RADIUS in Perl: Radiator

11. Deutscher Perl Workshop

Kurt Jaeger, pi@nepustil.net

http://www.nepustil.net/

Frankfurt, 27. Februar 2009

Übersicht

- Kurzvorstellung
- Meta-Ebene
- RADIUS
- Radiator
- Perl
- Beispiele

Kurzvorstellung

- Geschäftsführer eines regionalen ISPs (Dr.-Ing. Nepustil & Co. GmbH)
- Vorstand ISP Service eG
- Perl Anwender seit 1992 (ab 4.0)
- Radiator Anwender seit 1998

Meta-Ebene

- Anwendung vorstellen
- Nutzt Perl Stärken
- ist weltweit verbreitet
- und: völlig unbekannt
- wirtschaftliche Relevanz
  - Schlüsselfunktion Abrechnung
  - Lizenzpflichtige Software

Was ist RADIUS ?

- Remote Authentication Dial In User Service
- Spec: RFC2865 (und weitere), siehe auch RFC5080
- Kurz: Username + Passwort: Zugriff erlauben oder verweigern
- Zugangskontrolle für NAS Devices
- AAA:
  - Authentication: Who's calling whom ?
  - Authorisation: What resource is he allowed to access ?
  - Accounting: How much resources were used ?

Kurze Geschichte

- TACACS
- RADIUS
- Diameter (RFC3588)

Was sind NAS Devices ?

- Network Access Server
- Dialin-Router (Portmaster, Ascend, Cisco, Funkwerk, ...)
- BBRAS der Telekom
- WLAN Access Points
- Ethernet Switche
- Unix Hosts (PAM!), auch andersrum
- Anderer Name: RAS (Remote Access Server)
- Nicht verwechseln mit Network Attached Storage!
- ...

Geräte, die selbst keine Kennungen speichern, verwenden RADIUS

Ausführlicher: Welche Form von Zugriff ?

- address assignment
- address filtering
- route assignment
- QoS/differential services
- bandwidth control/traffic management
- compulsory tunneling to a specific endpoint
- encryption
- ...

Wie funktioniert RADIUS ?

- Clients
- Requests/Response
- Über UDP
- Notwendige Daten sind einfach strukturiert
- Pakete auch!
- tcpdump-kompatibel

RADIUS ist tcpdump kompatibel

```
auth# tcpdump -i fxp0 -n -s 1500 -vv host <radiushost>
      and port 1812
[...]
15:15:20.639322 <nasip>.1645 > <radiushost>.1812:
  [udp sum ok]
  rad-access-req 190 [id 79] Attr[  Framed_proto{PPP}
  User{username} Pass NAS_port{192}
  NAS_port_id{Uniq-Sess-ID192}
  Calling_station{eth 7/0/0:4096.4096 0/0/0/0/0/0/0}
  Connect_info{1184000/160000} NAS_port_type{Virtual}
  Service_type{Framed} NAS_ipaddr{<nasip>}
  NAS_id{nashostname} ]
  (ttl 254, id 9491, len 218)
```

RADIUS Benutzereintrag für Telnet

```
username User-Password = "password"
        Service-Type = Login-User,
        Login-Service = Telnet,
        Login-IP-Host = 192.168.10.1,
        Ascend-Idle-Limit = 600
```

RADIUS Benutzereintrag für PPP

```
username@my-dsl User-Password = "password"
        Service-Type = Framed-User,
        Framed-Protocol = PPP,
        Framed-MTU = 1456,
        Framed-IP-Address = 192.168.5.1,
        Framed-IP-Netmask = 255.255.255.255,
        Framed-Compression = Van-Jacobsen-TCP-IP
```

RADIUS Benutzereintrag für L2TP Tunnel

```
username
   Service-Type = Outbound-User,
   cisco-avpair = "vpdn:ip-addresses=10.1.1.1",
   cisco-avpair = "vpdn:tunnel-id=mytunnelid",
   cisco-avpair = "vpdn:tunnel-type=l2tp",
   cisco-avpair = "vpdn:l2tp-tunnel-password=tunnelpw",
   cisco-avpair = "vpdn:source-ip=192.168.1.1"
```

Was ist ein Radius-Request/Response ?

- Menge von Elementen: TLV
  - Type of Attribute
  - Length
  - Value
- id (8 bit)
- Authenticator (shared secret)

Welche Elemente sind möglich ?

- Viele
  - ca. 120 im Standard
    http://www.iana.org/assignments/radius-types
  - ca. 180 legacy
  - ca. 2000 bekannte herstellerspezifische
- Konfigurierbar
- Hersteller-spezifische Attribute möglich
  http://www.iana.org/assignments/enterprise-numbers
- dictionary

dictionary

```
ATTRIBUTE Service-Type  6                    integer
VALUE     Service-Type  Login-User             1
VALUE     Service-Type  Framed-User            2
VALUE     Service-Type  Callback-Login-User  3
[...]
VALUE     Service-Type  Fax                    13
```

Was ist ein Radius Accounting ?

- Dasselbe wie Requests
- nur andere Attribute und anderer Port
- Start- und Stop Records
- Wirklich wichtig sind nur die Stop-Records
- Geht einer verloren, verliert der NAS-Betreiber Geld

Beispiel Accounting Record Teil 1

```
Sun Oct 26 20:40:32 2008
        Acct-Session-Id = "00000130"
        Tunnel-Type:0 = L2TP
        Tunnel-Medium-Type:0 = IPv4
        Tunnel-Server-Endpoint:0 = "212.178.180.11"
        Tunnel-Client-Endpoint:0 = "212.118.171.165"
        Tunnel-Assignment-Id:0 = "ISPEG"
        Tunnel-Client-Auth-Id:0 = "lac_ispeg_opsec"
        Tunnel-Server-Auth-Id:0 = "LNS-OPSEC"
        Acct-Tunnel-Connection = "436601532"
        Framed-Protocol = PPP
        Framed-IP-Address = 195.30.35.16
        Framed-IPv6-Route = "2001:14f8:0700:0008::/64"
        Framed-IPv6-Route = "2001:14f8:0400::/48"
        Framed-Interface-Id = 0:0:0:1
        User-Name = "opsec-nep#eg@dsl-direkt"
```

Beispiel Accounting Record Teil 2

```
Acct-Authentic = RADIUS
X-Ascend-Connect-Progress = LAN-Session-Up
Cisco-AVPair = "connect-progress=LAN Ses Up"
X-Ascend-PreSession-Time = 0
X-Ascend-Xmit-Rate = 17696000
Cisco-AVPair = "nas-tx-speed=17696000"
X-Ascend-Data-Rate = 1184000
Cisco-AVPair = "nas-rx-speed=1184000"
Acct-Session-Time = 342
Acct-Input-Octets = 1102
Acct-Output-Octets = 1667
X-Ascend-Pre-Input-Octets = 0
X-Ascend-Pre-Output-Octets = 40
Acct-Input-Packets = 51
Acct-Output-Packets = 57
X-Ascend-Pre-Input-Packets = 0
```

Beispiel Accounting Record Teil 3

```
X-Ascend-Pre-Output-Packets = 2
Acct-Terminate-Cause = User-Request
X-Ascend-Disconnect-Cause = PPP-Rcv-Terminate-Req
Cisco-AVPair = "disc-cause-ext=PPP Receive Term"
Acct-Status-Type = Stop
NAS-Port = 105
NAS-Port-Id = "Uniq-Sess-ID105"
Connect-Info = "17696000/1184000"
NAS-Port-Type = Virtual
Service-Type = Framed-User
NAS-IP-Address = 212.178.180.11
NAS-Identifier = "vgate.opsec.eu"
Acct-Delay-Time = 0
Client-IP-Address = 212.178.180.11
Acct-Unique-Session-Id = "d03978a8140211a7"
Timestamp = 1225050032
```

Radiator

- Implementiert RADIUS Server
- 8000 Installationen in 180 Ländern
- 100% Perl
- Lizenzpflichtige Software!
- Entwickler: http://www.open.com.au
- Kosten: 1000 AU$/ca. 600 EUR, für eine Single-Instanz-Lizenz
- Läuft auf allen Plattformen, die Perl bereitstellen
- Sehr leicht erweiterbar
- Doku: http://www.open.com.au/radiator/ref.pdf

Technisch

- Radiator startet wie ein normaler Daemon (oder Dienst)
- Radiator liest config file
- Führt diverse Hooks aus
- Fängt dann an, auf eingehende Anfragen zu antworten
- Lang-laufender Prozess
- keine Threads
- in Beta: Serverfarm Option

Beispiel Config 1

```
# Allgemeine Angaben
Foreground
#LogStdout
Trace 5
AuthPort 1812
AcctPort 1813
LogDir /var/log/radiator
DbDir /usr/local/etc/radiator
DictionaryFile  /usr/local/etc/radiator/dictionary
PidFile /var/log/radiator/pid
LogFile /var/log/radiator/log.%Y%m%d
BindAddress 213.178.180.15,ipv6:2001:14f8:0200:0000:000
```

Beispiel Config 2

```
# NAS Devices (Clients)
<Client ipv6:2001:14f8:0200:0000:0000:0000:0000:000f>
        Secret ArAtVap1
        DupInterval 0
        IgnoreAcctSignature
</Client>

<SNMPAgent>
Port 1814
ROCommunity Ejukhacji
BindAddress 213.178.180.15
</SNMPAgent>
```

Beispiel Config 3

```
<AuthLog FILE>
  Identifier flat
  Filename /var/log/radiator/flat
  SuccessFormat %l:%u:%P:OK
  FailureFormat %l:%u:%P:FAIL
  LogSuccess 1
  LogFailure 1
</AuthLog>
<Handler>
  AuthLog flat
  AcctLogFileName /var/log/radiator/flat.%Y%m%d
  AuthByPolicy ContinueWhileReject
  <AuthBy FILE>
    Filename /usr/local/etc/radiator/users/flatfile
  </AuthBy>
</Handler>
```

Wie funktioniert Radiator ?

- Clients
- Usernames and Realms
- user@domain: user and realm
- Handler
- AuthBy Module

Welche AuthBy Module ?

- FILE
- Radius
- SQL
- LDAP
- IMAP
- NTLM
- ... (ca. 60!)

Welche Datenbanken ?

- Mysql
- Oracle
- Sybase
- Postgres
- ODBC
- Interbase
- Informix
- SQLite2
- CSV

TODO: Vergleich RADIUS gegen...

- LDAP
- Kerberos
- PAM
- NIS
- NTLM
- AD
- ...

Perl-Code

- ca. 60K LoC
  - 600 Zeilen für den Server
  - Rest: Eigene Module und CPAN
- Class Inheritance: siehe Seite 315
- Lesenswerte Module:
  - Radius/Radius.pm
  - Radius/ServerHTTP.pm: Einfacher Webserver
  - Radius/Resolver.pm: DNS-Lookup
  - Radius/SNMPAgent.pm: SNMP Server
  - Radius/ApplePasswordServer.pm
  - Radius/RSAAM.pm: SecureID
  - goodies/nntp-redirect.pl: NNTP Auth für Newsserver

Beispiele

- ISP Service eG: lokale Testuser, Radius Peering
- L2TP
- EAP: Extensible Authentication Protocol
- EDUROAM
- NNTP Proxy
- Mobilfunk-Anwendung
- IPv6

ISP Service eG

- Zusammenschaltungen mit diversen Carriern (Telekom u.a.) und unterschiedlichen DSL Plattformen
- einkommende DSL Sessions
  - Auth über Radius Peering (anhand des Benutzernamens)
  - lokal reinlassen oder per L2TP weiter zu den Mitglieds-ISPs
- Abrechnung der Nutzung über Radius Accounting
- Monitoring der Radius-Server der ISPs möglich, aber noch offen

L2TP Weiterleitung

- Einkommende PPPoE über L2TP Sessions werden angenommen
- Radius übergibt je nach Usernamen L2TP Tunnelparameter an den Gateway
- PPPoE Session wird per L2TP weitergeleitet

EAP: Extensible Authentication Protocol

- RFC2284 und RFC2869
- z.B. Ethernet oder WLAN
- siehe Doku, Seite 326ff
- siehe Demo

EDUROAM

- http://www.eduroam.org/, http://www.eduroam.edu.au/
- 33 Länder nehmen in EU teil
- 6 in Asien, u.a. Japan und China
- Handbuch für den Setup ist online
- behandelt u.a. Radiator

NNTP Proxy

- Sourcecode ist Teil von Radiator goodies/nntp-redirect.pl
- NNTP Proxy: Server und Client
- Spricht RADIUS für NNTP Authentisierung
- Leitet dann weiter an den ursprünglichen NNTP Server

Mobilfunk-Anwendung

- Intranet/Extranet-Zugriff
- 600K Benutzer aus den Netzen dreier Mobilfunkbetreiber
- im Peak: 180 requests/sec (auth, acct start/stop)
- Radius-Request mit Rufnummer kommt rein
- Antwort mit IP-Adresse geht zurück
- Benutzerdaten kommen aus Oracle-Datenbank
- 6 Server, zwei als Radius-Proxies, 4 als Backend-Radius
- Server: 8 GB RAM, Sun x4200, Dual-Core, Debian Linux
- Realisiert von T-Systems

IPv6

- RADIUS ist eine zentrale Anwendung für grosse Netze
- IPv6 Ready ?
  - Ja, aber manche NASe noch nicht
  - schicken nur ueber IPv4
  - aber können IPv6 Adressen austeilen/verwalten

Beispiel: IPv6 Adressvergabe

```
testingv6 User-Password == "testing"
    Service-Type == Framed-User,
    Framed-Protocol = PPP,
    Idle-Timeout = 86400,
    Framed-MTU = 1456,
    Framed-IP-Address = 197.30.35.16,
    Framed-IP-Netmask = 255.255.255.255,
    Framed-Interface-Id = "0:0:0:1",
    Cisco-AVPair = "ipv6:prefix=2001:14f8:0200:0008::/64
    Cisco-AVPair += "ipv6:route=2001:14f8:0700:0008::/64
    Cisco-AVPair += "ipv6:route=2001:14f8:0400::/48"
```

Probleme und Lösungen

RADIUS

- maximal 255 offene Anfragen: Loadbalancer
- Verzögerungen bei externe Datenquellen: Loadbalancer
- Sicherheit ? RADSEC, Diameter
- Radius Peering und Verzögerungen/Ausfälle
- Zustand und Radius: Das ls -l Problem
- Crash/Reboot eines NAS

Radiator

- Serielle Abarbeitung: Loadbalancer
- Not enterprisy enough
- Does not do the dishes

Literatur

- http://deployingradius.com/blog/
- http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470011947.html SIP/VoIP und Radius
- http://oreilly.com/catalog/9780596003227/

Danke!

- Hugh Irvine und Mike McCauley, Open System Consultants
- Stefan Feurle, T-Systems