TU Clausthal

Vorschau auf FreeRADIUS 4

C. Strauf
Rechenzentrum TU Clausthal
67. DFN Betriebstagung

Agenda

- Herausforderung FreeRADIUS-Migration
- Warum sollte man migrieren?
- Änderungen FreeRADIUS 3 → 4
- Zeitplan für FreeRADIUS 4?
- Tips für die Migration
- Fazit

Herausforderung FreeRADIUS-Migration

- FreeRADIUS ist sehr mächtig und stabil. **Aber…**
- Eine FreeRADIUS-Migration ist bei Major-Releases kein Spaß. 😣
- Probleme:
  - Änderungen in der Syntax der Konfiguration.
  - Konzeptionelle Änderungen (Beispiele: users-File vs. policy.d, Proxy- & LDAP-Load-Balancing etc.) oft tiefgreifend.
  - Es gibt Online-Dokumentation [1], aber es gilt das Prinzip „Beispielkonfiguration = Doku“.
  - Bei Updates:
    - Beispielkonfiguration mit produktiver Konfiguration vergleichen,
    - Konfigurationen abgleichen.
  - Die vorhandene Doku bietet noch Raum für Verbesserungen, hat sich aber über die Jahre bereits gebessert.

[1]
http://networkradius.com/doc/FreeRADIUS%20Technical%20Guide.pdf
https://github.com/FreeRADIUS/freeradius-server/tree/v3.0.x/doc/
http://wiki.freeradius.org/guide/Getting%20Started
http://wiki.freeradius.org/Home

Warum sollte man migrieren?

- Stabilisierung der Infrastruktur und der Performance.
- Bessere Möglichkeiten für die Load-Balancing, Verfügbarkeit und Anbindung an Verzeichnisdienste / DBs.
- Wichtigster und ausschlaggebender Grund: Stetige Beseitigung von Sicherheitslücken (**nicht nur im Code von FreeRADIUS, sondern auch mit Hilfe besserer Konzepte!**). Beispiel: „`copy_tunnel_reply=yes`“ vs. „`session-state`“-Methode (siehe [1]). Diese konzeptionellen Features werden nicht von den Distributionen per Backport in alte Versionen von FreeRADIUS portiert!
- Weiterer gewichtiger Grund: Alte Versionen werden von der Community nicht supportet. Der Support bei aktuellen stabilen Releases ist hingegen gut. [2]

[1] https://www.dfn.de/fileadmin/3Beratung/Betriebstagungen/bt64/BT64_MobileIT_EAP-PWD_Lawendy.pdf (Folie 13)
[2] http://freeradius.org/support/

Änderungen FreeRADIUS 3 → 4

- Die „schlechte Nachricht“: **Es wird wieder vieles anders.**
- Die gute Nachricht: **Vieles wird vermutlich besser.**
- Eine Übersicht über Änderungen gibt es im Changelog:

  https://github.com/FreeRADIUS/freeradius-server/blob/v4.0.x/doc/ChangeLog

- In jedem Fall lohnt es sich, die Dokumentation in github sorgfältig zu lesen.
- Besonders wichtiges Dokument für die Migration von Version 3 auf 4:

  https://github.com/FreeRADIUS/freeradius-server/blob/v4.0.x/raddb/README.md

  Die nun folgenden Informationen sind weitestgehend diesem Dokument entnommen.

Änderungen FreeRADIUS 3 → 4

- Aus folgenden Gründen gibt es diverse Änderungen in der Konfiguration von FreeRADIUS:
  - Die Struktur von FreeRADIUS 4 wurde gegenüber FreeRADIUS 3 geändert. Die State-Machine wurde überarbeitet und der Server-Core optimiert (Details dazu sind im github-Repo zu finden).
  - Die Konfiguration wurde der tatsächlichen Logik des RADIUS-Protokolls angepasst und ist jetzt verständlicher bzw. sauberer. Trotzdem bedeutet das für langjährige FreeRADIUS-Admins eine Umstellung.
- Beispiele für Konfigurationsänderungen:
  - Virtual Servers brauchen jetzt Namespaces der Form „`namespace = radius`“, damit die State-Engine weiß, dass hier RADIUS gesprochen wird.
  - Im „`listen`“-Abschnitt muss FreeRADIUS mitgeteilt werden, welche Pakettypen er annehmen soll. Beispiele: „`type = Access-Request`“ oder „`type = Accounting-Request`“.
  - Das Transportprotokoll muss im „`listen`“-Abschnitt definiert werden (z. B. „`transport = udp`“).

Änderungen FreeRADIUS 3 → 4

- Die Auffälligste Änderung ist die Ablöse der alten Processing Sections durch neue (logischer benannte) Processing Sections:

Old Name	New Name
authorize	recv Access-Request
authenticate	process
post-auth	send Access-Accept
preacct	recv Accounting-Request
accounting	send Access-Accept
recv-coa	recv CoA-Request
send-coa	send CoA-ACK
send-coa	send CoA-NAK
Post-Auth-Type Reject	send Access-Reject
Post-Auth-Type Challenge	send Access-Challenge

Quelle: https://github.com/FreeRADIUS/freeradius-server/blob/v4.0.x/raddb/README.md#processing-sections (20.9.2017)

Änderungen FreeRADIUS 3 → 4

- Proxying wurde stark überarbeitet:
  - proxy.conf existiert nicht mehr.
  - Die Schlüsselworte `realm`, `home_server` und `home_server_pool` existieren nicht mehr.
  - Proxying wird nun komplett vom `radius`-Modul erledigt.
  - Failover und Load-Balancing (vormals `home_server_pool`) wird nun durch unlang (der Skriptsprache in FreeRADIUS) geregelt. Neu ist, dass damit auch key-basiertes Load-Balancing möglich ist. [1]
  - Requests können nun zu mehreren Servern ge-proxy-t werden. Das war früher nicht möglich. Z. B. können so Accounting-Pakete an mehrere Server geschickt werden.

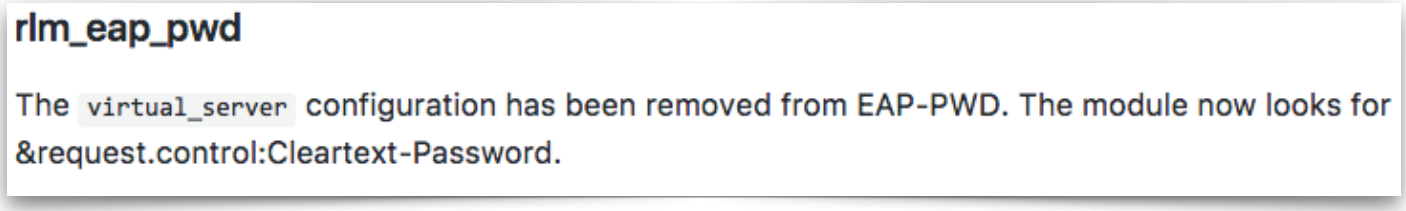
[1] https://github.com/FreeRADIUS/freeradius-server/blob/v4.0.x/raddb/README.md#home_server_pool

Änderungen FreeRADIUS 3 → 4

- Der Umgang mit Attributen in der Konfiguration hat sich geändert. Referenzierung mit „&“ ist nun zwingend erforderlich. Das mach die Konfiguration konsistenter und logischer.
- Diverse Module wurden geändert:
  - rlm_cache,
  - rlm_eap,
  - rlm_eap_pwd,
  - rlm_exec,
  - rlm_expr,
  - rlm_perl,
  - rlm_rest,
  - rlm_sqlcounter,
  - rlm_sql,
  - rlm_sql_mysql,
  - rlm_sql_postgres.

Änderungen FreeRADIUS 3 → 4

- Einige Module wurden gelöscht:
  - rlm_eap_ikev2,
  - rlm_eap_tnc,
  - rlm_counter,
  - rlm_ippool.
- **Achtung:** Manche Änderungen in den Modulen lesen sich übersichtlich, haben aber **signifikante Auswirkungen** in der Konfiguration und im Betrieb! Beispiel:



rlm_eap_pwd

The `virtual_server` configuration has been removed from EAP-PWD. The module now looks for &request.control:Cleartext-Password.

Quelle: https://github.com/FreeRADIUS/freeradius-server/blob/v4.0.x/raddb/README.md#rlm_eap_pwd (20.9.2017)

Zeitplan für FreeRADIUS 4?

- Alan De Kok, Chefentwickler von FreeRADIUS sagt in einer Mail vom 29.8.2017 auf der FreeRADIUS-User-Mailing-Liste, dass die Alpha im Herbst erscheinen soll.
- Es ist also noch Zeit.
- Aber: Es empfiehlt sich, sich unbedingt schon jetzt einen Überblick zu verschaffen, um die Migration planen zu können.

Tips für die Migration

- Führen Sie eine Migration nur von **FreeRADIUS 3 auf FreeRADIUS 4**, da eine Migration von FreeRADIUS 2 auf Grund der vielen Änderungen von Version 2 zu 3 sehr komplex wird. (Version 2 ist schon lange nicht mehr unterstützt und hat Sicherheitsprobleme und sollte nicht mehr verwendet werden!)
- Nutzen Sie Tools zum **Revisions-Management** der Konfiguration (git oder SVN).
  - Migration ist fortlaufender Prozess.
  - Rollback auf funktionierende Versionen bei im Prozess eingeschlichenen Fehlern möglich.
- Übertragen Sie die alte Konfiguration sukzessive in so **kleinen Schritten** wie möglich.
- Vergleichen Sie immer die Beispielkonfiguration mit Ihrer lokalen Konfiguration (auch bei späteren Minor-Releases).
- Testen Sie Änderungen auf **Staging-Systemen** und nicht am Produktivsystem (praktisch für Debugging).
- Planen Sie **ausreichend Zeit** und **personelle Ressourcen** für die Migration ein.

Fazit

- Die Migration auf FreeRADIUS 4 wird komplex sein.
- Die Konfiguration von FreeRADIUS 4 wird im Vergleich zu FreeRADIUS 3 oder älter logischer und transparenter.
- Eine sorgfältige Planung wird entscheidend sein und eine „Migration nebenbei“ wird schwierig.

Vielen Dank für Ihre Aufmerksamkeit!