|  |  |  |  |
| --- | --- | --- | --- |
| S04 T04 | | | File System Hardening |
| ACL (access control lists) | | |
| Sticky bit, SUID, SGID | | Caret Right with solid fill | در زمینه‌ی سخت‌کردن سرورهای لینوکس، یکی از مباحث کلیدی که باید به آن توجه داشت، مدیریت دسترسی‌ها به فایل‌ها و پوشه‌ها است. در کنار مجوزهای سنتی (مالک، گروه و دیگران)، لینوکس امکانات پیشرفته‌تری نظیر فهرست‌های کنترل دسترسی (ACL) را ارائه می‌دهد که انعطاف‌پذیری بیشتری در تعیین سطوح دسترسی فراهم می‌کند. |
| بعد از |
| File integrity checkers (AIDE, Tripwire) | | Caret Left with solid fill |
| قبل از |
| راهنمای عملی: بله | پژوهشی: **خیر** | | پیاده سازی عملی: **خیر** |

## آشنایی با ACL (فهرست‌های کنترل دسترسی) در لینوکس

در زمینه‌ی سخت‌کردن سرورهای لینوکس، یکی از مباحث کلیدی که باید به آن توجه داشت، مدیریت دسترسی‌ها به فایل‌ها و پوشه‌ها است. در کنار مجوزهای سنتی (مالک، گروه و دیگران)، لینوکس امکانات پیشرفته‌تری نظیر فهرست‌های کنترل دسترسی (ACL) را ارائه می‌دهد که انعطاف‌پذیری بیشتری در تعیین سطوح دسترسی فراهم می‌کند.

### ACL چیست؟

ACL یا فهرست‌های کنترل دسترسی، به مدیر سیستم اجازه می‌دهد تا سطح دسترسی دقیق‌تری برای کاربران و گروه‌ها بر روی فایل‌ها و پوشه‌ها تعیین کند. برخلاف مجوزهای سنتی که تنها سه سطح مالک، گروه و دیگران را شامل می‌شوند، ACL می‌تواند برای هر کاربر یا گروه خاص، مجوزهای جداگانه‌ای تعیین کند.

**مزایای استفاده از ACL**

* **انعطاف‌پذیری بیشتر**: با ACL می‌توان دسترسی‌های خاصی را برای کاربران و گروه‌های مختلف تعریف کرد.
* **کنترل دقیق‌تر**: می‌توان به کاربران خاص دسترسی‌های خواندن، نوشتن یا اجرایی را بدون تغییر مجوزهای اصلی داد.

### نحوه فعال‌سازی ACL

برای استفاده از ACL، سیستم فایل باید پشتیبانی لازم را داشته باشد و در زمان Mount، گزینه‌ی acl فعال باشد. می‌توان با ویرایش فایل /etc/fstab و افزودن گزینه‌ی acl به تنظیمات Mount، این ویژگی را فعال کرد:

/dev/sda1 / ext4 defaults,acl 0 1

پس از آن می‌توان با فرمان زیر سیستم فایل را مجدداً Mount کرد:

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

### ابزارها و فرمان‌های مربوط به ACL

برای مدیریت ACL، می‌توان از ابزارها و فرمان‌های زیر استفاده کرد:

* **setfacl:** این فرمان برای تنظیم و مدیریت ACL بر روی فایل‌ها و پوشه‌ها استفاده می‌شود.

**افزودن یک ورودی ACL:**

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

**حذف یک ورودی ACL:**

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

* **getfacl**: این فرمان برای مشاهده و نمایش ACL های تنظیم‌شده بر روی فایل‌ها و پوشه‌ها استفاده می‌شود.

getfacl /path/to/file

## مثال‌های عملی

1. **افزودن دسترسی خواندن و نوشتن به یک کاربر خاص**:

setfacl -m u:ali:rw /path/to/file

1. **مشاهده ACL های یک فایل**:

getfacl /path/to/file

1. **تنظیم ACL پیش‌فرض برای یک پوشه**: با استفاده از ACL پیش‌فرض، تمامی فایل‌ها و پوشه‌های جدیدی که در یک پوشه خاص ایجاد می‌شوند، ACL مشخصی را به ارث می‌برند.

setfacl -d -m u:ali:rw /path/to/directory

## نتیجه‌گیری

استفاده از فهرست‌های کنترل دسترسی (ACL) در لینوکس به مدیران سیستم امکان می‌دهد تا با دقت بیشتری دسترسی‌های کاربران و گروه‌ها به فایل‌ها و پوشه‌ها را مدیریت کنند. این ویژگی انعطاف‌پذیری بالاتری نسبت به مجوزهای سنتی ارائه می‌دهد و به مدیران کمک می‌کند تا امنیت سیستم‌های خود را بهبود بخشند. آشنایی و استفاده صحیح از ابزارها و فرمان‌های مرتبط با ACL، می‌تواند تأثیر بسزایی در افزایش امنیت و کارایی سیستم‌های لینوکسی داشته باشد.

## منابع و ارجاعات

* <https://roadmap.sh/linux>
* <https://manpages.ubuntu.com/manpages/noble/en/man1/setfacl.1.html>