AAA

Authentication, authorization, and accounting

Botló Bence Balázs, Forró David, Krajcsovics Christofer

Mi az AAA?

- Biztonsági keretrendszer

- Hozzáférés szabályozási modell

- 3 fő komponense:
  - Azonosítás (Authentication)
    Ki érheti el az információt?
  - Jogosultságkezelés (Authorization)
    Milyen információ érhető el?
  - Naplózás (Accounting)
    Milyen információ van elérve?

- Válalati hálózatok alapja

Authentication

Authorization

Accounting

Authentication - Azonosítás

Authentication

- Identitás azonosítása
- Azonosítás – Ki vagy?
- Azonosítás hibás, többi réteg értelmét veszti.

Azonosítási módszerek

Authentication

- Jelszó
- Tanusítvány
- Egyszer használatos jelszavak OTP – HOTP, TOTP
- Biometrikus azonosítás

Azonosítási faktorok

Authentication

- SFA
- 2FA
- MFA
- Miért?

Protokollok

Authentication

- RADIUS
- Kerberos
- LDAP

Támadás

Authentication

- Brute force
- Credential stuffing
- Phishing
- Keylogging
- Replay attack

Védelem

Authentication

- MFA
- Rate limiting
- Fiókzárolás
- Digitális tudatosság

Jelszókezelés

Authentication

- Hosszúság, bonyolultság
- Jelszómenedzser
- Jelszó ismétlés
- Hashelés

Authorization (Engedélyezés)

Authorization

- Információbiztonság és IAM alapfogalma
- A hitelesítés után következő folyamat
- Meghatározza: mit tehet a felhasználó a rendszerben

Mi az engedélyezés célja?

Authorization

- Jogosulatlan hozzáférés megakadályozása
- Hálózati szabályok érvényesítése
- Legkisebb szükséges jogosultság elvének biztosítása
- Érzékeny adatok védelme

Hozzáférés-vezérlési módszerek

Authorization

- ACL (Access Control List)
- RBAC (Role-Based Access Control)
- Házirend alapú vezérlés
- Központi AAA szerver alkalmazása

Access Control List

Példák

Authorization

- Junior hálózati mérnök hozzáfér egy ezközhöz
- Csak megjelenítő (show) parancsok futtatása
- Konfiguráció módosítására nincs jogosultsága
- Engedélyezési rendszer korlátozza a műveleteket

Központi engedélyezési protokolok

Authorization

- RADIUS
  - Hitelesítés és engedélyezés együtt
  - Gyakori VPN használat

- TAKACS+
  - Hitelesítés és engedélyezés külön kezelve
  - Részletes parancsszintű szabályzás

Accounting (Naplózás)

Accounting

- Mi az Accounting szerepe?
  - A felhasználói tevékenység rögzítése
  - Hozzáférési események dokumentálása
  - Biztonsági események követhetősége
  - Átláthatóság és elszámolhatóság biztosítása

- Kérdések
  - Mit csinált?
  - Mikor?
  - Mennyi ideig?
  - Milyen erőforrásokat használt?

Mit rögzít pontosan a naplózás

Accounting

- Bejelentkezési és kijelentkezési idő
- Sikertelen bejelentkezési próbálkozások
- Használt IP-cím
- Elért erőforrások
- Végrehajtott műveletek
- Konfigurációs változtatások
- Hálózati forgalom mennyisége

- Típusok:
  - Hálózati
  - Rendszer
  - Alkalmazás
  - Biztonsági

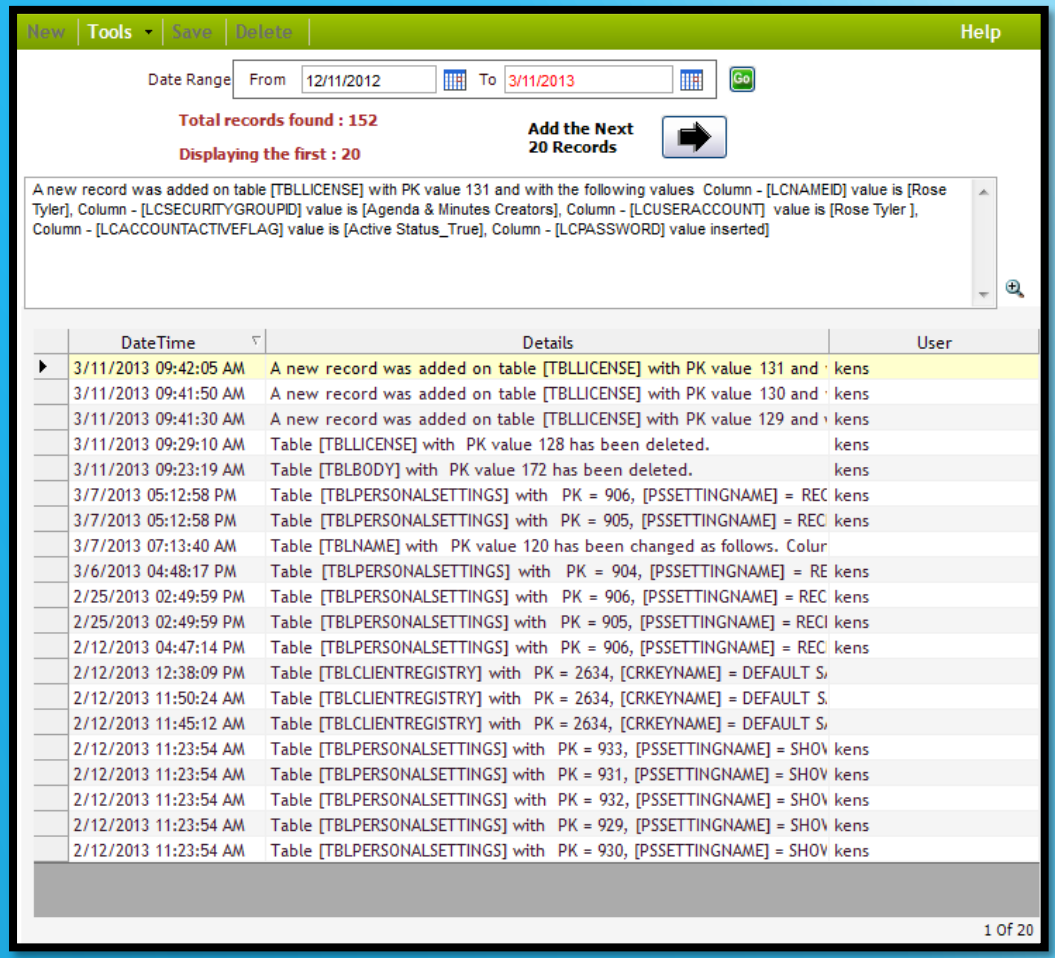
LOG Fájlok

Accounting

- LOG Fájl: Események rögzítése időrendben
- Automatikusan generáltak
- Cél:
  - Eseménykövetés
  - Hibakezelés
  - Biztonsági ellenőrzés
  - Incidensvizsgálat

- Tartalmazhat:
  - Timestamp
  - Esemény típusa
  - Felhasználónév
  - IP-cím
  - Művelet
  - Státusz

```
214.1.211.251 - - [15/Apr/2011:09:40:17 -0700] "GET /global.asa HTTP/1.0" 404 315 "-" "-"
214.1.211.251 - - [15/Apr/2011:09:40:17 -0700] "GET /~root HTTP/1.0" 404 310 "-" "-"
214.1.211.251 - - [15/Apr/2011:09:40:18 -0700] "GET /~apache HTTP/1.0" 404 312 "-" "-"
219.167.17.173 - - [17/Apr/2011:17:55:40 -0700] "POST /sony/mmr HTTP/1.1" 200 130 "-" "PS
218.41.54.67 - - [17/Apr/2011:18:20:18 -0700] "POST /sony/mmr HTTP/1.1" 200 130 "-" "PS3A
10.132.93.114 - - [18/Apr/2011:11:05:39 -0700] "POST /sony/mmr HTTP/1.1" 200 61 "-" "Ledi
10.132.93.114 - - [18/Apr/2011:11:07:07 -0700] "POST /sony/mmr HTTP/1.1" 200 61 "-" "Ledi
10.132.93.114 - - [18/Apr/2011:11:13:52 -0700] "POST /sony/mmr HTTP/1.1" 200 61 "-" "Ledi
218.41.54.67 - - [20/Apr/2011:17:42:37 -0700] "POST /sony/mmr HTTP/1.1" 200 100 "-" "PS3A
60.34.131.229 - - [20/Apr/2011:18:22:32 -0700] "POST /sony/mmr HTTP/1.1" 200 100 "-" "PS3
202.213.251.245 - - [21/Apr/2011:21:16:45 -0700] "POST /sony/mmr HTTP/1.1" 200 100 "-" "P
202.213.251.245 - - [21/Apr/2011:21:24:43 -0700] "POST /sony/mmr HTTP/1.1" 200 100 "-" "P
178.202.110.92 - - [22/Apr/2011:18:59:05 -0700] "GET / HTTP/1.1" 200 315 "-" "Mozilla/5.0
178.202.110.92 - - [22/Apr/2011:18:59:05 -0700] "GET /favicon.ico HTTP/1.1" 404 333 "-" "
178.202.110.92 - - [22/Apr/2011:18:59:05 -0700] "GET /favicon.ico HTTP/1.1" 404 333 "-" "
178.202.110.92 - - [22/Apr/2011:18:59:07 -0700] "GET /access-navigator-media HTTP/1.1" 20
178.202.110.92 - - [22/Apr/2011:19:05:00 -0700] "GET /admin/cdr/counter.txt HTTP/1.1" 404
178.202.110.92 - - [22/Apr/2011:19:05:41 -0700] "GET //help/readme.nsf?OpenAbout HTTP/1.1
178.202.110.92 - - [22/Apr/2011:19:05:54 -0700] "GET /catinfo?A HTTP/1.1" 404 329 "-" "Mo
178.202.110.92 - - [22/Apr/2011:19:06:08 -0700] "GET /errors-navigator-media HTTP/1.1" 20
178.202.110.92 - - [22/Apr/2011:19:27:04 -0700] "GET / HTTP/1.1" 200 315 "-" "Mozilla/5.0
```




```
2026-02-15 10:32:14 AUTH_SUCCESS user=david ip=192.168.1.25 method=password
2026-02-15 10:35:02 AUTH_FAILURE user=david ip=192.168.1.25 reason=wrong_password
2026-02-15 10:40:11 ACCESS_GRANTED user=david resource=/admin_panel role=admin
2026-02-15 10:55:47 LOGOUT user=david session_id=784512
```

Miért fontos?

Accounting

- Bejelentkezési és kijelentkezési idő
- Sikertelen bejelentkezési próbálkozások
- Használt IP-cím
- Elért erőforrások
- Végrehajtott műveletek
- Konfigurációs változtatások
- Hálózati forgalom mennyisége

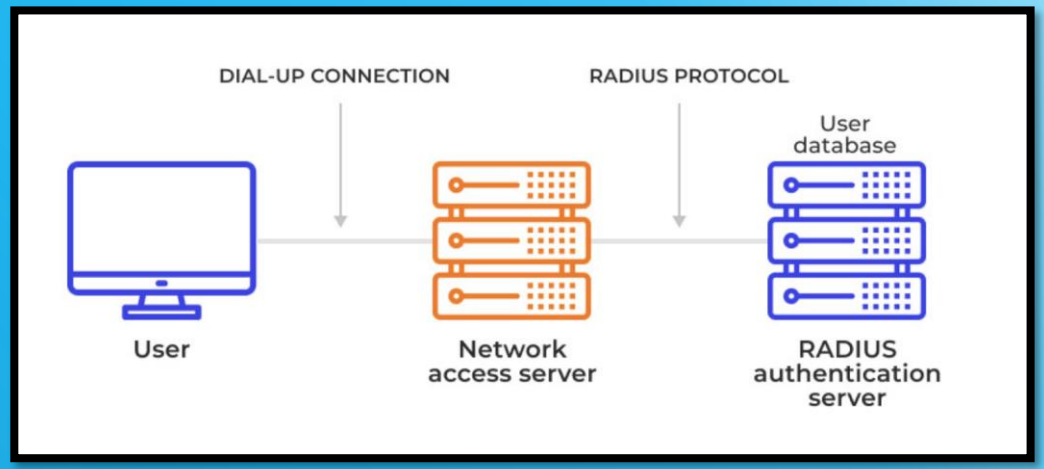
Példa egy incidensre

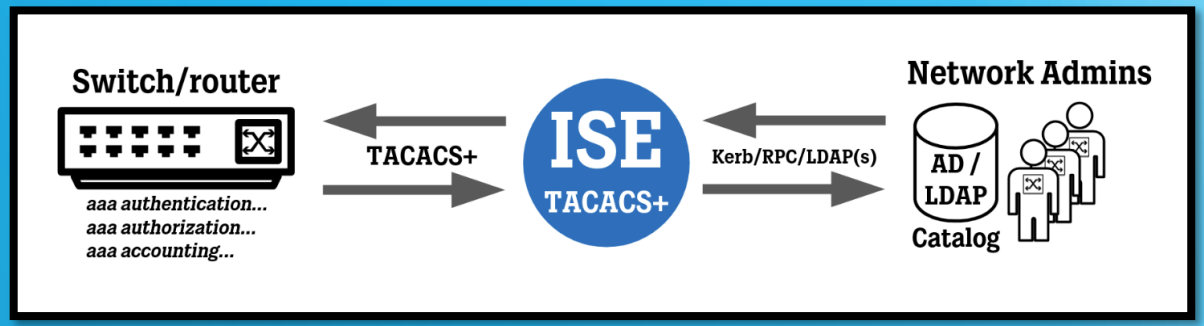
Accounting

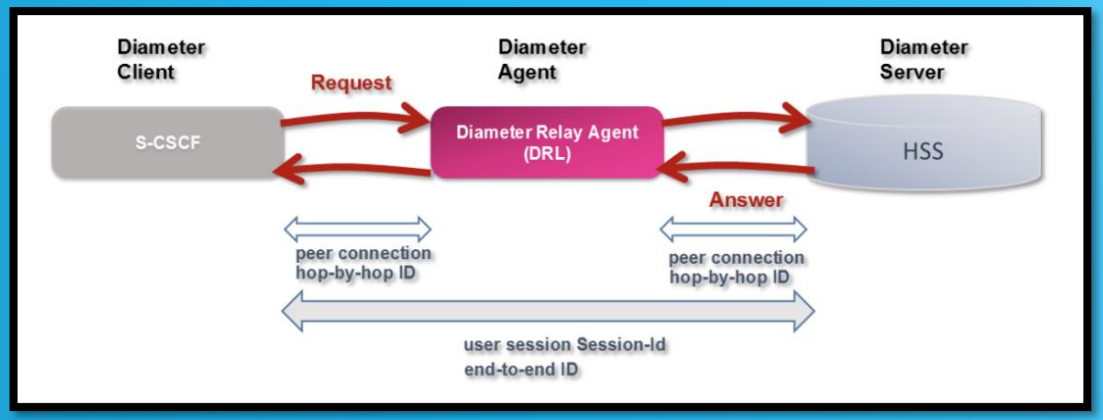
- Szituáció:
  - Gyanús adatletöltés történt
- Accounting segítségével:
  - Azonosítható a felhasználó
  - Megállapítható az időpont
  - Látható az érintett fájl
  - Követhető az IP-cím

Protokolok AAA-ra

- Leggyakrabban használt protokolok:
- RADIUS
- TAKACS+
- Diameter







Hivatkozások

- https://www.tmit.bme.hu/sites/default/files/RelNetik_20180918_InfSecurity.pdf
- https://noreg.hu/megoldasaink/azonositas-es-jogosultsag-kezeles-9
- https://www.fortinet.com/resources/cyberglossary/aaa-security
- https://www.strongdm.com/blog/aaa-security
- https://community.cisco.com/t5/networking-blogs/what-is-aaa-authentication-authorization-and-accounting/ba-p/5138307
- https://en.wikipedia.org/wiki/Authorization
- https://www.lenovo.com/us/en/glossary/aaa/
- https://www.geeksforgeeks.org/computer-networks/computer-network-aaa-authentication-authorization-and-accounting/
- https://securiti.ai/glossary/aaa-server/
- https://nordlayer.com/blog/the-role-of-access-control-lists/
- https://www.wiresandwi.fi/blog/solid-config-cisco-aaa-tacacs-and-password-best-practices
- https://www.wallarm.com/what/radius-remote-authentication-dial-in-user-service-protocol
- https://realtimecommunication.wordpress.com/2016/08/30/diameter-overview/