Freeradius telepítése RHEL/Almalinux 9 (x86_64) rendszeren

Előkészítés

Kiindulásként AlmaLinux 9 (x86_64) operációs rendszer telepítését kell elvégezni. A telepítés minimal telepítés.

Telepítést követő lépések

Módosítani kell a /etc/dnf/dnf.conf állományt a felesleges gyenge függőségek telepítésének tiltásához:

```
# if [ ! -f /etc/dnf/dnf.conf.orig ] ; then cp -a /etc/dnf/dnf.conf
/etc/dnf/dnf.conf.orig && echo 'install_weak_deps=False' >>
/etc/dnf/dnf.conf ; fi
```

Érdemes kikapcsolni a kernel üzenetek megjelenítését

```
# grubby --update-kernel=ALL --args=quiet
```

A SElinux-ot átmenetileg megengedő módba kell kapcsolni

```
# sed -i 's/^SELINUX=.*/SELINUX=permissive/' /etc/selinux/config
```

Be kell állítani a rendszer locale-t en_US.UTF-8-ra

```
# localectl
```

Listázzuk az elérhető csomagokat

```
# dnf list freeradius*
Last metadata expiration check: 1:14:21 ago on Mon 08 Sep 2025 07:24:49 PM
CEST.
Available Packages
freeradius.x86_64
3.0.21-44.el9_6
appstream
freeradius-devel.x86_64
3.0.21-44.el9_6
appstream
freeradius-doc.x86_64
3.0.21-44.el9_6
appstream
freeradius-krb5.x86_64
```

```
3.0.21-44.el9_6
appstream
freeradius-ldap.x86_64
3.0.21-44.el9_6
appstream
freeradius-utils.x86_64
3.0.21-44.el9_6
appstream
```

Telepítsük a szükséges csomagokat

```
# dnf install freeradius freeradius-utils
```

Futtassuk a radiusd programot debug módban ahol az alábbi hibát kapjuk

```
   tls-config tls-common {
    verify_depth = 0
    ca_path = "/etc/raddb/certs"
    pem_file_type = yes
    private_key_file = "/etc/raddb/certs/server.pem"
Unable to check file "/etc/raddb/certs/server.pem": No such file or
directory
/etc/raddb/mods-enabled/eap[183]: Failed parsing configuration item
"private_key_file"
rlm_eap_tls: Failed initializing SSL context
rlm_eap (EAP): Failed to initialise rlm_eap_tls
/etc/raddb/mods-enabled/eap[14]: Instantiation failed for module "eap"
```

Inicializáljuk a tanúsítványokat

```
# cd /etc/raddb/certs

# make ca.pem
make[1]: Entering directory '/etc/raddb/certs'
make[1]: Leaving directory '/etc/raddb/certs'
make[1]: Entering directory '/etc/raddb/certs'
make[1]: Leaving directory '/etc/raddb/certs'
openssl req -new -x509 -keyout ca.key -out ca.pem \
    -days '60' -config ./ca.cnf \
    -passin pass:'whatever' -passout pass:'whatever' -noenc
.+.......+...+......+..+++++++++++++++++++++++++++++++++++++++*..+...+.+...+
.....+...+...+......+.+...+++++++++++++++++++++++++++++++++++++++*..+...+...
.++++++
...+..........+......+.........+...+...+.....++++++++++++++++++++++++++++++
++++++++*.......+.............+.+.....+.+..++++++++++++++++++++++++++++++++
+++++++*........+...+...+............+...+..............+.............+.....
...+...+....+..+.........+............+...+......+...............+.+.....+..
..........+..+..................+...+...+.....+...+.+.........+......+....
.+...+.+.....+.+...........+...+......+.+...+..............+.......+.....+..
.+.......+.........+......+......++++++
-----
```

```
chmod g+r ca.key
chown root:radiusd ca.*
chmod 640 ca.*

# make server.pem
openssl req -new  -out server.csr -keyout server.key -config ./server.cnf -
noenc
.+.....+.....+..+.....+.....+.+.....+.....+.....+.+...
.....+....+.....+.+.....+.....+.....+...+.+.....+.....+.....+..
..+++++++++++++++++++++++++++++++++++++*.+.....+.....+.....+..
+....+.....+.++++++++++++++++++++++++++++++++++++*.....+.....
.....+..+...+.....+..+.....+...+..+....+.....++++++
.....+...+.....+.....+.....++++++++++++++++++++++++++++++++++++*.
.+.....+.....+.....+.....+....+.....++++++++++++++++++
++++++++++++++++*...+.....+...+.....+.+.....+.....+....
.....+...+...+...+.+...+...+...+.....+..+.....+.....+....+..+.
.....+.....+.....+.....+.....+.....+...+.....+..
.+...+.....+.....+.....+++++
-----
chmod g+r server.key
openssl ca -batch -keyfile ca.key -cert ca.pem -in server.csr  -key
'whatever' -out server.crt -extensions xpserver_ext -extfile xpextensions -
config ./server.cnf
Using configuration from ./server.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Sep  8 19:11:33 2025 GMT
            Not After : Nov  7 19:11:33 2025 GMT
        Subject:
            countryName               = FR
            stateOrProvinceName       = Radius
            organizationName          = Example Inc.
            commonName                = Example Server Certificate
            emailAddress              = admin@example.org
        X509v3 extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://www.example.com/example_ca.crl
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.40808.1.3.2
Certificate is to be certified until Nov  7 19:11:33 2025 GMT (60 days)

Write out database with 1 new entries
Database updated
openssl pkcs12 -export -in server.crt -inkey server.key -out server.p12  -
passin pass:'whatever' -passout pass:'whatever'
```

```
chmod g+r server.p12
openssl pkcs12 -in server.p12 -out server.pem -passin pass:'whatever' -
passout pass:'whatever'
chmod g+r server.pem
chown root:radiusd server.*
chmod 640 server.*
```

Amennyiben szeretnénk az eredeti állaporta állni, akkor az alábbu utasításokat futtassuk

```
# cd /etc/raddb/certs && rm -f *.pem *.der *.csr *.crt *.key *.p12 serial*
index.txt*
```

From:
https://wiki.r-l.hu/ - **Reverse-Logic wiki**

Permanent link:
https://wiki.r-l.hu/doku.php?id=linux:freeradius&rev=1757359708

Last update: **2025/09/08 19:28**