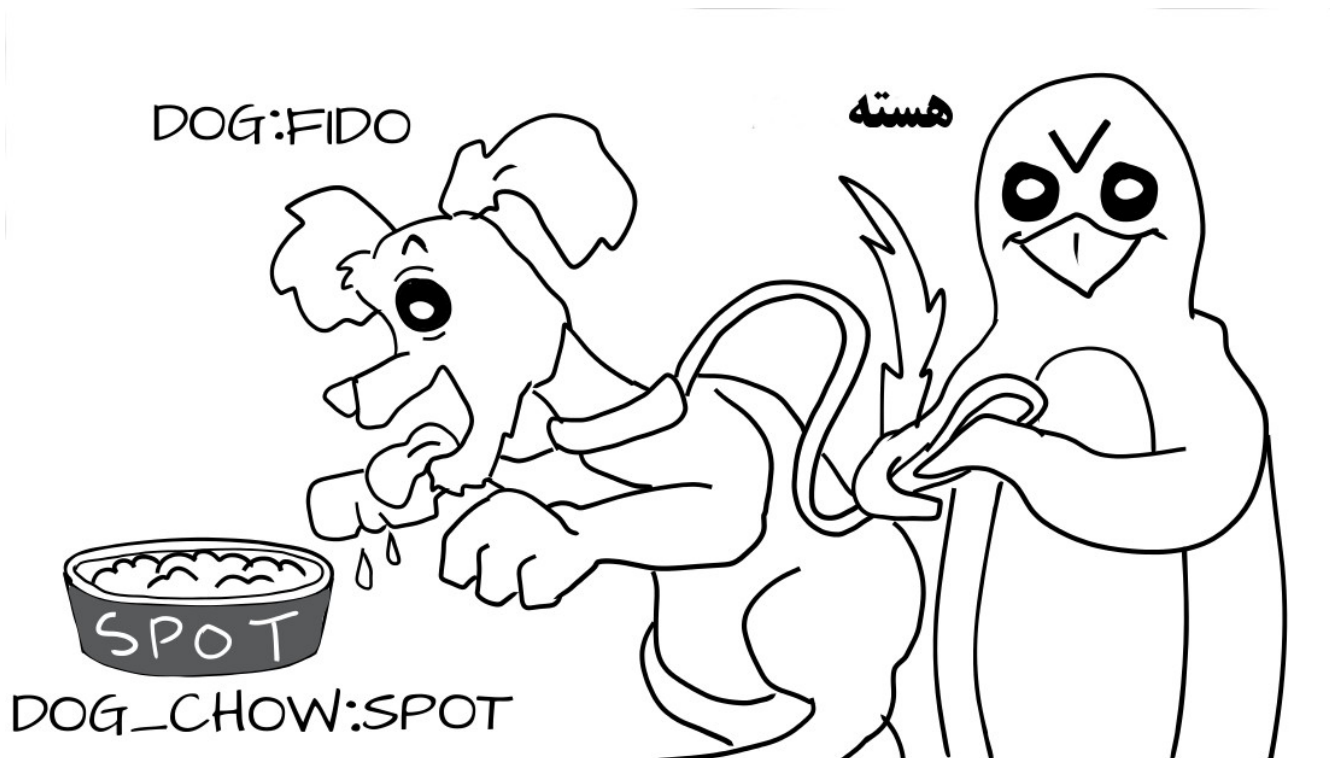


Fido (dog:random1) امکان خوردن dog\_chow:random1 را دارد.



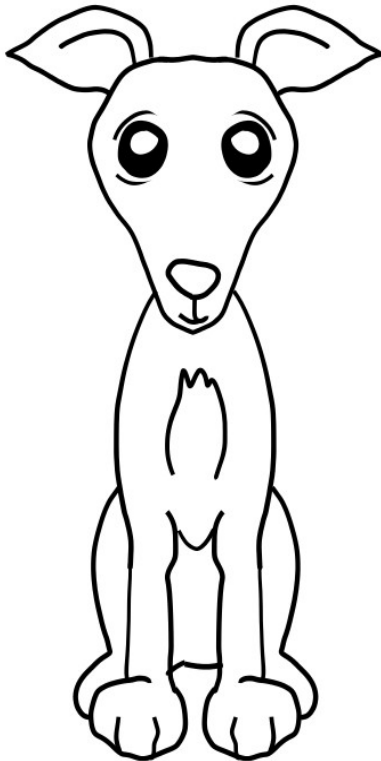
## MCS ENFORCEMENT

Fido (dog:random1) امکان خوردن غذای dog\_chow:random2 که مربوط به Spot است را ندارد.



## MLS Enforcement

یکی دیگر از اجراهای Selinux که اغلب کمتر استفاده می شود امنیت چند سطحی (MLS) نامیده می شود؛ توسعه آن به ۱۰ سال قبل بر می گردد و به طور عمده در سیستم عامل های مورد اعتماد مانند Solaris مطمئن استفاده می شده است. ایده اصلی کنترل فرایندها بر اساس سطحی از داده ها است که آن ها استفاده می کنند. یک فرایند سری نمی تواند داده های فوق سری را بخواند. به جای صحبت کردن در مورد سگ های مختلف، ما اکنون نگاهی به نژادهای مختلف می اندازیم. ما ممکن است سگ تازی یا چیهوا هوا داشته باشیم.



سگ تازی



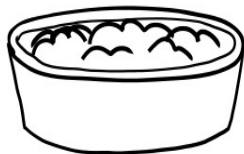
چیهوا هوا

ما ممکن است بخواهیم به سگ تازی اجازه دهیم تا هر غذای مربوط به سگ را بخورد، اما یک چیهوا هوا اگر تلاش به خوردن غذای سگ تازی کند باید مسدود شود...

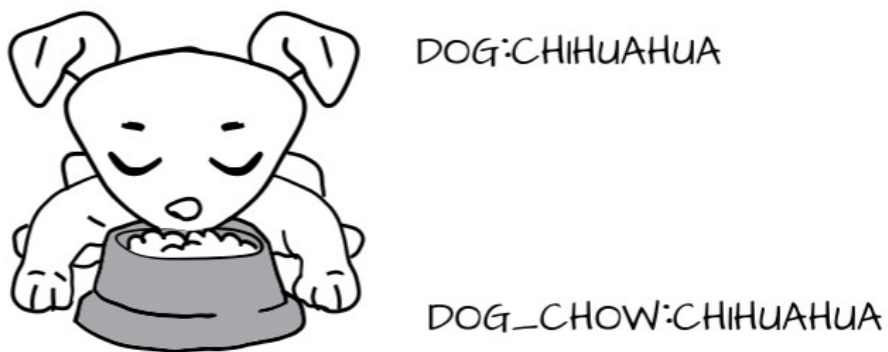
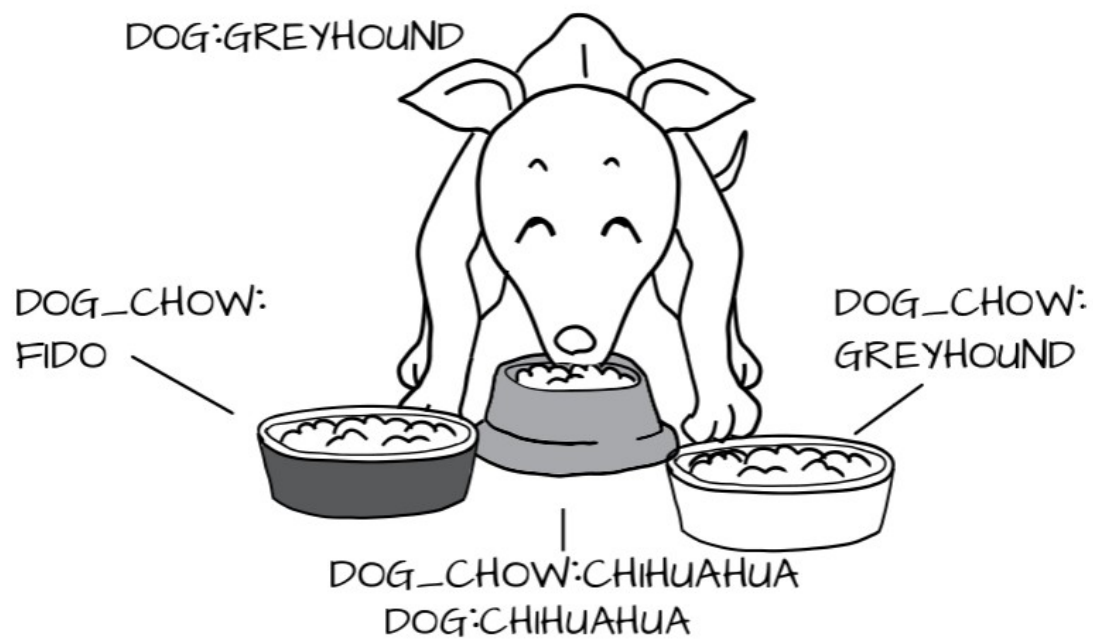
ما می‌خواهیم سگ تازی را به عنوان dog:Greyhound و غذای مربوط به آن را به صورت dog\_chow:Greyhound برچسب گذاری کنیم، و نیز چیهوا هوا را به صورت dog:Chihuahua و غذای مربوط به آن را به صورت dog\_chow:Chihuahua برچسب گذاری می‌کنیم.

DOG\_CHOW:GREYHOUND

DOG\_CHOW:CHIHUAHUA



با سیاست MLS ما باید یک برچسب MLS Greyhound داشته باشیم که بر برچسب چیهوا هوا برتری داشته باشد.

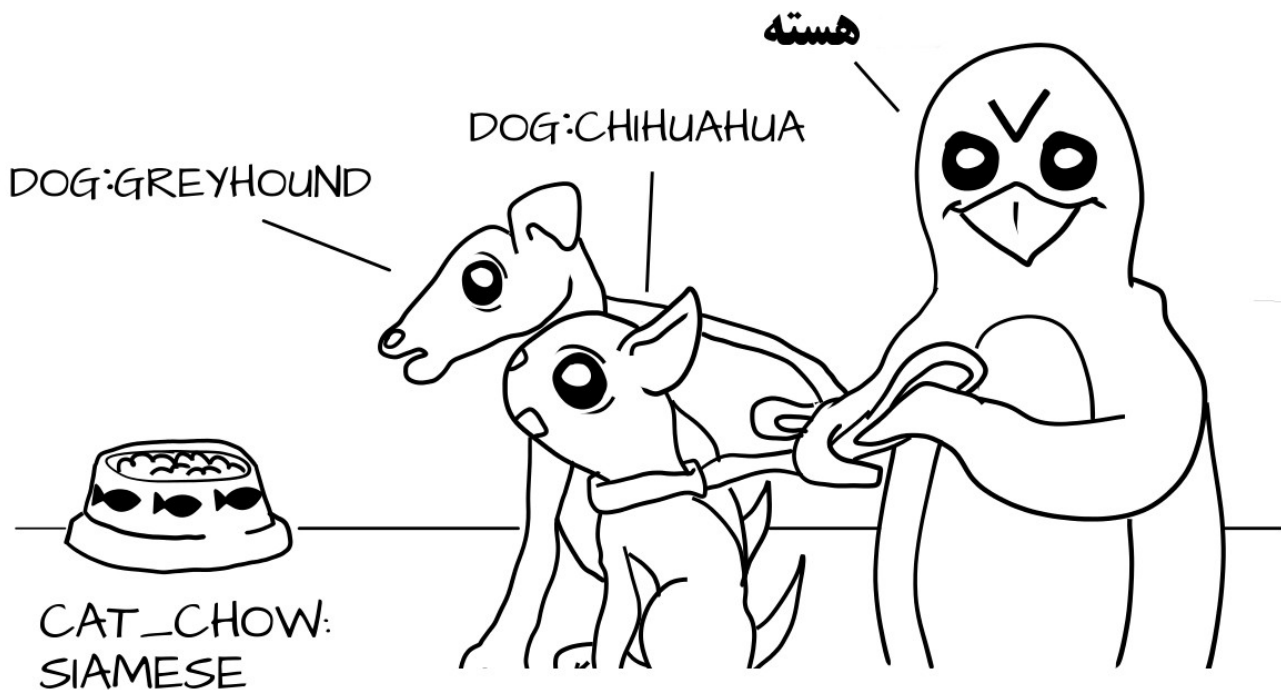


اما dog:Chihuahua امکان خوردن dog\_chow:Greyhound را ندارد.



DOG:CHIHUAHUA    DOG\_CHOW:GREYHOUND

البته dog:Chihuahua و dog:Greyhound توسط نوع enforcement هنوز هم امکان خوردن cat\_chow:Siamese را ندارند، و حتی اگر نوع MLS سگ تازی بر Siamese تسلط داشته باشد.





Learn more at [opensource.com](http://opensource.com):



<http://url.ca/g12br>