ACL – Access Control List

ACL (Seznam řízení přístupu) je tabulka nebo seznam pravidel, který určuje, jaká práva mají konkrétní uživatelé, systémy nebo síťové entity k určitému objektu či službě. Je to základní stavební kámen kybernetické bezpečnosti a správy identit.

1. Typy ACL podle oblasti využití

ACL se implementují v různých vrstvách IT infrastruktury, přičemž každá má svá specifika:

A. Síťové ACL (Network ACLs)

Používají se na routerech, switchích a firewallech k filtrování příchozího a odchozího provozu.

- **Standardní ACL:** Filtrují provoz pouze na základě zdrojové IP adresy.
- **Rozšířené ACL (Extended):** Dokáží filtrovat podle zdroje, cíle, čísla portu (např. 80 pro HTTP) a typu protokolu (TCP/UDP).
- **Význam:** Jsou klíčové pro segmentaci sítě a ochranu před neautorizovaným přístupem.

B. Souborové ACL (Filesystem ACLs)

Rozšiřují základní model oprávnění (jako je např. Linuxové **rwx** – read, write, execute).

- Umožňují přiřadit různá práva více uživatelům nebo skupinám k jednomu souboru či složce.
- **Příklad:** V systému Windows (NTFS) nebo v Linuxu (přes příkaz `setfacl`) můžete nastavit, že uživatel „Honza“ může soubor číst, ale uživatelka „Jana“ jej může i upravovat.

—

2. Struktura pravidla ACL

Každý záznam v ACL (označovaný jako **ACE** – Access Control Entry) obvykle obsahuje tyto složky:

- **Identifikátor (Subject):** Kdo chce přistupovat (uživatelské jméno, IP adresa, ID skupiny).
- **Objekt:** K čemu se přistupuje (soubor, síťové rozhraní, databázová tabulka).
- **Operace:** Co chce subjekt dělat (čtení, zápis, mazání, spuštění).
- **Povolení/Zákaz:** Výsledek pravidla (Allow / Deny).

—

3. Princip "Implicit Deny"

Jedním z nejdůležitějších bezpečnostních pravidel v ACL je **Implicit Deny** (Implicitní zákaz). To znamená, že pokud požadavek neodpovídá žádnému pravidlu v seznamu, je automaticky zamítnut.

> V konfiguraci síťových prvků se toto pravidlo často nachází na konci seznamu jako neviditelné „deny all“.

—

4. ACL vs. RBAC

Je důležité nezaměňovat ACL s **RBAC** (Role-Based Access Control):

- **ACL** se zaměřuje na **objekt** (seznam u souboru říká, kdo k němu může).
- **RBAC** se zaměřuje na **subjekt** (uživatel má roli „Manažer“, která mu dává přístup k celé sadě prostředků).
- V moderních systémech se oba přístupy často kombinují.

—

5. Výhody a správa

Výhody	Výzvy
Granularita: Velmi detailní nastavení práv pro jednotlivce.	**Složitost:** U velkých systémů může být seznam nepřehledný.
Bezpečnost: Rychlá implementace blokování útočníků (např. podle IP).	**Výkon:** Příliš dlouhé síťové ACL mohou zpomalit směrování paketů.
Audit: Snadnější sledování toho, kdo má kam přístup.	**Chyby v konfiguraci:** Stačí jedno špatné pravidlo a služba je nedostupná.

Související články:

- WAF a síťová bezpečnost
- Firewally a jejich typy
- Model OSI a síťové vrstvy

Tagy: security network acl access-control permissions administration

From:
https://serviceit.cz/ - **IT ENCYKLOPEDIE**

Permanent link:
https://serviceit.cz/doku.php?id=acl

Last update: **2026/01/02 17:40**