【Linux】【權限管理】【acl】設定/var/www/html for tomcat 可讀寫

以下是如何在 Ubuntu 中設置這些 ACL 權限的步驟。

步驟 1：啟用 ACL 支持

如果 ACL 尚未啟用，請確保相關功能已經安裝並啟用：

1. 安裝 ACL 工具：
   ```
   sudo apt install acl
   ```
2. 確保文件系統支持 ACL：
   ```
   sudo mount -o remount,acl /
   ```

步驟 2：設置基本權限

設定 `/var/www/html` 的基本權限：

```
sudo chmod 775 /var/www/html
sudo chown root:root /var/www/html
```

步驟 3：配置 ACL 權限

根據需求逐步配置 ACL：

1. **設置具體使用者和群組的 ACL 權限**：
   ```
   sudo setfacl -m u:tomcat:rwx /var/www/html
   sudo setfacl -m g::r-x /var/www/html
   sudo setfacl -m o::r-x /var/www/html
   ```
   - **`u:tomcat:rwx`**：給 `tomcat` 用戶設置 `rwx` 權限。
   - **`g::r-x`**：默認組的權限為 `r-x`。
   - **`o::r-x`**：其他人的權限為 `r-x`。
2. **設置默認 ACL（適用於未來子目錄和文件）**：
   ```
   sudo setfacl -d -m u::rwx /var/www/html
   sudo setfacl -d -m u:tomcat:rwx /var/www/html
   sudo setfacl -d -m g::r-x /var/www/html
   sudo setfacl -d -m o::r-x /var/www/html
   ```
   - **`-d`**：表示設置默認 ACL（對新創建的文件/目錄生效）。

步驟 4：檢查 ACL 設置

使用以下指令檢查 ACL 配置是否正確：

```
getfacl /var/www/html
```

輸出應類似於：

```
# file: var/www/html
# owner: root
# group: root
user::rwx
user:tomcat:rwx
```

```
group::r-x
mask::rwx
other::r-x
default:user::rwx
default:user:tomcat:rwx
default:group::r-x
default:mask::rwx
default:other::r-x
```

ACL 設置的解釋

1. **普通權限**：
   - `user::rwx`：目錄擁有者 `root` 的權限。
   - `user:tomcat:rwx`：為用戶 `tomcat` 設置的權限。
   - `group::r-x`：目錄的群組成員的權限。
   - `other::r-x`：其他用戶的權限。
   - `mask::rwx`：ACL 中權限的上限（最高可設置為 `rwx`）。
2. **默認權限（`default:` 開頭）**：
   - `default:user::rwx`：默認擁有者的權限。
   - `default:user:tomcat:rwx`：默認為 `tomcat` 設置的權限。
   - `default:group::r-x`：默認群組的權限。
   - `default:other::r-x`：默認其他用戶的權限。

總結指令

以下是一鍵完成配置的指令集合：

```
sudo setfacl -m u:tomcat:rwx /var/www/html
sudo setfacl -m g::r-x /var/www/html
sudo setfacl -m o::r-x /var/www/html
sudo setfacl -d -m u::rwx /var/www/html
sudo setfacl -d -m u:tomcat:rwx /var/www/html
sudo setfacl -d -m g::r-x /var/www/html
sudo setfacl -d -m o::r-x /var/www/html
```

執行後確認權限是否正確，應與您列出的設定一致！

是否需要設定 `-d` 取決於您的需求，以下是有關 **默認 ACL（`-d`）** 的詳細說明以及什麼情況下需要設定。

什麼是默認 ACL（`-d`）？

默認 ACL 是一組規則，會自動應用到 **新創建的文件或子目錄** 中。當一個目錄設置了默認 ACL，該目錄下創建的任何新文件或目錄都會繼承這些默認規則。

是否需要設定 `-d`

1. **需要設定 `-d` 的情況**
   - 如果您希望 **新創建的文件或子目錄** 自動繼承特定的 ACL 設置（如 `tomcat` 擁有特定權限），那麼您需要設置默認 ACL。例如：
     - `/var/www/html` 是一個共享的目錄，將會持續新增文件。
     - 您希望 `tomcat` 用戶對新增的文件有 `rwx` 權限。

     ```
     sudo setfacl -d -m u:tomcat:rwx /var/www/html
     ```

     當某人創建一個新文件時，`tomcat` 就會自動擁有該文件的權限。
2. **不需要設定 `-d` 的情況**
   - 如果您僅關心目錄 **當前的文件和目錄**，而不需要未來的新增文件繼承權限。
   - 如果您會手動或通過腳本為新文件設置權限，而不依賴默認 ACL。

   在這種情況下，您可以省略 `-d`，只設置當前的 ACL 即可：

   ```
   sudo setfacl -m u:tomcat:rwx /var/www/html
   ```

範例：對比是否設置 `-d` 的效果

假設您在 `/var/www/html` 下創建了兩個文件：

1. **沒有設置 `-d` 的情況**
   - 當您創建新文件時，不會繼承 `tomcat` 的權限。
   - 新文件的權限取決於當前的系統默認值（如 `umask`）。
2. **設置了 `-d` 的情況**
   - 新文件或目錄將繼承默認 ACL。例如，`tomcat` 將擁有對新文件的權限：

     ```
     touch /var/www/html/newfile
     getfacl /var/www/html/newfile
     ```

     結果顯示 `tomcat` 的權限被自動應用。

結論

- **需要持續新增文件/目錄並繼承權限**：建議使用 `-d` 設置默認 ACL。
- **僅對當前文件和目錄設置權限**：可以省略 `-d`。

建議根據場景選擇適合的設置，以滿足項目需求。

修訂版本 #2
★由 treeman 建立於 13 ?Q?G?? 2024 15:32:28
由 treeman 更新於 13 ?Q?G?? 2024 15:43:14