<table>
<tr><td rowspan="2">User Account Security</td><td colspan="2">S08 T05</td></tr>
<tr><td colspan="2">User-based access control lists</td></tr>
<tr><td rowspan="2">یکی از مفاهیم کلیدی در امنیت حساب‌های کاربری در سرورهای لینوکسی، استفاده از کنترل دسترسی مبتنی بر کاربر یا ACL است. این مفهوم به مدیران سیستم اجازه می‌دهد تا دسترسی‌های دقیقی را برای کاربران مختلف تعیین کرده و امنیت سیستم را بهبود بخشند. در این مقاله به معرفی مفهوم ACL ، اهمیت آن و نحوه پیاده‌سازی آن در لینوکس می‌پردازیم.</td><td>بعد از  </td><td>User environment restriction</td></tr>
<tr><td>قبل از  </td><td>Management of root access and sudo privileges</td></tr>
<tr><td>پیاده سازی عملی: خیر</td><td>پژوهشی: خیر</td><td>راهنمای عملی: بله</td></tr>
</table>

## کنترل دسترسی مبتنی بر کاربر در لینوکس

یکی از مفاهیم کلیدی در امنیت حساب‌های کاربری در سرورهای لینوکسی، استفاده از کنترل دسترسی مبتنی بر کاربر (User-Based Access Control Lists یا ACL) است. این مفهوم به مدیران سیستم اجازه می‌دهد تا دسترسی‌های دقیقی را برای کاربران مختلف تعیین کرده و امنیت سیستم را بهبود بخشند. در این مقاله به معرفی مفهومACL ، اهمیت آن و نحوه پیاده‌سازی آن در لینوکس می‌پردازیم.

## اهمیت کنترل دسترسی مبتنی بر کاربر

۱. **مدیریت دقیق دسترسی‌ها** :با استفاده ازACL ، مدیران سیستم می‌توانند دسترسی‌های خاصی را برای هر کاربر یا گروه تعیین کنند، که این امر به مدیریت بهتر منابع سیستم کمک می‌کند.

۲. **افزایش امنیت سیستم** :به مدیران امکان می‌دهد تا دسترسی‌های غیرضروری را محدود کرده و سطح امنیت سیستم را افزایش دهند.

۳. **انعطاف‌پذیری بیشتر** :برخلاف مدل‌های سنتی دسترسی که فقط سه سطح (مالک، گروه و دیگران) را شامل می‌شوند، ACLبه تعریف دسترسی‌های خاص برای کاربران یا گروه‌های متعدد کمک می‌کند.

## پیاده‌سازی ACL در لینوکس

۱. **فعال‌سازی :ACL** برای استفاده ازACL ، سیستم فایل باید از این قابلیت پشتیبانی کند. در زمان مونت کردن، باید گزینه aclفعال باشد:

```
sudo mount -o remount,acl /path/to/mountpoint
```

۲. **استفاده از ابزار setfacl**: این ابزار برای تنظیم و مدیریت ACL بر روی فایل‌ها و دایرکتوری‌ها استفاده می‌شود.

- افزودن یک ورودی ACL:

```
sudo setfacl -m u:username:rwx /path/to/file
```

- حذف یک ورودی ACL:

```
sudo setfacl -x u:username /path/to/file
```

۳. **استفاده از ابزار getfacl**: این ابزار برای مشاهده و نمایش ACL های تنظیم‌شده بر روی فایل‌ها و دایرکتوری‌ها استفاده می‌شود.

```
getfacl /path/to/file
```

٤. **تنظیم ACL پیش‌فرض**: با استفاده از ACL پیش‌فرض، تمامی فایل‌ها و دایرکتوری‌های جدیدی که در یک دایرکتوری خاص ایجاد می‌شوند، ACL مشخصی را به ارث می‌برند:

```
sudo setfacl -d -m u:username:rwx /path/to/directory
```

## نتیجه‌گیری

استفاده از کنترل دسترسی مبتنی بر کاربر (ACL) در لینوکس به مدیران سیستم امکان می‌دهد تا دسترسی‌ها را با دقت بیشتری مدیریت کنند و امنیت کلی سیستم را افزایش دهند. با استفاده از ابزارها و روش‌های مناسب، می‌توان دسترسی‌های غیرمجاز را محدود و از داده‌های حساس محافظت کرد. آشنایی و پیاده‌سازی صحیح این روش‌ها به مدیران کمک می‌کند تا از عملکرد بهینه سرورهای خود اطمینان حاصل کنند.

## منابع و ارجاعات


- https://roadmap.sh/linux
- https://roadmap.sh/r/general-linux-server-hardening