SQL alapú Radius szolgáltatás

Pásztor György
pasztor@bibl.u-szeged.hu
Szegedi Tudományegyetem - Egyetemi Könyvtár

Témák

- Usersfile vs. radius
- Auth*
- Accounting

Miről nem szól:

- *EAP*
- *Hitelesítés*
- 802.1X

Defaultok

Un*x	Debian GNU/Linux
SQL	Postgresql
Radius	Freeradius

Users

Statikus users fájlbeli bejegyzés pl.:

```
pasztor Auth-Type := Local, User-Password == "s3cr3t"
        cisco-avpair = "shell:priv-lvl=15",
        Service-Type = Login-User
```

Részei:

- Ellenőrzendő attributumok
- Válaszolandó attributumok

Csoportok

```
DEFAULT Group == "disabled", Auth-Type := Reject
        Reply-Message = "Your account has been disabled."
```

Users vs. SQL

- Szintaktikai hiba beláthatatlan zavarokat okozhat
- A users file-t vmilyen információk alapján elő kell állítani v. karban kell tartani
- Össze kell hangolni a ,,karbantartásokat” a `SIGHUP`pal
- Össze kell hangolni a ,,forrásadatok” változását a ,,karbantartásokkal”
- nincs lehetőségünk ,,egyéb” kiegészítő információk tárolására

Egyszerű WiFi-s példa

Felhasználók:

- VIP userek
- Automatikus felhasználók más adatbázis alapján
- Ideiglenes helyi accountok

VIPek

```
CREATE TABLE edusers (
        id      SERIAL PRIMARY KEY,
        UserName        VARCHAR(64) NOT NULL DEFAULT '',
        Password        VARCHAR(253) NOT NULL DEFAULT '',
        Comment         TEXT
);

CREATE VIEW eduroam_radcheck AS
        SELECT id, Username || '@bibl.u-szeged.hu'::text AS UserName,
        'Password'::text AS Attribute, '=='::text AS op,
        Password AS Value
        FROM edusers;
```

Automatikusak

```
CREATE TABLE corvusers (
        id      SERIAL PRIMARY KEY,
        UserName        VARCHAR(64) NOT NULL DEFAULT '',
        Password        VARCHAR(253) NOT NULL DEFAULT '',
        lastup  TIMESTAMP WITHOUT TIME ZONE
);

CREATE VIEW corvina_radcheck AS
        SELECT id, Username || '@bibl.u-szeged.hu'::text AS UserName,
        'User-Password'::text AS Attribute, '=='::text AS op,
        Password AS Value
        FROM corvusers;
```

Lejárósok I.

```
CREATE TABLE kvt_wifi_access (
        username TEXT,
        start_time TIMESTAMP WITHOUT TIME ZONE DEFAULT
             '1970-01-01 00:00:00'::timestamp without time zone,
        valid_period INTEGER DEFAULT 0,
        expire_date TIMESTAMP WITHOUT TIME ZONE DEFAULT
             '1970-01-01 00:00:00'::timestamp without time zone,
        id INTEGER DEFAULT
             nextval('public.static_radcheck_id_seq'::text) NOT NULL
);
```

Lejárósok II.

```
CREATE VIEW kvt_radcheck AS
     SELECT kwa.id, kwa.username,
            'User-Password'::text AS attribute,
            '=='::text AS op, 'guestwifi'::text AS value
     FROM kvt_wifi_access kwa
     WHERE ((kwa.expire_date =
              '1970-01-01 00:00:00'::timestamp without time zone)
       OR ((kwa.expire_date)::timestamp with time zone > now()));
```

Ellenőrzendő attributumok összekötése

```
CREATE VIEW radcheck AS
        SELECT id, Username, Attribute, op, Value
               FROM eduroam_radcheck UNION ALL
        SELECT id, Username, Attribute, op, Value
               FROM corvina_radcheck UNION ALL
        SELECT id, Username, Attribute, op, Value
               FROM kvt_radcheck UNION ALL
        SELECT id, Username, Attribute, op, Value
               FROM static_radcheck;
```

Válaszolandó attributumok

```
radius=# SELECT * from radgroupreply;
 id | groupname |          attribute          | op |    value
----+-----------+-----------------------------+----+-------------
  1 | eduroam   | Service-Type                | =  | Framed-User
  2 | lwifi     | Service-Type                | =  | Framed-User
  3 | lwifi     | Tunnel-Type:1               | =  | 13
  4 | lwifi     | Tunnel-Medium-Type:1        | =  | 6
  5 | lwifi     | Tunnel-Private-Group-ID:1 | =  | 210
(5 rows)
```

Csoportok I.

```
CREATE VIEW eduroam_usergroup AS
    SELECT UserName||'@bibl.u-szeged.hu'::text AS UserName,
          'eduroam'::text AS GroupName, 0 AS priority FROM edusers;
CREATE VIEW corvina_usergroup AS
    SELECT UserName||'@bibl.u-szeged.hu'::text AS UserName,
          'eduroam'::text AS GroupName, 0 AS priority FROM corvusers;
CREATE VIEW kvt_usergroup AS
    SELECT 0 AS priority, kwa.username, 'lwifi'::text AS groupname
    FROM kvt_wifi_access kwa
    WHERE ((kwa.expire_date =
                '1970-01-01 00:00:00'::timestamp without time zone)
           OR ((kwa.expire_date)::timestamp with time zone > now())) ;
```

Csoportok II.

```
CREATE VIEW usergroup AS
        SELECT UserName, GroupName, priority
          FROM eduroam_usergroup UNION ALL
        SELECT UserName, GroupName, priority
          FROM corvina_usergroup UNION ALL
        SELECT UserName, GroupName, priority
          FROM kvt_usergroup UNION ALL
        SELECT UserName, GroupName, priority
          FROM static_usergroup;
```

„lejáratás”

/etc/freeradius/postgresql.conf:

```
postauth_query = "UPDATE kvt_wifi_access SET start_time = 'now', \
        expire_date = now() + valid_period * interval '1 second' \
        WHERE username = '%User-Name' \
          AND start_time = '1970-01-01'::timestamp;"
```

„Betárcsázós” példa

- Felhasználói azonosítás
- Egyéb attributumok (pl. fix ip, rate limit)

Előfizetés-típusok

```
CREATE TABLE substypes (
        id SERIAL PRIMARY KEY,
        packname TEXT UNIQUE,
        price INTEGER,
        ratelimit TEXT,
        fwmark INTEGER
);
```

Felhasználók

```
CREATE TABLE subscribers (
        id SERIAL PRIMARY KEY,
        name TEXT,
        login TEXT UNIQUE,
        "password" TEXT,
        email TEXT,
        ftpquota INTEGER,
        subt INTEGER REFERENCES substypes(id)
);
```

Végpontok

```
CREATE TABLE netpoint (
        ip INET PRIMARY KEY,
        mac MACADDR,
        reverse TEXT,
        belongs INTEGER REFERENCES subscribers(id)
);
```

Jelszóellenőrzés

```
CREATE VIEW radpwcheck AS
     SELECT 0 AS id ,
            sub.login AS UserName,
            'User-Password'::text AS Attribute,
            '=='::text AS op,
            sub.password AS Value FROM public.subscribers sub ;
CREATE VIEW radcheck AS
      SELECT rpw.id, rpw.UserName, rpw.Attribute, rpw.op, rpw.Value
        FROM radpwcheck rpw UNION ALL
      SELECT src.id, src.UserName, src.Attribute, src.op, src.Value
        FROM static_radcheck src;
```

Kiegészítő ötletek

- a; cleartext eltárolás+view+tárolteljárás
- b; cleartext bevitel egy táblába, ahova rule-al és tárolt eljárással a kívánt hash-eket letároljuk (opcionálisan a cleartext-et is)
- jogosultságok sql szinten beszabályozása (pl. radius szerver csak crypt()-elt jelszót tudjon select-elni)

Előfizetés-típus vs. Rate-Limit

```
CREATE VIEW radgroupratelimit AS
  SELECT id,
         packname AS GroupName,
         'Mikrotik-Rate-Limit'::text AS Attribute,
         '='::text AS op, ratelimit AS Value FROM public.substypes;
CREATE VIEW radgroupreply AS
  SELECT rgrl.id, rgrl.GroupName, rgrl.Attribute, rgrl.op, rgrl.Value
    FROM radgroupratelimit rgrl UNION ALL
  SELECT srr.id, srr.GroupName, srr.Attribute, srr.op, srr.Value
    FROM static_radgroupreply srr;
```

Megj.: A felhasználót bele kell tenni az előfizetésének megfelelő csoportba!

Fix IP

```
CREATE VIEW radiprep AS
  SELECT 0 AS id,
         sub.login AS UserName,
         'Framed-IP-Address'::text AS Attribute,
         ':='::text AS op, host(net.ip)::text AS Value
  FROM public.netpoint net join public.subscribers sub on belongs=id;
CREATE VIEW radreply AS
  SELECT rip.id, rip.UserName, rip.Attribute, rip.op, rip.Value
    FROM radiprep rip UNION ALL
  SELECT srr.id, srr.UserName, srr.Attribute, srr.op, srr.Value
    FROM static_radreply srr;
```

Előfizetés-típus vs. Csoporttagság

```
CREATE VIEW radgroupsubstype AS
  SELECT sr.login AS UserName,
         st.packname AS GroupName,
         sr.id AS priority
  FROM public.subscribers sr
  JOIN public.substypes st ON sr.subt=st.id;

CREATE VIEW usergroup AS
  SELECT rgst.username, rgst.groupname, rgst.priority
    FROM radgroupsubstype rgst UNION ALL
  SELECT sup.username, sup.groupname, sup.priority
    FROM static_usergroup sup;
```

Wifi AP használati statisztika

```
radius=# SELECT nasipaddress,
                sum(acctinputoctets) AS inbytes,
                sum(acctoutputoctets) AS outbytes,
                sum(acctsessiontime) as time
          FROM radacct GROUP BY nasipaddress ;
 nasipaddress |    inbytes    |   outbytes    |  time
--------------+---------------+---------------+---------
 10.1.20.7    |  867620237436 | 2426845549902 |   58986
 10.1.20.8    |  874377164753 | 2204377713865 | 1529068
 10.1.20.3    |  311106808355 | 1145634452897 | 1250730
 10.1.20.2    | 1823688024005 | 5910224360551 | 2281496
 10.1.20.1    |  218044176865 |  546503489103 | 1501330
(5 rows)
```

Havi statisztika I.

```
radius=# select sum(acctsessiontime) AS Time,
                sum(acctinputoctets) AS inbytes,
                sum(acctoutputoctets) AS outbytes,
                CASE
  WHEN acctstarttime >'2006-01-01 00:00:00' AND
       acctstarttime < '2006-02-01 00:00:00' THEN '2006 Jan'::text
  WHEN acctstarttime >'2006-02-01 00:00:00' AND
       acctstarttime < '2006-03-01 00:00:00' THEN '2006 Feb'::text
...
  WHEN acctstarttime >'2006-12-01 00:00:00' AND
       acctstarttime < '2007-01-01 00:00:00' THEN '2006 Dec'::text
  ELSE 'Nem 2006'::text END AS month FROM radacct group by month ;
```

Havi statisztika II.

time	inbytes	outbytes	month
2473525	952836390429	16858726851 88	2006 Jan
3615012	1216182006767	3535199540846	2006 Feb
4283783	9972777554503	16575736347100	2006 Mar
2867992	3142345495240	5594229160085	2006 Apr
3596517	1987676878308	4441777734909	2006 May
2834506	804848847436	1825844487908	2006 Jun
2232458	1484048661591	2874316867047	2006 Jul
3398311	1303115272811	3152940391135	2006 Aug
4803248	1863407636928	5421228279910	2006 Sep
5122465	5040280320420	9241454069326	2006 Okt
5746381	3573540573888	8060708059590	2006 Nov
5348109	2094770601856	4970810330180	2006 Dec

További ötletek

- Letöltéskorlátos előfizetés: radreply és accounting táblák összekapcsolásával
- Időkorlátos előfizetés: radreply és accounting táblák összekapcsolásával
- Adott havi forgalom után „bünti” attributumok
- …

online cím:

`http://www.bibl.u-szeged.hu`
`/~pasztor/niif2k7radsql/`