FreeRadius

- 1 Introdução
  - 1.1 Resumo executivo
  - 1.2 Formatação do documento
- 2 A EDUROAM
  - 2.1 Objectivos da EDUROAM
  - 2.2 Tecnologia usada
    - 2.2.1 Protocolos usados
    - 2.2.2 EAP
    - 2.2.3 Hierarquia
  - 2.3 Termos de utilização
    - 2.3.1 Política de retenção de dados
    - 2.3.2 AUP de utilizadores
    - 2.3.3 Serviços suportados
- 3 RADIUS
  - 3.1 Realm
  - 3.2 Proxy
  - 3.3 Roaming
  - 3.4 Tipo de mensagens RADIUS
  - 3.5 Atributos
  - 3.6 Mensagens de Accounting
- 4 Descrição da solução
  - 4.1 Esquema de rede
  - 4.2 Esquema lógico da solução
- 5 Pré-requisitos
  - 5.1 Hardware
  - 5.2 Software
  - 5.3 Instalação de software
  - 5.4 Regras de firewall
  - 5.5 Redes/VLANS necessárias
- 6 Autenticação de utilizador local
  - 6.1 DNS
    - 6.1.1 NAPTR
  - 6.2 DHCP
  - 6.3 Tempo
    - 6.3.1 /etc/rc.local
  - 6.4 Kerberos
    - 6.4.1 /etc/krb5.conf
  - 6.5 SAMBA
    - 6.5.1 /etc/samba/smb.conf
  - 6.6 winbind
  - 6.7 ntlm_auth
- 7 FreeRADIUS
  - 7.1 Serviço de ponto de vista da rede
  - 7.2 unlang
  - 7.3 Como escolher a versão de FreeRadius
  - 7.4 Ubuntu
  - 7.5 Debian
  - 7.6 CentOS
  - 7.7 Signed Builds
  - 7.8 Instalação de versão de freeradius.org
  - 7.9 Configuração de FreeRadius
  - 7.10 Ligação ao LDAP da AD
    - 7.10.1 /etc/freeradius/modules/ldap (v2.x)
    - 7.10.2 /etc/freeradius/modules/ldap (v3.x)
    - 7.10.3 /etc/freeradius/ldap.attrmap
  - 7.11 Configuração do protocolo mschap
    - 7.11.1 /etc/freeradius/modules/mschap (v2.x)
    - 7.11.2 /etc/freeradius/mods-enabled/mschap (v3.x)
  - 7.12 F-Ticks
    - 7.12.1 /etc/freeradius/modules/f_ticks (v2.x)
    - 7.12.2 /etc/freeradius/mods-enabled/f_ticks (v3.x)
  - 7.13 Modulos do FreeRadius (3.x)
  - 7.14 Status
  - 7.15 Site virtual (domínio local) - Túnel externo
    - 7.15.1 /etc/freeradius/sites-enabled/default
  - 7.16 Inner-Tunnel - Túnel interno
    - 7.16.1 /etc/freeradius/sites-enabled/inner-tunnel
  - 7.17 Configurações do EAP/PEAP/TTLS
    - 7.17.1 /etc/freeradius/eap.conf (v2.x)
    - 7.17.2 /etc/freeradius/mods-enabled/eap (v3.x)
  - 7.18 Dicionários
    - 7.18.1 /etc/freeradius/dictionary
  - 7.19 Filtros/propriedades de utilizadores
    - 7.19.1 Filtros unlang

        - 7.19.2 /etc/freeradius/users (v2.x)
        - 7.19.3 /etc/freeradius/mods-config/files/authorize (v3.x)
        - 7.19.4 /etc/freeradius/preproxy_users
        - 7.19.5 /etc/freeradius/attrs (2.x)
        - 7.19.6 /etc/freeradius/mods-config/attr_filter/post-proxy (3.x)
        - 7.19.7 /etc/freeradius/attrs.pre-proxy (v2.x)
        - 7.19.8 /etc/freeradius/mods-config/attr_filter/pre-proxy (v3.x)
    - 7.20 Clientes / entrada da federação EDUROAM
        - 7.20.1 /etc/freeradius/clients.conf (v2.x)
        - 7.20.2 /etc/freeradius/clients.conf (v3.x)
    - 7.21 Saída para a (con)federação
        - 7.21.1 /etc/freeradius/proxy.conf
    - 7.22 Logs detalhados
        - 7.22.1 /var/log/freeradius/radacct
    - 7.23 Ligação ao MySQL
        - 7.23.1 /etc/freeradius/sql.conf (v2.x)
        - 7.23.2 /etc/freeradius/mods-available/sql (v3.x)
        - 7.23.3 /etc/freeradius/radiusd.conf
        - 7.23.4 /etc/freeradius/modules/sql_log (v2.x)
        - 7.23.5 Lista negra de utilizadores
            - 7.23.5.1 /etc/freeradius/policy.conf (v2.x)
            - 7.23.5.2 /etc/freeradius/policy.d/local_blacklist (v3.x)
    - 7.24 Socket de controlo
        - 7.24.1 /etc/freeradius/sites-enabled/control-socket
    - 7.25 Arranque do serviço
    - 7.26 Paragem do serviço
    - 7.27 Setup do serviço no arranque
    - 7.28 Certificado digital
        - 7.28.1 /usr/share/doc/freeradius/examples/certs/server.cnf
        - 7.28.2 Criação de certificado
            - 7.28.2.1 Certificado do servidor RADIUS
            - 7.28.2.2 Certificados de cliente
        - 7.28.3 Instalação do certificado root no servidor
    - 7.29 Problemas conhecidos
        - 7.29.1 /etc/logrotate.d/freeradius
        - 7.29.2 Problema de reinstalação/erro de statoverride
    - 7.30 Servidor Redundante
    - 7.31 RadSec
- 8 Monitorização
    - 8.1 Estatísticas mensais
        - 8.1.1 /opt/bin/eduroam/stats/e-U-hotspot.cfg
        - 8.1.2 /opt/bin/eduroam/stats.sh
        - 8.1.3 /opt/bin/eduroam/gzip_files.sh
    - 8.2 Recolha centralizada de Estatisticas
    - 8.3 Weathermap da FCCN
    - 8.4 Scripts de monitorização de accounting
    - 8.5 Recuperação de serviços
        - 8.5.1 /etc/default/monit
        - 8.5.2 /etc/monit/monitrc
        - 8.5.3 Teste e recuperação de serviços na camada 7 OSI
            - 8.5.3.1 /opt/bin/eduroam/recover.sh
    - 8.6 SNMP
        - 8.6.1 /opt/bin/eduroam/radstat.sh
        - 8.6.2 /etc/snmp/snmpd.conf
    - 8.7 NAGIOS
    - 8.8 Raptor
- 9 Resolução de problemas
    - 9.1 pcregrep
    - 9.2 ps
    - 9.3 wbinfo
    - 9.4 net
    - 9.5 ntlm_auth
    - 9.6 Kerberos
    - 9.7 testparm
    - 9.8 smbencrypt
    - 9.9 freeradius
    - 9.10 radclient
    - 9.11 radeapclient
    - 9.12 radtest
    - 9.13 EAPTest
    - 9.14 radperf
    - 9.15 raduat
    - 9.16 Radlogin
    - 9.17 LoadUI
    - 9.18 ldapperf
    - 9.19 ldapsearch
    - 9.20 tcpdump
    - 9.21 wireshark
    - 9.22 Wireless Diagnostics

- 9.23 tcpreplay
- 9.24 netstat
- 9.25 ngrep
- 9.26 SNMP
  - 9.26.1 snmpwalk
  - 9.26.2 snmpget
- 9.27 radmin
- 9.28 raddebug
  - 9.28.1 Patch de raddebug
  - 9.28.2 Operações de debugging
- 9.29 radsniff
- 9.30 radtee
- 9.31 eapol_test
  - 9.31.1 ttls-eap-mschapv2.conf
  - 9.31.2 Medição de tempos de pedidos
  - 9.31.3 rad_eap_test
- 9.32 time
- 9.33 Evolynx
- 9.34 JRadius
- 9.35 openssl
- 9.36 Outras ferramentas de medição de performance
  - 9.36.1 blktrace
  - 9.36.2 free
  - 9.36.3 top
  - 9.36.4 htop
  - 9.36.5 iftop
  - 9.36.6 iotop
  - 9.36.7 nicstat
  - 9.36.8 vmstat
- 9.37 Ferramentas de monitorização de sistema/mensagens
  - 9.37.1 strace
  - 9.37.2 sysdig
- 9.38 MySQL
- 9.39 /var/log/syslog
- 9.40 /var/log/freeradius/radius.log
- 9.41 /var/log/freeradius/radacct
  - 9.41.1 auth-detail
  - 9.41.2 detail
  - 9.41.3 reply-detail
  - 9.41.4 pre-proxy-detail
  - 9.41.5 post-proxy-detail

- 10 Instalação de equipamento
  - 10.1 NAS/APs
    - 10.1.1 Cisco WLC
    - 10.1.2 Xirrus
    - 10.1.3 Meru
    - 10.1.4 Cisco Catalyst
  - 10.2 Suporte de protocolos
  - 10.3 CAT
  - 10.4 Configurações manuais
    - 10.4.1 Android
- 11 Conclusão
  - 11.1 Evoluções futuras
- 12 Anexos
  - 12.1 Migração de FreeRadius 2.2.x para 3.x
  - 12.2 Logs em syslog
  - 12.3 A plataforma Apple
    - 12.3.1 iOS
      - 12.3.1.1 Iphone Configuration Utility
      - 12.3.1.2 Apple Configurator 2
      - 12.3.1.3 Activação de modo developer em iOS
    - 12.3.2 OS/X
      - 12.3.2.1 Gestão de perfis/profiles
  - 12.4 Reportar bugs de FreeRadius
  - 12.5 Obter certificados eduPKI
  - 12.6 Administração de sistemas sys V versus Systemd
  - 12.7 Criação de conta github com script ansible
  - 12.8 Script básico de ansible para instalação do software em Debian
  - 12.9 Monitorar FreeRadius com dtrace
  - 12.10 Usando Logstash
  - 12.11 Debugging em Meru
  - 12.12 Links úteis

Introdução

Este tutorial nasceu da necessidade de documentar o processo de implementação do FreeRADIUS no ISCTE-IUL, dado a complexidade do processo, a ausência de documentação de qualidade que suportasse o know-how, as dificuldades sentidas na implementação, as decisões técnicas no decorrer do processo e o servidor FreeRadius ser uma plataforma em movimento. Em adição pretende documentar a experiência acumulada do projecto.

As directrizes para seleccionar uma solução opensource, mais que o custo, foram:

- o know-how obtido no processo;
- as ferramentas disponíveis;
- a capacidade de customização mais alargada;
- a capacidade de fazer debug transversalmente a todos os níveis possíveis da solução - inclusive tendo um acesso mais alargado a logs;
- a possibilidade de desenvolver ferramentas in-house associadas para investigação/resolução de problemas;
- ter recuperação automática de serviços;
- ser uma solução menos exigente em recursos;
- e ultimamente ter uma solução maleável e mais estável que a anterior.

A ideia base é além do projecto ser útil, minimizar o tempo de pesquisa sobre o FreeRadius, quer internamente, quer para outras instituições.

Para já, note-se que o projecto é bastante interessante, quer na interacção com o Linux, quer na interacção com os serviços de AD. Relembre-se também que as disciplinas de engenharia de redes, sistemas, desenvolvimento e segurança estão todas interligadas, e acaba-se por se tocar um pouco de cada esta destas vertentes nestes projectos.

Consequentemente com esta ideia em mente, partilha-se este documento para uso interno da equipa do ISCTE, e da federação PT de EDUROAM.

Rui Ribeiro - 2013-2015

Por este documento ter nascido com inspiração num projecto interno, e o foco ser mais clarificar o FreeRADIUS que propriamente focar-se na sua adaptabilidade à distribuição Linux, não foram realizados esforços para documentar particularidades de outras distribuições que não a Debian. No entanto, cremos que este documento será útil para compreender e implementar EDUROAM em FreeRADIUS ligado a uma AD Windows em qualquer outra distribuição.

Resumo executivo

O documento actual pretende documentar a autenticação de utilizadores da EDUROAM. A implementação foi realizada no sistema operativo Linux /Debian configurando o FreeRADIUS como servidor de autenticação 802.1X (EAP-TTLS-MSCHAPv2 por defeito, e PEAP-MSCHAPv2). A autenticação é em Active Directory, e também se contempla a inserção na (con)federação EDUROAM de acordo com a implementação efectuada no ISCTE-IUL de 2013 a 2015. Este serviço anteriormente era assegurado por um Internet Authentication Service em Windows 2003 com o protocolo PEAP-MSCHAPv2.

Formatação do documento

Foram usadas determinadas convenções ao escrever o documento. É de salientar, para uma melhor compreensão:

- Os blocos de código, sempre que possível estão em devidamente assinalados;
- Os nomes dos ficheiros de configurações foram também colocados no índice para um fácil localização;
- Nos ficheiros de configuração, o que estiver a negrita foi o que foi mudado em relação à configuração por defeito.

A EDUROAM

A EDUROAM é um projecto da TERENA para implementar um serviço de roaming mundial ao nível da educação (**edu**cation **roam**ing service). Os seus objectivos são fornecer acesso a serviços de rede em qualquer ponto da confederação de uma forma segura, consistente e uniforme.

O projecto arrancou em 2002, e foi oficialmente inaugurado em 2008. Desde então, alargou-se a sua adopção, e neste momento, está presente em todos os continentes, em mais de 60 países. À data da escrita deste documento, existem mais de 6000 pólos com EDUROAM, sendo cerca de 160 em Portugal. Tal pode constatar-se pelo seguinte mapa online: http://monitor.eduroam.org/eduroam_map.php?type=all Em Portugal, hotspots de Internet já tinham sido criados pelo projecto e-U, e este foi integrado no projecto EDUROAM por volta de 2007, mudando os SSIDs dos hotspots de e-U para eduroam. No caso do ISCTE, o serviço arrancou em 2009.

TERENA: Trans-European Research and Education Networking Association http://www.terena.org

Objectivos da EDUROAM

Os requerimentos definidos para este serviço são portanto:

- Autenticar utilizadores na periferia da rede
- Permitir o acesso de "convidados"
- Gestão em larga escala, já que a administração e autenticação dos utilizadores é local e subordinada à instituição
- Facilidade de instalação e uso
- SSID eduroam
- Em resumo, usar o seu computador/telemóvel em qualquer ponto da confederação e ter acesso imediato.

Tecnologia usada

O serviço da EDUROAM engloba o uso de várias tecnologias para atingir os seus objectivos.

A segurança é baseada no emprego da tecnologia 802.1X, que assegura a integração com a atribuição de VLANs e a protecção das credenciais.

A autenticação é baseada em EAP, o que permite implementar diferentes mecanismos de autenticação.

O roaming é assegurado pelo protocolo RADIUS, que é o mecanismo de transporte para a informação de autenticação.

A teia de confiança é baseada, tecnicamente numa hierarquia RADIUS, e politicamente, em documentos/contractos que definem a responsabilidade de todos os intervenientes no processo.

Protocolos usados

Ao nível de protocolos, na EDUROAM e na presente configuração são contemplados os seguintes:

Para AAA (Accounting, Authentication, Authorize), o RADIUS (*Remote Access Dial In User Service)*;

Como método de transporte, baseado em EAP (Extensible Authentication Protocol), o PEAP (Protected Authentication Protocol) e o EAP-TTLS (Tunneled Transport Layer Security);

Na autenticação, o MSCHAPv2 (inner authentication protocol); ou seja, usamos o EAP-TTLS-MSCHAPv2 por defeito, suportando também o PEAP-MSCHAPv2.

Para autenticar o servidor, e como base para codificação, o X.509 para certificados digitais.

Do lado das redes wireless usa-se o 802.1Q para atribuição de VLANs que atribuem ao utilizador a rede eduroam de Funcionários, Alunos ou de Estudantes em roaming.

Ao nível do Wifi, o recomendado pela confederação EDUROAM é apenas implementar o serviço em WPA2 Enterprise, e AES, dado a vulnerabilidades no protocolo TKIP.

A vantagem de usar EAP-TTLS ao invés de EAP-TLS é que no EAP-TTLS não é obrigatório ter certificado do lado do cliente. No entanto que se pode configurar perfeitamente EAP-TTLS para ter também certificado do lado do cliente.
a obrigatoriedade de usar MSCHAPv2 deve-se a nos clientes Windows a implementação de EAP suportar este protocolo de autenticação mais seguro por defeito. O MSCHAP também não transmite passwords mas sim hashes de passwords. O PAP só é incorporado nativamente a partir de MS Windows 8, OS/X 10.7, iOS 4, Android v2, Ubuntu 10.10 e não é suportado por Windows Phone e BlackBerry.
as VLANs apenas têm efeito localmente, e ao autenticar um utilizador iscte.pt em roaming noutra instituição os atributos que definem as VLANs não são injectados na transacção, ou no caso de outras instituição os atributos são filtrados, sendo normalmente usada uma VLAN/rede pública da instituição em que o utilizador autenticado se encontra em roaming.
embora ao nível da confederação EDUROAM, seja recomendado usar PEAP ou EAP-TTLS, os protocolos de autenticação são largamente escolha da instituição. Existem várias instituições que usam PAP devido a ser mais simples de suportar com uma infra-estrutura de autenticação (Open)LDAP. Em Windows, TTLS+PAP suporta autenticação por kerberos ao invés de MSCHAP. Para a matriz da lista de protocolos suportados, visitar: http://deployingradius.com/documents/protocols/compatibility.html
A autenticação EDUROAM também pode ser implementada em rede cablada. A AUP menciona que acessos à EDUROAM apenas devem ser implementados em redes 802.1X

EAP

O Extensible Authentication protocol é o suporte de autenticação. O standard WPA2 adoptou o protocolo IEEE 802.1X com EAP como mecanismo oficial de autenticação. O 802.1X define o EAP em rede, conhecido como o protocolo EAPOL, que suporta redes sem fio e com cabo.

O túnel EAP tem o conceito de túnel exterior e interior, em que o túnel exterior é para estabelecer a conexão e reencaminhar para um proxy se necessário, e o interior para processar pedidos de autenticação locais. Os protocolos de autenticação apenas são processados no túnel interior.

Os métodos baseados em TLS involvem criar um túnel entre o cliente/PC e o servidor RADIUS. O processamento do túnel é realizado pelo túnel externo /servidor virtual "default".

Assim que o túnel TLS é estabelecido, a autenticação é enviada dentro do túnel. O servidor trata estes dados como se fossem outro pedido de autenticação, mas processa estes pelo túnel interno/servidor virtual inner-tunnel. Isto permite que as políticas do inner-tunnel sejam diferentes das do default. Alias, as políticas tem de ser diferentes, porque estão dentro do túnel.

Notavelmente, o túnel externo apenas encaminha trafego quando em roaming, ou desfaz o túnel TLS para o túnel interno processar os protocolos de autenticação, no nosso caso, o MSCHAP.

De notar que a negociação de ambos os túneis, não é apenas uma transacção por túnel, mas várias. No nosso caso, são cerca de 6 transacções por túneis. Cada transacção tem funções especificas na negociação, e as directivas de unlang foram razoavelmente ordenadas, também com o auxilio do modo debug, para minimizar a execução de certas tarefas no tempo (i.e. não as executar múltiplas vezes).

Embora ao nível da confederação EDUROAM, seja recomendado usar PEAP ou EAP-TTLS, os protocolos de autenticação (internos) são largamente escolha da instituição. Existem várias instituições que usam PAP devido a ser mais simples de suportar com uma infra-estrutura de autenticação (Open) LDAP.

A obrigatoriedade de usar MSCHAPv2 deve-se a nos clientes Windows a implementação de EAP apenas suportar este protocolo de autenticação, sem software extra. O MSCHAP também não transmite passwords mas sim hashes de passwords.

Depois de autenticado, a porta virtual autenticada pelo utilizador é colocada na VLAN fornecida pelo RADIUS, e fica com capacidades de comunicar.

Hierarquia

A rede EDUROAM tem uma hierarquia definida, a saber:

- TLRSs - Top-level RADIUS Servers
- FLRSs - *Federation-level RADIUS Server*
- servidores IdPs and SP RADIUS - servidores locais RADIUS Identity Providers e Service Providers
- elementos de rede activos (APs e switches)
- supplicant (software do sistema operativo cliente)

Termos de utilização

A participação na federação EDUROAM obriga a vários requerimentos, entre os quais se ressaltam:

- o uso exclusivo para fins académicos;
- o serviço ser disponibilizado gratuitamente;
- cumprir parâmetros mínimos de segurança e qualidade de serviço prestada;
- autenticação federada;
- gerar e guardar logs de autenticação;
- partilhar estatísticas com a federação;
- reforçar o branding da marca "eduroam".

Ao utilizadores em roaming é necessário fornecer:

- endereços IP públicos;
- serviços mínimos de TCP/IP bem definidos como baseline, no mínimo;
- suportar protocolos de autenticação diversos para roaming com o setup original da casa mãe.

Um dos fundamentos da necessidade de IP público para utilizadores de outras instituições é o suporte de software de VPNs remotamente, dado o NAT criar problema no uso de alguns protocolos.

De salientar que o helpdesk de utilizadores em roaming é primariamente realizado pela casa mãe. No entanto, que existem excepções, como por exemplo, utilizadores Eramus a que normalmente são atribuídas contas locais, sendo a sua nova "casa mãe" a instituição que lhes forneceu a conta. (i.e. não basta verificar a origem do estudante, mas também o domínio que este está a usar)

As contas fornecidas a fornecedores ou a contas temporárias de eventos deverão ser criadas num domínio à parte, que embora possam ser usadas localmente no ssid eduroam, não deverão ter a capacidade de fazer roaming na confederação EDUROAM.

Documentos da confederação EDUROAM: https://www.eduroam.org/downloads/docs/eduroam_Compliance_Statement_v1_0.pdf e da federação Portuguesa: http://www.fccn.pt/fotos/editor2/Eduroam/aup-termosecondicoesdeutilizacao.pdf

Política de retenção de dados

Embora a AUP da confederação eduroam mencione uma retenção dos dados de login dos utilizadores durante meio ano (hora, login, MAC de equipamento pelo menos), os fornecedores de serviço em Portugal são obrigados a manter registos durante dois anos, pelo que se aconselha a manter históricos durante dois anos. Os ficheiros de logs detail tem de ser armazenados durante 6 meses.

AUP de utilizadores

Os utilizadores em EDUROAM, também têm obrigações, como não usar a rede eduroam para fins comerciais e actividades duvidosas e/ou ilegais, incluindo a partilha de conteúdos protegidos por direitos de autor em redes p2p e hacking.

http://www.fccn.pt/pt/rede-academica/a-rede-ciencia-tecnologia-e-sociedade-rcts/carta-ao-utilizador-aup/

Os utilizadores podem ser banidos na instituição de origem ou mesmo na instituição visitante, ao nível do serviço EDUROAM, e a configuração do serviço deve suportar esta funcionalidade.

Serviços suportados

O serviço EDUROAM está também mencionado como tendo de suportar um conjunto mínimo de serviços, e não todas as portas TCP/IP. Ver para exemplo: https://www.cites.illinois.edu/wireless/eduroam/ports.html

RADIUS

O RADIUS é um protocolo que centraliza a gestão de serviços de autenticação, autorização e contabilização/accounting (AAA), para os utilizadores que usem um serviço de rede. Foi originalmente criado pela Livingston em 1991, para um cliente/ISP de dial up de grande dimensão, MichNet.

O serviço é usado por uma multitude de equipamentos, sendo um standard IETF que é fortemente implementado ao nível de fornecedores de serviços. É um protocolo cliente/servidor, que funciona em UDP. O 1812/UDP é usado para autenticação e o 1813/UDP é usado para contabilização.

O uso do RADIUS em 1645/UDP e 1646/UDP é obsoleto e o seu uso é desencorajado.

Realm

O Realm é, basicamente, o domínio do utilizador. O Realm local é tratado localmente pelo FreeRADIUS, saindo o seu processamento do outer tunnel para o inner tunnel. No caso do utilizador ter um domínio diferente da instituição, isto é, ser de outro domínio e de um realm diferente, o pedido será reencaminhado pelo(s) proxies nacionais. Também se pode definir o tratamento do realm NULL, para utilizadores sem domínio, mas tal prática é desencorajada já que utilizadores com estas configurações perdem a capacidade de se autenticar em roaming. Existe também um realm local de visitantes, que apenas é conhecido internamente à instituição mãe, e não é capaz de fazer roaming.

Um realm fixo tem sempre precedência a um realm com regexp, excepto se estivermos a falar de um script unlang

Proxy

Os proxies são pontos de contacto para reencaminhar pedidos com domínios/realms diferentes do nosso. Na configuração standard na RCTS, todas as instituições têm configurados os proxies nacionais. Podem também ser feitos acordos directamente entre instituições.

Roaming

Roaming é o processo pelo qual um utilizador é autenticado remotamente em RADIUS, e neste caso dentro da confederação EDUROAM. É realizado um túnel EAP para a instituição mãe, cujo mapeamento é realizado pelo realm/dominio do utilizador, e todo o processo de autenticação é realizado com base no utilizador presente no inner-tunnel. A informação de accounting também é enviada para roaming.

Tipo de mensagens RADIUS

Existem vários tipos de pacotes que podem ser recebidos num servidor RADIUS. Tipicamente as transacções de autorização são recebidas na porta 1812 /UDP e as de Accounting na porta 1813/UDP.

Tipo mensagem	Função
Access-Request	Enviada por um cliente RADIUS para solicitar autenticação e autorização
Access-Accept	Enviada pelo servidor RADIUS como resposta a um Access-Request. Informa o cliente RADIUS que a conexão foi autenticada e autorizada.
Access-Reject	Enviada em resposta a uma mensagem Access-Request. Esta mensagem informa o cliente que a conexão foi rejeitada. Um servidor RADIUS envia esta mensagem se o login ou password não estiverem correctas, se existirem problemas de configuração de cliente, ou se o cliente não estiver autorizado a usar o serviço.
Access-Challenge	Enviada pelo servidor RADIUS como resposta a um Access-Request. Esta mensagem é um desafio para o cliente RADIUS que exige uma resposta.
Accounting-Request	Enviada por um cliente RADIUS para enviar informações de contabilização da transmissão para uma conexão que foi autorizada.
Accounting-Response	Enviada pelo servidor como resposta a uma mensagem Accounting-Request. Confirma a recepção e o processamento do Accounting-Request.

se não se recebeu um access-accept com o par cipher keying não se pode fazer join ao SSID que tem o wpa2/aes cipher on it. Da mesma forma, se é um método de challenge response não se pode simplesmente aceitar. Outra dúvida frequente, é que depois de um Access-Reject, o papel do RADIUS estar terminado. Se houver colocação numa VLAN guest, isso será uma funcionalidade suportada e configurada no hardware.

Atributos

Os Atributos RADIUS são repositórios que guardam a informação trocada entre os clientes e os servidores RADIUS.Uma mensagem RADIUS pode ter vários atributos. O nome do atributo é transmitido no pacote como um número, e a correspondência com nome é feita por ficheiros chamados dicionários. Existem atributos "oficiais", extensões próprias de fabricantes, e extensões definidas pelo utilizador. No caso do Debian, o ficheiro principal é /etc /freeradius/dictionary, que contém no final os atributos privados/definidos pelo utilizador. O ficheiro /usr/share/freeradius/dictionary faz include de todos os outros "dicionários".

Para visualizar listas de atributos, consultar no site oficial do FreeRADIUS: http://freeradius.org/rfc/attributes.html

Tipicamente os atributos são necessários quer para fazer modificações ao código unlang, quer para fazer debugging da informação de accounting. Nomeadamente, usamos (pelo menos) os atributos do quadro seguinte nesta implementação. O equipamento em uso pode implementar mais atributos além dos listados.

Nome Atributo	Função	Exemplo
Access-Point-Name	Nome de AP real / atrás de controladora	"AP-1W3"
Access-Point-Id	Porta virtual de acesso.	19
Acct-Authentic		RADIUS
Acct-Delay-Time		0
Acct-Input-Gigawords		
Acct-Output-Gigawords		
Acct-Input-Octets	Número de bytes recebidos pelo utilizador.	65536
Acct-Output-Octets	Número de bytes transmitidos pelo utilizador.	128342
Acct-Input-Packets	Número de tramas recebidas pelo utilizador.	400
Acct-Output-Packets	Número de tramas transmitidas pelo utilizador.	200
Acct-Session-Time	Tempo de transmissão/online do utilizador (segundos)	123
Acct-Status-Type	Tipo de mensagem de Accounting, veja a descrição no capitulo correspondente.	Start
Acct-Session-Id	Identificador de sessão.	"526A7B1A-0000B9AF"
Acct-Unique-Session-Id	Identificador único de sessão.	"c7d7e685498a12c3"
Called-Station-Id	MAC do AP Virtual/Controladora	"00:50:56:80:36:73"
Calling-Station-Id	MAC do cliente	"50:46:5D:15:E7:6B"

Chargeable-User-Identity	Identificação única do utilizador. Usado por no outer tunnel ser possível colocar um utilizador privado. De momento, não usado na RCTS.	
Connect-Info	Tipo de conexão. Alguns fabricantes não preenchem devidamente este campo nomeadamente a Meru. Em Cisco dá para ter uma ideia da qualidade de ligação dos clientes.	"CONNECT 54Mbps/48Mbps 802.11g"
EAP-EMSK	`Extended Master Session Key`	0x05dd51368e0c1bc719c5b458cd5be508210bc4babab c972fd8aee257c0c654475bb3f6baa444ae676b535fd 914234fbe3ce9b48492308373bb8d877e68a05d92
EAP-MSK	Master Session Key	0x6cbfc95d2366dac1eb185115da4c55472647d5ae4cc f57fa49efb24a5bcad31777454ba737bdb96fe931bff7cc e77e433e5c20e47e9edb5a968bcb68fdf6eaef
EAP-Message		0x020100140161313632323040697363746 52e7074
Framed-Compression	Normalmente None em EDUROAM.	None
Framed-MTU	Tamanho máximo de Trama permitido.	1250
FreeRADIUS-Acct-Session-Start-Time	Tempo de começo de sessão corrente.	"Oct 29 2013 00:00:10 WET"
Message-Authenticator	Medida anti-spoofing de pacotes.	0xd5b4448372412026449920a88b2f5c12
MS-MPPE-Recv-Key	Negociação de hash de password no protocolo mschap. Derivada de parâmetros da sessão TLS	0x6cbfc95d2366dac1eb185115da4c55472647d5ae4cc f57fa49efb24a5bcad317
MS-MPPE-Send-Key	Negociação de hash de password no protocolo mschap. Derivada de parâmetros da sessão TLS	0x77454ba737bdb96fe931bff7cce77e433e5c20e47e9e db5a968bcb68fdf6eaef
NAS-Identifier	Mac da Controladora ou AP.	"00-50-56-80-36-73"
NAS-IP-Address	Endereço IP da Controladora ou AP.	10.61.10.11
NAS-Port	Porta virtual de conexão. Infelizmente alguns fabricantes têm bugs, em que dão sempre o mesmo número a esta porta, nomeadamente a Cisco.	2051
NAS-Port-Type	Tipo de conexão virtual.	Wireless-802.11
Operator-Name	Atributo definido pelo utilizador. É usado para acrescentar o operador em tramas enviadas em proxy, para facilitar o debbuging de transacções que envolvam várias instituições.	"1iscte.pt"
Packet-Type	Tipo de pacote RADIUS.	Access-Request
Proxy-State	Estado do ponto de negociação de mensagens em roaming.	0x3337
Realm	Domínio de utilizador criado em unlang para processamento de informação.	"iscte.pt"
Reply-Message	Resposta enviada por directivas para apresentação de mensagens ao utilizador. Infelizmente ignorada por muitas implementações.	"Eduroam Alunos"
Service-Type		Framed-User
Stripped-User-Name	Criado por directivas unlang para facilitar processamento.	"rui"
Timestamp	Tempo UNIX do evento.	1383004810
Tunnel-Type:0	Tipo de conexão virtual, normalmente VLAN.	VLAN
Tunnel-Medium-Type:0	Protocolo de conecção a ser usado.	IEEE-802

Tunnel-Private-Group-Id:0	Sinaliza ao AP a VLAN pretendida para a conexão virtual.	"200"
User-Name	Nome de utilizador enviado pelo AP. Atenção que o operador de unlang suffix trunca o dominio, sendo esta uma das razões porque evitamos o uso do suffix. No outer-tunnel, pode não corresponder ao endereço real do utilizador.	"rui@iscte.pt"

Como mencionado mais à frente, o unlang é a linguagem de scripting interna ao FreeRadius.

Mensagens de Accounting

O accounting no RADIUS é enviado na porta 1813/UDP para o servidor RADIUS. Envia várias informações, entre as quais mensagens de Start e Stop Accounting. A informação de accounting permite contabilizar os consumos e tempo de utilização por utilizador autenticado. Saliente-se também que se as APs são desligadas cortando a energia, provavelmente a mensagem de Accounting-Off nunca ou raramente é vista.

Tipo de mensagem	Função
Stop	Fim de sessão de accounting.
Start	Inicio de sessão de accounting.
Update	Mensagem intermediária de accounting.
Alive	Mensagens de keep-alive para manter a tabela de sessão activa no AP/Controlador.
Accounting-On	Recebido quando um AP é ligado. Envia o nome do AP.
Accounting-Off	Recebido quando um AP é desligado. Envia o nome do AP.

http://www.juniper.net/techpubs/en_US/uac/topics/reference/general/uac-authentication-servers-radius-accounting.html

http://www.stat.ufl.edu/system/man/portmaster/RADIUS/guide/7account.html

http://tools.ietf.org/html/rfc2866

Limites em accounting de 4GB - http://www.netexpertise.eu/en/freeradius/gigawords-support.html
O formato de vários campos de accounting variam de vendor para vendor, incluíndo alguns que seria de esperar que fossem mais constantes, como por exemplo, o MAC do cliente.
O FreeRadius está dependente de receber mensagens de Accounting on de APs a arrancarem para limpar a BD de clientes que já não estão activos. Ele faz isto em On, porque muitas vezes os APs ao serem desligados manualmente, não têm oportunidade de enviar o Accounting-Off.

Descrição da solução

A infra-estrutura de autenticação FreeRadius assenta em vários pressupostos, e como tal vamos apresentar diagramas nesta secção para suportar de forma visual a teoria e procedimentos apresentados neste documento.

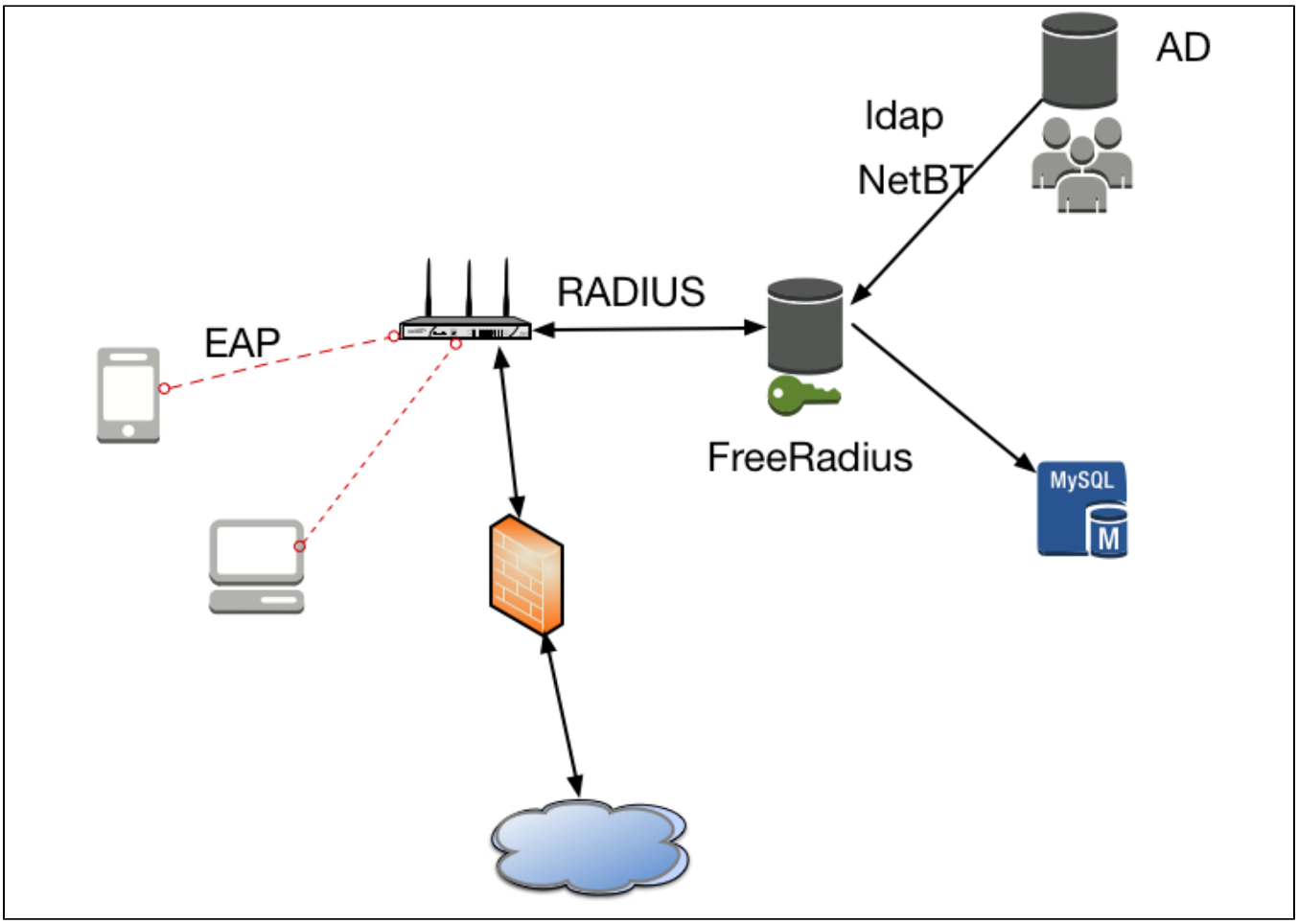
Esquema de rede

O esquema de rede (simplificado) da solução é o apresentado em seguida. Os clientes falam por EAP(ol) com os APs. O AP, através do protocolo RADIUS, reencaminha os pedidos de autenticação para o servidor FreeRadius.

O servidor FreeRadius, trata o pedido de autenticação da seguinte forma:

- utilizador local : autenticado em AD
- utilizador remoto: reencaminhamento da transacção para os servidores da federação local (PT no nosso caso).

Depois do processo de autenticação efectuado, são escritos logs em disco (detail) e em MySQL. Além da autenticação são também recebidos e colocados em logs dados de accounting.



O serviço de Active Directory pode estar em Windows ou ser implementado em SAMBA.

Esquema lógico da solução

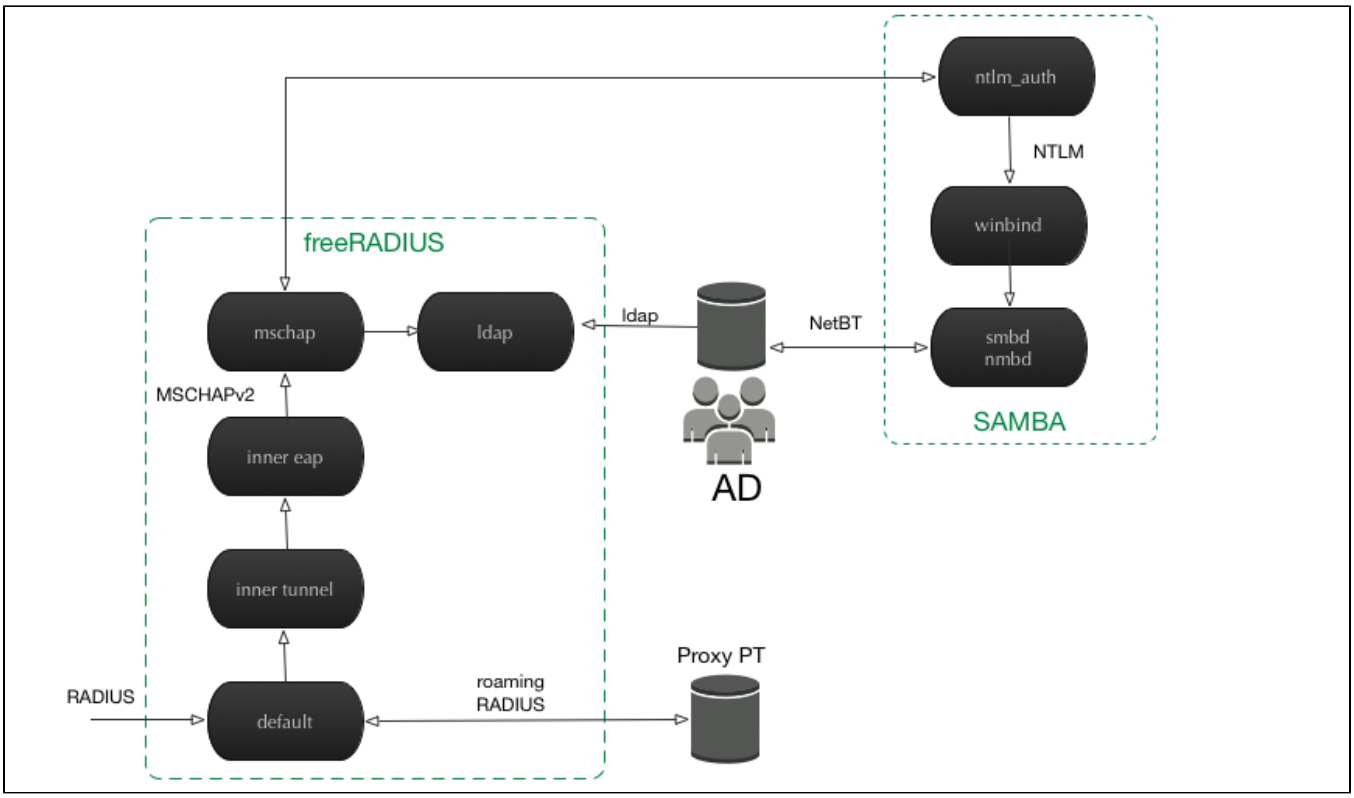
Em comparação com o esquema de rede, a interligação dos diversos componentes do sistema, FreeRADIUS e respectivos módulos que descreveremos mais à frente neste documento, é a exposta no seguinte diagrama. Neste fluxo de informação, se o utilizador for de um domínio externo, o modulo default /outer tunnel, reencaminha os dados para os servidores da federação PT.

Para um utilizador local o circuito é:

1. O AP envia um pacote RADIUS ao FreeRadius
2. o default/outer tunnel valida a conexão, desfaz o túnel externo EAP
3. O inner tunnel faz decoding do inner tunnel e passa para o inner eap
4. O inner eap autentica o utilizador, invocando o mschap (no nosso caso)
5. O modulo mschap/o FreeRadius chama o ntml_auth com o pacote MSCHAP challenge/response
6. O ntml_auth passa-o para o winbind por um pipe unix
7. o winbind comunica com o smbd/nmbd por um SMB2 pipe Unix em NTLMv2
8. o SAMBA comunica com o controlador de dominio por RPC

Para um utilizador remoto:

1. O AP envia um pacote RADIUS ao FreeRadius
2. O default/outer tunnel valida a conexão, e reencaminha-a para o proxy PT.



Pré-requisitos

Hardware

O FreeRADIUS não é exigente em termos computacionais.

Em RAM, o processo freeradius usa aproximadamente 11MB. Para um cenário de 15000 utilizadores, 3000 diários, o sistema operativo+FreeRadius, (sem MySQL) no nosso servidor Debian 7/64 bits, ocupa cerca de 60MB, sendo frequente com os buffers ir para 100-150MB, já com servidor web, pelo que um servidor de 512MB é mais que suficiente. A correr os perl do awesant e da recolha de estatísticas mensal, recomenda-se 1GB. Com MySQL, será mais aconselhado 1GB/1.5GB, ou com o awesant+o e-U-Stats, 2GGB/2.5GB.

Os responsáveis pelo FreeRadius aconselham um servidor com 4 CPUs e 8GB.

Em termos de processamento, verificamos na nosso servidor virtual que a média de processamento ao longo do dia são 14MHz (sem MySQL - load average típica: 0.00, 0.03, 0.05).

Em disco necessário, uma instalação mínima de Debian necessita cerca de 2GB, e instalações com mais software podem ir até aos 6GB (no entanto, não se recomenda instalar interface gráficas em servidores desta natureza). Dependendo do tamanho da instituição, recomenda-se ter mais cautela com a partição /var/log, já que o /var/log/radacct, já que facilmente se poderá ter nos logs detalhados do RADIUS, especialmente guardando-os durante dois ou três meses, entre 3GB a 10GB; em adicão as estatisticas da FCCN também podem atingir cerca de 3GB/ano. Ou seja, um valor médio para um disco para este servidor poderá ser de uns 3-5GB para testes, mas terá de ser 10GB a 20GB para um servidor de produção sem MySQL, ou considerando uma média de crescimento de 5GB da DB MySQL por ano, 20GB a 50GB para um servidor com logging num MySQL local.

Software

Neste documento vamos portanto, descrever a instalação, usando os seguintes componentes de software que testamos ao longo do tempo:

- Debian 7 e 8
- FreeRadius 2.2.4/5/6/ e 3.0.3 até 3.0.9
- SAMBA 3.6 e 4.1
- MySQL 5.5

O SAMBA e o MySQL são os pacotes por defeito do Debian, sendo que ter-se-á de compilar o freeradius por ser demasiado antigo, e o eapol_test para proceder a testes.

Instalação de software

Para instalar o software, depois de ter um servidor a funcionar, em Debian, é recomendado seguir os seguintes procedimentos:

apt-get install aptitude

aptitude install ntp (se se pretender gestão do tempo local)

aptitude install krb5-user

aptitude install freeradius freeradius-utils freeradius-mysql freeradius-ldap (se se optar por instalar o FreeRADIUS por defeito da distribuição. Não aconselhado em Debian)

aptitude install samba winbind samba-common-bin openssl

aptitude install make (caso se pretenda mudar o certificado instalado por defeito)

aptitude install mysql-server (caso se pretenda que o servidor MySQL de logging seja instalado no mesmo servidor do FreeeRADIUS)

aptitude install libperl4-corelibs-perl (para os scripts das estatísticas mensais)

aptitude install lighttpd (web server para as estatisticas e scripts)

aptitude install phpmyadmin (edição gráfica de BD - opcional)

aptitude install radsecproxy (caso se pretenda configurar radsec em Freeradius 2 - não necessário em FreeRadius 3)

aptitude install libnl-dev libssl-dev apt-src (kit de desenvolvimento para compilar eapol_test pré-Debian 8)

aptitude install libnl-3-200 libssl-dev apt-src (kit de desenvolvimento para compilar eapol_test pós-Debian 8)

aptitude install monit (recuperação de serviço)

aptitude install ldap-utils (para debugging de problemas de LDAP/AD)

aptitude install chkconfig (gestão de arranque de serviços)

aptitude install nagios-nrpe-server (para monitorização NAGIOS)

aptitude install libssl-dev quilt libtool libltdl3-dev libpam0g-dev libmysqlclient-dev libgdbm-dev libldap2-dev libsasl2-dev libiodbc2-dev libkrb5-dev libperl-dev libpcap-dev python-dev libsnmp-dev libpq-dev debhelper wget curl (para compilar e criar um pacote deb de FreeRADIUS)

aptitude install mysql-client-5.5 (para testar ligação mysql)

aptitude install liblog-handler-perl libjson-perl libparams-validate-perl libio-string-perl libsys-hostname-log-perl libclass-accessor-perl (para estatisticas em real time com o awesant - o libsys-hostname-log-perl só em Debian 7)

aptitude install snmpd (agente SNMP para recolha de dados estatísticos)

aptitude install snmp (aplicações clientes)

aptitude install makepasswd (para o script de criação de utilizadores guest temporários)

Em Debian 8, é necessário também fazer o seguinte comando em Debian 8 para ser capaz de compilar o eapol_test

```
ln -s /lib/x86_64-linux-gnu/libnl-3.so.200 /lib/x86_64-linux-gnu/libnl.so
```

Regras de firewall

Para o serviço funcionar, é necessário realizar as seguintes autorização ao nível da firewall.

origem	destino	serviço	função
<rede APs/WLC>	radius.iscte.pt radius2.iscte.pt	1812/UDP	autorização
<rede APs/WLC>	radius.iscte.pt radius2.iscte.pt	1813/UDP	contabilização

193.136.192.43 193.136.192.44 193.137.196.43	radius.iscte.pt radius2.iscte.pt	1812/UDP	autorização
radius.iscte.pt radius2.iscte.pt	TBD	2083/TCP	RadSec
TBD	radius.iscte.pt radius2.iscte.pt	2083/TCP	RadSec
193.136.192.44	radius.iscte.pt radius2.iscte.pt	443/TCP	Recolha estatísticas mensais
<redes gestão>	radius.iscte.pt	80/TCP	acesso a scripts
radius.iscte.pt	mysql	3306/TCP	(MySQL externo ao servidor)
radius.iscte.pt radius2.iscte.pt	AD	389/TCP,389/UDP	LDAP
radius.iscte.pt radius2.iscte.pt	AD	445/TCP, 137-139/UDP	NETBIOS
radius.iscte.pt radius2.iscte.pt	AD	88/UDP, 88/TCP	KDC
radius.iscte.pt radius2.iscte.pt	AD	749/UDP, 749/TCP	KERBEROS
radius.iscte.pt	193.137.197.22	6379/TCP	Recolha estatísticas em real-time f-ticks/accounting(awesant)

193.137.196.43 = weathermap RCTS
a Microsoft usa o LDAP em UDP para fazer o join e leave de uma AD/DC. Os protocolos 173-139/UDP, 389/UDP, 749/TCP, 749/UDP e 88/UDP e 88/TCP apenas são necessários na altura da adição do servidor de (free)RADIUS à AD.

Redes/VLANS necessárias

Embora a EDUROAM seja visível para o utilizador comum, esta é separada em várias redes de acordo com o realm e com o grupo associado ao login na active directory.

função	VLAN	netblock	netmask	router	endereços IP disponíveis	Realm	grupo AD
alunos	200	172.1.1.0	255.255.240.0	172.1.1.1	4094	iscte.pt	Alunos
não-estudantes	201	172.1.16.0	255.255.252.0	172.1.16.1	1022	iscte.pt	Funcionarios
guest	202	172.1.20.0	255.255.255.0	172.1.20.1	253	guest.iscte	--
alunos de outras instituições	203	183.136.189.0	255.255.255.0	193.136.189.1	253	--	--

Autenticação de utilizador local

É necessário ter o layer de SAMBA antes do FreeRADIUS, já que as parametrizações de segurança da AD não permitem ler passwords. A autenticação tem de ser realizada por NETBIOS/TCP, sendo separadamente, depois **consultados** os grupos de um utilizador já autenticado por LDAP para determinar que VLAN será configurada.

Para a autenticação de utilizadores na AD, é necessário verificar a autenticação dos utilizadores através do hash das passwords, usando o protocolo MSCHAPv2. Portanto, para tal, é necessário configurar o SAMBA, que fará a ligação por NETBIOS à AD.

Em seguida descrevemos como configurar os serviços de suporte NETBIOS em Linux.

DNS

Recomenda-se que os DNS direitos (A) e reversos (PTR) estejam devidamente configurados do servidor RADIUS, por uma questão de boas práticas e para o kerberos/SAMBA funcionar melhor. Recomenda-se registar também no DNS os direitos e reversos de todos os APs/controladores usados.

Se estiver no DNS da AD e a Windows/AD for autoritária para o domínio de utilizador, os registos de DNS já estão lá por defeito. Para quem esteja a usar outra solução, ter-se-ão de colocar registos extra.

Fica a seguir o exemplo, no caso do BIND. Nesta configuração definimos no domínio DNS iscte.pt o master da AD, os serviços de kerberos e os serviços de ldap.

A literatura da Microsoft diz que o servidor DNS a usar para um cliente de AD, tem de ser a própria AD (no nosso caso, é BIND)

```
dc01                                    IN A 10.10.1.1
@                                       IN A 10.10.1.1
ForestDnsZones                                IN A 10.10.1.1
DomainDnsZones                          IN A 10.10.1.1
_kerberos-master._udp                   IN SRV 0 100 88  dc01
_kerberos-master._tcp                   IN SRV 0 100 88  dc01
_kerberos._udp                          IN SRV 0 0   88  dc01
_kerberos._tcp                          IN SRV 0 0   88  dc01
_kerberos._tcp.dc._msdcs                IN SRV 0 100 88  dc01
_kerberos-adm._tcp                      IN SRV 0 0   749 dc01
_ldap._tcp.dc._msdcs                    IN SRV 0 100 389 dc01
_ldap._tcp                              IN SRV 0 100 389 dc01
_kerberos._tcp.ISCTE._sites             IN SRV 0 100 88  dc01
_ldap._tcp.ISCTE._sites                 IN SRV 0 100 389 dc01
_ldap._tcp.ISCTE._sites.DomainDnsZones  IN SRV 0 100 389 dc01
_ldap._tcp.DomainDnsZones               IN SRV 0 100 389 dc01
_ldap._tcp.ISCTE._sites.ForestDnsZones  IN SRV 0 100 389 dc01
_ldap._tcp.ForestDnsZones               IN SRV 0 100 389 dc01
_ldap._tcp.Default-First-Site-Name._sites.dc._msdcs IN SRV 0 100 389 dc01.
```

Para os equipamentos que suportarem uma rede captiva/de quarentena em caso de falha de autenticação, definimos também a seguinte zona no DNS. Esta zona responde a todos os pedidos que lhe forem feitos, transformando-os num IP. A ideia é reencaminhar toda e qualquer página aberta para um site interno. Apenas definimos para o exterior a saída para página do CAT. Existe também a possibilidade dos profiles do CAT serem copiados para esse site, e assim não ter que definir saídas externas para esta rede.

```
$TTL    604800
@       IN      SOA     . root.localhost. (
                              1
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL


        IN      NS      .


.       IN      A       192.168.1.5
*.      IN      A       192.168.1.5

cat.eduroam.org. IN      A       161.53.2.204
```

NAPTR

```
@               IN      NAPTR   100 10 "s" "x-eduroam:radius.tls" "" _radsec._tcp.eduroam.pt.
```

NAPRT http://slideplayer.com/slide/2506870/ a key one is that the traffic DOES NOT go the same way... if a visitor from the UK is in, for example, Germany... if the home site doesnt have NAPTR, the request goes
German SP, German NTLR, European root proxies, UK NTLR, UK IDP
if the home site DOES use NAPTR, request goes
German SP, German NTLR , UK NTLR, UK IDP

so we now bypass a whole tier of proxy....and thus *2* UDP/RADIUS hops. we are also then using RADIUS over TCP between Germany and UK so able to detect issues, retransmit etc.

DHCP

Há que definir as redes DHCPs a ser usadas nas VLANs onde opera a EDUROAM. Para isso define-se os netblocks na configuração do isc-dhcp. O FreeRadius também tem suporte para DHCP, mas além de no inicio do projecto nós não confiarmos nele (hoje em dia é mais estavel), também gerimos as redes de DHCP centralmente para toda a instituição em dois servidores DHCP configurados em failover.

/etc/dhcp/dhcpd.conf

```
# rdw-alunos (VLAN 200), for ISCTE students connecting via wireless:
subnet 172.1.1.0 netmask 255.255.240.0 {
  option routers 172.1.1.1
  option domain-name-servers dns1.iscte.pt, dns2.iscte.pt;
  option domain-name "iscte.pt"
  pool {
    default-lease-time  600000;
    min-lease-time  300000;
    max-lease-time  600000;
    failover peer "iscte";
    range 172.1.1.2 172.1.15.254;
  }
}
# rdw-iscte (VLAN 201), for ISCTE non-students connecting via wireless:
subnet 172.1.16.0 netmask 255.255.252.0 {
  option routers 172.1.16.1;
 option domain-name-servers dns1.iscte.pt, dns2.iscte.pt;

  pool {
    failover peer "iscte";
    range 172.1.16.2 172.1.19.254;
    default-lease-time  600000;
    min-lease-time  300000;
    max-lease-time  600000;
  }
}
# rdw-iscte (VLAN 202), for guests connecting via wireless:
subnet 172.1.20.0 netmask 255.255.255.0 {
  option routers 172.1.20.1;
 option domain-name-servers dns1.iscte.pt, dns2.iscte.pt;

  pool {
    failover peer "iscte";
    range 172.1.20.2 172.1.20.254;
    default-lease-time  600000;
    min-lease-time  300000;
    max-lease-time  600000;
  }
}
# e-U (VLAN 203), para utilizadores eduroam em roaming
subnet 193.136.189.0 netmask 255.255.255.0 {
  option routers 193.136.189.1;
  option domain-name-servers dns1.iscte.pt, dns2.iscte.pt;

  pool {
    failover peer "iscte";
    range 193.136.189.2 193.136.189.254;
    default-lease-time 7200;
    min-lease-time 3600;
    max-lease-time 7200;
  }
}
```

Tempo

É essencial que o servidor esteja sincronizado por NTP ou pelas vmtools da vmware. Notavelmente o kerberos necessita do tempo certo para operar bem. (tendo uma margem de erro de 300 seg). Pode-se instalar o pacote ntp ou então , numa máquina virtual em vmware, colocar no ficheiro rc.local em debian a directiva de vmtools para sincronizar o tempo. É também boa prática ter o tempo/serviços NTP e timezones devidamente configuradas para cruzamento de logs com os vários sistemas.

No nosso caso, activamos explicitamente a sincronização de tempo da máquina virtual com o host vmware.

/etc/rc.local

/etc/rc.local

```
/usr/bin/vmware-toolbox-cmd timesync enable
```

Caso se pretenda acertar o tempo sem ser pelo vmware, em alternativa:

```
#aptitude install ntp
```

Não se recomenda acertar o tempo em servidores desta natureza com utilitários no cron, como por exemplo, o ntpdate ou o sntp.

Kerberos

O kerberos é usado essencialmente para negociar com a AD a entrada do servidor RADIUS (e saída) do dominio da AD. Depois de o configurar, recomenda-se testar com um kinit <utilizador da AD>

/etc/krb5.conf

/etc/krb5.conf

```
[libdefaults]
default_realm = ISCTE.LOCAL
ticket_lifetime = 36000
renew_lifetime = 604800
clockskew = 300
dns_lookup_realm = false
dns_lookup_kdc = false
dns_fallback = false

[realms]
ISCTE.LOCAL = {
kdc = 10.10.1.1:88
default_domain = iscte.local
admin_server = 10.10.1.1:749
}
[domain_realm]
.iscte.local = ISCTE.LOCAL
iscte.local = ISCTE.LOCAL
```

o ficheiro krb5.conf não pode ter qualquer tipo de comentários, ou não funciona
é essencial ter o kerberos a funcionar para inserir o servidor/SAMBA no domínio
a conta usada para inserir o servidor no domínio tem de ter privilégios para realizar essa operação.

SAMBA

O SAMBA implementa a pilha NETBIOS para podermos falar MSCHAPv2 com a AD, ou seja para realizarmos a autenticação.

Como optimização na configuração SAMBA, desactiva-se o sistema de impressão para não ser necessário correr o daemon CUPs, e faz-se bind à interface de loopback, já que os serviços do SAMBA local são apenas para ser consumidos pelo ntlmauth/FreeRADIUS.

/etc/samba/smb.conf

/etc/samba/smb.conf

```
workgroup = ISCTE
interfaces = lo
bind interfaces only = yes
security = ads
encrypt passwords = true
passdb backend = tdbsam
realm = ISCTE.LOCAL
unix password sync = no
load printers = no
printing = bsd
printcap name = /dev/null
disable spoolss = yes
domain master = no
local master = no
preferred master = no
winbind enum groups = yes
winbind enum users = yes
winbind use default domain = yes
winbind max domain connections = 30
```

winbind max domain connections tem de ser ajustada de acordo com a dimensão da infra-estrutura.

Para falar NETBIOS com a AD, é necessário acrescentar o servidor de RADIUS ao dominio. Para tal, corre-se o seguinte comando (como root):

```
$kinit user
$sudo net rpc join -U administrator -S dc01 -I 10.10.1.1
em seguida:
$sudo net ads join -U administror -S dc01 -I 10.10.1.1
Enter administrator's password:
Using short domain name -- ISCTE
Joined 'RADIUS' to dns domain 'ISCTE.LOCAL'
DNS update failed: NT_STATUS_INVALID_PARAMETER
```

ignore o erro de DNS update failed.

Em configurações de SAMBA 4 poderá ser necessário fazer

```
samba-tool user setexpiry administrator --noexpiry
```

depois de adicionar ao domínio, é necessário fazer restart ao winbind e testar:

```
# /etc/init.d/winbind restart
[ ok ] Stopping the Winbind daemon: winbind.
[ ok ] Starting the Winbind daemon: winbind.
r# /usr/bin/ntlm_auth --request-nt-key --username=rffro --domain=ISCTE
password:
NT_STATUS_OK: Success (0x0)
#
# se der erro
/usr/bin/ntlm_auth --request-nt-key --username=rffro
Password:
NT_STATUS_CANT_ACCESS_DOMAIN_INFO: NT_STATUS_CANT_ACCESS_DOMAIN_INFO (0xc00000da)
# o mais certo é o winbind estar em baixo, e o servidor ainda não estar inserido no domínio
```

podem existir "bugs" em versões de SAMBA, pelo que aconselhamos neste passo adicionar o servidor de RADIUS manualmente na AD, no caso das instruções anteriores terem falhado.

O serviço/processo winbind não sobe/arranca se o servidor não fizer ainda parte do dominio windows.
para optimizar o ficheiro smb.conf pode-se correr cd /etc/samba ; cp smb.conf /tmp/a.conf ; testparm -s a.conf > smb.conf

winbind

O Winbind implementa uma camada de ligação entre o SAMBA e o linux (pam/outros). Fornece também o mecanismo de tradução entre SIDs e utilizadores Unix, embora esta parte não seja usada pelo FreeRADIUS. O método de comunicação são sockets/pipes Unix, e no Debian 7, está em /var /run/samba/winbindd_privileged/pipe.

Para aceder ao pipe do winbind, já que o FreeRadius corre com o seu utilizador próprio é necessário correr os comandos:

```
usermod -G winbindd_priv freerad
sudo chgrp  winbindd_priv /var/lib/samba/winbindd_privileged/
sudo winbind restart
sudo service freeradius restart # (caso o freeradius já esteja configurado)
```

Depois de uma reinstalação de uma versão nova de samba é necessário repetir este passo.
Caso o winbind ou o ntlm_auth dê erros, verifique de novo as permissões de acesso ao ficheiro /var/run/samba/winbindd_privileged/pipe. No caso de LinuxSE é necessário também correr o seguinte comando: setfacl -m u:radiusd:rx /var/run/samba/winbindd_privileged.

ntlm_auth

O ntlm_auth fala directamente com o winbind, e o FreeRADIUS usa este utilitário para ir buscar os dados de autenticação de utilizadores na configuração descrita neste documento. O binário encontra-se em /usr/bin/ntlm_auth e pode ser invocado directamente para fazer troubleshooting da parte de autenticação. Consulte o capitulo de Resolução de Problemas para ver a sintaxe do comando.

FreeRADIUS

O FreeRADIUS é um software opensource, que é um fork do Cistron, que por sua vez tomou como modelo a implementação original da Livingston. Data de 1999, e está disponível em todas as plataformas Unix. É da firma Network RADIUS, que disponibiliza a versão opensource e a versão comercial. Para Windows, não existe implementação, chegou a aparecer uma adaptação, mas não era autorizada.

O FreeRADIUS tem um desenho modular e a sua configuração assenta num conjunto de ficheiros que deverão ser parametrizados para adaptar o servidor ao cenário da Instituição. Os ficheiros são colocados na directoria de configuração do servidor (/etc/freeradius em Debian) e parametrizados genericamente. Estes ficheiros são separados sem secções de acordo com as diferentes funcionalidades/ponto do processo de autenticação RADIUS, e estão escritos numa linguagem interna chamada unlang misturada com invocação de módulos. O directório dos módulos está em /etc/freeradius/modules. Sempre que possível, evitamos mexer demasiado no unlang, e realizar as parametrizações pelos ficheiros de configuração.

Os ficheiros principais e abordados nesta secção do documento são os seguintes:

- radius.conf - ficheiro de parametrização global do servidor
- proxy.conf - ficheiro de configuração para proxy de pedidos (correntemente não usado)
- clients.conf - ficheiro de configuração de clientes (ex: AP's; proxy nacional)
- users - ficheiro de tratamento de utilizadores
- dictionary - ficheiro que referencia dicionários de atributos RADIUS

Os directórios a salientar são:

- /etc/freeradius - raiz das configurações de freeradius
- /etc/freeradius/modules - configuração/criação de módulos invocados em unlang
- /etc/freeradius/sites-enabled - configurações de "sites", nomeadamente o inner-tunnel, default e control-socket
- /etc/freeradius/certs - configurações de certificados digitais

E a acrescentar em FR 3

- /etc/freeradius/mods-available
- /etc/freeradius/mods-enabled - configuração base de módulos

Em distribuições não-Debian, o daemon é chamado radiusd ao invés de freeradius a raiz das configurações é /etc/raddb em substituição de /etc /freeradius. O directório de logging é também /var/log/radius em vez de /var/log/freeradius

Serviço de ponto de vista da rede

Em relação ao serviço fornecido pelo FreeRADIUS, este escuta nas portas:

1812/UDP - RADIUS authentication

1813/UDP - RADIUS accounting

2083/TCP - RadSec

1814/UDP - proxy port

18120/UDP - inner Tunnel do FreeRADIUS (as portas anteriores dão ligação ao outer Tunnel) - apenas disponível no localhost

As portas 1812/UDP, 1813/UDP e 1814/UDP poderão ser associadas ao IP público, e isto será mesmo necessário caso o FreeRADIUS forneça mais serviços além dos descritos neste documento. A 18120 está associada ao interface loopback, sendo apenas acedida localmente ao servidor.

unlang

O unlang é a (pseudo)linguagem própria dos ficheiros de configuração do freeradius. A linguagem é relativamente básica e a ideia é escrever políticas simples rapidamente e facilitar a construção de add-ons para outras linguagens.

A linguagem é bastante simples, sendo uma espécie de linguagem de scripting para os ficheiros de configuração.

Usa () para directivas de condições, e {} para separa blocos de código.

Suporta também variáveis, que podem ser atribuídas com o operador =. As variáveis usam-se no formato ${var}. (foo = "hello" bar = ${foo}# hello)

Pode-se aceder a atributos, usando o seu nome no dicionário no formato %{}. Existe também uma notação mais recente, &var

Tem também um caso especial de atribuição, v=a:-b, em que b é atribuído se a não existir.

Possuí a capacidade de invocar código sql directamente com a directiva %{sql: }.

Suporta operadores de comparação C-like, como o ==, !=, > e <.

Na comparação também se podem usar expressões regulares, usado o =~.

As strings são delimitadas por " ".

Os comentários são precedidos de #.

Tem directivas especiais que são dependentes do contexto, para "massajar" a mensagem RADIUS, sendo estes: update control , update reply , update request e Auth-Type.

Suporta construções especiais como o if else e o switch case. Um if ou switch é obrigatoriamente seguido de um bloco {}.

Um /i colocado no fim de uma regexp é para ignorar se são maiúsculas ou minúsculas;

Colocar um nome só por si em unlang é equivalente a invocar uma rotina/modulo.

A directiva $INCLUDE <ficheiro> também é usada.

Existem instruções condicionais, como var = %{ %{a}:-%{b}} onde var = a e se a for vazio, var = b.

Também existem nas últimas versões mais capacidades de tratamento de variáveis, e variáveis internas.

Consultar: http://wiki.freeradius.org/config/Run-time-variables (falta a esta lista a %v - versão de FreeRadius, introduzida na v2.2.5)

Ver a página para a sintaxe: http://freeradius.org/radiusd/man/unlang.html

Para uma introdução a expressões regulares, consultar: http://net.tutsplus.com/tutorials/other/8-regular-expressions-you-should-know/ e http://www.zytrax.com/tech/web/regex.htm

A partir da versão 3, o FreeRadius também carrega módulos condicionamente. Colocando - antes da invocação de um modulo, este apenas é usado se estiver configurado.

A partir da versão 3, o unlang também suporta casting de variáveis, nomeadamente entre outras <date>, <ipaddr>, <cidr>. A partir da versão 2.2 do FreeRadius foram também implementadas várias variáveis internas, como o por exemplo o %l. A partir da v2.2.5 foi implementando o %v.

Como escolher a versão de FreeRadius

Tipicamente a melhor escolha é compilar as últimas versões do tar.gz ou do repositório git do site oficial (freeradius.org), pelo menos em Debian ou sistemas derivados. As versões das distribuições normalmente estão desactualizadas, e embora a situação esteja a melhorar, por na versão 6 da Debian por exemplo, a versão do FreeRadius já estava com cerca de 2 anos de atraso.

A versão 1 neste momento está completamente obsoleta. A versão 2, apenas atingiu características mais desenvolvidas e algumas variáveis necessárias neste tutorial por volta da 2.2.2. A versão 2.1.12 que vem por defeito com o Debian 7, é completamente desaconselhada. Neste momento a versão 2, embora seja a mais estável e conhecida, já não evolui mais. Para quem quer usar a versão 2, neste momento dado a substancias melhoras em várias e protocolos, o mínimo recomendado é a 2.2.6.

A versão 3 é a que obtêm funcionalidades novas ao longo do tempo.

Em comparação à versão 2, tem as seguintes melhoras:

- maiores capacidades de debugging;
- novas funcionalidades e melhorias em várias frentes no unlang;
- suporta RadSec nativamente;
- As configurações são também tokenizadas no arranque, e erros são logo apontados;
- várias optimizações de código para aumentar a performance em run time;
- mais paralelismo em queries LDAP/AD;
- A parte de LDAP também é mais flexível;
- O protocolo PAP é melhor suportado (não o usamos);
- A estrutura de directórios foi mudada para ser mais lógica, tipo estrutura de servidores virtuais e módulos à semelhança do Apache;
- mais estatísticas de uso;
- e por último, as mensagens de debug são mais completas e coloridas;
- na 3.0.7, limpeza de código, erros mais descritivos na parte de tratamento de queries SQL;
- a 3.0.8 possibilita a autenticação directa no SAMBA sem usar o binário ntml_auth e dá erros mais claros em autenticação winbind;
- a 3.0.9 introduz limpezas do código, correcções no RadSec e plug-ins novos para memcache e redis.

Recomenda-se que quem está a começar a investir tempo nesta tecnologia que use desde logo a versão 3. De momento, a versão em produção estável é a 3.0.9, em git no branch 3.0x, é a 3.0.9.

No entanto, não recomendamos a v3.0.6 por ter um bug de roaming de accounting que detectamos, e bugs em passwords com caracteres não-ASCII como "%", nem a v3.07 com vários bugs pelo menos em Debian. O 3.0.8 tem também bugs conhecidos com RadSec, pelo que recomendados o git 3.0.9.

Quanto a outras versões de FreeRadius, além das que vêm com distribuições, existem outros repositórios:

Ubuntu

For Trusty Tahr (14.04), add to your apt source list (/etc/apt/sources.list):

```
deb http://packages.networkradius.com/ubuntu trusty main
```

Debian

For Debian 7.0 "Wheezy", add to your apt source list (/etc/apt/sources.list):

```
deb http://packages.networkradius.com/debian wheezy main
```

For Debian 8.0 "Jessie", add to your apt source list (/etc/apt/sources.list):

```
deb http://packages.networkradius.com/debian jessie main
```

CentOS

The RPMs are available in the centos/ directory

Signed Builds

The builds are signed with our PGP key. To add it to the apt keyring, run the following commands:

```
sudo apt-key adv --keyserver keys.gnupg.net --recv-key 0x41382202
sudo apt-get update
```

Instalação de versão de freeradius.org

Dada a evolução da versão do FreeRADIUS, e o bug periódico do mschap e do raddebug, é de considerar criar um pacote de instalação para Debian (deb), e fazer a instalação. A partir da versão 2.2.x faz um parsing mais completo no arranque, incluído a expressões que na 2.1.12 só seriam parsed em runtime, tem optimizações de desempenho, e mais bugs corrigidos. Aliás, em várias distribuições Linux normalmente o atraso das versões em produção em relação à versão de freeradius estável chega a ser dois anos - ou mais - pelo que normalmente o upgrade é aconselhado. Note-se que, pacotes oficiais recentes, que tenhamos conhecimento, de momento, só a fedora e o repositório PPA da Ubuntu é que os disponibilizam.

Ubuntu: https://launchpad.net/~freeradius

Fedora: https://apps.fedoraproject.org/packages/freeradius

De momento, a versão 2.2.4/5 é bastante estável, pelo que a vamos usar como exemplo. Aliás, não se aconselha de todo usar versões anteriores à 2.2.4, já que possuem bugs que as tornam instáveis. No passo de instalação, caso esteja a fazer um upgrade, seleccionar ENTER sempre nas perguntas, para manter os ficheiros de configuração já modificados.

Da primeira vez, instalar os pacotes necessários:

```
sudo aptitude install libssl-dev quilt libtool libltdl3-dev libpam0g-dev libmysqlclient-dev libgdbm-dev
libldap2-dev libsasl2-dev libiodbc2-dev libkrb5-dev libperl-dev libpcap-dev python-dev libsnmp-dev libpq-dev
debhelper wget git fakeroot openssl ssl-cert ?libwbclient-dev
```

Caso se opte pelo tar corrente da versão estável:

```
wget ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-2.2.6.tar.gz
tar -zxvf freeradius-server-2.2.6.tar.gz
cd freeradius-server-2.2.6
```

Ou então para a versão 3:

```
wget ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-3.0.7.tar.gz
tar -zxvf freeradius-server-3.0.7.tar.gz
cd freeradius-server-3.0.7
```

ou em alternativa ao wget, pelo sistema de gestão de versão git, ou se define a versão, ou faz checkout da última versão:

```
git clone https://github.com/FreeRADIUS/freeradius-server.git
cd freeradius-server
git fetch origin v2.x.x:v2.x.x
git checkout v2.x.x
```

Ou então para a versão 3:

```
git clone https://github.com/FreeRADIUS/freeradius-server.git
cd freeradius-server
git fetch origin v3.0.x:v3.0.x
git checkout v3.0.x
```

O público geral deixou de ter acesso a git://git.freeradius.org/freeradius-server.git . Só para developers registados.

Por último para compilar e instalar:

```
fakeroot dpkg-buildpackage -b -uc # compila e cria os debs
cd .. # no directório anterior
# para 32 bits (ls para ver ficheiros ou uname -m para ver arquitectura) - instala os pacotes
# de notar que está dpkg tem opções para não reescrever ficheiros alterados
sudo dpkg --force-confold --force-confdef -i freeradius_2.2.*+git_i386.deb freeradius-common_2.2.*git_all.deb
freeradius-ldap_2.2.*git_i386.deb freeradius-mysql_2.2.*git_i386.deb freeradius-utils_2.2.*git_i386.deb
libfreeradius2_2.2.*git_i386.deb
# para 64 bits
sudo dpkg --force-confold --force-confdef -i freeradius_2.2.*git_amd64.deb freeradius-common_2.2.*git_all.deb
freeradius-ldap_2.2.*git_amd64.deb freeradius-mysql_2.2.*git_amd64.deb freeradius-utils_2.2.*git_amd64.deb
libfreeradius2_2.2.*git_amd64.deb

# 64 bits v3.x
sudo dpkg --force-confold --force-confdef -i freeradius-config_3.0.7+git_amd64.deb freeradius-common_3.0.7
+git_all.deb freeradius_3.0.7+git_amd64.deb freeradius-ldap_3.0.7+git_amd64.deb freeradius-mysql_3.0.7
+git_amd64.deb freeradius-utils_3.0.7+git_amd64.deb libfreeradius3_3.0.7+git_amd64.deb

# para versão 3 em repositório local do ISCTE
sudo apt-get install freeradius-config freeradius  freeradius-common freeradius-ldap freeradius-utils
libfreeradius3 freeradius-mysql
```

A necessidade de criação de um pacote Debian e a instalação deste ao invés de compilar directamente, tem a ver com a compatibilização com a gestão de versões Debian, evitar complicações posteriores, e não baralhar a administração de pacotes do sistema. De outra forma, as próximas actualizações esmagariam as mudanças, ou teria de se fazer frozen ao pacote de freeradius, e arruinar a integridade do sistema de gestão de pacotes. Em adição, o dpkg também faz a gestão dos upgrades, o que permite de uma forma relativamente simples e rápida fazer upgrades para versões mais recentes, preservando as configurações correntes automaticamente. Os pacotes podem ser colocados num repositório ou passados para outro servidor, no entanto, por limitações de bibliotecas e especialmente da versão de openssl, os servidores têm de ser do mesmo SO e da mesma versão. Além das questões de dependências de bibliotecas, o código do FreeRadius verifica a versão de openssl e recusa-se a funcionar com versões de openssl diferentes. Isto tem a ver com verificações de sanidade, por as bibliotecas de SSL mudarem estruturas internas de versão para versão.
Passos para criar Debs Freeradius 3

```
aptitude install libssl-dev quilt libtool libltdl3-dev libpam0g-dev libmysqlclient-dev libgdbm-dev libldap2-dev
libsasl2-dev libiodbc2-dev libkrb5-dev libperl-dev libpcap-dev python-dev libsnmp-dev libpq-dev debhelper wget
git fakeroot openssl ssl-cert libcap-dev libpcap-dev
```

apt-get install build-essential:native libcurl4-openssl-dev libjson0-dev libreadline-dev libsqlite3-dev libtalloc-dev libyubikey-dev

fakeroot dpkg-buildpackage -b -uc

dpkg -i freeradius_3.0.3+git_amd64.deb freeradius-common_3.0.3+git_all.deb freeradius-config_3.0.3+git_amd64.deb freeradius-utils_3.0.3+git_amd64.deb libfreeradius3_3.0.3+git_amd64.deb
Se ao reinstalarem debs, forem apresentados erros de statoverride, o workaround é apagar todas as linhas que tenham freerad

```
$sudo sed -i '/freerad/d' /var/lib/dpkg/statoverride
```

Pode-se mudar configurações base do deb em debian/rules antes de compilar. Uma delas pode ser colocar o FreeRadius em developer mode para fazer debugging de problemas no código, a outra colocar o parâmetro --disable-openssl-version-check.

Configuração de FreeRadius

Embora este documento siga uma estrutura de configurar de uma vez tudo na configuração do FreeRadius, aconselha-se, tendo como base uma versão a trabalhar, e modificar opção a opção e testar. Saliente-se, aconselhamos fazer uma mudança, configuração ou optimização apenas de cada vez, testar, corrigir e apenas aí seguir para o próximo passo. Desta forma é mais fácil perceber o que terá corrido bem ou mal. Se tiver corrido bem, aconselha-se a documentar.

Ligação ao LDAP da AD

A autenticação dos utilizadores é realizada pelo SAMBA, pelo que neste caso, a configuração base do módulo de LDAP do FreeRADIUS foi mudada para só fazer o query dos grupos a que pertence o utilizador. Estas queries são efectuadas quando são processadas as queries presentes no ficheiro /etc /freeradius/users, para determinar em que VLAN vai um utilizador trabalhar.

/etc/freeradius/modules/ldap (v2.x)

/etc/freeradius/modules/ldap

```
#
ldap {
server = 10.10.1.1
identity = "CN=Radius,CN=Users,DC=ISCTE,DC=LOCAL"
basedn = "CN=Users,DC=ISCTE,DC=LOCAL"
password=pass_do_user_Radius_na_AD
filter = "(sAMAccountName=%{Stripped-User-Name})"
ldap_connections_number = 20
timeout = 10
timelimit = 10
net_timeout = 10
tls {
start_tls = no
}
dictionary_mapping = ${confdir}/ldap.attrmap
edir_account_policy_check = no
groupname_attribute = sAMAccountName
groupmembership_filter = "(sAMAccountName=%{Stripped-User-Name})"
groupmembership_attribute = memberOf
rebind = yes
set_auth_type = no
keepalive {
idle = 60
probes = 3
interval = 3
}
}
```

/etc/freeradius/modules/ldap (v3.x)

etc/freeradius/mods-enabled/ldap

```
ldap {

 server = 10.20.10.78

 identity = "CN=Radius,CN=Users,DC=wiscte,DC=wfarm"

 password = pass_do_user_Radius_na_AD

 base_dn = "DC=wiscte,DC=wfarm"


 user {

 base_dn = "CN=Users,DC=wiscte,DC=wfarm"

  filter = "(sAMAccountName=%{Stripped-User-Name})"

 }

 group {

 base_dn = "CN=Users,DC=wiscte,DC=wfarm"

 membership_filter = "(sAMAccountName=%{Stripped-User-Name})"

 membership_attribute = "memberOf"

 }



 client {
```

```
base_dn = "${..base_dn}"
filter = '(objectClass=frClient)'
attribute {
identifier = 'radiusClientIdentifier'
secret = 'radiusClientSecret'
}
}
}
}

options {
chase_referrals = yes
rebind = yes
timeout = 10
timelimit = 3
net_timeout = 1
idle = 60
probes = 3
interval = 3
ldap_debug = 0x0028
}
 pool {
start = 5
min = 1
max = ${thread[pool].max_servers}
spare = 3
uses = 0
lifetime = 0
idle_timeout = 60
}
}
```

O groupmembership_filter poderá ter de ser mudado de acordo com os critérios da organização. Por exemplo, se o utilizador de AD for definido por email pelo nome@domínio completo ter-se-á de usar o atributo User-Name no lugar de Stripped-User-Name. Aconselha-se a consulta dos seguintes URLs https://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx, http://linax.wordpress.com/2012/07/17/freeradius-check-nested-ldap-group-membership/ e http://msdn.microsoft.com/en-us/library/aa746475(v=vs.85).aspx.
Veja o KB da Microsoft, sobre os novos limites sobre queries LDAP a partir do Server 2008 http://msdn.microsoft.com/en-us/library/cc223376.aspx , http://technet.microsoft.com/en-us/library/bb124171(v=exchg.65).aspx e https://social.technet.microsoft.com/wiki/contents/articles/14559.active-directory-ldap-policy.aspx

v2.x

/etc/freeradius/ldap.attrmap

Este ficheiro faz o mapeamento entre os atributos de RADIUS e os atributos de LDAP. Em 2.x aconselha-se editar e deixar apenas os dois seguintes atributos.

/etc/freeradius/ldap.attrmap

```
checkItem $GENERIC$ radiusCheckItem
replyItem $GENERIC$ radiusReplyItem
```

No caso do ficheiro attrmap, na v2.x, e uma vez que não usamos LDAP para gestão do FreeRADIUS, mas apenas para ligação, é necessário no ficheiro deixar apenas estas duas linhas, e apagar todas as outras de checkItem para o FreeRadius não tentar escrever todos esses atributos de volta no servidor LDAP/AD. Em 3.x não existe esta necessidade.

Configuração do protocolo mschap

É necessário configurar o módulo mschap para falar o protocolo necessário com o SAMBA/Windows AD, e também corrigir a PATH do binário ntlm_auth. Atente-se à configuração necessária de métodos mais fortes de encriptação, que se tornaram obrigatórios em versões mais recentes de Windows.

/etc/freeradius/modules/mschap (v2.x)

/etc/freeradius/mods-enabled/mschap (v3.x)

/etc/freeradius/modules/mschap

mschap {

use_mppe = yes

require_encryption = yes

require_strong = yes

with_ntdomain_hack = no

ntlm_auth = "**/usr/bin/ntlm_auth** --request-nt-key --username=%{%{Stripped-User-Name}:-%{%{User-Name}:-None}} --challenge=%{%{mschap:Challenge}:-00} --nt-response=%{%{mschap:NT-Response}:-00}"

# retry_msg = "Re-enter (or reset) the password"
}

Versões novas irão falar directamente com o SAMBA, e esta configuração poderá ficar obsoleta a curto prazo. De momento, a parte mais complicada de configurar manualmente o setup novo é que o SAMBA tem de ser compilado. http://wiki.freeradius.org/guide/Active-Directory-direct-via-winbind

F-Ticks

O F-ticks (Federate Ticker System for eduroam) é um sistema de verificação dupla de logging que coloca os logs de logins no syslog. Além de possibilitar a capacidade de cruzar dados para verificar a integridade do sistema, permite também ter um feedback visual dos logins para um administrador de sistemas no syslog.

Para tal, além das directivas f_ticks que estão presentes nas configurações deste documento, cria-se o módulo, criando um ficheiro com o conteúdo a seguir.

Escrevemos também o Accounting-Request em unlang para facilitar o envio de estatísticas de acordo com os requerimentos da federação PT.

/etc/freeradius/modules/f_ticks (v2.x)

/etc/freeradius/mods-enabled/f_ticks (v3.x)

/etc/freeradius/modules/f_ticks

```
linelog f_ticks {
       filename = ${logdir}/awesant/Stats-Awesant-Auth.log
       format = ""
       reference = "f_ticks.%{%{reply:Packet-Type}:-format}"
       f_ticks {
          #Access-Accept = "F-TICKS/eduroam/1.0#REALM=%{Realm}#VISCOUNTRY=PT#VISINST=ISCTE#CSI=%{Calling-
Station-Id}#RESULT=OK#"
          #Access-Reject = "F-TICKS/eduroam/1.0#REALM=%{Realm}#VISCOUNTRY=PT#VISINST=ISCTE#CSI=%{Calling-
Station-Id}#RESULT=FAIL#"
          Access-Accept = "AUTH-ID=%I#TIME=%l#REALM=%{Realm}#CSI=%{Calling-Station-Id}/%{Called-Station-Id}
#USER=%{md5:%{User-Name}}#NASIP=%{NAS-IP-Address}#RESULT=OK"
          Access-Reject = "AUTH-ID=%I#TIME=%l#REALM=%{Realm}#CSI=%{Calling-Station-Id}/%{Called-Station-Id}
#USER=%{md5:%{User-Name}}#NASIP=%{NAS-IP-Address}#RESULT=FAIL"
       }
}

linelog Accounting-Request {
    filename = ${logdir}/awesant/Stats-Awesant-Acct.log

    format = ""
    reference = "Accounting-Request.%{%{Acct-Status-Type}:-unknown}"
    Accounting-Request {
    Stop = "ACCT-ID=%{Acct-Session-Id}#TIME=%l#TYPE=Stop#CSI=%{Calling-Station-Id}/%{Called-Station-Id}#NASIP=%
{NAS-IP-Address}#USER=%{md5:%{User-Name}}#REALM=%{Realm}#DURACAO=%{Acct-Session-Time}#REDE_OCT=%{Acct-Input-
Octets}/%{Acct-Output-Octets}#REDE_PAC=%{Acct-Input-Packets}/%{Acct-Output-Packets}#REDE_GIGA=%{Acct-Input-
Gigawords}/%{Acct-Output-Gigawords}"
    Start = "ACCT-ID=%{Acct-Session-Id}#TIME=%l#TYPE=Start#CSI=%{Calling-Station-Id}/%{Called-Station-Id}
#NASIP=%{NAS-IP-Address}#USER=%{md5:%{User-Name}}#REALM=%{Realm}"
    #  Don't log anything for these packets.
    Alive = ""
    Accounting-On = ""
    Accounting-Off = ""
        Interim-Update = ""
    #Accounting-On = "NAS %C (%{NAS-IP-Address}) just came online"
    #Accounting-Off = "NAS %C (%{NAS-IP-Address}) just went offline"
    # don't log anything for other Acct-Status-Types.
    unknown = ""
    }
}
```

O f-ticks (também) permite enviar logs de autenticação EDUROAM em tempo real para servidores remotos. A federação PT/RCTS usa estas configurações.

Modulos do FreeRadius (3.x)

O FreeRadius 3.x tem uma estrutura de activação e desactivação dos módulos em que se tenta seguir uma configuração semi-standard à semelhança do software Apache.

Apagamos os links de /etc/freeradius/mods-enabled para desactivar os modulos/serviços que não usamos na configuração descrita, e activamos o módulo de ldap por este não estar activado na configuração por defeito.

```
cd /etc/freeradius/mods-enabled
rm -f chap dhcp digest echo exec expiration dynamic_clients logintime passwd radutmp replicate soh sradutmp
unix pap
ln -s /etc/freeradius/mods-available/ldap /etc/freeradius/mods-enabled/ldap
ln -s /etc/freeradius/mods-available/sql /etc/freeradius/mods-enabled/sql
```

Evidentemente, a desactivação de modulos depende da sua arquitectura. Se usar PAP não apaga o modulo pap, por exemplo. Um modulo que não é imediatamente visível que não pode ser desactivado é o always, que fornece a directiva ok e reject. É comum colocar costumizações em mods-enabled e deixar as configurações originais em mods-available. Isto dá problemas nos scripts de upgrade. O directório mods-enabled deve apenas conter links simbólicos para mods-available. O modulo preprocess fornece o atributo Event-Timestamp.

Status

Para recolher estatísticas localmente, há que activar o serviço de Status. Para activar o serviço virtual, fazer os seguintes passos.

```
cd /etc/freeradius/sites-enabled

ln ../sites-available/status .
```

Depois de activar, o serviço fica disponível na porta 18121. No entanto, por razões de segurança só pode ser invocado a partir do próprio servidor.

Site virtual (domínio local) - Túnel externo

Este ficheiro, que trata do túnel externo das conexões, reencaminha utilizadores eduroam para o proxy nacional, ou utilizadores locais para o inner-tunnel. As ligações à porta RADIUS dos equipamentos e da federação são processadas nesta secção. Esta secção basicamente invoca módulos para lidar com os diferentes protocolos envolvidos. Além de verificação da sintaxe do nome do utilizador, logging, autenticação, EAP, e tratamento das mensagens do accounting pouco mais é feito nesta secção.

Neste ponto de processamento, que é o equivalente ao outer-tunnel do EAP, apenas temos acesso à identidade anónima do utilizador. A identidade do utilizador real, a verificação do certificado e os protocolos de autenticação apenas se verificam no inner tunnel, quer local, no caso de utilizadores da instituição, ou quer no inner-tunnel de servidor de RADIUS remoto no caso de utilizadores em roaming.

A ordem das directivas é importante, e notavelmente o eap ok=return antes das queries MySQL, de forma a não desdobrar uma autenticação em múltiplas queries repetidas à BD.

O nome do dominio local também poderá ser algo mais descritivo, como eduroam, ao invés de default.

Note-se que para maior controle, o reencaminhamento para realms é feito com unlang. Alguns domínios conhecidos que costuma estar pre-configurados em mobile são bloqueados para não fazerem entropia ao nível da EDUROAM; os realms internos e de convidados são passados para o túnel interno, e todos os restantes domínios são reencaminhados para o nó de EDUROAM da federação nacional.

/etc/freeradius/sites-enabled/default

/etc/freeradius/sites-enabled/default

```
server default {
listen {
        type = auth
        ipaddr = *
        port = 0

        limit {
             max_connections = 16
             lifetime = 0
             idle_timeout = 30
        }
}

#
#  This second "listen" section is for listening on the accounting
#  port, too.
#
```

```
listen {
        ipaddr = *
        port = 0
        type = acct

        limit {
#               lifetime = 0
#               max_connections = 0
        }
}

authorize {
# weathermap
          if ( User-name == "radius-teste@iscte.pt" ) {
            update reply {
              Reply-Message = "RADIUS OK"
            }
            reject
          }
          else {
    #rewrite_calling_station_id
    #rewrite_called_station_id
    auth_log
    if(!(User-Name =~ /^([^@]*)@(.+)$/)) {
            update reply {
              Reply-Message := "malformed username"
            }
            reject
          }
          else {
# necessário para utilizadores em roaming - tem de estar antes do tratamento do EAP
            update request {
              Stripped-User-Name := "%{1}"
              Realm := "%{2}"
            }
            if ( (Realm == "iscte.pt") || (Realm == "guest.iscte")) {
              update control {
                 Proxy-To-Realm := LOCAL
              }
            }
```

```
            else {


# myabc.com is commonly used by default by Intel supplicant software
 if (User-Name =~ /@myabc\\.com$/i){
        update reply {
                Reply-Message := "Your realm is invalid (it is myabc.com)"
        }
 reject
 } elsif (User-Name =~ /@wlan\\.[[:alnum:]]+\\.[[:alnum:]]+\\.3gppnetwork\\.org$/i){
 # 3gppnetwork.org, another common default realm
        update reply {
                Reply-Message := "Your realm is invalid (it matches a wlan. subrealm of 3gppnetwork.org)"
        }
 reject
 }
# utilizadores em roaming
                update control {
                   Proxy-To-Realm := TO_EDUROAM
                }
             }
          }
 }
# retorna na negociação do túnel EAP (i.e. se o túnel já estiver estabelecido)
       eap {
              ok = return
       }
# filtro de MACs/users
 local_blacklist
 #expiration
 #logintime
 Autz-Type Status-Server {
 }
}


## Autenticações só no inner-tunnel, pelo que aqui limitamo-nos a ter a directiva eap
authenticate {
        #Auth-Type MS-CHAP {
        #        mschap
        #}
 eap
```

```
}

preacct {
 update request {
    FreeRADIUS-Acct-Session-Start-Time = "%{expr: %l - %{%{Acct-Session-Time}:-0} - %{%{Acct-Delay-Time}:-0}}"
 }
 if (!Event-TimeStamp) {
 update request {
 Event-Timestamp := "%l"
 }
 }
 #rewrite_calling_station_id
        #rewrite_called_station_id
 acct_unique
 suffix
}

#
# Accounting. Log the accounting data.
#
accounting {
 #
 # Accounting. Log the accounting data.
 #
 # # Log traffic to an SQL database.
 detail
 redundant {
   sql
   ok
 }
 ## escreve linha de log accounting para o awesant (ver fticks)
 Accounting-Request
 if (noop) {
 ok
 }
 # Filter attributes from the accounting response.
 attr_filter.accounting_response
}

# Session database, used for checking Simultaneous-Use. Either the radutmp
```

```
# or rlm_sql module can handle this.
# The rlm_sql module is *much* faster
session {
        redundant {
    sql
    ok
        }
}

# Post-Authentication
# Once we KNOW that the user has been authenticated, there are
# additional steps we can take.
post-auth {
 reply_log
 f_ticks

        if ( User-Name != "radius_user@iscte.pt" ) {
     redundant {
        sql
        ok
    }
        }
 Post-Auth-Type REJECT {
    # log failed authentications in SQL, too.
    f_ticks
    redundant {
       sql
       ok
    }
    attr_filter.access_reject
 }
       if( ("%{Realm}" != "iscte.pt") && ("%{Realm}" != "guest.iscte") ) {
     update reply {
                User-Name  := "%{request:User-Name}"
                Service-Type := "Framed-User"
                Framed-MTU := 1300
                Tunnel-Type := VLAN
                Tunnel-Medium-Type := IEEE-802
          Tunnel-Private-Group-Id := "203"
Reply-Message := "Eduroam roaming"
```

```
        }
       }
}



#
# When the server decides to proxy a request to a home server,
# the proxied request is first passed through the pre-proxy
# stage. This stage can re-write the request, or decide to
# cancel the proxy.
pre-proxy {
 files
 if("%{Packet-Type}" != "Accounting-Request") {
    attr_filter.pre-proxy
 }
 pre_proxy_log
}

#
# When the server receives a reply to a request it proxied
# to a home server, the request may be massaged here, in the
# post-proxy stage.
#
post-proxy {
 post_proxy_log
 attr_filter.post-proxy
       if (!(proxy-reply:Operator-Name)) {
          update proxy-reply {
             Operator-Name := "1iscte.pt"
          }
       }
 eap
 files.authorize
 Post-Proxy-Type Fail {
 detail
 }
}
}
```

De salientar que é importante desactivar directivas que alimentem ficheiros como o radutmp, já que há medida que estes ficheiros crescem, a performance do servidor sofre significativamente.

Se não quiser responder aquando de falha do sql, uma alternativa é:

```
sql {
        fail = 1
}
if (fail) {
        do_not_respond
}
```

Inner-Tunnel - Túnel interno

O inner-tunnel além de desfazer o túnel interno do protocolo EAP, vai autenticar localmente os utilizadores. No caso do ficheiro a seguir, eles são autenticados no módulo eap, e o modulo ldap que modificamos anteriormente preenche as variáveis necessárias para o ficheiro users poder ter as directivas para solicitar à AD os grupos, e assim atribuir VLANs diferenciadas. Enquanto no outer-tunnel não é necessário suportar protocolos de autenticação, no inner-tunnel, embora estes estando presentes, apenas se implementam os protocolos suportados na instituição.

Neste ponto de processamento da mensagem temos acesso à entidade real do User-Name dos utilizadores (locais).

Este ficheiro aceita várias configurações:

- PEAP-MSCHAPv2
- TTLS-EAP-MSCHAPv2

O domínio de convidados (guest.iscte) é definido em unlang, e os utilizadores são consultados no ficheiro mods-config/files/authorize. Ver a secção sobre este ficheiro para ver como os utilizadores são criados.

As configurações com MSCHAPv2 consultam uma AD em Windows para autenticar e verificar os grupos de utilizadores de foram a coloca-los na VLAN de funcionários ou na VLAN de alunos.

Tentamos também usar um servidor SAMBA para ser autenticados com utilizadores SAMBA. Nessa situação o MSCHAPv2 não é suportado. O SAMBA também tem a desvantagem de os utilizadores terem de ser mapeados para utilizadores Unix, pelo que preferimos optar pelo ficheiro authorize.
O accounting é realizado sempre no túnel externo.

/etc/freeradius/sites-enabled/inner-tunnel

/etc/freeradius/sites-enabled/inner-tunnel

```
# # bind da port de escuta do inner tunnel a loopback:18120

listen {
ipaddr = 127.0.0.1
port = 18120
type = auth
}


# Authorization. First preprocess (hints and huntgroups files),
# then realms, and finally look in the "users" file.
#
authorize {

## obriga a ser login@iscte.pt no inner tunnel

if (!(User-Name =~ /^([^@]*)@(.+)$/)) {

reject

}

else {

# este update é mais controlavel do que a directiva suffix

update request {

                Stripped-User-Name := "%{1}"

                Realm := "%{2}"

   }
```

```
   if (( Realm != "iscte.pt" ) && (Realm != "guest.iscte" ) ) {

           reject

   }

 }

 if ( Realm == "guest.iscte" ) {

  update control {

     MS-CHAP-Use-NTLM-Auth := No # não usa o ntml_auth, ligação à AD

     }

 }

# comentamos chap, porque não usamos.
#chap

mschap

#suffix

#

# This module takes care of EAP-MSCHAPv2 authentication.
#
eap {
ok = return

}

ldap # v2.x, em v3.x não incluir esta linha

#
# Read the 'users' file

## não forçamos protocolos
#files

# expiration

# logintime

if ( Realm == "guest.iscte" ) {

         files # lê tabelas de utilizadores

       }

#pap

}


# Authentication.
# This section lists which modules are available for authentication.

# The common reasons to set the Auth-Type attribute by hand
# is to either forcibly reject the user, or forcibly accept him.
#

authenticate {

## comentamos chap, porque não usamos

#Auth-Type CHAP {
#chap
#}

#
# MSCHAP authentication.
Auth-Type MS-CHAP {
mschap
}
```

```
#authenticate {
#Auth-Type PAP {
#pap
#}
#unix

eap
}



# Session database, used for checking Simultaneous-Use. Either the radutmp
# or rlm_sql module can handle this.
# The rlm_sql module is *much* faster
session {
#radutmp

#
# See "Simultaneous Use Checking Queries" in sql.conf
sql
}


# Post-Authentication
post-auth {

# reply_log

## não faz log de utilizador de teste de serviço que usamos nos nossos scripts

#if ( User-Name != "radius_teste@iscte.pt" ) {
#sql
#}

# passagem de User-Name para o outer tunnel para alguns NAS conhecerem o utilizador.

# Sem esta entrada, enquanto os APs da Cisco mostram o user correcto, nos APs da Meru aparece apenas o user sem domínio

  update reply {

            User-Name  := "%{request:User-Name}"

    }



#
# Access-Reject packets are sent through the REJECT sub-section of the
# post-auth section.
Post-Auth-Type REJECT {
sql
attr_filter.access_reject
}

  if ( Realm == "guest.iscte" ) {

                    update reply {

                          User-Name  := "%{request:User-Name}"

                          Service-Type := "Framed-User"

                          Framed-MTU := 1300

                          Tunnel-Type := VLAN

                          Tunnel-Medium-Type := IEEE-802

                          Tunnel-Private-Group-Id := "202"

                          Reply-Message := "Eduroam guest"

                    }

      }

      elsif ( Ldap-Group == "Alunos" ) {

            if (!(Operator-Name)) {
```

```
            update reply {
                User-Name  := "%{request:User-Name}"
                Service-Type := "Framed-User"
                Framed-MTU := 1300
                Tunnel-Type := VLAN
                Tunnel-Medium-Type := IEEE-802
                Tunnel-Private-Group-Id := "200"
                Reply-Message := "Eduroam Alunos"
            }
        }
    }
    elsif ( Ldap-Group == "Funcionarios" ) {
        if (!(Operator-Name)) {
            update reply {
                User-Name  := "%{request:User-Name}"
                Service-Type := "Framed-User"
                Framed-MTU := 1300
                Tunnel-Type := VLAN
                Tunnel-Medium-Type := IEEE-802
                Tunnel-Private-Group-Id := "201"
                Reply-Message := "Eduroam Funcionarios"
            }
        }
    }
    else {
        reject
    }
}

pre-proxy {
# attr_rewrite

# Uncomment the following line if you want to change attributes
# as defined in the preproxy_users file.
files

# Uncomment the following line if you want to filter requests
# sent to remote servers based on the rules defined in the
# 'attrs.pre-proxy' file.
# attr_filter.pre-proxy

# If you want to have a log of packets proxied to a home
# server, un-comment the following line, and the
# 'detail pre_proxy_log' section, above.
# pre_proxy_log
}
```

```
#
# When the server receives a reply to a request it proxied
# to a home server, the request may be massaged here, in the
# post-proxy stage.
#
post-proxy {

# If you want to have a log of replies from a home server,
# un-comment the following line, and the 'detail post_proxy_log'
# section, above.
# post_proxy_log

# attr_rewrite

# Uncomment the following line if you want to filter replies from
# remote proxies based on the rules defined in the 'attrs' file.
# attr_filter.post-proxy


eap

files.authorize
Post-Proxy-Type Fail {
 detail
}

}

} # inner-tunnel server block
```

Configurações do EAP/PEAP/TTLS

Esta secção trata de configurar os protocolos de tunneling e autenticação que são suportados em EAP. Quando invocado a partir do inner_tunnel, será também esta a rotina que irá invocar o modulo mschap para autenticar o utilizador através do ntlmauth. Também se define nesta secção o certificado a usar no TTLS e a password que protege a chave privada. É também configurado aqui que quer em TTLS, quer em PEAP, usamos como protocolo de autenticação do túnel interior o MSCHAPv2.

/etc/freeradius/eap.conf (v2.x)

/etc/freeradius/eap.conf

```
eap {
## por defeito, usamos TTLS
default_eap_type = ttls # para eap-ttls-mschapv2, seria peap para peap-mschapv2

timer_expire = 60

ignore_unknown_eap_types = no

cisco_accounting_username_bug = no

max_sessions = 4096

# Supported EAP-types

#  estes protocolos não são próprios para eduroam, e são desactivados

#md5 {
#}

#leap {
#}

#gtc {

#auth_type = mschap
#}
```

```
## EAP-TLS
# # é necessário configurar esta secção para o TTLS
tls {
#
# These is used to simplify later configurations.
#
certdir = ${confdir}/certs
cadir = ${confdir}/certs

## isto é a password que foi usada para assinar o certificado.

private_key_password = yyyyyyyy

# colocamos no mesmo ficheiro o certificado e chave privada.

private_key_file = ${certdir}/server.pem

certificate_file = ${certdir}/server.pem


# Não usamos TLS - e enviar mais dados de certificados atrasa o login/autenticação

#CA_file = ${cadir}/ca.pem


dh_file = ${certdir}/dh
random_file = /dev/urandom

fragment_size = 1024

CA_path = ${cadir}


# check_cert_issuer = "/C=GB/ST=Berkshire/L=Newbury/O=My Company Ltd"

# check_cert_cn = %{User-Name}
cipher_list = "DEFAULT"

make_cert_command = "${certdir}/bootstrap"

ecdh_curve = "prime256v1"

}

# The TTLS module implements the EAP-TTLS protocol,
ttls {

## obrigatoriamente para nos ligarmos à AD, o protocolo de autenticação tem de ser MSCHAPv2
default_eap_type = mschapv2

copy_request_to_tunnel = yes

# # para respostas do inner-tunnel serem devolvidas de volta para o AP

use_tunneled_reply = yes

virtual_server = "inner-tunnel"

}


peap {
default_eap_type = mschapv2

copy_request_to_tunnel = yes
use_tunneled_reply = yes

virtual_server = "inner-tunnel"

}


mschapv2 {
}

}
```

A configuração de cache de sessão, não é suficiente para fazer a recuperação rápida de sessões, sendo necessário escrever mais código em unlang; como tal não foi usada na v2.x.

/etc/freeradius/mods-enabled/eap (v3.x)

/etc/freeradius/mods-enabled/eap

```
# -*- text -*-
##
##  eap.conf -- Configuration for EAP types (PEAP, TTLS, etc.)
##
## $Id: 9ac2a74cfb6be82624664c0586382138a686c609 $


#######################################################################
#
#  Whatever you do, do NOT set 'Auth-Type := EAP'.  The server
#  is smart enough to figure this out on its own.  The most
#  common side effect of setting 'Auth-Type := EAP' is that the
#  users then cannot use ANY other authentication method.
#
#  EAP types NOT listed here may be supported via the "eap2" module.
#  See experimental.conf for documentation.
#
eap {
 #  Invoke the default supported EAP type when
 #  EAP-Identity response is received.
 #
 #  The incoming EAP messages DO NOT specify which EAP
 #  type they will be using, so it MUST be set here.
 #
 #  For now, only one default EAP type may be used at a time.
 #
 #  If the EAP-Type attribute is set by another module,
 #  then that EAP type takes precedence over the
 #  default type configured here.
 #
 default_eap_type = peap

 #  A list is maintained to correlate EAP-Response
 #  packets with EAP-Request packets.  After a
 #  configurable length of time, entries in the list
```

```
#  expire, and are deleted.
#
timer_expire     = 60

#  There are many EAP types, but the server has support
#  for only a limited subset.  If the server receives
#  a request for an EAP type it does not support, then
#  it normally rejects the request.  By setting this
#  configuration to "yes", you can tell the server to
#  instead keep processing the request.  Another module
#  MUST then be configured to proxy the request to
#  another RADIUS server which supports that EAP type.
#
#  If another module is NOT configured to handle the
#  request, then the request will still end up being
#  rejected.
ignore_unknown_eap_types = no

# Cisco AP1230B firmware 12.2(13)JA1 has a bug.  When given
# a User-Name attribute in an Access-Accept, it copies one
# more byte than it should.
#
# We can work around it by configurably adding an extra
# zero byte.
cisco_accounting_username_bug = no

#
#  Help prevent DoS attacks by limiting the number of
#  sessions that the server is tracking.  For simplicity,
#  this is taken from the "max_requests" directive in
#  radiusd.conf.
max_sessions = ${max_requests}

# Supported EAP-types

#
#  We do NOT recommend using EAP-MD5 authentication
#  for wireless connections.  It is insecure, and does
#  not provide for dynamic WEP keys.
#
```

```
 #md5 {
 #}

 #
 # EAP-pwd -- secure password-based authentication
 #
# pwd {
# group = 19

 #
# server_id = theserver@example.com

 #  This has the same meaning as for TLS.
# fragment_size = 1020

 # The virtual server which determines the
 # "known good" password for the user.
 # Note that unlike TLS, only the "authorize"
 # section is processed.  EAP-PWD requests can be
 # distinguished by having a User-Name, but
 # no User-Password, CHAP-Password, EAP-Message, etc.
# virtual_server = "inner-tunnel"
# }

 # Cisco LEAP
 #
 #  We do not recommend using LEAP in new deployments.  See:
 #  http://www.securiteam.com/tools/5TP012ACKE.html
 #
 #  Cisco LEAP uses the MS-CHAP algorithm (but not
 #  the MS-CHAP attributes) to perform it's authentication.
 #
 #  As a result, LEAP *requires* access to the plain-text
 #  User-Password, or the NT-Password attributes.
 #  'System' authentication is impossible with LEAP.
 #
 #leap {
 #}

 #  Generic Token Card.
```

```
#
#  Currently, this is only permitted inside of EAP-TTLS,
#  or EAP-PEAP.  The module "challenges" the user with
#  text, and the response from the user is taken to be
#  the User-Password.
#
#  Proxying the tunneled EAP-GTC session is a bad idea,
#  the users password will go over the wire in plain-text,
#  for anyone to see.
#
#gtc {
#  The default challenge, which many clients
#  ignore..
#challenge = "Password: "

#  The plain-text response which comes back
#  is put into a User-Password attribute,
#  and passed to another module for
#  authentication.  This allows the EAP-GTC
#  response to be checked against plain-text,
#  or crypt'd passwords.
#
#  If you say "Local" instead of "PAP", then
#  the module will look for a User-Password
#  configured for the request, and do the
#  authentication itself.
#
# auth_type = PAP
#}

## Common TLS configuration for TLS-based EAP types
#
#  See raddb/certs/README for additional comments
#  on certificates.
#
#  If OpenSSL was not found at the time the server was
#  built, the "tls", "ttls", and "peap" sections will
#  be ignored.
#
#  If you do not currently have certificates signed by
```

```
#  a trusted CA you may use the 'snakeoil' certificates.
#  Included with the server in raddb/certs.
#
#  If these certificates have not been auto-generated:
#    cd raddb/certs
#    make
#
#  These test certificates SHOULD NOT be used in a normal
#  deployment.  They are created only to make it easier
#  to install the server, and to perform some simple
#  tests with EAP-TLS, TTLS, or PEAP.
#
#  See also:
#
#  http://www.dslreports.com/forum/remark,9286052~mode=flat
#
#  Note that you should NOT use a globally known CA here!
#  e.g. using a Verisign cert as a "known CA" means that
#  ANYONE who has a certificate signed by them can
#  authenticate via EAP-TLS!  This is likely not what you want.
tls-config tls-common {
private_key_password = yyyyyyyy
private_key_file = ${certdir}/key.pem

#  If Private key & Certificate are located in
#  the same file, then private_key_file &
#  certificate_file must contain the same file
#  name.
#
#  If ca_file (below) is not used, then the
#  certificate_file below MUST include not
#  only the server certificate, but ALSO all
#  of the CA certificates used to sign the
#  server certificate.
certificate_file = ${certdir}/server.pem

#  Trusted Root CA list
#
#  ALL of the CA's in this list will be trusted
#  to issue client certificates for authentication.
```

```
#
#  In general, you should use self-signed
#  certificates for 802.1x (EAP) authentication.
#  In that case, this CA file should contain
#  *one* CA certificate.
#
#  This parameter is used only for EAP-TLS,
#  when you issue client certificates.  If you do
#  not use client certificates, and you do not want
#  to permit EAP-TLS authentication, then delete
#  this configuration item.
#ca_file = ${cadir}/ca.pem

#
#  If OpenSSL supports TLS-PSK, then we can use
#  a PSK identity and (hex) password.  When the
#  following two configuration items are specified,
#  then certificate-based configuration items are
#  not allowed.  e.g.:
#
# private_key_password
# private_key_file
# certificate_file
# ca_file
# ca_path
#
#  For now, the identity is fixed, and must be the
#  same on the client.  The passphrase must be a hex
#  value, and can be up to 256 hex digits.
#
#  Future versions of the server may be able to
#  look up the shared key (hexphrase) based on the
#  identity.
#
# psk_identity = "test"
# psk_hexphrase = "036363823"

#
#  For DH cipher suites to work, you have to
#  run OpenSSL to create the DH file first:
```

```
#
#   openssl dhparam -out certs/dh 1024
#
dh_file = ${certdir}/dh

#
#  If your system doesn't have /dev/urandom,
#  you will need to create this file, and
#  periodically change its contents.
#
#  For security reasons, FreeRADIUS doesn't
#  write to files in its configuration
#  directory.
#
# random_file = ${certdir}/random

#
#  This can never exceed the size of a RADIUS
#  packet (4096 bytes), and is preferably half
#  that, to accommodate other attributes in
#  RADIUS packet.  On most APs the MAX packet
#  length is configured between 1500 - 1600
#  In these cases, fragment size should be
#  1024 or less.
#
fragment_size = 1024

#  include_length is a flag which is
#  by default set to yes If set to
#  yes, Total Length of the message is
#  included in EVERY packet we send.
#  If set to no, Total Length of the
#  message is included ONLY in the
#  First packet of a fragment series.
#
# include_length = yes

#  Check the Certificate Revocation List
#
#  1) Copy CA certificates and CRLs to same directory.
```

```
#  2) Execute 'c_rehash <CA certs&CRLs Directory>'.
#    'c_rehash' is OpenSSL's command.
#  3) uncomment the line below.
#  5) Restart radiusd
check_crl = no
#ca_path = ${cadir}

#
#  If check_cert_issuer is set, the value will
#  be checked against the DN of the issuer in
#  the client certificate.  If the values do not
#  match, the certificate verification will fail,
#  rejecting the user.
#
#  In 2.1.10 and later, this check can be done
#  more generally by checking the value of the
#  TLS-Client-Cert-Issuer attribute.  This check
#  can be done via any mechanism you choose.
#
# check_cert_issuer = "/C=GB/ST=Berkshire/L=Newbury/O=My Company Ltd"

#
#  If check_cert_cn is set, the value will
#  be xlat'ed and checked against the CN
#  in the client certificate.  If the values
#  do not match, the certificate verification
#  will fail rejecting the user.
#
#  This check is done only if the previous
#  "check_cert_issuer" is not set, or if
#  the check succeeds.
#
#  In 2.1.10 and later, this check can be done
#  more generally by checking the value of the
#  TLS-Client-Cert-CN attribute.  This check
#  can be done via any mechanism you choose.
#
# check_cert_cn = %{User-Name}
#
# Set this option to specify the allowed
```

```
# TLS cipher suites.  The format is listed
# in "man 1 ciphers".
cipher_list = "DEFAULT"

#


#
#  Elliptical cryptography configuration
#
#  Only for OpenSSL >= 0.9.8.f
#
ecdh_curve = "prime256v1"

#
#  Session resumption / fast reauthentication
#  cache.
#
#  The cache contains the following information:
#
#  session Id - unique identifier, managed by SSL
#  User-Name  - from the Access-Accept
#  Stripped-User-Name - from the Access-Request
#  Cached-Session-Policy - from the Access-Accept
#
#  The "Cached-Session-Policy" is the name of a
#  policy which should be applied to the cached
#  session.  This policy can be used to assign
#  VLANs, IP addresses, etc.  It serves as a useful
#  way to re-apply the policy from the original
#  Access-Accept to the subsequent Access-Accept
#  for the cached session.
#
#  On session resumption, these attributes are
#  copied from the cache, and placed into the
#  reply list.
#
#  You probably also want "use_tunneled_reply = yes"
#  when using fast session resumption.
#
cache {
```

```
#
#  Enable it.  The default is "no".
#  Deleting the entire "cache" subsection
#  also disables caching.
#
#  You can disallow resumption for a
#  particular user by adding the following
#  attribute to the control item list:
#
# Allow-Session-Resumption = No
#
#  If "enable = no" below, you CANNOT
#  enable resumption for just one user
#  by setting the above attribute to "yes".
#
enable = yes

#
#  Lifetime of the cached entries, in hours.
#  The sessions will be deleted after this
#  time.
#
lifetime = 24 # hours

#
#  The maximum number of entries in the
#  cache.  Set to "0" for "infinite".
#
#  This could be set to the number of users
#  who are logged in... which can be a LOT.
#
max_entries = 255

#
#  Internal "name" of the session cache.
#  Used to distinguish which TLS context
#  sessions belong to.
#
#  The server will generate a random value
#  if unset. This will change across server
```

```
#  restart so you MUST set the "name" if you
#  want to persist sessions (see below).
#
#name = "EAP module"

#
#  Simple directory-based storage of sessions.
#  Two files per session will be written, the SSL
#  state and the cached VPs. This will persist session
#  across server restarts.
#
#  The server will need write perms, and the directory
#  should be secured from anyone else. You might want
#  a script to remove old files from here periodically:
#
#    find ${logdir}/tlscache -mtime +2 -exec rm -f {} \;
#
#  This feature REQUIRES "name" option be set above.
#
#persist_dir = "${logdir}/tlscache"
}

#
#  As of version 2.1.10, client certificates can be
#  validated via an external command.  This allows
#  dynamic CRLs or OCSP to be used.
#
#  This configuration is commented out in the
#  default configuration.  Uncomment it, and configure
#  the correct paths below to enable it.
#
#verify {
#  A temporary directory where the client
#  certificates are stored.  This directory
#  MUST be owned by the UID of the server,
#  and MUST not be accessible by any other
#  users.  When the server starts, it will do
#  "chmod go-rwx" on the directory, for
#  security reasons.  The directory MUST
#  exist when the server starts.
```

```
#
#  You should also delete all of the files
#  in the directory when the server starts.
# tmpdir = /tmp/radiusd

#  The command used to verify the client cert.
#  We recommend using the OpenSSL command-line
#  tool.
#
#  The ${..ca_path} text is a reference to
#  the ca_path variable defined above.
#
#  The %{TLS-Client-Cert-Filename} is the name
#  of the temporary file containing the cert
#  in PEM format.  This file is automatically
#  deleted by the server when the command
#  returns.
# client = "/path/to/openssl verify -CApath ${..ca_path} %{TLS-Client-Cert-Filename}"
#}

#
#  OCSP Configuration
#  Certificates can be verified against an OCSP
#  Responder. This makes it possible to immediately
#  revoke certificates without the distribution of
#  new Certificate Revocation Lists (CRLs).
#
ocsp {
#
#  Enable it.  The default is "no".
#  Deleting the entire "ocsp" subsection
#  also disables ocsp checking
#
enable = no

#
#  The OCSP Responder URL can be automatically
#  extracted from the certificate in question.
#  To override the OCSP Responder URL set
#  "override_cert_url = yes".
```

```
#
override_cert_url = yes


#
#  If the OCSP Responder address is not
#  extracted from the certificate, the
#  URL can be defined here.

#
#  Limitation: Currently the HTTP
#  Request is not sending the "Host: "
#  information to the web-server.  This
#  can be a problem if the OCSP
#  Responder is running as a vhost.
#
url = "http://127.0.0.1/ocsp/"


#
# If the OCSP Responder can not cope with nonce
# in the request, then it can be disabled here.
#
# For security reasons, disabling this option
# is not recommended as nonce protects against
# replay attacks.
#
# Note that Microsoft AD Certificate Services OCSP
# Responder does not enable nonce by default. It is
# more secure to enable nonce on the responder than
# to disable it in the query here.
# See http://technet.microsoft.com/en-us/library/cc770413%28WS.10%29.aspx
#
# use_nonce = yes


#
# Number of seconds before giving up waiting
# for OCSP response. 0 uses system default.
#
# timeout = 0


#
```

```
# Normally an error in querying the OCSP
# responder (no response from server, server did
# not understand the request, etc) will result in
# a validation failure.
#
# To treat these errors as 'soft' failures and
# still accept the certificate, enable this
# option.
#
# Warning: this may enable clients with revoked
# certificates to connect if the OCSP responder
# is not available. Use with caution.
#
# softfail = no
}
}

## EAP-TLS
#
#  As of Version 3.0, the TLS configuration for TLS-based
#  EAP types is above in the "tls-config" section.
#
#tls {
# Point to the common TLS configuration
tls = tls-common

#
# As part of checking a client certificate, the EAP-TLS
# sets some attributes such as TLS-Client-Cert-CN. This
# virtual server has access to these attributes, and can
# be used to accept or reject the request.
#
# virtual_server = check-eap-tls
#}


## EAP-TTLS
#
#  The TTLS module implements the EAP-TTLS protocol,
#  which can be described as EAP inside of Diameter,
```

```
#  inside of TLS, inside of EAP, inside of RADIUS...
#
#  Surprisingly, it works quite well.
#
ttls {
#  Which tls-config section the TLS negotiation parameters
#  are in - see EAP-TLS above for an explanation.
#
#  In the case that an old configuration from FreeRADIUS
#  v2.x is being used, all the options of the tls-config
#  section may also appear instead in the 'tls' section
#  above. If that is done, the tls= option here (and in
#  tls above) MUST be commented out.
#
tls = tls-common

#  The tunneled EAP session needs a default EAP type
#  which is separate from the one for the non-tunneled
#  EAP module.  Inside of the TTLS tunnel, we recommend
#  using EAP-MD5.  If the request does not contain an
#  EAP conversation, then this configuration entry is
#  ignored.
#
default_eap_type = mschapv2

#  The tunneled authentication request does not usually
#  contain useful attributes like 'Calling-Station-Id',
#  etc.  These attributes are outside of the tunnel,
#  and normally unavailable to the tunneled
#  authentication request.
#
#  By setting this configuration entry to 'yes',
#  any attribute which is NOT in the tunneled
#  authentication request, but which IS available
#  outside of the tunnel, is copied to the tunneled
#  request.
#
#  allowed values: {no, yes}
#
copy_request_to_tunnel = yes
```

```
#  The reply attributes sent to the NAS are usually
#  based on the name of the user 'outside' of the
#  tunnel (usually 'anonymous').  If you want to send
#  the reply attributes based on the user name inside
#  of the tunnel, then set this configuration entry to
#  'yes', and the reply to the NAS will be taken from
#  the reply to the tunneled request.
#
#  allowed values: {no, yes}
#
use_tunneled_reply = yes

#
#  The inner tunneled request can be sent
#  through a virtual server constructed
#  specifically for this purpose.
#
#  If this entry is commented out, the inner
#  tunneled request will be sent through
#  the virtual server that processed the
#  outer requests.
#
virtual_server = "inner-tunnel"

#  This has the same meaning, and overwrites, the
#  same field in the "tls" configuration, above.
#  The default value here is "yes".
#
# include_length = yes

#
# Unlike EAP-TLS, EAP-TTLS does not require a client
# certificate. However, you can require one by setting the
# following option. You can also override this option by
# setting
#
# EAP-TLS-Require-Client-Cert = Yes
#
# in the control items for a request.
```

```
#
require_client_cert = no
}



## EAP-PEAP
#


#####################################################
#
#  !!!!! WARNINGS for Windows compatibility  !!!!!
#
#####################################################
#
#  If you see the server send an Access-Challenge,
#  and the client never sends another Access-Request,
#  then
#
# STOP!
#
#  The server certificate has to have special OID's
#  in it, or else the Microsoft clients will silently
#  fail.  See the "scripts/xpextensions" file for
#  details, and the following page:
#
# http://support.microsoft.com/kb/814394/en-us
#
#  For additional Windows XP SP2 issues, see:
#
# http://support.microsoft.com/kb/885453/en-us
#
#
#  If is still doesn't work, and you're using Samba,
#  you may be encountering a Samba bug.  See:
#
# https://bugzilla.samba.org/show_bug.cgi?id=6563
#
#  Note that we do not necessarily agree with their
#  explanation... but the fix does appear to work.
#
```

```
##################################################

#
#  The tunneled EAP session needs a default EAP type
#  which is separate from the one for the non-tunneled
#  EAP module.  Inside of the TLS/PEAP tunnel, we
#  recommend using EAP-MS-CHAPv2.
#
peap {
#  Which tls-config section the TLS negotiation parameters
#  are in - see EAP-TLS above for an explanation.
#
#  In the case that an old configuration from FreeRADIUS
#  v2.x is being used, all the options of the tls-config
#  section may also appear instead in the 'tls' section
#  above. If that is done, the tls= option here (and in
#  tls above) MUST be commented out.
#
tls = tls-common

#  The tunneled EAP session needs a default
#  EAP type which is separate from the one for
#  the non-tunneled EAP module.  Inside of the
#  PEAP tunnel, we recommend using MS-CHAPv2,
#  as that is the default type supported by
#  Windows clients.
#
default_eap_type = mschapv2

#  The PEAP module also has these configuration
#  items, which are the same as for TTLS.
#
copy_request_to_tunnel = yes
use_tunneled_reply = yes

#  When the tunneled session is proxied, the
#  home server may not understand EAP-MSCHAP-V2.
#  Set this entry to "no" to proxy the tunneled
#  EAP-MSCHAP-V2 as normal MSCHAPv2.
#
```

```
proxy_tunneled_request_as_eap = yes

#
#  The inner tunneled request can be sent
#  through a virtual server constructed
#  specifically for this purpose.
#
#  If this entry is commented out, the inner
#  tunneled request will be sent through
#  the virtual server that processed the
#  outer requests.
#
virtual_server = "inner-tunnel"

# This option enables support for MS-SoH
# see doc/SoH.txt for more info.
# It is disabled by default.
#
# soh = yes

#
# The SoH reply will be turned into a request which
# can be sent to a specific virtual server:
#
# soh_virtual_server = "soh-server"

#
# Unlike EAP-TLS, PEAP does not require a client certificate.
# However, you can require one by setting the following
# option. You can also override this option by setting
#
# EAP-TLS-Require-Client-Cert = Yes
#
# in the control items for a request.
#
require_client_cert = no
}

#
#  This takes no configuration.
```

```
 #
 #  Note that it is the EAP MS-CHAPv2 sub-module, not
 #  the main 'mschap' module.
 #
 #  Note also that in order for this sub-module to work,
 #  the main 'mschap' module MUST ALSO be configured.
 #
 #  This module is the *Microsoft* implementation of MS-CHAPv2
 #  in EAP.  There is another (incompatible) implementation
 #  of MS-CHAPv2 in EAP by Cisco, which FreeRADIUS does not
 #  currently support.
 #
 mschapv2 {
 #  Prior to version 2.1.11, the module never
 #  sent the MS-CHAP-Error message to the
 #  client.  This worked, but it had issues
 #  when the cached password was wrong.  The
 #  server *should* send "E=691 R=0" to the
 #  client, which tells it to prompt the user
 #  for a new password.
 #
 #  The default is to behave as in 2.1.10 and
 #  earlier, which is known to work.  If you
 #  set "send_error = yes", then the error
 #  message will be sent back to the client.
 #  This *may* help some clients work better,
 #  but *may* also cause other clients to stop
 #  working.
 #
# send_error = no
 }
}
```

Dicionários

Os dicionários são o que permite referenciar atributos RADIUS por nomes. Ou seja, são tabelas que traduzem um valor inteiro para um nome/string. Como já referimos, existem atributos standard e atributos associados a fabricantes.

/etc/freeradius/dictionary

Estabelece a relação entre atributos/nomes e os códigos transmitidos nos pacotes RADIUS. Aquando o suporte de hardware novo, se se pretende usar atributos específicos de algum vendor, há que verificar se o freeradius já trás o dicionário, ou inclui-lo neste ficheiro.

O atributo acrescentado, Operator-Name, é único a cada instituição na confederação EDUROAM, e pretende identificar a instituição nas mensagens trocadas para facilitar o processo de debugging de problemas. Entretanto, há também que use o CUI, mas ao nível da federação PT ainda não é usado.

/etc/freeradius/dictionary

ATTRIBUTE Operator-Name 126 string

ATTRIBUTE Chargeable-User-Identity 89 string

Veja mais sobre Attribute-Value Pairs (AVP) em http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_chapter09186a008007e6b7.html

Filtros/propriedades de utilizadores

Existem vários capacidades de tratamento da autenticação de utilizadores ao nível do FreeRADIUS, desde:

- as directivas unlang para reenforçar o formato user@domínio, na secção authorize do túnel exterior;
- a lista de MACs/utilizadores bloqueados em unland/MySQL;
- os ficheiros da família users, que lidam com propriedades de utilizadores;
- os ficheiros da família attrs, que permitem construir filtros baseados nas propriedades RADIUS relacionadas com as mensagens trocadas para autenticação.

Filtros unlang

Existem vários filtros unlang que acrescentamos, entre os quais, os filtros da entrada do processamento do túnel exterior e a blacklist eduroam, no ficheiro default. Ver também o capitulo lista negra/ficheiro policy.conf.

/etc/freeradius/users (v2.x)

/etc/freeradius/mods-config/files/authorize (v3.x)

Já usamos em tempos o ficheiro de users como ponto central para definir a autenticação de utilizadores; no entanto, um unlang temos mais controle, e conseguimos definir melhor em que pontos do processo as ligações ao LDAP são feitas. Hoje em dia, só usamos este ficheiro para definir as passwords temporárias do nosso realm para eventos guest.iscte. Neste ficheiro, pode-se "programar" o tratamento dado aos utilizadores, de forma a descrever a interacções destes com as várias fases do tratamento da autenticação, que tipo de logins são aceitados ou rejeitados, e a atribuição de VLANs de acordo com grupos. É mais simples lidar com questões de utilizadores neste ficheiro do que com unlang (ou não é, na altura de run-time torna-se mais complicado perceber onde as directivas têm efeito).

Note-se que o processamento de directivas neste ficheiro é ligeiramente mais lento que através do unlang.

Neste ficheiro, a sintaxe é colocar os itens a verificar na primeira linha, e as respostas a devolver na(s) linha(s) seguintes. Uma linha em branco significa que esse bloco de tratamento terminou, e se pretendermos outro seguimos a mesma sintaxe.

Para equipamento Cisco as VLAN's fornecidas pelo FREERADIUS têm de estar configuradas no equipamento. Caso falte a configuração no equipamento da VLAN enviada pelo FreeRadius o AP utiliza a VLAN associada ao SSID a que o utilizador se associou. O protocolo RADIUS não tem qualquer provisão para colocar em VLANs de quarentena autenticações falhadas. Uma autenticação falhada é um acesso rejeitado.

embora exista um campo Reply-Message, a maior parte dos drivers de sistemas operativos ignoram a mensagem que têm de volta.

Como exemplo, aqui ficam alguns utilizadores definidos para a rede guest, que é usada em EAP-TTLS +MSCHAPv2

/etc/freeradius/mods-config/files/authorize

```
guest1        Cleartext-Password := "xxxxxxxxxxx"

guest2        Cleartext-Password := "yyyyyyyyyyy"

guest3        Cleartext-Password := "zzzzzzzzzzz"

guest4        Cleartext-Password := "kkkkkkkkkkk"

guest5        Cleartext-Password := "wwwwwwwwwww"
```

Para gerar o ficheiro de users guest, cada vez que há um evento, é necessário correr o seguinte script e fazer restart ao FreeRadius.

make_guest.sh

```
#!/bin/bash
FILE=/etc/freeradius/mods-config/files/authorize
cat /dev/null > $FILE
for i in {1..40}
do
   PASS=`makepasswd --chars=12`
   echo -e guest$i@guest.iscte"\t"$PASS
   echo -e guest$i"\tCleartext-Password := \"$PASS\"" >> $FILE
   echo >> $FILE
done
```

O Ficheiro users exemplo está aqui apenas por uma razão histórica, e não é para usar na configuração corrente. O trabalho de atribuição de VLAN está feito em unlang na secção de servidores virtuais.

/etc/freeradius/users

```
# Rejeita tentativas de autenticação de utilizadores com domínios locais
DEFAULT Realm =~ ".*\\.iscte\\.local", Auth-Type := Reject
# Rejeita utilizadores de subdominios
DEFAULT Realm =~ ".*\\.iscte\\.pt", Auth-Type := Reject

# se em roaming, não retorna atributos - mas autentica.
# A verificação de Operator-Name deve vir em primeiro, para minimizar queries LDAP.
DEFAULT Operator-Name =~ "1*", Realm == "iscte.pt", Ldap-Group == "Funcionarios"

# autenticação do Dominio
DEFAULT Realm == "iscte.pt", Ldap-Group == "Funcionarios"
                        Service-Type = "Framed-User",
                        Reply-Message = "Eduroam ISCTE",
                        Framed-MTU = 1300,
                        Tunnel-Type = VLAN,
                        Tunnel-Medium-Type = IEEE-802,
                        Tunnel-Private-Group-Id = "200"

# se em roaming, não retorna atributos
DEFAULT Operator-Name =~ "1*", Realm == "iscte.pt", Ldap-Group == "Alunos"

DEFAULT Realm == "iscte.pt", Ldap-Group == "Alunos"
                        Service-Type = "Framed-User",
                        Reply-Message = "Eduroam Alunos",
                        Framed-MTU = 1300,
                        Tunnel-Type = VLAN,
                        Tunnel-Medium-Type = IEEE-802,
                        Tunnel-Private-Group-Id = "201"

# não necessita de testar se roaming, porque convidado.local não é um endereço privado
DEFAULT Realm == "guest.iscte", Ldap-Group == "Convidados"
                        Service-Type = "Framed-User",
                        Reply-Message = "Convidados Eventos",
                        Framed-MTU = 1300,
                        Tunnel-Type = VLAN,
                        Tunnel-Medium-Type = IEEE-802,
                        Tunnel-Private-Group-Id = "202"

## os utilizadores que não sejam do domínio local, ficam na VLAN EDUROAM
DEFAULT Realm != iscte.pt"
                        Service-Type = "Framed-User",
                        Reply-Message = "Eduroam Roaming",
                        Tunnel-Medium-Type = IEEE-802,
                        Tunnel-Type = VLAN,
                        Tunnel-Private-Group-Id = "203"

## rejeita autenticação dos utilizadores locais que não tenham nenhum dos grupos anteriores
DEFAULT
                        Auth-Type := Reject
```

O processamento deste ficheiro é mais lento que as directivas unlang, pelo que algum esforço foi realizado para minimizar o seu uso, balanceando a rapidez de execução com a compreensão da configuração. O atributo Operator-Name não existe em pedidos locais, pelo que usamos a sua presença para saber que estamos a tratar de autenticação em roaming. Embora de qualquer forma, nos filtros de saída a informação de VLAN seja filtrada, assim também usamos menos recursos, incluindo menos espaço em disco e menos I/O para quem tem logs detalhados activos. No entanto expressões regulares nunca funcionarem muito bem neste ficheiro, pelo que nesses casos, é mesmo melhor usar unlang.
no passado o suporte para weathermap estava neste ficheiro, mas dado termos configurado o freeradius para minimizar as consultas a este ficheiro, e ser mais lento, ele já não é consultado na secção authorize. Em consequência, adicionamos directivas unlang na secção authorize. A configuração que estava no freeradius, aconselhada pela federação, no ficheiro users era:

```
# weatherman FCCN - obsoleta, não usar.
radius-teste    Auth-Type := Reject
                Reply-Message == "RADIUS OK",
                User-Password == "xxxxx"
```

Podem se fazer curtos testes também neste ficheiro, desde que a directiva files seja activa no inner-tunnel. Por exemplo, para testar uma password em Windows:

```
# smbencrypt kakao
LM Hash                          NT Hash
————————————_        ————————————_
3658E2D04E81CC72AAD3B435B51404EE        30600A1973AA628A1F4C2F828C1CFF0C


rui    NT-Password := 0x30600A1973AA628A1F4C2F828C1CFF0C
```

/etc/freeradius/preproxy_users

Este ficheiro em seguida é consultado antes do reencaminhamento para proxies externos. Se o domínio a tratarmos não for local, identificamos o nosso operador para em debugging de situações de roaming, facilitar a identificação da precedência das ligações; substituímos também qualquer referência a NAS/APs internos pelo nosso endereço de servidor RADIUS. Mascaramos também os IPs internos dos APs locais.

/etc/freeradius/preproxy_users

```
# This file is similar to the "users" file. The check items
# are compared against the request, but the "reply" items are
# used to update the proxied packet, not the reply to the NAS.
#
# You can use this file to re-write requests which are about to
# be sent to a home server.
DEFAULT Realm != "iscte.pt"
    NAS-IP-Address := 193.136.188.36,
    Operator-Name := "1iscte.pt"
```

Pode se optar para não mascarar o IP de APs internos para facilitar o debugging de problemas de autenticação de utilizadores em roaming.
O 1 em 1iscte.pt não é um erro, mas sim uma convenção.

/etc/freeradius/attrs (2.x)

/etc/freeradius/mods-config/attr_filter/post-proxy (3.x)

Filtra atributos e valores nos pacotes de RADIUS recebidos e transmitidos. Estabelece políticas de filtragem de mensagens trocadas com NAS e home servers.

/etc/freeradius/attrs

DEFAULT

Service-Type == Framed-User,
Service-Type == Login-User,
Login-Service == TCP-Clear,
Login-TCP-Port <= 65536,
Framed-IP-Address == 255.255.255.254,
Framed-IP-Netmask == 255.255.255.255,
Framed-Protocol == PPP,
Framed-Compression == Van-Jacobson-TCP-IP,
Framed-MTU >= 576,
Framed-Filter-ID =* ANY,
Reply-Message =* ANY,
Proxy-State =* ANY,
EAP-Message =* ANY,
Message-Authenticator =* ANY,
MS-MPPE-Recv-Key =* ANY,
MS-MPPE-Send-Key =* ANY,
MS-CHAP-MPPE-Keys =* ANY,
State =* ANY,
Session-Timeout <= 28800,
Idle-Timeout <= 600,
Port-Limit <= 2,

User-Name=* ANY,

Operator-Name =* ANY,

Class =* ANY,

Calling-Station-ID =* ANY,

Chargeable-User-Identity =* ANY,

Called-Station-Id =* ANY,

Acct-Status-Type =* ANY,

Acct-Session-ID =* ANY,

Cached-Session-Policy =* ANY

Para ver mais sobre filtros, consultar: http://freeradius.org/radiusd/man/rlm_attr_filter.html

/etc/freeradius/attrs.pre-proxy (v2.x)

/etc/freeradius/mods-config/attr_filter/pre-proxy (v3.x)

O ficheiro attrs.pre-proxy é consultado para filtrar os atributos e correspondentes valores associados que que é permitido enviar para proxies. Ou seja, são reencaminhado para os proxies os atributos presentes neste ficheiro.

/etc/freeradius/attrs.pre-proxy

DEFAULT

```
        User-Name =* ANY,
        User-Password =* ANY,
        CHAP-Password =* ANY,
        CHAP-Challenge =* ANY,
        MS-CHAP-Challenge =* ANY,
        MS-CHAP-Response =* ANY,
        EAP-Message =* ANY,
        Message-Authenticator =* ANY,
        State =* ANY,
        NAS-IP-Address =* ANY,
        NAS-Identifier =* ANY,
        Proxy-State =* ANY,

 NAS-IP-Address =* ANY,

 NAS-Identifier =* ANY,

 NAS-Port-Type =* ANY,

 Calling-Station-Id =* ANY
```

Clientes / entrada da federação EDUROAM

O ficheiro clients.conf destina-se a configurar/autorizar todos os clientes passíveis de fazer perguntas ao nosso servidor de Freeradius. Podem usar-se IPs ou nomes de DNS para identificar equipamentos. A menos que o cliente especial “DEFAULT” seja definido, todos os pedidos de clientes não implicitamente configurados serão ignorados.

São clientes tanto os AP’s como outros servidores RADIUS que utilizem o servidor para efectuar pedidos de autenticação/accounting, estejam abaixo ou acima na hierarquia. O nastype é cisco para equipamento Cisco ou other para outros fabricantes. O campo shortname deverá ter nomes diferentes em todas as suas ocorrências neste ficheiro.

/etc/freeradius/clients.conf (v2.x)

/etc/freeradius/clients.conf

```
client localhost {
ipaddr = 127.0.0.1
# netmask = 32
secret = kkkkkk
require_message_authenticator = no
nastype = other # localhost isn't usually a NAS...
}
client 193.136.188.36 {
ipaddr = 193.136.188.36
netmask = 32
secret = xxxxxxx
require_message_authenticator = no
nastype = other
}

client 192.168.10.0/24 {
nastype = cisco
secret = qqqqqqqqqq
shortname = rede1_aps
}
# PROXY NACIONAL
client 193.136.192.43 {
nastype = other
secret = password_a_combinar_com_FCCN
shortname = proxyNacional1
}
# PROXY NACIONAL
client 193.136.192.44 {
nastype = other
secret = password_a_combinar_com_FCCN
shortname = proxyNacional2
}
```

/etc/freeradius/clients.conf (v3.x)

/etc/freeradius/clients.conf

```
client localhost {
ipaddr = 127.0.0.1
# netmask = 32
secret = kkkkkk
require_message_authenticator = no
nas_type = other # localhost isn't usually a NAS...
}
client 193.136.188.36 {
ipaddr = 193.136.188.36
netmask = 32
secret = xxxxxxx
require_message_authenticator = no
nas_type = other
}

client 192.168.10.0/24 {
nas_type = cisco
secret = qqqqqqqqqq
shortname = rede1_aps
}
# PROXY NACIONAL
client 193.136.192.43 {
nas_type = other
secret = password_a_combinar_com_FCCN
shortname = proxyNacional1
}
# PROXY NACIONAL
client 193.136.192.44 {
nas_type = other
secret = password_a_combinar_com_FCCN
shortname = proxyNacional2
}
```

um AP que não estiver neste ficheiro, provocará uma entrada em log: "Ignoring request from unknow client endereço-IP"

Saída para a (con)federação

O proxy.conf destina-se a configurar a localidade dos domínios, e o reencaminhamento dos domínios a que não respondemos (proxying). Neste caso define-se o iscte.pt como local, define-se domínios internos ou logins sem domínio como vazios, para estes não serem reencaminhados para a federação, e define-se uma configuração de alta disponibilidade usando os dois proxies nacionais da FCCN.

Neste ficheiro são definidos os parâmetros globais para proxying (retrys; timeouts; etc.) bem como os pedidos que serão “alvo” de proxy ou não. O proxy de um pedido de autenticação é decidido com base no Realm contido no User- Name do utilizador que se pretende autenticar.

O Realm é a parte do login que sucede uma ‘@’ ou seja, para um login user@fccn.pt , fccn.pt é o Realm. O Realm especial "~.*.~*" será utilizado para tratar de todos os pedidos que não foram tratados por Realm’s conhecidos.
È necessário definir o(s) realm’s que são conhecidos do servidor para os pedidos de autenticação sejam “entregues” no servidor local, e um Realm "~.*" para encaminhar todos os outros para o servidor acima na hierarquia de autenticação.

A directiva NULL é usada para os casos de utilizadores sem domínio. Se for pretendido que utilizadores sem domínio se autentiquem, ter-se-á de colocar uma configuração idêntica ao domínio, e modificar o ficheiro users para permitir na regexp utilizadores sem @.

Já não usamos suffix em todos os locais que fazemos proxying, mas sim unlang, o que nos dá mais controle sobre o processo.

Nos pedidos a encaminhar para o Proxy Nacional é fundamental ter a opção nostrip, porque por omissão o servidor retirará o REALM do username. Os pedidos que saiam da instituição sem REALM serão descartados no Proxy Nacional por não ser possível identificar qual o seu destino.
O "~.*" substituí o DEFAULT, para nos logs do f_ticks aparecer o domínio ao invés da string DEFAULT.

/etc/freeradius/proxy.conf

O proxy.conf define a configuração de tratamento a dar aos realms, e decidir quando se reencaminha pacotes para a federação.

/etc/freeradius/proxy.conf

```
## autenticação local de @iscte.pt
realm iscte.pt {
type = auth+acct
secret = wirelessiscte
authhost = LOCAL
accthost = LOCAL
nostrip
}
## autenticação de convidados (opcional)
realm guest.iscte {
type = auth+acct
secret = wirelessiscte
authhost = LOCAL
accthost = LOCAL
}
## ignore users@dominiolocalwindows
realm "~.*\\.iscte\\.local$" {
}
## ignora subdominos de iscte.pt
realm "~.*\\.iscte\\.pt$" {
}
realm LOCAL {
# If we do not specify a server pool, the realm is LOCAL, and
# requests are not proxied to it.
}
realm NULL {
}
## 1o proxy nacional
home_server cv-radius {
type = auth+acct
ipaddr = 193.136.192.43
port = 1812
secret = password_a_combinar_com_FCCN
status_check = status-server
require_message_authenticator = yes
num_answers_to_alive = 3
}
## 2o proxy nacional
home_server cv2-radius {
type = auth+acct
ipaddr = 193.136.192.44
port = 1812
secret = password_a_combinar_com_FCCN
status_check = status-server
require_message_authenticator = yes
num_answers_to_alive = 3
}

## configuração de failover, se falha o primeiro, tenta o segundo
home_server_pool EDUROAM {
type = fail-over
home_server = cv-radius
home_server = cv2-radius
}
## todos os domínios que não seja iscte.pt caem aqui
##para tratamento da instrução suffix
realm "~.*" {
        pool                    = EDUROAM
        nostrip
}

## para tratamento de roteamento de PROXY em unlang
realm TO_EDUROAM {
        pool                    = EDUROAM
        nostrip
}
```

o realm/domínio guest.iscte nem sequer precisa de existir no DNS, já que pela AUP da EDUROAM, não pode fazer roaming. Tem é de ser configurado no ficheiro users para ter VLAN e nas estatísticas para não contar como domínios de roaming.
com ligações EAP, não é recomendado fazer load-balancing, daí a configuração de fail-over. Já vimos referências ao uso de keyed-balance, mas ainda não o conseguimos colocar a trabalhar com sucesso.

Logs detalhados

O FreeRadius nesta corrente configuração, está configurado para criar logs detalhados das diversas fases transacções de autenticação, para as processar no fim do mês, de forma a possibilitar à FCCN recolher dados estatisticos.

Estes logs são guardados no directório a seguir descrito. Consulte o capitulo de Resolução de Problemas para descrição do formato deste directório.

/var/log/freeradius/radacct

Para os logs detalhados configurados a seguir em vários locais funcionarem, tem de se criar o directório que os vai alojar:

Portanto, faça-se:

mkdir -p /var/log/freeradius/radacct

chown -R freerad.freerad /var/log/freeradius

chmod 755 /var/log/freeradius/radacct

Mesmo que se decida não usar o detail, nomeadamente por usar possívelmente de futuro uma alternativa às estatísticas, convém criar este directório já que em caso de necessidade de debugging, ele já estará lá. As permissões tem de ser freerad.freerad o daemon freeradius escrever no directório.

Ligação ao MySQL

O FreeRADIUS tem a possibilidade de fazer trabalhar com bases de dados, sendo que desta forma, torna-se mais fácil consultar o histórico dos logins efectuados.

No nosso caso, seleccionamos o MySQL.

Poderão ser criadas várias tabelas nesta modalidade, no entanto para logging e accounting, só são usadas as tabelas radacct e radpostauth. Usamos também uma tabela criada por nós, banned_list para cumprir a exigência da confederação EDUROAM de ter capacidade de banir MACs de máquinas /utilizadores.

Do lado do servidor MySQL, faz-se:

```
create database radius;
grant all on radius.* to radius@radius.iscte.pt identified by "xxxxxxxxx";
flush privileges;
```

Em seguida para popular a BD radius, há que correr um script em SQL presente no servidor:

(sql remoto)

```
mysql -u root -p radius --host=mysql.local < /etc/freeradius/sql/mysql/schema.sql # (v2.x)
mysql -u root -p radius --host=mysql.local < /etc/freeradius/mods-config/sql/main/mysql/schema.sql # (v3.x)
```

(sql local)

```
mysql -u root -p radius  < /etc/freeradius/sql/mysql/schema.sql # (v2.x)
mysql -u root -p radius  < /etc/freeradius/mods-config/sql/main/mysql/schema.sql # (v3.x)
```

Caso tenha problemas com o schema.sql, as instruções de criação são as seguintes (v2.x):

```
CREATE TABLE radacct (
radacctid bigint(21) NOT NULL auto_increment,
acctsessionid varchar(64) NOT NULL default '',
acctuniqueid varchar(32) NOT NULL default '',
username varchar(64) NOT NULL default '',
groupname varchar(64) NOT NULL default '',
realm varchar(64) default '',
nasipaddress varchar(15) NOT NULL default '',
nasportid varchar(15) default NULL,
nasporttype varchar(32) default NULL,
acctstarttime datetime NULL default NULL,
acctstoptime datetime NULL default NULL,
acctsessiontime int(12) default NULL,
acctauthentic varchar(32) default NULL,
connectinfo_start varchar(50) default NULL,
connectinfo_stop varchar(50) default NULL,
acctinputoctets bigint(20) default NULL,
acctoutputoctets bigint(20) default NULL,
calledstationid varchar(50) NOT NULL default '',
callingstationid varchar(50) NOT NULL default '',
acctterminatecause varchar(32) NOT NULL default '',
servicetype varchar(32) default NULL,
framedprotocol varchar(32) default NULL,
framedipaddress varchar(15) NOT NULL default '',
acctstartdelay int(12) default NULL,
acctstopdelay int(12) default NULL,
xascendsessionsvrkey varchar(10) default NULL,
PRIMARY KEY (radacctid),
KEY username (username),
KEY framedipaddress (framedipaddress),
KEY acctsessionid (acctsessionid),
KEY acctsessiontime (acctsessiontime),
KEY acctuniqueid (acctuniqueid),
KEY acctstarttime (acctstarttime),
KEY acctstoptime (acctstoptime),
KEY nasipaddress (nasipaddress)
) ;
```

v3.x

```
CREATE TABLE radacct (
  radacctid bigint(21) NOT NULL auto_increment,
  acctsessionid varchar(64) NOT NULL default '',
  acctuniqueid varchar(32) NOT NULL default '',
  username varchar(64) NOT NULL default '',
  groupname varchar(64) NOT NULL default '',
  realm varchar(64) default '',
  nasipaddress varchar(15) NOT NULL default '',
  nasportid varchar(50) default NULL,
  nasporttype varchar(32) default NULL,
  acctstarttime datetime NULL default NULL,
  acctupdatetime datetime NULL default NULL,
  acctstoptime datetime NULL default NULL,
  acctinterval int(12) default NULL,
  acctsessiontime int(12) unsigned default NULL,
  acctauthentic varchar(32) default NULL,
  connectinfo_start varchar(50) default NULL,
  connectinfo_stop varchar(50) default NULL,
  acctinputoctets bigint(20) default NULL,
  acctoutputoctets bigint(20) default NULL,
  calledstationid varchar(50) NOT NULL default '',
  callingstationid varchar(50) NOT NULL default '',
  acctterminatecause varchar(32) NOT NULL default '',
  servicetype varchar(32) default NULL,
  framedprotocol varchar(32) default NULL,
  framedipaddress varchar(15) NOT NULL default '',
  PRIMARY KEY (radacctid),
  UNIQUE KEY acctuniqueid (acctuniqueid),
  KEY username (username),
  KEY framedipaddress (framedipaddress),
  KEY acctsessionid (acctsessionid),
  KEY acctsessiontime (acctsessiontime),
  KEY acctstarttime (acctstarttime),
  KEY acctinterval (acctinterval),
  KEY acctstoptime (acctstoptime),
  KEY nasipaddress (nasipaddress)
) ENGINE = INNODB;


CREATE TABLE radpostauth (
  id int(11) NOT NULL auto_increment,
  username varchar(64) NOT NULL default '',
  pass varchar(64) NOT NULL default '',
  reply varchar(32) NOT NULL default '',
  authdate timestamp NOT NULL,
  PRIMARY KEY  (id)
) ENGINE = INNODB;
```

Como optimização para ambientes de largo uso, pode também fazer-se partitioning das tabelas. Atenção que isso tem consequências ao nivel dos queries, entre os quais se necessitar de usar ORDER BY para ter resultados de queries ordenados por id ou no tempo (o comportamento por defeito sem o partitioning). Outra das optimizações que se pode fazer em innoDB é usar a directiva innodb_file_per_table=1 na secção [mysqld] do ficheiro my.cnf, para criar um ficheiro por cada tabela.

```
use radius
ALTER TABLE radacct PARTITION BY HASH(radacctid) PARTITIONS 32;
ALTER TABLE radpostauth PARTITION BY HASH(id) PARTITIONS 32;
```

O que é partitioning: http://dev.mysql.com/tech-resources/articles/partitioning.html

Para mais optimizações do MySQL, corra o Tunning Primer script https://launchpad.net/mysql-tuning-primer/ e em http://mysqltuner.com

Do lado do freeRADIUS, é necessário editar vários ficheiros para activar esta configuração. Nos ficheiros anteriormente revistos, esta opção já foi activada quando possível. No caso de se não optar por esta configuração, todos as directivas "sql" activadas nos ficheiros anteriores terão de ser comentadas.

Sendo assim, tem-se de definir qual o endereço do servidor, a BD, o login e a password a usar.

das tabelas criadas pelo schema.sql, a corrente configuração só usa a radacct e a radpostauth.
na directiva server, deve-se indicar o IP do servidor MySQL e não o nome. Os pedidos de DNS caso se indique o nome são frequentes.

/etc/freeradius/sql.conf (v2.x)

/etc/freeradius/sql.conf

```
sql {
database = "mysql"
server = "10.10.1.2" # (mysql.local)
login = "radius"
password = "xxxxxxxxx"
radius_db = "radius"

...
num_sql_socks = 50
...
```

/etc/freeradius/mods-available/sql (v3.x)

/etc/freeradius/mods-available/sql

```
# -*- text -*-
##
## sql.conf -- SQL modules
##

sql {
        driver = "rlm_sql_mysql"


        # The dialect of SQL you want to use, this should usually match
        # the driver you selected above.
        #
        # If you're using rlm_sql_null, then it should be the type of
        # database the logged queries are going to be executed against.
        dialect = "mysql"


        # Connection info:
        #
        server = "10.10.1.2"
        port = 3306
        login = "radius"
        password = "xxxxxx"

        # Database table configuration for everything except Oracle
        radius_db = "radius"


        acct_table1 = "radacct"
        acct_table2 = "radacct"


        # Allow for storing data after authentication
        postauth_table = "radpostauth"
```

```
# Remove stale session if checkrad does not see a double login
delete_stale_sessions = yes

#  As of version 3.0, the "pool" section has replaced the
#  following configuration items:
#
#  num_sql_socks
#  connect_failure_retry_delay
#  lifetime
#  max_queries


#
#  The connection pool is new for 3.0, and will be used in many
#  modules, for all kinds of connection-related activity.
#
# When the server is not threaded, the connection pool
# limits are ignored, and only one connection is used.
#
pool {
        # Number of connections to start
        start = 5

        # Minimum number of connections to keep open
        min = 4


        # Maximum number of connections
        #
        # If these connections are all in use and a new one
        # is requested, the request will NOT get a connection.
        #
        # Setting 'max' to LESS than the number of threads means
        # that some threads may starve, and you will see errors
        # like "No connections available and at max connection limit"
        #
        # Setting 'max' to MORE than the number of threads means
        # that there are more connections than necessary.
        #
        max = ${thread[pool].max_servers}

        # Spare connections to be left idle
        #
        # NOTE: Idle connections WILL be closed if "idle_timeout"
        # is set.
        spare = 20
        # Number of uses before the connection is closed
        # 0 means "infinite"
        uses = 0

        # The lifetime (in seconds) of the connection
        lifetime = 0

        # idle timeout (in seconds).  A connection which is
        # unused for this length of time will be closed.
        idle_timeout = 0

        # NOTE: All configuration settings are enforced.  If a
        # connection is closed because of "idle_timeout",
        # "uses", or "lifetime", then the total number of
        # connections MAY fall below "min".  When that
        # happens, it will open a new connection.  It will
        # also log a WARNING message.
        #
        # The solution is to either lower the "min" connections,
        # or increase lifetime/idle_timeout.

}
```

```
        # Read database-specific queries
        $INCLUDE ${modconfdir}/${.:name}/main/${dialect}/queries.conf
}
```

/etc/freeradius/radiusd.conf

Em seguida, aumentam-se também o número de pedidos e remove-se o comentário da directiva no ficheiro principal de configuração que vai incluir as configurações do ficheiro anterior. O max_servers tem de ser idêntico ao num_sql_socks, já que é criado um socket por thread.

/etc/freeradius/radiusd.conf
max_requests = 10024 **max_servers = 50** **$INCLUDE sql.conf**

A partir da v2.2.4, o servidor freeradius faz uma verificação da versão da libssl devido ao heartbleed. No entanto, como a Debian faz patching sem alterar versões, esta verificação não está correcta, pelo que nos obriga a incluir no radiusd.conf a directiva seguinte para arrancar o serviço.

security {

allow_vulnerable_openssl = yes

}
A partir da versão 3.0.6 é também necessário incluir **correct_escapes = true** para processar os filtros regexp.

/etc/freeradius/modules/sql_log (v2.x)

No ficheiro de configuração sql_log, é também configurado a possibilidade de usar caracteres em codepage UTF-8. Na v3, é só activar o utf8 em mods-enabled

/etc/freeradius/modules/sql_log

```
sql_log {
        path = "${radacctdir}/sql-relay"
        acct_table = "radacct"
        postauth_table = "radpostauth"
        sql_user_name = "%{%{User-Name}:-DEFAULT}"

        #
        #  Setting this to "yes" will allow UTF-8 characters to be
        #  written to the log file.  Otherwise, they are escaped
        #  as being potentially invalid.
        #
        utf8 = yes

        Start = "INSERT INTO ${acct_table} (AcctSessionId, UserName, \
         NASIPAddress, FramedIPAddress, AcctStartTime, AcctStopTime, \
         AcctSessionTime, AcctTerminateCause) VALUES                 \
         ('%{Acct-Session-Id}', '%{User-Name}', '%{NAS-IP-Address}', \
         '%{Framed-IP-Address}', '%S', '0', '0', '');"
        Stop = "INSERT INTO ${acct_table} (AcctSessionId, UserName,  \
         NASIPAddress, FramedIPAddress, AcctStartTime, AcctStopTime, \
         AcctSessionTime, AcctTerminateCause) VALUES                 \
         ('%{Acct-Session-Id}', '%{User-Name}', '%{NAS-IP-Address}', \
         '%{Framed-IP-Address}', '0', '%S', '%{Acct-Session-Time}',  \
         '%{Acct-Terminate-Cause}');"
        Alive = "INSERT INTO ${acct_table} (AcctSessionId, UserName, \
         NASIPAddress, FramedIPAddress, AcctStartTime, AcctStopTime, \
         AcctSessionTime, AcctTerminateCause) VALUES                 \
         ('%{Acct-Session-Id}', '%{User-Name}', '%{NAS-IP-Address}', \
         '%{Framed-IP-Address}', '0', '0', '%{Acct-Session-Time}','');"

        Post-Auth = "INSERT INTO ${postauth_table}                   \
         (username, pass, reply, authdate) VALUES                    \
         ('%{User-Name}', '%{User-Password:-Chap-Password}',         \
         '%{reply:Packet-Type}', '%S');"
}
```

Lista negra de utilizadores

A AUP da EDUROAM define que a instituição tem de ter mecanismos para bloquear utilizadores. À partida, implementar uma lista para este efeito do lado do servidor RADIUS tem as suas limitações. Nomeadamente, a AUP define que qualquer instituição tem de ter a capacidade de bloquear MACs de equipamento.

Para situações complicadas de ataques de serviço, faz mais sentido bloquear MACs nos próprios APs que sobrecarregar os APs e RADIUS com pedidos de autenticação, mesmo que estes não sejam autorizados. O bloqueio de MACs também não é das melhores formas de bloquear equipamento, devido a diversos factores, entre os quais não é a alheio a facilidade em fazer spoofing de MACs.

Quanto a bloquear utilizadores, também não é uma questão linear. Apenas se consegue bloquear utilizadores eficientemente no túnel interior, sendo que no externo, o utilizador pode perfeitamente colocar outro utilizador. Ao nível da instituição mãe, poderá também fazer mais sentido retirar o utilizador de grupos que lhe permitam usar a EDUROAM de que o colocar numa lista negra local. No entanto, tal hipótese não estará colocada de lado, quer por a vertente transitória da acção, quer em virtude de configurações locais a isso nos forçarem.

/etc/freeradius/policy.conf (v2.x)

/etc/freeradius/policy.conf

```
policy {
.......
local_blacklist {
        # Reject Calling-Station-Id-less authentications
        if (!(Calling-Station-Id)) {
          update reply {
            Reply-Message := "No Calling-Station-Id"
          }
          reject
        }

        if (!(User-Name)) {
          update reply {
            Reply-Message := "No User-Name"
          }
          reject
        }
        filter_username
        if (Calling-Station-Id =~ /([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})/i){
          update request {
            Calling-Station-Id := "%{toupper:%{1}:%{2}:%{3}:%{4}:%{5}:%{6}}"
          }
        }
        else {
          noop
        }
        if ( "%{sql: SELECT count(*) FROM banned_list WHERE mac_address = '%{Calling-Station-Id}' or username = LOWER('%{User-Name}') }" != 0 ) {
          update reply {
            Reply-Message = "quarantined, contact ISCTE"
          }
        reject
        }
}
}
```

/etc/freeradius/policy.d/local_blacklist (v3.x)

/etc/freeradius/policy.d/local_blacklist

```
local_blacklist {
        # Reject Calling-Station-Id-less authentications
        if (!(Calling-Station-Id)) {
          update reply {
            Reply-Message := "No Calling-Station-Id"
          }
          reject
        }

        if (!(User-Name)) {
          update reply {
            Reply-Message := "No User-Name"
          }
          reject
        }
        filter_username
        if (Calling-Station-Id =~ /([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})/i){
          update request {
            Calling-Station-Id := "%{toupper:%{1}:%{2}:%{3}:%{4}:%{5}:%{6}}"
          }
  updated
        }
        else {
          noop
        }
#         if ( "%{sql: SELECT count(*) FROM banned_list WHERE mac_address = '%{Calling-Station-Id}' or username = LOWER('%{User-Name}') }" != 0 ) {
#           update reply {
#             Reply-Message = "quarantined, contact ISCTE"
#           }
#         reject
#         }
}
```

Para criar uma BD de utilizadores banidos:

```
create TABLE banned_list (
id int auto_increment,
mac_address varchar(50) NOT NULL default '',
username varchar(64) NOT NULL default '',
PRIMARY KEY (id)
);
```

Nota: os mac_address tem de usar apenas letras maiúsculas, e o username letras minúsculas.

Para inserir um utilizador/equipamento na lista:

```
use radius
insert into banned_list (mac_address, username) values ("60:C5:47:8B:FF:44", "rffro@iscte.pt");
Query OK, 1 row affected (0.00 sec)
```

Para retirar um utilizador/equipamento da lista:

```
use radius
delete from banned_list where username="rffro@iscte.pt";
```

O acesso a esta tabela é feito no domínio default/outer tunnel no bloco authorize, com a instrução i**f ("%{sql: SELECT count(*) FROM banned_list WHERE mac_address = '%{Calling-Station-Id}' or username=LOWER('%{User-Name}') }" != 0)**

Socket de controlo

Ao nível do freeradius, pode-se também configurar um control socket para controlar directamente diversas operações e fazer debugging com o comando radmin, e um script wrapper do radmin, o raddebug.

Para tal fazer:

```
#cd /etc/freeradius/sites-enabled
#ln -s ../sites-available/control-socket
#addgroup radius
#adduser root radius
```

editar o ficheiro control-socket e modificar:

/etc/freeradius/sites-enabled/control-socket

/etc/freeradius/sites-enabled/control/socket

```
listen {
type = control
socket = ${run_dir}/${name}.sock
gid = radius
mode = rw
}
```

Embora o ficheiro diga que esta funcionalidade é experimental, já deixou de o ser há muito tempo. O grupo radius tem de ser diferente do grupo freerad, por uma questão de segurança, e o socket de controle não ficar desprotegido no caso do serviço ser comprometido remotamente.

Arranque do serviço

No final do serviço estar configurado pode arrancar com o comando:

```
service freeradius start
```

Caso o serviço esteja a correr, usa-se:

```
service freeradius restart
```

Se o serviço der erros ou não funcionar como o esperado, será melhor ver na secção de Resolução de Problemas como arrancar com o freeRADIUS em modo de debug.

Paragem do serviço

E para o parar:

```
service freeradius stop
```

em versões mais antigas de Debian o comando service não era suportado, e era necessário fazer /etc/init.d/freeradius start

Se parar o serviço com o monit e/ou o script de recuperação de serviço operacional, o serviço arranca de novo. Para o parar de vez, é necessário comentar no crontab a chamada ao recover.sh e fazer:

```
service monit stop
service freeradius stop
```

Setup do serviço no arranque

Em principio, os pacotes de Debian ao instalar o freeradius, colocaram-no no arranque.

Para verificar isso basta fazer:

```
#chkconfig freeradius
freeradius  on
```

Caso isso não tenha acontecido, ou se esteja a compilar à mão:

```
chkconfig freeradius on
```

Certificado digital

O protocolo TTLS usa um certificado X.509 do lado do servidor para codificar as comunicações.

A primeira vez que o freeradius é levantado em Debian, este cria imediatamente um certificado com assinatura privada.

Para mudar a palavra chave e os dados com que o certificado aparece, é recomendável mudar a descrição do mesmo e a password por defeito que vem com o Debian.

Para tal, é necessário editar o ficheiro /usr/share/doc/freeradius/examples/certs/server.cnf e mudar os seguintes parâmetros.

/usr/share/doc/freeradius/examples/certs/server.cnf

Configuração de CA em Debian 7.

/usr/share/doc/freeradius/examples/certs/server.cnf

```
HOME                    = .
RANDFILE                = $ENV::HOME/.rnd


# Extra OBJECT IDENTIFIER info:
#oid_file               = $ENV::HOME/.oid
oid_section             = new_oids


# To use this configuration file with the "-extfile" option of the
# "openssl x509" utility, name here the section containing the
# X.509v3 extensions to use:
# extensions            =
# (Alternatively, use a configuration file that has only
# X.509v3 extensions in its main [= default] section.)

[ new_oids ]

# We can add new OIDs in here for use by 'ca', 'req' and 'ts'.

# Add a simple OID like this:

# testoid1=1.2.3.4

# Or use config file substitution like this:

# testoid2=${testoid1}.5.6



# Policies used by the TSA examples.

tsa_policy1 = 1.2.3.4.1

tsa_policy2 = 1.2.3.4.5.6

tsa_policy3 = 1.2.3.4.5.7



####################################################################

[ ca ]

default_ca      = CA_default            # The default ca section



####################################################################

[ CA_default ]
```

```
dir               = ./demoCA               # Where everything is kept
certs               = $dir/certs               # Where the issued certs are kept
crl_dir               = $dir/crl               # Where the issued crl are kept
database        = $dir/index.txt        # database index file.
#unique_subject        = no                        # Set to 'no' to allow creation of
                                        # several ctificates with same subject.
new_certs_dir        = $dir/newcerts                # default place for new certs.


certificate        = $dir/cacert.pem         # The CA certificate
serial                = $dir/serial                # The current serial number
crlnumber        = $dir/crlnumber        # the current crl number
                                        # must be commented out to leave a V1 CRL
crl               = $dir/crl.pem                # The current CRL
private_key        = $dir/private/cakey.pem# The private key
RANDFILE        = $dir/private/.rand        # private random number file


x509_extensions        = usr_cert               # The extentions to add to the cert


# Comment out the following two lines for the "traditional"
# (and highly broken) format.
name_opt         = ca_default               # Subject Name options
cert_opt         = ca_default               # Certificate field options


# Extension copying option: use with caution.
# copy_extensions = copy


# Extensions to add to a CRL. Note: Netscape communicator chokes on V2 CRLs
# so this is commented out by default to leave a V1 CRL.
# crlnumber must also be commented out to leave a V1 CRL.
# crl_extensions        = crl_ext
```

```
default_days        = 365                       # how long to certify for
default_crl_days= 30                        # how long before next CRL
default_md        = default                # use public key default MD
preserve        = no                        # keep passed DN ordering


# A few difference way of specifying how similar the request should look
# For type CA, the listed attributes must be the same, and the optional
# and supplied fields are just that :-)
policy                = policy_match


# For the CA policy
[ policy_match ]
countryName                = match
stateOrProvinceName        = match
organizationName        = match
organizationalUnitName        = optional
commonName                = supplied
emailAddress                = optional


# For the 'anything' policy
# At this point in time, you must list all acceptable 'object'
# types.
[ policy_anything ]
countryName                = optional
stateOrProvinceName        = optional
localityName                = optional
organizationName        = optional
organizationalUnitName        = optional
commonName                = supplied
emailAddress                = optional


####################################################################
[ req ]
default_bits                = 2048
```

```
default_keyfile         = privkey.pem
distinguished_name        = req_distinguished_name
attributes                = req_attributes
x509_extensions        = v3_ca        # The extentions to add to the self signed cert


# Passwords for private keys if not present they will be prompted for
# input_password = secret
# output_password = secret


# This sets a mask for permitted string types. There are several options.
# default: PrintableString, T61String, BMPString.
# pkix         : PrintableString, BMPString (PKIX recommendation before 2004)
# utf8only: only UTF8Strings (PKIX recommendation after 2004).
# nombstr : PrintableString, T61String (no BMPStrings or UTF8Strings).
# MASK:XXXX a literal mask value.
# WARNING: ancient versions of Netscape crash on BMPStrings or UTF8Strings.
string_mask = utf8only


# req_extensions = v3_req # The extensions to add to a certificate request


[ req_distinguished_name ]
countryName                        = Country Name (2 letter code)
countryName_default                = AU
countryName_min                        = 2
countryName_max                        = 2


stateOrProvinceName                = State or Province Name (full name)
stateOrProvinceName_default        = Some-State


localityName                         = Locality Name (eg, city)


0.organizationName                = Organization Name (eg, company)
```

```
0.organizationName_default        = Internet Widgits Pty Ltd


# we can do this but it is not needed normally :-)
#1.organizationName                = Second Organization Name (eg, company)
#1.organizationName_default        = World Wide Web Pty Ltd


organizationalUnitName                = Organizational Unit Name (eg, section)
#organizationalUnitName_default        =


commonName                          = Common Name (e.g. server FQDN or YOUR name)
commonName_max                          = 64


emailAddress                          = Email Address
emailAddress_max                = 64


# SET-ex3                          = SET extension number 3


[ req_attributes ]
challengePassword                = A challenge password
challengePassword_min                = 4
challengePassword_max                = 20


unstructuredName                = An optional company name


[ usr_cert ]


# These extensions are added when 'ca' signs a request.


# This goes against PKIX guidelines but some CAs do it and some software
# requires this to avoid interpreting an end user certificate as a CA.
```

```
basicConstraints=CA:FALSE

# Here are some examples of the usage of nsCertType. If it is omitted
# the certificate can be used for anything *except* object signing.

# This is OK for an SSL server.
# nsCertType                        = server

# For an object signing certificate this would be used.
# nsCertType = objsign

# For normal client use this is typical
# nsCertType = client, email

# and for everything including object signing:
# nsCertType = client, email, objsign

# This is typical in keyUsage for a client certificate.
# keyUsage = nonRepudiation, digitalSignature, keyEncipherment

# This will be displayed in Netscape's comment listbox.
nsComment                         = "OpenSSL Generated Certificate"

# PKIX recommendations harmless if included in all certificates.
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer

# This stuff is for subjectAltName and issuerAltname.
# Import the email address.
# subjectAltName=email:copy
```

```
# An alternative to produce certificates that aren't

# deprecated according to PKIX.

# subjectAltName=email:move



# Copy subject details

# issuerAltName=issuer:copy



#nsCaRevocationUrl                = http://www.domain.dom/ca-crl.pem

#nsBaseUrl

#nsRevocationUrl

#nsRenewalUrl

#nsCaPolicyUrl

#nsSslServerName



# This is required for TSA certificates.

# extendedKeyUsage = critical,timeStamping



[ v3_req ]



# Extensions to add to a certificate request



basicConstraints = CA:FALSE

keyUsage = nonRepudiation, digitalSignature, keyEncipherment



[ v3_ca ]







# Extensions for a typical CA
```

```
# PKIX recommendation.


subjectKeyIdentifier=hash


authorityKeyIdentifier=keyid:always,issuer


# This is what PKIX recommends but some broken software chokes on critical
# extensions.
#basicConstraints = critical,CA:true
# So we do this instead.
basicConstraints = CA:true


# Key usage: this is typical for a CA certificate. However since it will
# prevent it being used as an test self-signed certificate it is best
# left out by default.
# keyUsage = cRLSign, keyCertSign


# Some might want this also
# nsCertType = sslCA, emailCA


# Include email address in subject alt name: another PKIX recommendation
# subjectAltName=email:copy
# Copy issuer details
# issuerAltName=issuer:copy


# DER hex encoding of an extension: beware experts only!
# obj=DER:02:03
# Where 'obj' is a standard or added object
# You can even override a supported extension:
# basicConstraints= critical, DER:30:03:01:01:FF
```

```
[ crl_ext ]

# CRL extensions.
# Only issuerAltName and authorityKeyIdentifier make any sense in a CRL.

# issuerAltName=issuer:copy
authorityKeyIdentifier=keyid:always

[ proxy_cert_ext ]
# These extensions should be added when creating a proxy certificate

# This goes against PKIX guidelines but some CAs do it and some software
# requires this to avoid interpreting an end user certificate as a CA.

basicConstraints=CA:FALSE

# Here are some examples of the usage of nsCertType. If it is omitted
# the certificate can be used for anything *except* object signing.

# This is OK for an SSL server.
# nsCertType                        = server

# For an object signing certificate this would be used.
# nsCertType = objsign

# For normal client use this is typical
# nsCertType = client, email

# and for everything including object signing:
# nsCertType = client, email, objsign
```

```
# This is typical in keyUsage for a client certificate.
# keyUsage = nonRepudiation, digitalSignature, keyEncipherment

# This will be displayed in Netscape's comment listbox.
nsComment                       = "OpenSSL Generated Certificate"

# PKIX recommendations harmless if included in all certificates.
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer

# This stuff is for subjectAltName and issuerAltname.
# Import the email address.
# subjectAltName=email:copy
# An alternative to produce certificates that aren't
# deprecated according to PKIX.
# subjectAltName=email:move

# Copy subject details
# issuerAltName=issuer:copy

#nsCaRevocationUrl                = http://www.domain.dom/ca-crl.pem
#nsBaseUrl
#nsRevocationUrl
#nsRenewalUrl
#nsCaPolicyUrl
#nsSslServerName

# This really needs to be in place for it to be a proxy certificate.
proxyCertInfo=critical,language:id-ppl-anyLanguage,pathlen:3,policy:foo

####################################################################
```

```
[ tsa ]


default_tsa = tsa_config1        # the default TSA section


[ tsa_config1 ]


# These are used by the TSA reply generation only.
dir                = ./demoCA                # TSA root directory
serial                = $dir/tsaserial        # The current serial number (mandatory)
crypto_device        = builtin                # OpenSSL engine to use for signing
signer_cert        = $dir/tsacert.pem         # The TSA signing certificate
                                        # (optional)
certs                = $dir/cacert.pem        # Certificate chain to include in reply
                                        # (optional)
signer_key        = $dir/private/tsakey.pem # The TSA private key (optional)


default_policy        = tsa_policy1                # Policy if request did not specify it
                                        # (optional)
other_policies        = tsa_policy2, tsa_policy3        # acceptable policies (optional)
digests                = md5, sha1                # Acceptable message digests (mandatory)
accuracy        = secs:1, millisecs:500, microsecs:100        # (optional)
clock_precision_digits  = 0        # number of digits after dot. (optional)
ordering                = yes        # Is ordering defined for timestamps?
                                # (optional, default: no)
tsa_name                = yes        # Must the TSA name be included in the reply?
                                # (optional, default: no)
ess_cert_id_chain        = no        # Must the ESS cert id chain be included?
                                # (optional, default: no)
```

Para criar o novo certificado, fazer:

```
cd  /usr/share/doc/freeradius/examples/certs
aptitude install make
make
```

em seguida, ou fazer:

```
mv /etc/freeradius/certs /etc/freeradius/cert.orig
cd /etc/freeradius/
 ln -s /usr/share/doc/freeradius/examples/certs certs
```

ou fazer em vez disso:

```
cp ca.pem dh  server.key server.pem /etc/freeradius/certs
```

ou então em vez das duas operações anteriores, mudar as directivas certdir e cadir no /etc/freeradius/eap.conf para apontar para os ficheiros correntes.

No final, fazer restart com o comando /etc/init.d/freeradius restart ou service freeradius restart

É preciso ter atenção ao algoritmo das Digest Messages/hashing. Embora certificados públicos hoje em dia venham (quase) todos com SHA-2, o openssl pode por defeito estar configurado para outro algoritmo ao gerar certificados privados. O dispositivos Apple a partir do iOS 5 não suportam MD5. Correntemente se os certificados não forem pelo menos SHA-1, não são aceites. A Microsoft também não aceita qualquer certificado SHA-1 como cliente a partir de 1 de Janeiro de 2017. Para quem esteja também a gerar certificados numa CA Microsoft, os servidores SHA-1 não são suportados em CAs a partir de 1 de Janeiro de 2016.

Criação de certificado

Para criar sem ser por os scripts dos FreeRadius, ou certificado públicos, há que o gerar ou no Certificate Server da Microsoft como web server, ou no openssl com as seguintes propriedades para ser aceite por estações de trabalho Windows:

Certificado do servidor RADIUS

```
[ xpserver_ext]
extendedKeyUsage = 1.3.6.1.5.5.7.3.1
```

OID 1.3.6.1.5.5.7.3.1 = serverAuth / TLS Web Server Authentication - Indicates that a certificate can be used as an SSL server certificate.

Certificados de cliente

Os certificados para autenticar clientes, que são usados em configurações com EAP-TLS ou EAP-TTLS autenticadas por certificado, e não por password tem de ter estes atributos. Apenas incluímos isto neste documento por uma questão de completar a documentação, já que não usamos certificados para autenticar clientes.

```
[ xpclient_ext]
extendedKeyUsage = 1.3.6.1.5.5.7.3.2
```

Se pretender autenticação a máquina e não o utilizador, a extensão é:

```
[ xpclient_ext]
extendedKeyUsage = 1.3.6.1.4.1.311.17.2
```

OID 1.3.6.1.5.5.7.3.2 = clientAuth / TLS Web Client Authentication - Indicates that a certificate can be used as an SSL client certificate.

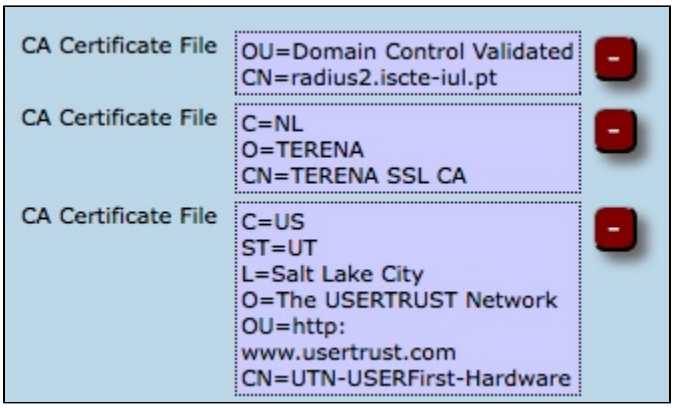
OID 1.3.6.1.4.1.311.17.2 = LocalKeySet

Note-se que se pretender ter autenticação do lado do cliente por certificado, é aconselhado usar um certificado assinado numa CA privada.

Tem-se em seguida de criar um csr do pedido, e solicitar o certificado.

Depois deste passo, tem-se de transformar quer o certificado da CA, quer o certificado obtido a partir do pedido csr, em formato PEM.

Para mais considerações se um certificado publico ou privado, consultar este endereço: https://confluence.terena.org/display/H2eduroam/EAP+Server+Certificate+considerations



Estrutura de certificado server.pem que usamos.

Pistas para criação de certificado em Windows. https://confluence.fccn.pt/display/tcs/SO%27s+Windows

Instalação do certificado root no servidor

Uma vez que o certificado entregue pela TERENA é um certificado intermédio, recomenda-se também instalar certificado root no Linux/Debian, já que o debian 7 e 8 não o trazem. Para tal colocamos o ficheiro TERENA_SSL_CA.pem http://www.terena.org/activities/tcs/repository/ em /etc/ssl/certs.

Construimos também o ficheiro /etc/freeradius/certs/ca.pem. Para tal colocamos neste ficheiro a cadeia de certificados AddTrust External CA Root+ UTN-USERFirst-Hardware+TERENA SSL CA .

Estes certificados/ficheiros estão em http://www.terena.org/activities/tcs/repository/ debaixo de Server Certificate, e é necessário ter em atenção que de acordo com o certificado do servidor ser SHA-1 ou SHA-2, é preciso também o cuidado de ser realizado o download dos pem aqui descritos assinados com o protocolo correspondente (i.e. existem dois conjuntos diferentes, um para SHA-1, e outro mais recente para SHA-2).

Como exemplo para criar o ca.pem em SHA-2:

```
curl -k https://www.terena.org/activities/tcs/repository/AddTrust_External_CA_Root.pem > /etc/freeradius/certs
/ca.pem
curl -k https://www.terena.org/activities/tcs/repository/sha2/USERtrust_RSA_Certification_Authority.pem >> /etc
/freeradius/certs/ca.pem
curl -k https://www.terena.org/activities/tcs/repository/sha2/TERENA_SSL_CA_2.pem >> /etc/freeradius/certs/ca.
pem
```

Ao fazer a renovação de um certificado antigo, o mais certo é ester ter passado de SHA-1 para SHA-2, e é necessário renovar também o ficheiro ca.pem. Também poderão ter de ser mudados certificados no CAT.

Problemas conhecidos

De momento, existem dois problemas conhecidos neste setup em especial:

- a construção do certificado com a chain toda de trust, já descrita;
- a desinstalação por vezes deixar algumas linhas residuais no /var/lib/dpkg/statoverride que dá problemas ao tentar reinstalar;
- em Debian 7, com o pacote de base freeradius 2.1.x, a paragem de tempos a tempos de autenticação de users em AD locais;
- crashes do serviço também com pacotes 2.1.x.

Estas últimas duas razões são o fundamento de recomendarmos construir os pacotes deb.

/etc/logrotate.d/freeradius

Se foi instalada a versão de freeradius.org, não se recomenda fazer esta alteração. Apenas será feita por quem não se sentir confortável em compilar código, e tenha mantido a versão stock 2.1.12 do Debian 7.

Em relação a este último bug da versão 2.1.12 presente no Debian 7, este já é conhecido, e já corrigido na versão 2.2.x, e deve-se a o HUP do daemon freeradius de tempos a tempos colocar fora de serviço o modulo mschap.

A forma de tornear isto, é além de colocar o nosso script de testes de serviço, a que chamamos recover.sh e descrevemos mais à frente, é modificar a rotação de logs (logrotate) para fazer restart ao serviço em vez de reload.

Sendo assim, a alteração é a seguinte:

/etc/logrotate.d/freeradius

```
/var/log/freeradius/*.log {
        weekly
        rotate 52
        compress
        delaycompress
        notifempty
        missingok
        postrotate
                /etc/init.d/freeradius restart > /dev/null
        endscript
}
```

Em Debian, por defeito, o logrotate é realizado por volta das 6.30AM.

Problema de reinstalação/erro de statoverride

Aquando da reinstalação de freeradius, por vezes o erro seguinte surge.

```
root@xen3:/home/rui# aptitude install freeradius
The following NEW packages will be installed:
  freeradius freeradius-common{a} freeradius-config{a} libfreeradius3{a}
The following packages are RECOMMENDED but will NOT be installed:
  freeradius-utils
0 packages upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 2,246 kB of archives. After unpacking 5,009 kB will be used.
Do you want to continue? [Y/n/?]
Get: 1 http://debian.srv.rede/local/ iscte/wheezy freeradius-common all 3.1.0+git [263 kB]
Get: 2 http://debian.srv.rede/local/ iscte/wheezy freeradius-config amd64 3.1.0+git [201 kB]
Get: 3 http://debian.srv.rede/local/ iscte/wheezy libfreeradius3 amd64 3.1.0+git [182 kB]
Get: 4 http://debian.srv.rede/local/ iscte/wheezy freeradius amd64 3.1.0+git [1,600 kB]
Fetched 4 B in 0s (51 B/s)
dpkg: unrecoverable fatal error, aborting:
 syntax error: unknown user 'freerad' in statoverride file
E: Sub-process /usr/bin/dpkg returned an error code (2)
A package failed to install.  Trying to recover:
```

De alguma forma, as rotinas de desinstalação do freeradius não limpam este ficheiro, e é necessário apagar as linhas que mencionem o utilizador freerad para continuar a instalação.

Servidor Redundante

Para fazer setup de um servidor redundante, a configuração é idêntica ao aqui exposto, excepto sendo necessário comentar no inner e outer tunnel as directivas de sql. Não é necessário fazer configurações complicadas de cluster. Basta colocar nos APs um segundo servidor RADIUS para autenticação e accounting. Normalmente, quando o primeiro servidor (Free)Radius não trata um pacote, o controlador/AP envia de novo esse pacote para o servidor redundante.

Pode haver fabricantes que não cumpram o reenvio de pacote para o servidor redundante, pelo que se recomenda uma fase de testes desta configuração.

Recomenda-se no entanto, que idealmente estejam em:

- ambientes virtuais diferentes;
- redes diferentes;
- conectados a ADs diferentes;
- e a servidores SQL diferentes (caso se opte por ter SQL no servidor redundante);
- e que tenham versão de FreeRadius diferentes (para por exemplo, se um bug crashar o primário, o secundário ser capaz de satisfazer o pedido).

No nosso caso, o master conecta-se a uma replica da AD, e não faz logging em MySQL. Tivemos também o cuidado de lhe dar exactamente o mesmo certificado, e de no reverso de DNS dar o mesmo nome do RADIUS primário, já que os clientes verificam o certificado e o reverso de DNS. A utilização deste depois de o colocar como segundo servidor RADIUS nos nossos controladores é transparente.

Recomendados vivamente o uso de um servidor redundante para manter a continuidade do serviço.

Pode-se enviar as queries do MySQL à posteriori, fazendo-as offline, no secundário, de forma a não ficar dependentes da disponibilidade do serviço MySQL para este trabalhar.
Notavelmente os clientes Windows não aceitam certificados wildcard no (T)TLS.

RadSec

Aqui descrevemos como fazer setup do RadSec. O RadSec é RADIUS encapsulado em TLS, a porta por defeito é a 2083/TCP e está formalizado no RFC 6614.Toda e qualquer conexão RADIUS tem os dados em claro, e de acordo com as configurações, o RadSec permite que qualquer conectividade do servidor RADIUS pode ser efectuada em TLS como medida de protecção.

Normalmente, as configurações mais comuns são para estabelecer ligações RadSec com os servidores da federação.

O RadSec é implementado directamente na versão 3 do FreeRadius. Para configurar o RadSec na versão 2, é necessário usar o software radsecproxy.

Existe a necessidade de criar certificados de servidor e cliente. Para a fase inicial até poderão ser idênticos aos dos servidor nas duas pontas. Em produção, serão usados os certificados da eduPKI em servidores da infra-estruturas EDUROAM.

Nos ficheiros de configuração, na parte de cliente, existe também um novo protocolo chamado tls.

Em seguida descrevemos como fazer setup em FreeRadius 3.

Ver apêndice para ver como obter certificados da eduPKI.

/etc/init.d/freeradius/sites-available/tls

```
listen {
    ipaddr = *
    port = 2083
    type = auth+acct

    # For now, only TCP transport is allowed.
    proto = tcp

    # Send packets to the default virtual server
    virtual_server = default
    clients = radsec

    #  This is *exactly* the same configuration as used by the EAP-TLS
    #  module.  It's OK for testing, but for production use it's a good
    #  idea to use different server certificates for EAP and for RADIUS
    #  transport.
    tls {
        #  These are used to simplify later configurations.
        certdir = ${confdir}/radsec
        cadir = ${confdir}/radsec

        private_key_password = whatever
        private_key_file = ${certdir}/server.realm.tld-key.pem

        #  If Private key & Certificate are located in
        #  the same file, then private_key_file &
        #  certificate_file must contain the same file
        #  name.
        #
        #  If CA_file (below) is not used, then the
        #  certificate_file below MUST include not
        #  only the server certificate, but ALSO all
        #  of the CA certificates used to sign the
        #  server certificate.
        certificate_file = ${certdir}/server.realm.tld-eduPKI.pem

        #  Trusted Root CA list
        #
        #  ALL of the CA's in this list will be trusted
        #  to issue client certificates for authentication.
        #
        #  In general, you should use self-signed
        #  certificates for 802.1x (EAP) authentication.
        #  In that case, this CA file should contain
        #  *one* CA certificate.
        #
        #  This parameter is used only for EAP-TLS,
        #  when you issue client certificates.  If you do
        #  not use client certificates, and you do not want
        #  to permit EAP-TLS authentication, then delete
        #  this configuration item.
        CA_file = ${cadir}/eduPKI-CA.crt

        #
        #  For DH cipher suites to work, you have to
        #  run OpenSSL to create the DH file first:
        #
        #   openssl dhparam -out certs/dh 1024
        #
        dh_file = ${certdir}/dh
        random_file = ${certdir}/random

        #
        #  This can never exceed the size of a RADIUS
        #  packet (4096 bytes), and is preferably half
        #  that, to accomodate other attributes in
```

```
#  RADIUS packet.  On most APs the MAX packet
#  length is configured between 1500 - 1600
#  In these cases, fragment size should be
#  1024 or less.
#
fragment_size = 1024

#  include_length is a flag which is
#  by default set to yes If set to
#  yes, Total Length of the message is
#  included in EVERY packet we send.
#  If set to no, Total Length of the
#  message is included ONLY in the
#  First packet of a fragment series.
#
include_length = yes

#  Check the Certificate Revocation List
#
#  1) Copy CA certificates and CRLs to same directory.
#  2) Execute 'c_rehash <CA certs&CRLs Directory>'.
#    'c_rehash' is OpenSSL's command.
#  3) uncomment the line below.
#  5) Restart radiusd
    #   check_crl = yes
    #   CA_path = ${cadir}

   #
   #  If check_cert_issuer is set, the value will
   #  be checked against the DN of the issuer in
   #  the client certificate.  If the values do not
   #  match, the cerficate verification will fail,
   #  rejecting the user.
   #
   #  In 2.1.10 and later, this check can be done
   #  more generally by checking the value of the
   #  TLS-Client-Cert-Issuer attribute.  This check
   #  can be done via any mechanism you choose.
   #
       # this doesnt work yet
   # check_cert_issuer = "/DC=org/DC=edupki/CN=eduPKI"

   #
   #  If check_cert_cn is set, the value will
   #  be xlat'ed and checked against the CN
   #  in the client certificate.  If the values
   #  do not match, the certificate verification
   #  will fail rejecting the user.
   #
   #  This check is done only if the previous
   #  "check_cert_issuer" is not set, or if
   #  the check succeeds.
   #
   #  In 2.1.10 and later, this check can be done
   #  more generally by checking the value of the
   #  TLS-Client-Cert-CN attribute.  This check
   #  can be done via any mechanism you choose.
   #
   #    check_cert_cn = %{User-Name}
   #
       # Set this option to specify the allowed
# TLS cipher suites.  The format is listed
# in "man 1 ciphers".
cipher_list = "DEFAULT"

#

#  This configuration entry should be deleted
#  once the server is running in a normal
#  configuration.  It is here ONLY to make
#  initial deployments easier.
```

```
        #
        #
        #  This is enabled in eap.conf, so we don't need it here.
        #
#       make_cert_command = "${certdir}/bootstrap"

        #
        #  Session resumption / fast reauthentication
        #  cache.
        #
        #  The cache contains the following information:
        #
        #  session Id - unique identifier, managed by SSL
        #  User-Name  - from the Access-Accept
        #  Stripped-User-Name - from the Access-Request
        #  Cached-Session-Policy - from the Access-Accept
        #
        #  The "Cached-Session-Policy" is the name of a
        #  policy which should be applied to the cached
        #  session.  This policy can be used to assign
        #  VLANs, IP addresses, etc.  It serves as a useful
        #  way to re-apply the policy from the original
        #  Access-Accept to the subsequent Access-Accept
        #  for the cached session.
        #
        #  On session resumption, these attributes are
        #  copied from the cache, and placed into the
        #  reply list.
        #
        #  You probably also want "use_tunneled_reply = yes"
        #  when using fast session resumption.
        #
        cache {
              #
              #  Enable it.  The default is "no".
              #  Deleting the entire "cache" subsection
              #  Also disables caching.
              #
              #  You can disallow resumption for a
              #  particular user by adding the following
              #  attribute to the control item list:
              #
              #     Allow-Session-Resumption = No
              #
              #  If "enable = no" below, you CANNOT
              #  enable resumption for just one user
              #  by setting the above attribute to "yes".
              #
              enable = yes

              #
              #  Lifetime of the cached entries, in hours.
              #  The sessions will be deleted after this
              #  time.
              #
              lifetime = 24 # hours

              #
              #  The maximum number of entries in the
              #  cache.  Set to "0" for "infinite".
              #
              #  This could be set to the number of users
              #  who are logged in... which can be a LOT.
              #
              max_entries = 255
        }

        #
        #  Require a client certificate.
        #
        require_client_cert = yes
```

```
        #
        #  As of version 2.1.10, client certificates can be
        #  validated via an external command.  This allows
        #  dynamic CRLs or OCSP to be used.
        #
        #  This configuration is commented out in the
        #  default configuration.  Uncomment it, and configure
        #  the correct paths below to enable it.
        #
        verify {
            #  A temporary directory where the client
            #  certificates are stored.  This directory
            #  MUST be owned by the UID of the server,
            #  and MUST not be accessible by any other
            #  users.  When the server starts, it will do
            #  "chmod go-rwx" on the directory, for
            #  security reasons.  The directory MUST
            #  exist when the server starts.
            #
            #  You should also delete all of the files
            #  in the directory when the server starts.
                tmpdir = /etc/raddb/temporary

            #  The command used to verify the client cert.
            #  We recommend using the OpenSSL command-line
            #  tool.
            #
            #  The ${..CA_path} text is a reference to
            #  the CA_path variable defined above.
            #
            #  The %{TLS-Client-Cert-Filename} is the name
            #  of the temporary file containing the cert
            #  in PEM format.  This file is automatically
            #  deleted by the server when the command
            #  returns.

            # this doesnt work yet either
                #client = "/usr/bin/openssl verify -CAfile /etc/raddb/radsec/eduPKI-CA.crt -purpose crlsign  %
{TLS-Client-Cert-Filename}"
        }
    }
}

clients radsec {
    client 127.0.0.1 {
        ipaddr = 127.0.0.1
        proto = tcp
        secret = testing123
    }
    client cv-radius.fccn.pt {
        ipaddr = 193.136.192.43
        proto = tls
        secret = radsec
    }
        client cv2-radius.fccn.pt {
        ipaddr = 193.136.192.44
        proto = tls
        secret = radsec
       }

}


# local test listener for debug (present by default)
listen {
       ipaddr = 127.0.0.1
       port = 4000
       type = auth
}
```

```
home_server cv-radius-radsec {
    ipaddr 193.136.192.43
    port = 2083
    type = auth
    secret = radsec
    proto = tcp
    status_check = status-server

    tls {
        #
        #  These are used to simplify later configurations.
        #
        certdir = ${confdir}/radsec
        cadir = ${confdir}/radsec

        private_key_password = whatever
        private_key_file = ${certdir}/server.realm.tld-key.pem

        #  If Private key & Certificate are located in
        #  the same file, then private_key_file &
        #  certificate_file must contain the same file
        #  name.
        #
        #  If CA_file (below) is not used, then the
        #  certificate_file below MUST include not
        #  only the server certificate, but ALSO all
        #  of the CA certificates used to sign the
        #  server certificate.
        certificate_file = ${certdir}/server.realm.tld-eduPKI.pem

        #  Trusted Root CA list
        #
        #  ALL of the CA's in this list will be trusted
        #  to issue client certificates for authentication.
        #
        #  In general, you should use self-signed
        #  certificates for 802.1x (EAP) authentication.
        #  In that case, this CA file should contain
        #  *one* CA certificate.
        #
        #  This parameter is used only for EAP-TLS,
        #  when you issue client certificates.  If you do
        #  not use client certificates, and you do not want
        #  to permit EAP-TLS authentication, then delete
        #  this configuration item.
        CA_file = ${cadir}/eduPKI-CA.crt

        #
        #  For DH cipher suites to work, you have to
        #  run OpenSSL to create the DH file first:
        #
        #   openssl dhparam -out certs/dh 1024
        #
        dh_file = ${certdir}/dh
        random_file = ${certdir}/random

        #
        #  This can never exceed the size of a RADIUS
        #  packet (4096 bytes), and is preferably half
        #  that, to accomodate other attributes in
        #  RADIUS packet.  On most APs the MAX packet
        #  length is configured between 1500 - 1600
        #  In these cases, fragment size should be
        #  1024 or less.
        #
        fragment_size = 1024

        #  include_length is a flag which is
        #  by default set to yes If set to
        #  yes, Total Length of the message is
        #  included in EVERY packet we send.
```

```
        #  If set to no, Total Length of the
        #  message is included ONLY in the
        #  First packet of a fragment series.
        #
        include_length = yes

        #  Check the Certificate Revocation List
        #
        #  1) Copy CA certificates and CRLs to same directory.
        #  2) Execute 'c_rehash <CA certs&CRLs Directory>'.
        #    'c_rehash' is OpenSSL's command.
        #  3) uncomment the line below.
        #  5) Restart radiusd
    #   check_crl = yes
#       CA_path = ${cadir}

           #
           #  If check_cert_issuer is set, the value will
           #  be checked against the DN of the issuer in
           #  the client certificate.  If the values do not
           #  match, the cerficate verification will fail,
           #  rejecting the user.
           #
           #  In 2.1.10 and later, this check can be done
           #  more generally by checking the value of the
           #  TLS-Client-Cert-Issuer attribute.  This check
           #  can be done via any mechanism you choose.
           #
    #       check_cert_issuer = "/C=GB/ST=Berkshire/L=Newbury/O=My Company Ltd"

           #
           #  If check_cert_cn is set, the value will
           #  be xlat'ed and checked against the CN
           #  in the client certificate.  If the values
           #  do not match, the certificate verification
           #  will fail rejecting the user.
           #
           #  This check is done only if the previous
           #  "check_cert_issuer" is not set, or if
           #  the check succeeds.
           #
           #  In 2.1.10 and later, this check can be done
           #  more generally by checking the value of the
           #  TLS-Client-Cert-CN attribute.  This check
           #  can be done via any mechanism you choose.
           #
    #   check_cert_cn = %{User-Name}
    #
        # Set this option to specify the allowed
        # TLS cipher suites.  The format is listed
        # in "man 1 ciphers".
        cipher_list = "DEFAULT"
    }

}

#second home server config cleared to the values required for brevity

home_server cv2-radius-radsec {
        ipaddr 193.136.192.44
        port = 2083
        type = auth
        secret = radsec
        proto = tcp
        status_check = status-server

        tls {
                certdir = ${confdir}/radsec
                cadir = ${confdir}/radsec
                private_key_password = whatever
                private_key_file = ${certdir}/server.realm.tld-key.pem
```

```
                certificate_file = ${certdir}/server.realm.tld-eduPKI.pem
                CA_file = ${cadir}/eduPKI-CA.crt
                dh_file = ${certdir}/dh
                random_file = ${certdir}/random
                fragment_size = 1024
                include_length = yes
                cipher_list = "DEFAULT"
        }

home_server_pool CV {
         type = fail-over
         home_server = cv-radius-radsec
         home_server = cv2-radius-radsec
}

realm eduroam {
      auth_pool = CV
}
```

Em seguida:

```
$sudo ln -s /etc/freeradius/sites-enabled/tls
$service freeradius restart
```

Depois do RadSec estar a funcional, o modo normal de debugging não funciona. Isto porque o código TLS necessita de threads para trabalhar.
⚠️
Portanto em substituição de

$ radiusd -X

faz-se:

$ radiusd -fxx -l stdout

Monitorização

Existem vários níveis de monitorização, desde ao nível do:

- host
- portas TCP/IP
- serviço layer 7
- logs syslog
- logs detalhados em /var/log/freeradius/radacct
- logs e accounting em MySQL
- monitorização em real-time e agregados de recolha de estatísticas por parte da federação.

Estatísticas mensais

A FCCN tem também um serviço que recolhe as estatísticas mensais do serviço de todos os intervenientes nacionais na federação.

Para tal, é necessário:

- ter os logs detalhados do FreeRADIUS configurado;
- configurar um servidor de páginas um vhost com nome de DNS a combinar com a FCCN;
- acordar também num utilizador/palavra chave de acesso a este vhost;
- obter o hotstop id, pivot id e nome de hotspot atribuido à instituição pela FCCN;
- fazer download do script stats.1.2.1.zip fornecido pela FCCN na página http://www.fccn.pt/pt/servicos/conectividade-e-infraestrutura/rede-de-mobilidade-e-u-eduroam/documentos/;
- descompactar este ficheiro em /opt/bin/eduroam e fazer um link do directório criado para stats;
- configurar o ficheiro e-U-hotspot.cfg tal como se mostra no exemplo abaixo, adaptado para a instituição;
- colocar o script stats.sh abaixo escrito em /opt/bin/eduroam;

- colocar no crontab a linha seguinte, a correr dia 1 do mês:

```
0 7 1 * * /usr/bin/nice -n 19 /opt/bin/eduroam/stats.sh
0 6 * * * /usr/bin/nice -n 19 /opt/bin/eduroam/gzip_files.sh
```

```
# wget http://www.fccn.pt/fotos/editor2/Eduroam/stats.1.2.1.zip
# unzip stats.1.2.1.zip
# ln -s STATS.1.2.1 stats
```

para acrescentar algo no contrab, terá de fazer: sudo crontab -e ou caso não use sudo ou não tenha permissões sudo, correr como root crontab -e

/opt/bin/eduroam/stats/e-U-hotspot.cfg

Este ficheiro é a configuração do script, em que se define o hotspot, o pivot, o nome do hotspot, o realm, a path onde os ficheiros serão armazenados, e expressares regulares para serem vistas como os endereços locais. Note-se que 10.10.2 é a rede local de controladoras/APs.

/opt/bin/eduroam/stats/e-U-hotspot.cfg

```
#### Inicio de codigos
#### Estes ID's devem ser solicitados a FCCN
$id_hotspot = "182";
$id_pivot = "39";
$nome_hotspot = "ISCTE";
#### Fim de codigos
## Preencher com a localização no filesystem para a criação do XML
$file_path = "/var/www";
# Realm utilizado para registos sem realm
$default_realm = "iscte.pt";
# Nome e Descrição de todos os Realms do hotspot que se querem listar como "locais"
%LOCAL_REALM = ("iscte.pt", "Instituto Superior de Ciencias do Trabalho e da Empresa", guest.iscte,
"Convidados");
# Expressao regular para seleccionar os registos "locais"
# A verificação só é efectuada para realms locais (definidos em LOCAL_REALM)
%CHECK_ORIGIN_ATTR = ("NAS-IP-Address", "^10\.10\.2\.", "WISPr-Location-Name", "^ISCTE");
$cipher = 1;
1;
```

/opt/bin/eduroam/stats.sh

Este script em seguida, automatiza o processo de gerar os ficheiros xml com estatísticas para a FCCN os recolher todos os meses. De notar que está configurado para guardar 90 dias de accounting detalhado; se se achar que esta a consumir disco, no minimo, pode se colocar 33 dias; no entanto atente-se aos requerimentos da AUP da federação já referidos anteriormente.

/opt/bin/eduroam/stats.sh

```
#!/bin/bash
##Rui Ribeiro/ISCTE/2013-2015
DAYS_TO_KEEP_ACCT=180 # 6 months
STATS=/opt/bin/eduroam/stats
DIRACCT=/var/log/freeradius/radacct
YEAR=`date +%Y --date="last month"`
MONTH=`date +%m --date="last month"`
cd $STATS
cat $DIRACCT/*/*detail-${YEAR}${MONTH}* | ./e-U-Stats.pl $YEAR $MONTH -xml 2> /dev/null
find $DIRACCT -type f -mtime +$DAYS_TO_KEEP_ACCT -exec rm {} \;
```

/opt/bin/eduroam/gzip_files.sh

Compress log detail files to save space and allow for more months. The gzip saves 85% of space.

/opt/bin/eduroam/gzip_files.sh

```
##Rui Ribeiro/ISCTE/2015
DAYS_TO_KEEP_ACCT=32
DIRACCT=/var/log/freeradius/radacct
# compress if not last month detail files
find $DIRACCT -type f -mtime +$DAYS_TO_KEEP_ACCT -not -name "*gz" -exec gzip {} \;
```

O e-U-Stats.pl tem instruções obsoletas de perl, e o separador de strings nos logs detalhados mudou de ser no FR 2 ", para ser no FR 3 ', pelo que se recomenda o seguinte patch, que reconhece quer ", quer ' como separadores válidos de strings.

euStats.patch

```
110c110
<                         if (defined %TEMPREC) {process_last_record();}
---
>                         if (%TEMPREC) {process_last_record();}
170c170
<         return if (! defined %TEMPREC);
---
>         return if (! %TEMPREC);
429,430c429,430
<         $s =~ s/^"//g;
<         $s =~ s/"$//g;
---
>         $s =~ s/^['"]//g;
>         $s =~ s/['"]$//g;
```

patch e-U-Stats.pl < euStats.patch

Recolha centralizada de Estatisticas

Existe de momento uma funcionalidade recente da RCTS, para recolher estatísticas em paralelo à recolha mensal.

Para tal é necessário obter o awesant do confluence da página oficial das novas estatísticas da FCCN, dado ter algumas modificações locais. Em seguida fazer:

```
# instalar pacotes necessários
sudo apt-get install liblog-handler-perl libjson-perl libparams-validate-perl libio-string-perl libsys-hostname-long-perl libclass-accessor-perl
# descomprimir a versão de awesant alterada pela FCCN
tar -zxvf awesant.tar.gz
apt-get install apt-src
# compilar/contruir o deb
dpkg-buildpackage
cd ..
# instalar o deb
dpkg -i awesant_*deb
# correcção de erro na configuração
sed "s/radius/freeradius/g" /etc/awesant/agent.conf
sed "s/\/var\/log\/freeradius\/awesant/g" /etc/awesant/agent.conf
# arrancar o serviço
service awesant-agent start
```

Os ficheiros produzidos pelo fticks também devem ser rodados. O daemon apercebe-se que eles foram rodados, só há que ter o cuidado de não comprimir após a primeira rotação, para não se perderem logs/não dar erro. A rotação será diária, com backups de 30 dias.

Para isso criar um ficheiro /etc/logrotate.d/fticks

/etc/logrotate.d/fticks

```
/var/log/freeradius/awesant/*.log
{
    rotate 30
    daily
    missingok
    notifempty
    compress
    delaycompress
    create 640 freerad freerad
}
```

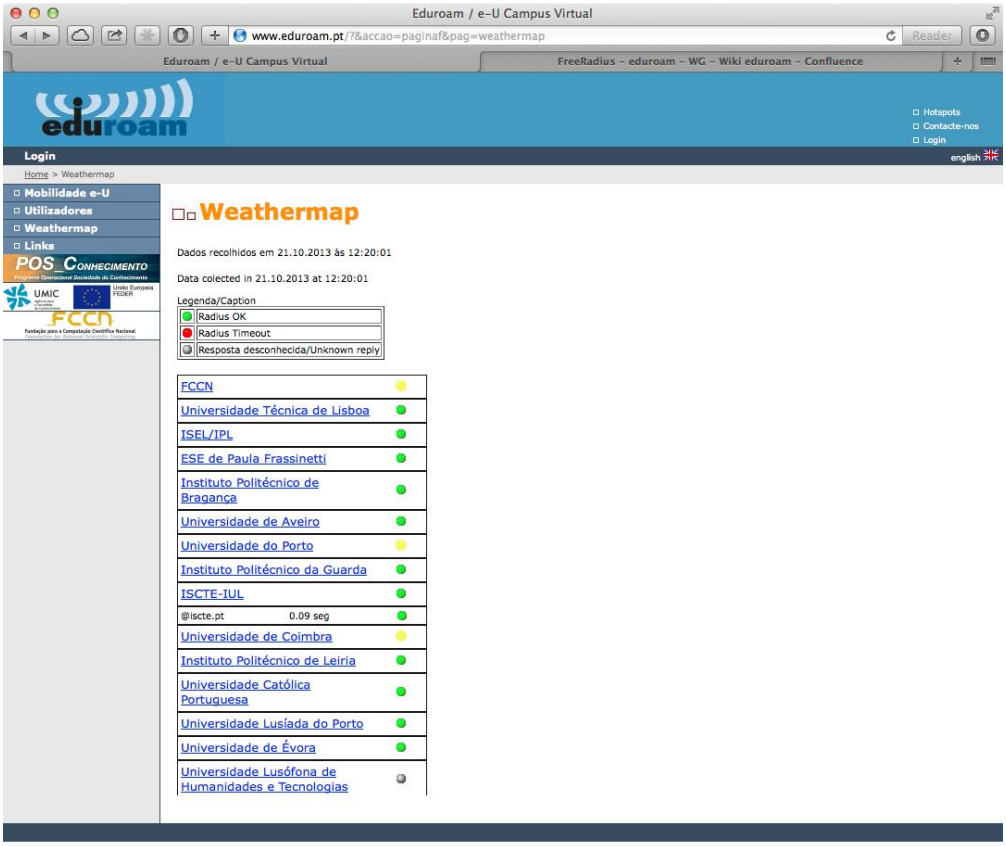
Weathermap da FCCN

Como monitorização do estado do serviços momentâneo, a FCCN disponibiliza o serviço weathermap em, que faz um teste ao serviço RADIUS cada 15 minutos.

http://www.eduroam.pt/?&accao=paginaf&pag=weathermap ou http://mon.e-u.pt:8080/wm.html

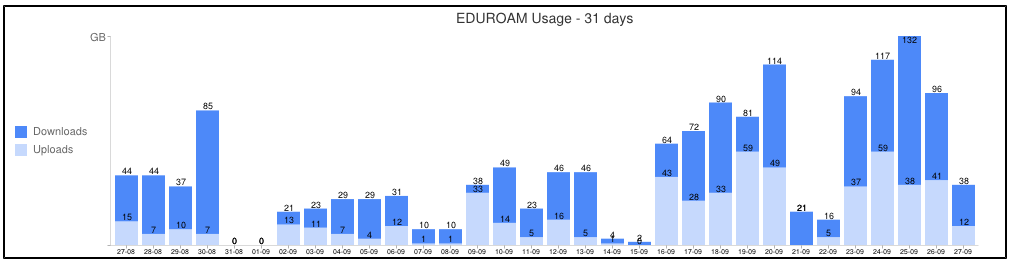
O NAS-IP-ADDRESS do serviço de weathermap aparece como 127.0.0.1 do lado do servidor RADIUS da instituição. O tempo mínimo medido pelo serviço são 90 ms.
ver o ficheiro de domínio default para ver a configuração do serviço de suporte para weathermap em unlang.

Página da RCTS de Weathermap:



Para mais dados sobre a monitorização da confederação, a página http://monitor.eduroam.org é também bastante útil.

Scripts de monitorização de accounting



Recuperação de serviços

Uma das estratégias para recuperação de serviços poderá ser usar localmente o serviço monit.

Para activar o serviço:

/etc/default/monit

startup=1

/etc/monit/monitrc

/etc/monit/monit.rc

```
set daemon 60 # espera 60 segundos antes de começar a monitorar
set eventqueue
basedir /var/monit # set the base directory where events will be stored
slots 100
set mail-format { from: monit@iscte.pt
subject: monit alert -- $EVENT $SERVICE
message: $EVENT Service $SERVICE
Date: $DATE
Action: $ACTION
Host: $HOST
Description: $DESCRIPTION
Best regards,
syslog
}
set alert sistema.alertas@iscte.pt
check process freeradius with pidfile /var/run/freeradius/freeradius.pid
    start program = "/etc/init.d/freeradius start"
    stop program = "/etc/init.d/freeradius stop"
    if failed host 193.136.188.36 port 1812 type UDP  then restart

check process smbd with pidfile /var/run/samba/smbd.pid
        start program = "/etc/init.d/samba start"
        stop program = "/etc/init.d/samba stop"
        if failed host 127.0.0.1 port 139 type TCP then restart
        if 5 restarts within 5 cycles then timeout
check process nmbd with pidfile /var/run/samba/nmbd.pid
        start program = "/etc/init.d/samba start"
        stop program = "/etc/init.d/samba stop"
        if failed host 127.0.0.1 port 138 type UDP then restart
        if failed host 127.0.0.1 port 137 type UDP then restart
        if 5 restarts within 5 cycles then timeout
check process winbindd with pidfile /var/run/samba/winbindd.pid
        start program = "/etc/init.d/winbind start"
        stop program = "/etc/init.d/winbind stop"
```

Em seguida, fazer:

```
service monit restart
```

Teste e recuperação de serviços na camada 7 OSI

Este script destina-se a testar várias condições, desde o funcionamento do SAMBA, até o ntlm_auth/winbind, acabando em testes do FreeRADIUS, pela autenticação normal e em seguida testando uma conexão EAP.

/opt/bin/eduroam/recover.sh

/opt/bin/eduroam/recover.sh

```
#!/bin/bash
/etc/init.d/samba status > /dev/null
if [ $? -ne 0 ]
then
/etc/init.d/samba restart
fi
/usr/bin/wbinfo -a radius_teste%xxxpass > /dev/null
if [ $? -ne 0 ]
then
/etc/init.d/winbind restart
fi
/opt/bin/eapol_test -c /opt/bin/eduroam/conf/peap-mschapv2.conf -s testing123 -a 193.136.188.36 > /dev/null
if [ $? -ne 0 ]
then
/etc/init.d/freeradius stop
/etc/init.d/freeradius start
echo $HOSTNAME:"restarted due to PEAP failure" | mail -s "radius restart" alertas@iscte.pt
fi
```

Depois de testar, acrescentar no crontab:

```
*/5 * * * * /opt/bin/eduroam/recover.sh
```

Aconselha-se a ter este script activo, já que em caso de falha sobe o serviço. Se se persistir em usar a versão de stock Debian 7, 2.1.12, é obrigatório, já que com demasiada frequência, esta versão de FreeRADIUS deixa de autenticar devidamente utilizadores locais, e apenas o faz com utilizadores em roaming.
A versão 2.12 em Debian Wheezy tem um bug conhecido no HUP, que é realizado todos os dias na rotação do syslog. Com alguma regularidade, depois de receber múltiplos sinais HUP, o módulo mschap deixa de trabalhar. Tem também problemas de estabilidade, e deadlocks. Recorda-se no entanto novamente que o mínimo que recomendamos usar à data da escrita deste documento è a versão 2.2.7 ou a 3.0.9. A versão Debian 8 Jessie vem com o FreeRadius 2.2.5.

SNMP

Também se pode recolher estatísticas de uso do FreeRadius a partir do agente snmpd.

Criar o script a ser invocado pelas extensões do snmpd

/opt/bin/eduroam/radstat.sh

/opt/bin/eduroam/radstat.sh

```
#!/bin/bash
echo "Message-Authenticator = 0x00,FreeRADIUS-Statistics-Type = 31" | radclient localhost:18121 status
adminsecret
```

Não esquecer fazer:

```
#chmod a+rx /opt/bin/eduroam/radstat.sh
```

Em seguida, instalamos o agente/server snmp(d) e as tools:

```
#aptitude install snmpd snmp
```

Em seguida editamos a configuração do snmp.

/etc/snmp/snmpd.conf

/etc/snmp/snmpd.conf

Comentar bind ao localhost

#agentAddress udp:127.0.0.1:167

definir comunidade snmp e acesso a partir do servidor de monitorização

rocommunity suacomunidadesnmp 10.2.2.12

extender os comandos
extend radstat /opt/bin/eduroam/radstat.sh

Em seguida fazer restart ao serviço snmp para activar esta configuração

```
#service snmpd restart
```

Para invocar a extensão/script através de snmp, ou através de Nagios/Cacti/Observium/NNMP usar a OID 1.3.6.1.4.1.8072.1.3 (nsExtensions)

```
#snmpwalk -v2c -c suacomunidadesnmp radius2.iscte.pt 1.3.6.1.4.1.8072.1.3
iso.3.6.1.4.1.8072.1.3.2.1.0 = INTEGER: 1
iso.3.6.1.4.1.8072.1.3.2.2.1.2.7.114.97.100.115.116.97.116 = STRING: "/opt/bin/eduroam/radstat.sh"
iso.3.6.1.4.1.8072.1.3.2.2.1.3.7.114.97.100.115.116.97.116 = ""
iso.3.6.1.4.1.8072.1.3.2.2.1.4.7.114.97.100.115.116.97.116 = ""
iso.3.6.1.4.1.8072.1.3.2.2.1.5.7.114.97.100.115.116.97.116 = INTEGER: 5
iso.3.6.1.4.1.8072.1.3.2.2.1.6.7.114.97.100.115.116.97.116 = INTEGER: 1
iso.3.6.1.4.1.8072.1.3.2.2.1.7.7.114.97.100.115.116.97.116 = INTEGER: 1
iso.3.6.1.4.1.8072.1.3.2.2.1.20.7.114.97.100.115.116.97.116 = INTEGER: 4
iso.3.6.1.4.1.8072.1.3.2.2.1.21.7.114.97.100.115.116.97.116 = INTEGER: 1
iso.3.6.1.4.1.8072.1.3.2.3.1.1.7.114.97.100.115.116.97.116 = STRING: "Received response ID 96, code 2, length =
512"
iso.3.6.1.4.1.8072.1.3.2.3.1.2.7.114.97.100.115.116.97.116 = STRING: "Received response ID 96, code 2, length =
512
        FreeRADIUS-Total-Access-Requests = 1012398
        FreeRADIUS-Total-Access-Accepts = 81957
        FreeRADIUS-Total-Access-Rejects = 55766
        FreeRADIUS-Total-Access-Challenges = 874305
        FreeRADIUS-Total-Auth-Responses = 1012028
        FreeRADIUS-Total-Auth-Duplicate-Requests = 336
        FreeRADIUS-Total-Auth-Malformed-Requests = 0
        FreeRADIUS-Total-Auth-Invalid-Requests = 0
        FreeRADIUS-Total-Auth-Dropped-Requests = 370
        FreeRADIUS-Total-Auth-Unknown-Types = 0
        FreeRADIUS-Total-Accounting-Requests = 221333
        FreeRADIUS-Total-Accounting-Responses = 220546
        FreeRADIUS-Total-Acct-Duplicate-Requests = 652
        FreeRADIUS-Total-Acct-Malformed-Requests = 0
        FreeRADIUS-Total-Acct-Invalid-Requests = 0
        FreeRADIUS-Total-Acct-Dropped-Requests = 787
        FreeRADIUS-Total-Acct-Unknown-Types = 0
        FreeRADIUS-Total-Proxy-Access-Requests = 87580
        FreeRADIUS-Total-Proxy-Access-Accepts = 5488
        FreeRADIUS-Total-Proxy-Access-Rejects = 8744
        FreeRADIUS-Total-Proxy-Access-Challenges = 73018
        FreeRADIUS-Total-Proxy-Auth-Responses = 87250
        FreeRADIUS-Total-Proxy-Auth-Duplicate-Requests = 0
        FreeRADIUS-Total-Proxy-Auth-Malformed-Requests = 0
        FreeRADIUS-Total-Proxy-Auth-Invalid-Requests = 0
        FreeRADIUS-Total-Proxy-Auth-Dropped-Requests = 0
        FreeRADIUS-Total-Proxy-Auth-Unknown-Types = 0
        FreeRADIUS-Total-Proxy-Accounting-Requests = 16595
```

```
        FreeRADIUS-Total-Proxy-Accounting-Responses = 16461
        FreeRADIUS-Total-Proxy-Acct-Duplicate-Requests = 0
        FreeRADIUS-Total-Proxy-Acct-Malformed-Requests = 0
        FreeRADIUS-Total-Proxy-Acct-Invalid-Requests = 0
        FreeRADIUS-Total-Proxy-Acct-Dropped-Requests = 0
        FreeRADIUS-Total-Proxy-Acct-Unknown-Types = 0
        FreeRADIUS-Stats-Start-Time = \"May  6 2014 16:16:36 WEST\"
        FreeRADIUS-Stats-HUP-Time = \"May 10 2014 06:25:04 WEST\"
        FreeRADIUS-Queue-Len-Internal = 0
        FreeRADIUS-Queue-Len-Proxy = 0
        FreeRADIUS-Queue-Len-Auth = 0
        FreeRADIUS-Queue-Len-Acct = 0
        FreeRADIUS-Queue-Len-Detail = 0"
iso.3.6.1.4.1.8072.1.3.2.3.1.3.7.114.97.100.115.116.97.116 = INTEGER: 42
iso.3.6.1.4.1.8072.1.3.2.3.1.4.7.114.97.100.115.116.97.116 = INTEGER: 0
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.1 = STRING: "Received response ID 96, code 2, length
= 512"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.2 = STRING: "        FreeRADIUS-Total-Access-
Requests = 1012398"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.3 = STRING: "        FreeRADIUS-Total-Access-Accepts
= 81957"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.4 = STRING: "        FreeRADIUS-Total-Access-Rejects
= 55766"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.5 = STRING: "        FreeRADIUS-Total-Access-
Challenges = 874305"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.6 = STRING: "        FreeRADIUS-Total-Auth-Responses
= 1012028"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.7 = STRING: "        FreeRADIUS-Total-Auth-Duplicate-
Requests = 336"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.8 = STRING: "        FreeRADIUS-Total-Auth-Malformed-
Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.9 = STRING: "        FreeRADIUS-Total-Auth-Invalid-
Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.10 = STRING: "        FreeRADIUS-Total-Auth-Dropped-
Requests = 370"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.11 = STRING: "        FreeRADIUS-Total-Auth-Unknown-
Types = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.12 = STRING: "        FreeRADIUS-Total-Accounting-
Requests = 221333"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.13 = STRING: "        FreeRADIUS-Total-Accounting-
Responses = 220546"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.14 = STRING: "        FreeRADIUS-Total-Acct-
Duplicate-Requests = 652"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.15 = STRING: "        FreeRADIUS-Total-Acct-
Malformed-Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.16 = STRING: "        FreeRADIUS-Total-Acct-Invalid-
Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.17 = STRING: "        FreeRADIUS-Total-Acct-Dropped-
Requests = 787"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.18 = STRING: "        FreeRADIUS-Total-Acct-Unknown-
Types = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.19 = STRING: "        FreeRADIUS-Total-Proxy-Access-
Requests = 87580"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.20 = STRING: "        FreeRADIUS-Total-Proxy-Access-
Accepts = 5488"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.21 = STRING: "        FreeRADIUS-Total-Proxy-Access-
Rejects = 8744"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.22 = STRING: "        FreeRADIUS-Total-Proxy-Access-
Challenges = 73018"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.23 = STRING: "        FreeRADIUS-Total-Proxy-Auth-
Responses = 87250"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.24 = STRING: "        FreeRADIUS-Total-Proxy-Auth-
Duplicate-Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.25 = STRING: "        FreeRADIUS-Total-Proxy-Auth-
Malformed-Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.26 = STRING: "        FreeRADIUS-Total-Proxy-Auth-
Invalid-Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.27 = STRING: "        FreeRADIUS-Total-Proxy-Auth-
Dropped-Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.28 = STRING: "        FreeRADIUS-Total-Proxy-Auth-
Unknown-Types = 0"
```

```
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.29 = STRING: "        FreeRADIUS-Total-Proxy-
Accounting-Requests = 16595"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.30 = STRING: "        FreeRADIUS-Total-Proxy-
Accounting-Responses = 16461"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.31 = STRING: "        FreeRADIUS-Total-Proxy-Acct-
Duplicate-Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.32 = STRING: "        FreeRADIUS-Total-Proxy-Acct-
Malformed-Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.33 = STRING: "        FreeRADIUS-Total-Proxy-Acct-
Invalid-Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.34 = STRING: "        FreeRADIUS-Total-Proxy-Acct-
Dropped-Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.35 = STRING: "        FreeRADIUS-Total-Proxy-Acct-
Unknown-Types = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.36 = STRING: "        FreeRADIUS-Stats-Start-Time =
\"May  6 2014 16:16:36 WEST\""
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.37 = STRING: "        FreeRADIUS-Stats-HUP-Time = \"
May 10 2014 06:25:04 WEST\""
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.38 = STRING: "        FreeRADIUS-Queue-Len-Internal
= 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.39 = STRING: "        FreeRADIUS-Queue-Len-Proxy = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.40 = STRING: "        FreeRADIUS-Queue-Len-Auth = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.41 = STRING: "        FreeRADIUS-Queue-Len-Acct = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.42 = STRING: "        FreeRADIUS-Queue-Len-Detail =
0"
```

Pode usar as extensões SNMP/nsExtentions para invocar os scripts necessários para monitorizar por Nagios, e assim não ter o nagios-nrpe-server instalado.

NAGIOS

Colocar o script em /opt/bin/nagios_radius.sh

/opt/bin/nagios_radius.sh

```
#!/bin/bash
cd /opt/bin/eduroam
OUT=$(/opt/bin/eapol_test -c conf/peap-mschapv2.conf -s testing123 -a 193.136.188.36)
V=$?
if [ $? -ne 0 ]
then
   V=2
fi
echo $OUT  | sed -n "s/.*\(FreeRADIUS: time.*seconds\).*/\1/p"
exit $V
```

Fazer:

```
chmod a+rx /opt/bin/nagios_radius.sh
```

Adicionar em /etc/nagios/nrpe.cfg

```
command[check_dp]=/opt/bin/nagios_radius.sh
```

Fazer

```
service nagios-nrpe-server restart
```

com nConf

Fazer login no nConf

escolher: advanced-services add

advanced service name Check Radius

FreeRADIUS

check_nrpe

check 24x7

notification 24x7

assign to host radius2

assign to servicegroup check_nrpe

service template - generic-service

contact groups network-admins

notification options w,c,r,u

active checking: 1

notification enable: 1

params for check command: check_radius

Generate Nagios config

Deploy

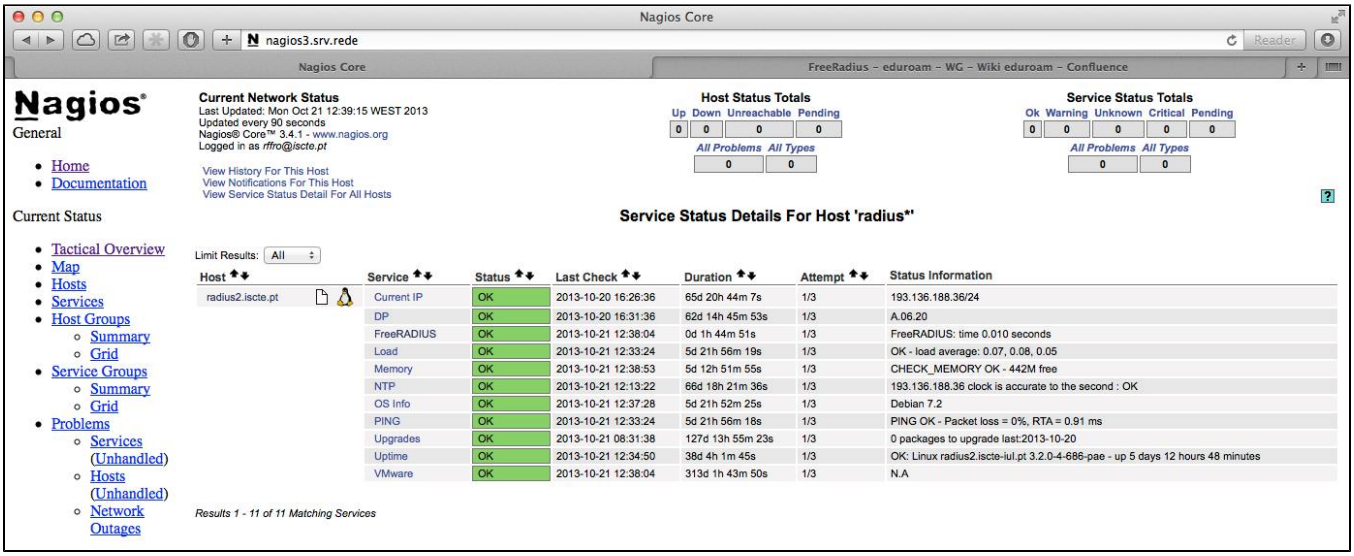
Em alternativa, configurando à mão:

advanced_services.cfg

```
define service {
        service_description             FreeRADIUS
        notification_options            w,c,r,u
        active_checks_enabled           1
        notifications_enabled           1
        check_command                   check_nrpe!check_radius
        check_period                    24x7
        notification_period             24x7
        host_name                       radius2.iscte.pt
        servicegroups                   check_nrpe
        contact_groups                  network-admins
        use                             generic-service
}
```

Para este script trabalhar tem de se compilar e aplicar as patches ao eapol_test

Página de NAGIOS de monitorização do servidor/serviço:



Raptor

Há quem use o Raptor para fazer loggings das autenticações no FreeRadius. Não usamos o Raptor, mas deixamos um link aqui. https://community.ja.net/groups/dot1x-sig/document/format-freeradius-log-enable-interoperation-raptor

Resolução de problemas

A resolução de problemas pode ser realizada em diferentes camadas da infra-estrutura do servidor, com diversos comandos especializados.

De seguida vamos dar alguns exemplos, com o output esperado. Aqui fica uma breve resenha da sintaxe de ferramentas opensource para despistar problemas, embora relembremos que mais importante que ter ferramentas disponíveis, é ter a capacidade de interpretar os seus outputs.

De notar que o site freeradius.org e as mailing list associadas são também bastante activas e úteis. Antes de enviar algo para a mailing list, também é recomendado procurar nos arquivos em

htpp://freeradius.org/list/users.html

Podem também contactar o autor deste documento em rui.ribeiro@iscte.pt ou ruyrybeyro@gmail.com Dentro dos limites do possível será feito um esforço para responder.

Ressalve-se no entanto, que existem várias camadas de troubleshooting, mas neste documento centramo-nos mais na parte do FreeRadius. Existem também limitações da tecnologia conhecida, como a dificuldade de migração entre diferentes tecnologias de APs ou mesmo migrando entre diferentes famílias do mesmo fabricante (quando o utilizador se desloca dentro de um espaço físico e muda de AP). Normalmente para ultrapassar estas situações, o melhor será fechar e abrir o wifi, ou activar momentaneamente o modo vôo do aparelho. Temos também casos raros de iPhones, de utilizadores ao migrarem entre faculdades, serem forçados a fazer reboot para usar a EDUROAM. Instalando um profile de iOS de eduroam (por exemplo do CAT), aparentemente o iPhone não é bloqueado pelo AP. Os SSIDs do profile são testados primeiro, e em vez de testar vários métodos de autenticação, o profile define o método usado.

Existem também problemas conhecidos com bugs de Android entre a versão 2.3 e a versão 2.5. http://blogs.it.ox.ac.uk/networks/2012/01/25/eduroam-connectivity-issues-on-android-2-3/comment-page-1/#comment-8606

pcregrep

Mostrar entradas de um log de utilizador individual.

```
pcregrep -M "manuel@iscte.pt(.*\n){0,12}" detail-20140115*
```

ps

Verificar se processos estão a correr.

SAMBA:

```
#ps  ax | grep [n]mbd
 1618 ?        Ss     0:20 /usr/sbin/nmbd -D
```

SAMBA:

```
# ps ax | grep [s]mbd
 1638 ?        Ss     0:06 /usr/sbin/smbd -D
 1684 ?        S      0:00 /usr/sbin/smbd -D
```

winbind

```
# ps ax | grep [w]inbindd
16817 ?        Ss     0:28 /usr/sbin/winbindd
16830 ?        S      0:36 /usr/sbin/winbindd
```

FreeRADIUS

```
# ps ax | grep [f]reeradius
21981 ?        Ssl    0:10 /usr/sbin/freeradius
```

wbinfo

Para verificar se estamos joined à AD.

```
radius:/home/rui# wbinfo -t
checking the trust secret for domain ISCTE via RPC calls succeeded
```

Fazer uma lista dos nossos trusted domains:

```
radius:/home/rui# wbinfo --trusted-domains
BUILTIN
RADIUS
ISCTE
```

Listar os dominios activos:

```
radius:/home/rui# wbinfo --online-status
BUILTIN : online
RADIUS2 : online
ISCTE : online
```

Verificar a validade de um utilizador/password. Password errada:

```
wbinfo -a user%pass

plaintext password authentication failed

Could not authenticate user user%pass with plaintext password

challenge/response password authentication failed

error code was NT_STATUS_NO_SUCH_USER (0xc0000064)

error message was: No such user

Could not authenticate user user with challenge/response
```

Password correcta:

```
# wbinfo -a radius%xxxxxx

plaintext password authentication succeeded

challenge/response password authentication succeeded
```

Verificar password usando o protocolo kerberos:

```
# wbinfo --krb5auth=radius_user%password

plaintext kerberos password authentication for [radius_user%password] succeeded (requesting cctype: FILE)

credentials were put in: FILE:/tmp/krb5cc_0
```

wbinfo -u | wc -l (numero de utilizadores na AD)

```
radius:/home/rui# wbinfo -u | wc -l
42619
```

numero de grupos

```
wbinfo -g | wc -l
radius:/home/rui# wbinfo -g | wc -l
81
```

Descobrir o DC que estamos a usar.

```
#wbinfo --dc-info=ISCTE
dc01.iscte.local (10.1.1.1)
```

Descobrir se a pilha bind/winbind está a trabalhar bem e fazer ligação ao socket.

```
radius:/home/rui# wbinfo -p
Ping to winbindd succeeded
```

Testar a ligação ao DC.

```
# wbinfo -P
checking the NETLOGON dc connection succeeded
```

net

Fazer queries de capacidade de auditing do domínio a que estamos conectados:

```
#net rpc audit list -U rffro
Enter rffro's password:
Auditing: Enabled
Auditing categories: 7
Auditing settings:
 System Events                Success, Failure
 Logon events                 Success, Failure
 Object Access                Success, Failure
 Privilege Use                Success, Failure
 Process Tracking             Success, Failure
 Policy Change                Success, Failure
 Account Management           Success, Failure
```

Ver shares disponíveis:

```
#net rpc share -U rffro
Enter rffro's password:
IPC$
```

Descobrir quem trata do LDAP de um domínio:

```
#net lookup ldap ISCTE.LOCAL
10.1.1.1:389
```

ntlm_auth

Testar a password de um utilizador no domínio.

```
/usr/bin/ntlm_auth --request-nt-key --username=radius --domain=ISCTE
password:
NT_STATUS_OK: Success (0x0) ou  NT_STATUS_WRONG_PASSWORD: Wrong Password (0xc000006a)
```

Neste caso, corria tudo bem, os diagnósticos de estarmos joined na AD, também estavam bem, sendo que acabamos por descobrir que o DC estava com problemas.

```
/usr/bin/ntlm_auth --username=radius --domain=ISCTE
password:
NT_STATUS_ACCESS_DENIED: Access denied (0xc0000022)
```

Erro do winbind antes de fazer join ao domínio e consequentemente ter o winbind em baixo.

```
# /usr/bin/ntlm_auth --request-nt-key --username=rffro --domain=WISCTE
password:
NT_STATUS_CANT_ACCESS_DOMAIN_INFO: NT_STATUS_CANT_ACCESS_DOMAIN_INFO (0xc00000da)
```

E em caso de erro no nome do utilizador:

```
# /usr/bin/ntlm_auth --request-nt-key --username=rui --domain=ISCTE
password:
NT_STATUS_NO_SUCH_USER: No such user (0xc0000064)
```

Kerberos

Gestão de tickets kerberos.

```
# kinit rffro
Password for administrator@ISCTE.LOCAL
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@WISCTE.WFARM

Valid starting    Expires           Service principal
22/10/2013 10:47  22/10/2013 20:47  krbtgt/ISCTE.LOCAL@ISCTE.LOCAL
 renew until 23/10/2013 10:47
kdestroy
```

testparm

O testparm verifica se existem erros no ficheiro de configuração do SAMBA.

```
#testparm
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Loaded services file OK.
Server role: ROLE_DOMAIN_MEMBER
Press enter to see a dump of your service definitions

[global]
 workgroup = ISCTE
 realm = ISCTE.WFARM
 server string = %h server
 interfaces = lo
 bind interfaces only = Yes
 security = ADS
 obey pam restrictions = Yes
 pam password change = Yes
 passwd program = /usr/bin/passwd %u
 passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n *password\supdated\ssuccessfully* .
 syslog = 0
 log file = /var/log/samba/log.%m
 max log size = 1000
 load printers = No
 printcap name = /dev/null
 disable spoolss = Yes
 os level = 0
 local master = No
 domain master = No
 dns proxy = No
 panic action = /usr/share/samba/panic-action %d
 winbind enum users = Yes
 winbind enum groups = Yes
 winbind use default domain = Yes
 idmap config * : range = 10000-20000
 idmap config * : backend = tdb
 printing = bsd
 print command = lpr -r -P'%p' %s
 lpq command = lpq -P'%p'
 lprm command = lprm -P'%p' %j
```

Pode-se usar o output do testparm para criar um smb.conf mais "limpo".

smbencrypt

O smbencrypt pode ser usado para gerar NT hashes de passwords, para colocar um ficheiros de FreeRadius ou testar em unlang.

```
$ smbencrypt kakao
LM Hash                                                  NT Hash
--------------------------------        --------------------------------
3658E2D04E81CC72AAD3B435B51404EE        30600A1973AA628A1F4C2F828C1CFF0C
```

password user = 0x30600A1973AA628A1F4C2F828C1CFF0C

freeradius

Para verificar erros ao nível dos ficheiros de configuração, e da camada aplicacional do FreeRADIUS, pode-se correr o freeradius em modo debug:

```
/etc/init.d/monit stop #  (se se estiver a correr o monit para recuperar o serviço)
/etc/init.d/freeradius stop
freeradius -X
#ou
freeradius -Xxx # para ter mais detalhe nos erros gerados
```

No caso de ao arranque, apresentar o erro seguinte, este deve-se ao Debian não aumentar as versões das aplicações com patch. Ver o comentário do ssl no radiusd.conf

```
[FAIL] Checking FreeRADIUS daemon configuration...failed (Once you have verified libssl has been correctly
patched, set security.allow_vulnerable_openssl = 'CVE-2014-0160').
```

Salienta-se que é mandatório usar o formato freeradius -X para colocar problemas na mailing list oficial.

e para rearrancar de novo:

```
/etc/init.d/freeradius start
/etc/init.d/monit start
```

Aconselha-se o uso do modo de debug desta forma apenas nas fases anteriores à entrada em produção, sendo que em produção, aconselha-se o uso do radmin/raddebug, que tem menos implicações na estabilidade do serviço. Note-se também, e isto é importante, que é importante apagar passwords do ficheiro de debug antes de o enviar a alguém.
Em freeradius3 com configurações radsec, usar em alternativa para debugging *freeradius -fxx -l stdout*

Para ver a versão de freeradius, opções de compilação, e a partir da v2.2.4, a versão do libssl (depois do heartbleed), fazer:

```
$ freeradius -xv
Tue May  6 16:20:09 2014 : Info: freeradius: FreeRADIUS Version 2.2.5 (git #b75980d), for host x86_64-pc-linux-
gnu, built on May  6 2014 at 16:15:19
Tue May  6 16:20:09 2014 : Debug: Server was built with:
Tue May  6 16:20:09 2014 : Debug:   accounting
Tue May  6 16:20:09 2014 : Debug:   authentication
Tue May  6 16:20:09 2014 : Debug:  WITH_DHCP
Tue May  6 16:20:09 2014 : Debug:  WITH_VMPS
Tue May  6 16:20:09 2014 : Debug: Server core libs:
Tue May  6 16:20:09 2014 : Debug:   ssl: OpenSSL 1.0.1e 11 Feb 2013
Tue May  6 16:20:09 2014 : Info: Copyright (C) 1999-2013 The FreeRADIUS server project and contributors.
Tue May  6 16:20:09 2014 : Info: There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A
Tue May  6 16:20:09 2014 : Info: PARTICULAR PURPOSE.
Tue May  6 16:20:09 2014 : Info: You may redistribute copies of FreeRADIUS under the terms of the
Tue May  6 16:20:09 2014 : Info: GNU General Public License.
Tue May  6 16:20:09 2014 : Info: For more information about these matters, see the file named COPYRIGHT.
```

Para correr sem threads, usar a opção -t.

radclient

Para obter dados de status localmente no servidor freeradius fazer:

```
$echo "Message-Authenticator = 0x00,FreeRADIUS-Statistics-Type = 31" | radclient localhost:18121 status
adminsecret
Received response ID 18, code 2, length = 512
        FreeRADIUS-Total-Access-Requests = 74084
        FreeRADIUS-Total-Access-Accepts = 5921
        FreeRADIUS-Total-Access-Rejects = 5207
        FreeRADIUS-Total-Access-Challenges = 62942
        FreeRADIUS-Total-Auth-Responses = 74070
        FreeRADIUS-Total-Auth-Duplicate-Requests = 4
        FreeRADIUS-Total-Auth-Malformed-Requests = 0
        FreeRADIUS-Total-Auth-Invalid-Requests = 0
        FreeRADIUS-Total-Auth-Dropped-Requests = 5
        FreeRADIUS-Total-Auth-Unknown-Types = 0
        FreeRADIUS-Total-Accounting-Requests = 17155
        FreeRADIUS-Total-Accounting-Responses = 17110
        FreeRADIUS-Total-Acct-Duplicate-Requests = 35
        FreeRADIUS-Total-Acct-Malformed-Requests = 0
        FreeRADIUS-Total-Acct-Invalid-Requests = 0
        FreeRADIUS-Total-Acct-Dropped-Requests = 44
        FreeRADIUS-Total-Acct-Unknown-Types = 0
        FreeRADIUS-Total-Proxy-Access-Requests = 4779
        FreeRADIUS-Total-Proxy-Access-Accepts = 282
        FreeRADIUS-Total-Proxy-Access-Rejects = 852
        FreeRADIUS-Total-Proxy-Access-Challenges = 3640
        FreeRADIUS-Total-Proxy-Auth-Responses = 4774
        FreeRADIUS-Total-Proxy-Auth-Duplicate-Requests = 0
        FreeRADIUS-Total-Proxy-Auth-Malformed-Requests = 0
        FreeRADIUS-Total-Proxy-Auth-Invalid-Requests = 0
        FreeRADIUS-Total-Proxy-Auth-Dropped-Requests = 0
        FreeRADIUS-Total-Proxy-Auth-Unknown-Types = 0
        FreeRADIUS-Total-Proxy-Accounting-Requests = 748
        FreeRADIUS-Total-Proxy-Accounting-Responses = 737
        FreeRADIUS-Total-Proxy-Acct-Duplicate-Requests = 0
        FreeRADIUS-Total-Proxy-Acct-Malformed-Requests = 0
        FreeRADIUS-Total-Proxy-Acct-Invalid-Requests = 0
        FreeRADIUS-Total-Proxy-Acct-Dropped-Requests = 0
        FreeRADIUS-Total-Proxy-Acct-Unknown-Types = 0
        FreeRADIUS-Stats-Start-Time = "Mar 31 2014 13:02:27 WEST"
        FreeRADIUS-Stats-HUP-Time = "Mar 31 2014 13:02:27 WEST"
        FreeRADIUS-Queue-Len-Internal = 0
        FreeRADIUS-Queue-Len-Proxy = 0
        FreeRADIUS-Queue-Len-Auth = 0
        FreeRADIUS-Queue-Len-Acct = 0
        FreeRADIUS-Queue-Len-Detail = 0
```

Este comando pode ser invocado do snmp para uma ligação a uma ferramenta de monitorização, Observium ou Cacti, ou então invocado a partir de um scripts para o Nagios. O radclient também tem a opção -c para invocar várias vezes os mesmos dados, -q para quiet mode e -x para descrever o que faz.

radeapclient

O radeapclient é baseado no radclient, mas tem mais opções e funciona em eap. Tem também umas operações bastante interessantes para auditing de serviços, que infelizmente só foram inserias no git 3.1.x. Poderá valer a pena fazer backporting/compilar essa versão

- added option -n (rate limit)
- fixed option -q (quiet mode)
- improved option -s (statistics)
- added option -o (periodic report)
- added option -c (send each packet several times)

De futuro, o código poderá ser fundido com o radclient, e este comando poderá desaparecer.

radtest

Para verificar se o freeradius está a autenticar correctamente um utilizador também se pode executar o comando:

```
$radtest -t mschap radius_teste@iscte.pt password radius2.iscte.pt:1812 0 password_de_IP_no_clients.conf
Sending Access-Request of id 207 to 193.136.188.36 port 1812
User-Name = "radius_teste@iscte.pt"
NAS-IP-Address = 193.136.188.36
NAS-Port = 0
Message-Authenticator = 0x00000000000000000000000000000000
MS-CHAP-Challenge = 0x7f50f83fb8726022
MS-CHAP-Response =
0x000100000000000000000000000000000000000000000000000009278635d44ade71b8e24950df3eae8878cc85fe7f379fd25
rad_recv: Access-Accept packet from host 193.136.188.36 port 1812, id=207, length=128
Service-Type = Framed-User
Reply-Message = "Eduroam ISCTE"
Framed-MTU = 1300
Tunnel-Type:0 = VLAN
Tunnel-Medium-Type:0 = IEEE-802
Tunnel-Private-Group-Id:0 = "201"
MS-CHAP-MPPE-Keys = 0x00000000000000000454848d8fcaab877388d5d6adfefe07e0000000000000000
MS-MPPE-Encryption-Policy = 0x00000002
MS-MPPE-Encryption-Types = 0x00000004
```

EAPTest

Ferramenta gráfica para Mac para testar autenticações EAP, suportando uma série de protocolos. Código de eapol_test adaptado para uma interface OS /X. Pago.

http://www.macupdate.com/app/mac/49625/eaptest

radperf

A ferramenta *radperf* propõe-se ser uma ferramenta de referência de análise de performance RADIUS, escrita pelo autor do FreeRadius. Eram disponibilizados binários para 32 bits no passado para Windows, OS/X e Linux. Hoje em dia os binários são para 64 bits. É extremamente compacta e rápida. O URL é http://networkradius.com/radperf.html

```
$radperf - Performance testing tool for RADIUS systems.
          Copyright (C) 2012 Network RADIUS SARL.  All rights reserved.
Usage: radperf [options] server[:port] <command> [<secret>]
  <command>    One of auth, acct, status, coa, or disconnect.
  -a type     Use authentication method <type> (pap, chap, none)
  -A d,l      After Access-Accept, send accounting packets.
  -c count    Send each packet 'count' times.
  -d raddb    Set dictionary directory.
  -D file     Print packet statistics to file
  -f file     Read packets from file, not stdin.
  -F          Update Framed-IP-Address, too.
  -n num      Send a maximum of 'num' packets per second
  -p num      Send a maximum of 'num' packets in parallel.
  -q          Do not print anything out.
  -r retries  If timeout, retry sending the packet 'retries' times.
  -R realm    Realm name to append to the User-Name
  -s          Print out summary information of auth results.
  -S file     read secret from file, not command line.
  -t timeout  Wait 'timeout' seconds before retrying (may be a floating point number).
  -T template Use template file with every request
  -u number   Generate requests for 'number' users.
  -v          Show program version information.
  -x          Debugging mode.
  -4          Use IPv4 address of server
  -6          Use IPv6 address of server.
```

Em seguida, usando a versão antiga de 32 bits, editamos o ficheiro bob.csv, e colocamos o utilizador do weathermap, que retorna um reply message e falha de autenticação.

radius-teste@iscte.pt,hello

```
$LD_LIBRARY_PATH=./lib ./radperf -f bob.csv -a pap -c 200000 -s 193.136.188.36 auth test
Received response ID 186, code 3, length = 31
        Reply-Message = "RADIUS OK"
Received response ID 214, code 3, length = 31
        Reply-Message = "RADIUS OK"
Received response ID 31, code 3, length = 31
        Reply-Message = "RADIUS OK"
Received response ID 70, code 3, length = 31
        Reply-Message = "RADIUS OK"
Received response ID 40, code 3, length = 31
        Reply-Message = "RADIUS OK"
             Total succeeded   :  0
             Total failed      :  200000
             Total no reply    :  0
             Total time (s)    :  143.890
             Packets/s         :  1390
             Response times:
                < 10 usec  : 0
                < 100 usec : 0
                < msec     : 192122
                < 10 msec  : 7718
                < 0.1s     : 157
                < s        : 3
                < 10s      : 0
                < 100s     : 0
```

O teste foi realizado com um utilizador com negação de autenticação em unlang, e não é representativo da capacidade de autenticar utilizadores com MSCHAP. É também de ter em atenção que utilizadores com autenticação negada têm um atraso de processamento parametrizado no freeradius.

raduat

http://wiki.freeradius.org/guide/raduat

Radlogin

http://www.iea-software.com/products/radlogin4.cfm

LoadUI

Outra ferramenta interessante para análise de performance é o LOADUI; permite entre outras coisas, configurar o uso de vários scripts simultaneamente.

Pode-se obter a versão grátis em http://sourceforge.net/projects/loadui/ e a paga, LoadUiPro, em http://www.loadui.org. A versão free está limitada a 300 users simultâneos.

ldapperf

Para fazer testes de velocidade à camada LDAP de queries.

https://github.com/arr2036/ldapperf/

ldapsearch

Para verificar se um utilizador local existe/está em pelo menos um dos grupos necessários para atribuir uma vlan:

ldapsearch -x -LLL -E pr=200/noprompt -h your_ad_server -D "CN=Radius,CN=Users,DC=iscte,DC=local" -w pass_Radius_AD_user -b "cn=users, dc=iscte,dc=local" -s sub "(sAMAccountName=utilizador_a_fazer_debugging sem dominio)" memberOf

```
$ldapsearch -x -LLL -E pr=200/noprompt -h 10.1.1.1 -D "CN=radius_bind,CN=Users,DC=iscte,DC=local" -w passord -b
"cn=users,dc=iscte,dc=local" -s sub "(sAMAccountName=aluno_teste)" memberOf
dn: CN=aluno_teste,CN=Users,DC=iscte,DC=local
memberOf: CN=Alunos,CN=Users,DC=iscte,DC=local
```

tcpdump

Ao nível de rede, também se pode escutar se recebemos pacotes RADIUS dos APs e da federação com o comando:

```
# tcpdump -n port 1812 or port 1813
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
12:17:21.788969 IP 10.61.10.11.60207 > 193.136.188.36.1813: RADIUS, Accounting Request (4), id: 0x7f length: 201
12:17:21.790276 IP 193.136.188.36.1813 > 10.61.10.11.60207: RADIUS, Accounting Response (5), id: 0x7f length: 20
12:17:21.826514 IP 10.61.10.11.60207 > 193.136.188.36.1813: RADIUS, Accounting Request (4), id: 0x80 length: 237
12:17:21.831775 IP 193.136.188.36.1813 > 10.61.10.11.60207: RADIUS, Accounting Response (5), id: 0x80 length: 20
12:17:21.865924 IP 10.61.10.12.56350 > 193.136.188.36.1812: RADIUS, Access Request (1), id: 0xc7 length: 182
12:17:21.866695 IP 193.136.188.36.1812 > 10.61.10.12.56350: RADIUS, Access Challenge (11), id: 0xc7 length: 64
12:17:21.923641 IP 10.61.10.12.56350 > 193.136.188.36.1812: RADIUS, Access Request (1), id: 0xc8 length: 187
12:17:21.924383 IP 193.136.188.36.1812 > 10.61.10.12.56350: RADIUS, Access Challenge (11), id: 0xc8 length: 64
12:17:21.953319 IP 10.61.10.11.60207 > 193.136.188.36.1813: RADIUS, Accounting Request (4), id: 0x81 length: 200
12:17:21.954237 IP 10.61.10.11.60207 > 193.136.188.36.1813: RADIUS, Accounting Request (4), id: 0x82 length: 242
12:17:21.955787 IP 10.61.10.12.56350 > 193.136.188.36.1812: RADIUS, Access Request (1), id: 0xc9 length: 286
12:17:21.956498 IP 193.136.188.36.1812 > 10.61.10.12.56350: RADIUS, Access Challenge (11), id: 0xc9 length: 1090
12:17:21.968523 IP 193.136.188.36.1813 > 10.61.10.11.60207: RADIUS, Accounting Response (5), id: 0x81 length: 20
12:17:21.969503 IP 193.136.188.36.1813 > 10.61.10.11.60207: RADIUS, Accounting Response (5), id: 0x82 length: 20
12:17:21.978805 IP 10.10.66.5.32770 > 193.136.188.36.1812: RADIUS, Access Request (1), id: 0x17 length: 185
12:17:21.979368 IP 193.136.188.36.1812 > 10.10.66.5.32770: RADIUS, Access Challenge (11), id: 0x17 length: 64
12:17:21.988407 IP 10.61.10.12.56350 > 193.136.188.36.1812: RADIUS, Access Request (1), id: 0xca length: 187
12:17:21.988953 IP 193.136.188.36.1812 > 10.61.10.12.56350: RADIUS, Access Challenge (11), id: 0xca length: 1086
12:17:22.052088 IP 10.61.10.12.56350 > 193.136.188.36.1812: RADIUS, Access Request (1), id: 0xcb length: 187
12:17:22.052719 IP 193.136.188.36.1812 > 10.61.10.12.56350: RADIUS, Access Challenge (11), id: 0xcb length: 1086
12:17:22.086430 IP 10.61.10.12.56350 > 193.136.188.36.1812: RADIUS, Access Request (1), id: 0xcc length: 187
12:17:22.087093 IP 193.136.188.36.1812 > 10.61.10.12.56350: RADIUS, Access Challenge (11), id: 0xcc length: 522
12:17:22.119212 IP 10.61.10.12.56350 > 193.136.188.36.1812: RADIUS, Access Request (1), id: 0xcd length: 519
12:17:22.136861 IP 193.136.188.36.1812 > 10.61.10.12.56350: RADIUS, Access Challenge (11), id: 0xcd length: 123
12:17:22.172056 IP 10.61.10.12.56350 > 193.136.188.36.1812: RADIUS, Access Request (1), id: 0xce length: 187
12:17:22.172740 IP 193.136.188.36.1812 > 10.61.10.12.56350: RADIUS, Access Challenge (11), id: 0xce length: 101
```

Pedido com secret errado (gerado com radtest no localhost):

```
# tcpdump -n port 1812 -i lo
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 65535 bytes
12:32:10.587369 IP 193.136.188.36.52547 > 193.136.188.36.1812: RADIUS, Access Request (1), id: 0x85 length: 146
12:32:14.492220 IP 193.136.188.36.32963 > 193.136.188.36.1812: RADIUS, Access Request (1), id: 0x1d length: 146
12:32:15.504623 IP 193.136.188.36.38887 > 193.136.188.36.1812: RADIUS, Access Request (1), id: 0x56 length: 146
12:32:16.371053 IP 193.136.188.36.32921 > 193.136.188.36.1812: RADIUS, Access Request (1), id: 0x52 length: 146
12:32:17.214224 IP 193.136.188.36.34200 > 193.136.188.36.1812: RADIUS, Access Request (1), id: 0xa8 length: 146
12:32:17.983684 IP 193.136.188.36.47958 > 193.136.188.36.1812: RADIUS, Access Request (1), id: 0x48 length: 146
12:32:18.756234 IP 193.136.188.36.60883 > 193.136.188.36.1812: RADIUS, Access Request (1), id: 0x9a length: 146
12:32:19.520513 IP 193.136.188.36.48594 > 193.136.188.36.1812: RADIUS, Access Request (1), id: 0x43 length: 146
```

Para ver com mais detalhe uma transacção RADIUS normal:

```
# tcpdump -n -vvv port 1812 or port 1813
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
12:19:43.875217 IP (tos 0x0, ttl 63, id 58184, offset 0, flags [none], proto UDP (17), length 228)
    10.61.10.11.60207 > 193.136.188.36.1813: [udp sum ok] RADIUS, length: 200
 Accounting Request (4), id: 0x85, Authenticator: 442bdc2391bace09f3fe02d47babf12a
   Accounting Status Attribute (40), length: 6, Value: Start
     0x0000:  0000 0001
   Accounting Session ID Attribute (44), length: 19, Value: 5256C7CF-0001B5AC
     0x0000:  3532 3536 4337 4346 2d30 3030 3142 3541
     0x0010:  43
   Accounting Authentication Attribute (45), length: 6, Value: RADIUS
     0x0000:  0000 0001
   Username Attribute (1), length: 7, Value: facaf
     0x0000:  6661 6361 66
   NAS IP Address Attribute (4), length: 6, Value: 10.61.10.11
     0x0000:  0a3d 0a0b
```

```
   NAS Port Attribute (5), length: 6, Value: 0
     0x0000:  0000 0000
   NAS Port Type Attribute (61), length: 6, Value: Wireless - IEEE 802.11
     0x0000:  0000 0013
   NAS ID Attribute (32), length: 19, Value: 00-50-56-80-36-73
     0x0000:  3030 2d35 302d 3536 2d38 302d 3336 2d37
     0x0010:  33
   Called Station Attribute (30), length: 32, Value: 00-50-56-80-36-73:EDUROAM_1020
     0x0000:  3030 2d35 302d 3536 2d38 302d 3336 2d37
     0x0010:  333a 4544 5552 4f41 4d5f 3130 3230
   Calling Station Attribute (31), length: 19, Value: A0-0B-BA-28-2B-EB
     0x0000:  4130 2d30 422d 4241 2d32 382d 3242 2d45
     0x0010:  42
   Connect Info Attribute (77), length: 23, Value: CONNECT Unknown radio
     0x0000:  434f 4e4e 4543 5420 556e 6b6e 6f77 6e20
     0x0010:  7261 6469 6f
   Accounting Delay Attribute (41), length: 6, Value: 00 secs
     0x0000:  0000 0000
   Vendor Specific Attribute (26), length: 12, Value: Vendor: Unknown (15983)
     Vendor Attribute: 1, Length: 4, Value: ...H
     0x0000:  0000 3e6f 0106 0000 0048
   Vendor Specific Attribute (26), length: 13, Value: Vendor: Unknown (15983)
     Vendor Attribute: 2, Length: 5, Value: AP-72
     0x0000:  0000 3e6f 0207 4150 2d37 32
12:19:43.876022 IP (tos 0x0, ttl 63, id 58185, offset 0, flags [none], proto UDP (17), length 264)
    10.61.10.11.60207 > 193.136.188.36.1813: [udp sum ok] RADIUS, length: 236
 Accounting Request (4), id: 0x86, Authenticator: 0272945202b30d20b3ac76f37cac1b93
   Accounting Status Attribute (40), length: 6, Value: Stop
     0x0000:  0000 0002
   Accounting Session ID Attribute (44), length: 19, Value: 5256C7CF-0001B5A4
     0x0000:  3532 3536 4337 4346 2d30 3030 3142 3541
     0x0010:  34
   Accounting Authentication Attribute (45), length: 6, Value: RADIUS
     0x0000:  0000 0001
   Username Attribute (1), length: 7, Value: facaf
     0x0000:  6661 6361 66
   NAS IP Address Attribute (4), length: 6, Value: 10.61.10.11
     0x0000:  0a3d 0a0b
   NAS Port Attribute (5), length: 6, Value: 2118
     0x0000:  0000 0846
   NAS Port Type Attribute (61), length: 6, Value: Wireless - IEEE 802.11
     0x0000:  0000 0013
   NAS ID Attribute (32), length: 19, Value: 00-50-56-80-36-73
     0x0000:  3030 2d35 302d 3536 2d38 302d 3336 2d37
     0x0010:  33
   Called Station Attribute (30), length: 32, Value: 00-50-56-80-36-73:EDUROAM_1020
     0x0000:  3030 2d35 302d 3536 2d38 302d 3336 2d37
     0x0010:  333a 4544 5552 4f41 4d5f 3130 3230
   Calling Station Attribute (31), length: 19, Value: A0-0B-BA-28-2B-EB
     0x0000:  4130 2d30 422d 4241 2d32 382d 3242 2d45
     0x0010:  42
   Connect Info Attribute (77), length: 23, Value: CONNECT Unknown radio
     0x0000:  434f 4e4e 4543 5420 556e 6b6e 6f77 6e20
     0x0010:  7261 6469 6f
   Accounting Session Time Attribute (46), length: 6, Value: 14 secs
     0x0000:  0000 000e
   Accounting Delay Attribute (41), length: 6, Value: 00 secs
     0x0000:  0000 0000
   Accounting Termination Cause Attribute (49), length: 6, Value: User Request
     0x0000:  0000 0001
   Accounting Input Packets Attribute (47), length: 6, Value: 0
     0x0000:  0000 0000
   Accounting Output Packets Attribute (48), length: 6, Value: 0
     0x0000:  0000 0000
   Accounting Input Octets Attribute (42), length: 6, Value: 0
     0x0000:  0000 0000
   Accounting Output Octets Attribute (43), length: 6, Value: 0
     0x0000:  0000 0000
   Vendor Specific Attribute (26), length: 12, Value: Vendor: Unknown (15983)
     Vendor Attribute: 1, Length: 4, Value: ...H
     0x0000:  0000 3e6f 0106 0000 0048
```

```
   Vendor Specific Attribute (26), length: 13, Value: Vendor: Unknown (15983)
     Vendor Attribute: 2, Length: 5, Value: AP-72
     0x0000:  0000 3e6f 0207 4150 2d37 32
12:19:43.893929 IP (tos 0x0, ttl 64, id 11300, offset 0, flags [none], proto UDP (17), length 48)
    193.136.188.36.1813 > 10.61.10.11.60207: [bad udp cksum 0x9222 -> 0x8506!] RADIUS, length: 20
 Accounting Response (5), id: 0x85, Authenticator: 5be45f6cea7fbdf3702a8a87c62ecc37
12:19:43.896277 IP (tos 0x0, ttl 64, id 11301, offset 0, flags [none], proto UDP (17), length 48)
    193.136.188.36.1813 > 10.61.10.11.60207: [bad udp cksum 0x9222 -> 0xd776!] RADIUS, length: 20
 Accounting Response (5), id: 0x86, Authenticator: f93f30017d5e717abc070c6edb5ae280
12:19:44.004734 IP (tos 0x0, ttl 63, id 58186, offset 0, flags [none], proto UDP (17), length 210)
    10.61.10.11.36000 > 193.136.188.36.1812: [udp sum ok] RADIUS, length: 182
 Access Request (1), id: 0x87, Authenticator: b574c133ecbd4f00f003cc4094279bb3
   Username Attribute (1), length: 16, Value: facaf@iscte.pt
     0x0000:  6661 6361 6640 6973 6374 652e 7074
   NAS IP Address Attribute (4), length: 6, Value: 10.61.10.11
     0x0000:  0a3d 0a0b
   NAS Port Attribute (5), length: 6, Value: 2118
     0x0000:  0000 0846
   Called Station Attribute (30), length: 32, Value: 00-50-56-80-36-73:EDUROAM_1020
     0x0000:  3030 2d35 302d 3536 2d38 302d 3336 2d37
     0x0010:  333a 4544 5552 4f41 4d5f 3130 3230
   Calling Station Attribute (31), length: 19, Value: A0-0B-BA-28-2B-EB
     0x0000:  4130 2d30 422d 4241 2d32 382d 3242 2d45
     0x0010:  42
   Framed MTU Attribute (12), length: 6, Value: 1250
     0x0000:  0000 04e2
   NAS Port Type Attribute (61), length: 6, Value: Wireless - IEEE 802.11
     0x0000:  0000 0013
   Framed Compression Attribute (13), length: 6, Value: None
     0x0000:  0000 0000
   Connect Info Attribute (77), length: 23, Value: CONNECT Unknown radio
     0x0000:  434f 4e4e 4543 5420 556e 6b6e 6f77 6e20
     0x0010:  7261 6469 6f
   Unassigned Attribute (89), length: 3, Value:
     0x0000:  00
   EAP Message Attribute (79), length: 21, Value: ..
     0x0000:  0201 0013 0166 6163 6166 4069 7363 7465
     0x0010:  2e70 74
   Message Authentication Attribute (80), length: 18, Value: &..K....5......G
     0x0000:  2684 e34b 8c16 0987 3503 eb8a f5ee dd47
12:19:44.005604 IP (tos 0x0, ttl 64, id 11302, offset 0, flags [none], proto UDP (17), length 92)
    193.136.188.36.1812 > 10.61.10.11.36000: [bad udp cksum 0x924e -> 0xa68c!] RADIUS, length: 64
 Access Challenge (11), id: 0x87, Authenticator: 09926dd7fdcc6651dca88dfdb1964ddf
   EAP Message Attribute (79), length: 8, Value: ..
     0x0000:  0102 0006 1520
   Message Authentication Attribute (80), length: 18, Value: oRV..sA..h..P.K.
     0x0000:  6f52 56a4 eb73 419b 8f68 b0f9 50c2 4b0c
   State Attribute (24), length: 18, Value: .Ta..Vt.z0J.i..A
     0x0000:  1a54 618f 1a56 74f6 7a30 4a97 69f8 0b41
```

Para sniffar as transacções LDAP:

```
# tcpdump -n -vvv port 389
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
12:21:49.097061 IP (tos 0x0, ttl 64, id 13945, offset 0, flags [DF], proto TCP (6), length 192)
    193.136.188.36.50435 > 10.20.10.78.389: Flags [P.], cksum 0x92c1 (incorrect -> 0xff42), seq 3599505020:
3599505160, ack 1435163761, win 4103, options [nop,nop,TS val 140856200 ecr 171411212], length 140
12:21:49.097965 IP (tos 0x0, ttl 127, id 27275, offset 0, flags [DF], proto TCP (6), length 154)
    10.20.10.78.389 > 193.136.188.36.50435: Flags [P.], cksum 0xe0f1 (correct), seq 1:103, ack 140, win 510,
options [nop,nop,TS val 171411492 ecr 140856200], length 102
12:21:49.097981 IP (tos 0x0, ttl 64, id 13946, offset 0, flags [DF], proto TCP (6), length 52)
    193.136.188.36.50435 > 10.20.10.78.389: Flags [.], cksum 0x9235 (incorrect -> 0x07de), seq 140, ack 103,
win 4103, options [nop,nop,TS val 140856201 ecr 171411492], length 0
12:21:49.098109 IP (tos 0x0, ttl 64, id 13947, offset 0, flags [DF], proto TCP (6), length 162)
    193.136.188.36.50435 > 10.20.10.78.389: Flags [P.], cksum 0x92a3 (incorrect -> 0x582b), seq 140:250, ack
103, win 4103, options [nop,nop,TS val 140856201 ecr 171411492], length 110
12:21:49.098728 IP (tos 0x0, ttl 127, id 27276, offset 0, flags [DF], proto TCP (6), length 75)
    10.20.10.78.389 > 193.136.188.36.50435: Flags [P.], cksum 0x7034 (correct), seq 103:126, ack 250, win 509,
options [nop,nop,TS val 171411492 ecr 140856201], length 23
12:21:49.098904 IP (tos 0x0, ttl 64, id 13948, offset 0, flags [DF], proto TCP (6), length 157)
    193.136.188.36.50435 > 10.20.10.78.389: Flags [P.], cksum 0x929e (incorrect -> 0xb59a), seq 250:355, ack
126, win 4103, options [nop,nop,TS val 140856201 ecr 171411492], length 105
12:21:49.099505 IP (tos 0x0, ttl 127, id 27277, offset 0, flags [DF], proto TCP (6), length 215)
    10.20.10.78.389 > 193.136.188.36.50435: Flags [P.], cksum 0xc2ae (correct), seq 126:289, ack 355, win 509,
options [nop,nop,TS val 171411492 ecr 140856201], length 163
12:21:49.099664 IP (tos 0x0, ttl 64, id 13949, offset 0, flags [DF], proto TCP (6), length 145)
    193.136.188.36.50435 > 10.20.10.78.389: Flags [P.], cksum 0x9292 (incorrect -> 0xe7d6), seq 355:448, ack
289, win 4103, options [nop,nop,TS val 140856201 ecr 171411492], length 93
12:21:49.100227 IP (tos 0x0, ttl 127, id 27278, offset 0, flags [DF], proto TCP (6), length 75)
    10.20.10.78.389 > 193.136.188.36.50435: Flags [P.], cksum 0x6eb2 (correct), seq 289:312, ack 448, win 508,
options [nop,nop,TS val 171411493 ecr 140856201], length 23
12:21:49.100445 IP (tos 0x0, ttl 64, id 13950, offset 0, flags [DF], proto TCP (6), length 163)
    193.136.188.36.50435 > 10.20.10.78.389: Flags [P.], cksum 0x92a4 (incorrect -> 0x1b5c), seq 448:559, ack
312, win 4103, options [nop,nop,TS val 140856201 ecr 171411493], length 111
12:21:49.101059 IP (tos 0x0, ttl 127, id 27279, offset 0, flags [DF], proto TCP (6), length 75)
    10.20.10.78.389 > 193.136.188.36.50435: Flags [P.], cksum 0x6e2b (correct), seq 312:335, ack 559, win 508,
options [nop,nop,TS val 171411493 ecr 140856201], length 23
12:21:49.101159 IP (tos 0x0, ttl 64, id 13951, offset 0, flags [DF], proto TCP (6), length 157)
    193.136.188.36.50435 > 10.20.10.78.389: Flags [P.], cksum 0x929e (incorrect -> 0xb390), seq 559:664, ack
335, win 4103, options [nop,nop,TS val 140856201 ecr 171411493], length 105
12:21:49.101828 IP (tos 0x0, ttl 127, id 27280, offset 0, flags [DF], proto TCP (6), length 215)
    10.20.10.78.389 > 193.136.188.36.50435: Flags [P.], cksum 0xc0a3 (correct), seq 335:498, ack 664, win 507,
options [nop,nop,TS val 171411493 ecr 140856201], length 163
12:21:49.102017 IP (tos 0x0, ttl 64, id 13952, offset 0, flags [DF], proto TCP (6), length 146)
    193.136.188.36.50435 > 10.20.10.78.389: Flags [P.], cksum 0x9293 (incorrect -> 0x6d44), seq 664:758, ack
498, win 4103, options [nop,nop,TS val 140856202 ecr 171411493], length 94
12:21:49.102588 IP (tos 0x0, ttl 127, id 27281, offset 0, flags [DF], proto TCP (6), length 136)
    10.20.10.78.389 > 193.136.188.36.50435: Flags [P.], cksum 0x09fc (correct), seq 498:582, ack 758, win 513,
options [nop,nop,TS val 171411493 ecr 140856202], length 84
12:21:49.141698 IP (tos 0x0, ttl 64, id 13953, offset 0, flags [DF], proto TCP (6), length 52)
    193.136.188.36.50435 > 10.20.10.78.389: Flags [.], cksum 0x9235 (incorrect -> 0x0389), seq 758, ack 582,
win 4103, options [nop,nop,TS val 140856212 ecr 171411493], length 0
12:21:50.680844 IP (tos 0x0, ttl 64, id 13954, offset 0, flags [DF], proto TCP (6), length 192)
    193.136.188.36.50435 > 10.20.10.78.389: Flags [P.], cksum 0x92c1 (incorrect -> 0xf769), seq 758:898, ack
582, win 4103, options [nop,nop,TS val 140856596 ecr 171411493], length 140
12:21:50.681647 IP (tos 0x0, ttl 127, id 27286, offset 0, flags [DF], proto TCP (6), length 159)
    10.20.10.78.389 > 193.136.188.36.50435: Flags [P.], cksum 0xf2ba (correct), seq 582:689, ack 898, win 512,
options [nop,nop,TS val 171411651 ecr 140856596], length 107
12:21:50.681671 IP (tos 0x0, ttl 64, id 13955, offset 0, flags [DF], proto TCP (6), length 52)
    193.136.188.36.50435 > 10.20.10.78.389: Flags [.], cksum 0x9235 (incorrect -> 0x0073), seq 898, ack 689,
win 4103, options [nop,nop,TS val 140856597 ecr 171411651], length 0
12:21:50.682018 IP (tos 0x0, ttl 64, id 13956, offset 0, flags [DF], proto TCP (6), length 162)
    193.136.188.36.50435 > 10.20.10.78.389: Flags [P.], cksum 0x92a3 (incorrect -> 0x57c0), seq 898:1008, ack
689, win 4103, options [nop,nop,TS val 140856597 ecr 171411651], length 110
```

É normal ver pacotes a sair com checksum incorrecto num host vmware, sendo que isto é um problema/optimização conhecida para ganhar tempo de processamento, e o pacote ao sair do servidor/ambiente virtual já sai com o checksum corrigido.

Escutar começo e fim de transações TCP

```
# tcpdump 'tcp[13] & 3 != 0'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
12:37:28.178811 IP nagios3.srv.rede.45224 > radius2.iscte.pt.nrpe: Flags [S], seq 1549761472, win 14600,
options [mss 1460,sackOK,TS val 845939632 ecr 0,nop,wscale 4], length 0
12:37:28.178850 IP radius2.iscte.pt.nrpe > nagios3.srv.rede.45224: Flags [S.], seq 2953569873, ack 1549761473,
win 14480, options [mss 1460,sackOK,TS val 141090971 ecr 845939632,nop,wscale 3], length 0
12:37:28.220497 IP radius2.iscte.pt.nrpe > nagios3.srv.rede.45224: Flags [F.], seq 1037, ack 1037, win 2069,
options [nop,nop,TS val 141090981 ecr 845939634], length 0
12:37:28.221356 IP nagios3.srv.rede.45224 > radius2.iscte.pt.nrpe: Flags [F.], seq 1037, ack 1038, win 1042,
options [nop,nop,TS val 845939643 ecr 141090981], length 0
12:38:19.425347 IP radius2.iscte.pt.50496 > horus2.wiscte.wfarm.ldap: Flags [S], seq 1561846426, win 14600,
options [mss 1460,sackOK,TS val 141103782 ecr 0,nop,wscale 3], length 0
12:38:19.426046 IP horus2.wiscte.wfarm.ldap > radius2.iscte.pt.50496: Flags [S.], seq 832389402, ack
1561846427, win 8192, options [mss 1380,nop,wscale 8,sackOK,TS val 171510525 ecr 141103782], length 0
12:38:40.296018 IP nagios3.srv.rede.45302 > radius2.iscte.pt.nrpe: Flags [S], seq 2618866886, win 14600,
options [mss 1460,sackOK,TS val 845957661 ecr 0,nop,wscale 4], length 0
12:38:40.296061 IP radius2.iscte.pt.nrpe > nagios3.srv.rede.45302: Flags [S.], seq 1631463945, ack 2618866887,
win 14480, options [mss 1460,sackOK,TS val 141109000 ecr 845957661,nop,wscale 3], length 0
12:38:40.550782 IP radius2.iscte.pt.nrpe > nagios3.srv.rede.45302: Flags [F.], seq 1037, ack 1037, win 2069,
options [nop,nop,TS val 141109064 ecr 845957662], length 0
12:38:40.551293 IP nagios3.srv.rede.45302 > radius2.iscte.pt.nrpe: Flags [F.], seq 1037, ack 1038, win 1042,
options [nop,nop,TS val 845957725 ecr 141109064], length 0
12:39:09.180239 IP nagios3.srv.rede.45380 > radius2.iscte.pt.nrpe: Flags [S], seq 2280252685, win 14600,
options [mss 1460,sackOK,TS val 845964882 ecr 0,nop,wscale 4], length 0
12:39:09.180279 IP radius2.iscte.pt.nrpe > nagios3.srv.rede.45380: Flags [S.], seq 1198201210, ack 2280252686,
win 14480, options [mss 1460,sackOK,TS val 141116221 ecr 845964882,nop,wscale 3], length 0
12:39:09.271131 IP radius2.iscte.pt.nrpe > nagios3.srv.rede.45380: Flags [F.], seq 1037, ack 1037, win 2069,
options [nop,nop,TS val 141116244 ecr 845964886], length 0
12:39:09.271632 IP nagios3.srv.rede.45380 > radius2.iscte.pt.nrpe: Flags [F.], seq 1037, ack 1038, win 1042,
options [nop,nop,TS val 845964905 ecr 141116244], length 0
```

wireshark

Pode-se colocar no wireshark o shared secret do RADIUS.

Wireless Diagnostics

Em OS/X, no 10.10/yosemite e em 10.9/Mavericks, é possível fazer sniffing ao trafego wifi com mecanismos do SO. Para tal, faz-se ALT-icon wifi->open wireless diagnostics->window (menu)->sniffer. Isto deixa um processo a escutar as transacções de wireless num determinado canal. Quando se termina, cria um ficheiro raw em formato tcpdump no Desktop.

tcpreplay

O comando tcpreplay pode ser usado para fazer replay de capturas realizadas com tcpdump para efeitos de teste. < a completar>

netstat

Para ver as portas ocupadas com serviços, pode-se usar o comando netstat. Chama-se a atenção para os LISTEN nos sockets TCP, os sockets unix /ficheiros e as portas UDP no segundo comando.

```
$ netstat -an | grep LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:445           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:139           0.0.0.0:*               LISTEN
unix  2      [ ACC ]     STREAM     LISTENING     1088011  /var/run/samba/winbindd_privileged/pipe
unix  2      [ ACC ]     STREAM     LISTENING     1088010  /tmp/.winbindd/pipe
unix  2      [ ACC ]     STREAM     LISTENING     2276476  /usr/local/var/run/freeradius/freeradius.sock
$ netstat -an | grep 181[23]
udp        0      0 193.136.188.36:1812     0.0.0.0:*
udp        0      0 193.136.188.36:1813     0.0.0.0:*
udp        0      0 127.0.0.1:18120         0.0.0.0:*
$sudo netstat -ltunp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1306/sshd
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      1410/lighttpd
tcp        0      0 127.0.0.1:445           0.0.0.0:*               LISTEN      1430/smbd
tcp        0      0 127.0.0.1:139           0.0.0.0:*               LISTEN      1430/smbd
tcp6       0      0 :::22                   :::*                    LISTEN      1306/sshd
tcp6       0      0 :::443                  :::*                    LISTEN      1410/lighttpd
udp   214016      0 0.0.0.0:137             0.0.0.0:*                           1327/nmbd
udp   213248      0 0.0.0.0:138             0.0.0.0:*                           1327/nmbd
udp        0      0 0.0.0.0:54929           0.0.0.0:*                           2871/freeradius
udp        0      0 0.0.0.0:161             0.0.0.0:*                           1357/snmpd
udp        0      0 127.0.0.1:18120         0.0.0.0:*                           2871/freeradius
udp        0      0 127.0.0.1:18121         0.0.0.0:*                           2871/freeradius
udp        0      0 0.0.0.0:1812            0.0.0.0:*                           2871/freeradius
udp        0      0 0.0.0.0:1813            0.0.0.0:*                           2871/freeradius
udp        0      0 0.0.0.0:46418           0.0.0.0:*                           2871/freeradius
```

ngrep

O ngrep é bastante interessante para trafego não codificado, como por exemplo, para ouvir os pedidos ldap. Foi através do ngrep que percebemos que as configurações ldap precisavam de mudanças.

```
#ngrep -q  "."  "port 389"
T 193.136.188.36:54884 -> 10.1.1.1:389 [AP]
  0o.....ch..CN=Users,DC=wiscte,DC=wfarm..............4....sAMAccountName..Alunos....sAMAccountName..
a221270...dn

T 10.1.1.1:389 -> 193.136.188.36:54884 [AP]
  0..........
e............


T 193.136.188.36:54884 -> 10.1.1.1:389 [AP]
  0x.....cq.GCN=nome  completo de utilizadora apagado,CN=Users,DC=iscte,DC=local.................objectclass0...
memberOf

T 10.1.1.1:389 -> 193.136.188.36:54884 [AP]
  0..........d......GCN=nome completo de utilizadora pagado,CN=Users,DC=iscte,DC=lcaol0....=0....7..
memberOf1....'.%CN=Alunos,C
  N=Users,DC=iscte,DC=local0..........
e............

T 193.136.188.36:54884 -> 10.1.1.1:389 [AP]
  0].....cV.%CN=Alunos,CN=Users,DC=iscte,DC=local..................sAMAccountName..Alunos0...
dn

T 10.1.1.1:389 -> 193.136.188.36:54884 [AP]
  0....8.....d....-.%CN=Alunos,CN=Users,DC=iscte,DC=local0.....0..........e............
```

SNMP

snmpwalk

```
#snmpwalk -v2c -c suacomunidadesnmp radius2.iscte.pt 1.3.6.1.4.1.8072.1.3
iso.3.6.1.4.1.8072.1.3.2.1.0 = INTEGER: 1
iso.3.6.1.4.1.8072.1.3.2.2.1.2.7.114.97.100.115.116.97.116 = STRING: "/opt/bin/eduroam/radstat.sh"
iso.3.6.1.4.1.8072.1.3.2.2.1.3.7.114.97.100.115.116.97.116 = ""
iso.3.6.1.4.1.8072.1.3.2.2.1.4.7.114.97.100.115.116.97.116 = ""
iso.3.6.1.4.1.8072.1.3.2.2.1.5.7.114.97.100.115.116.97.116 = INTEGER: 5
iso.3.6.1.4.1.8072.1.3.2.2.1.6.7.114.97.100.115.116.97.116 = INTEGER: 1
iso.3.6.1.4.1.8072.1.3.2.2.1.7.7.114.97.100.115.116.97.116 = INTEGER: 1
iso.3.6.1.4.1.8072.1.3.2.2.1.20.7.114.97.100.115.116.97.116 = INTEGER: 4
iso.3.6.1.4.1.8072.1.3.2.2.1.21.7.114.97.100.115.116.97.116 = INTEGER: 1
iso.3.6.1.4.1.8072.1.3.2.3.1.1.7.114.97.100.115.116.97.116 = STRING: "Received response ID 96, code 2, length =
512"
iso.3.6.1.4.1.8072.1.3.2.3.1.2.7.114.97.100.115.116.97.116 = STRING: "Received response ID 96, code 2, length =
512
        FreeRADIUS-Total-Access-Requests = 1012398
        FreeRADIUS-Total-Access-Accepts = 81957
        FreeRADIUS-Total-Access-Rejects = 55766
        FreeRADIUS-Total-Access-Challenges = 874305
        FreeRADIUS-Total-Auth-Responses = 1012028
        FreeRADIUS-Total-Auth-Duplicate-Requests = 336
        FreeRADIUS-Total-Auth-Malformed-Requests = 0
        FreeRADIUS-Total-Auth-Invalid-Requests = 0
        FreeRADIUS-Total-Auth-Dropped-Requests = 370
        FreeRADIUS-Total-Auth-Unknown-Types = 0
        FreeRADIUS-Total-Accounting-Requests = 221333
        FreeRADIUS-Total-Accounting-Responses = 220546
        FreeRADIUS-Total-Acct-Duplicate-Requests = 652
        FreeRADIUS-Total-Acct-Malformed-Requests = 0
        FreeRADIUS-Total-Acct-Invalid-Requests = 0
        FreeRADIUS-Total-Acct-Dropped-Requests = 787
        FreeRADIUS-Total-Acct-Unknown-Types = 0
        FreeRADIUS-Total-Proxy-Access-Requests = 87580
        FreeRADIUS-Total-Proxy-Access-Accepts = 5488
        FreeRADIUS-Total-Proxy-Access-Rejects = 8744
        FreeRADIUS-Total-Proxy-Access-Challenges = 73018
        FreeRADIUS-Total-Proxy-Auth-Responses = 87250
        FreeRADIUS-Total-Proxy-Auth-Duplicate-Requests = 0
        FreeRADIUS-Total-Proxy-Auth-Malformed-Requests = 0
        FreeRADIUS-Total-Proxy-Auth-Invalid-Requests = 0
        FreeRADIUS-Total-Proxy-Auth-Dropped-Requests = 0
        FreeRADIUS-Total-Proxy-Auth-Unknown-Types = 0
        FreeRADIUS-Total-Proxy-Accounting-Requests = 16595
        FreeRADIUS-Total-Proxy-Accounting-Responses = 16461
        FreeRADIUS-Total-Proxy-Acct-Duplicate-Requests = 0
        FreeRADIUS-Total-Proxy-Acct-Malformed-Requests = 0
        FreeRADIUS-Total-Proxy-Acct-Invalid-Requests = 0
        FreeRADIUS-Total-Proxy-Acct-Dropped-Requests = 0
        FreeRADIUS-Total-Proxy-Acct-Unknown-Types = 0
        FreeRADIUS-Stats-Start-Time = \"May  6 2014 16:16:36 WEST\"
        FreeRADIUS-Stats-HUP-Time = \"May 10 2014 06:25:04 WEST\"
        FreeRADIUS-Queue-Len-Internal = 0
        FreeRADIUS-Queue-Len-Proxy = 0
        FreeRADIUS-Queue-Len-Auth = 0
        FreeRADIUS-Queue-Len-Acct = 0
        FreeRADIUS-Queue-Len-Detail = 0"
iso.3.6.1.4.1.8072.1.3.2.3.1.3.7.114.97.100.115.116.97.116 = INTEGER: 42
iso.3.6.1.4.1.8072.1.3.2.3.1.4.7.114.97.100.115.116.97.116 = INTEGER: 0
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.1 = STRING: "Received response ID 96, code 2, length
= 512"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.2 = STRING: "        FreeRADIUS-Total-Access-
Requests = 1012398"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.3 = STRING: "        FreeRADIUS-Total-Access-Accepts
```

```
= 81957"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.4 = STRING: "       FreeRADIUS-Total-Access-Rejects
= 55766"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.5 = STRING: "       FreeRADIUS-Total-Access-
Challenges = 874305"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.6 = STRING: "       FreeRADIUS-Total-Auth-Responses
= 1012028"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.7 = STRING: "       FreeRADIUS-Total-Auth-Duplicate-
Requests = 336"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.8 = STRING: "       FreeRADIUS-Total-Auth-Malformed-
Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.9 = STRING: "       FreeRADIUS-Total-Auth-Invalid-
Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.10 = STRING: "       FreeRADIUS-Total-Auth-Dropped-
Requests = 370"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.11 = STRING: "       FreeRADIUS-Total-Auth-Unknown-
Types = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.12 = STRING: "       FreeRADIUS-Total-Accounting-
Requests = 221333"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.13 = STRING: "       FreeRADIUS-Total-Accounting-
Responses = 220546"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.14 = STRING: "       FreeRADIUS-Total-Acct-
Duplicate-Requests = 652"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.15 = STRING: "       FreeRADIUS-Total-Acct-
Malformed-Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.16 = STRING: "       FreeRADIUS-Total-Acct-Invalid-
Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.17 = STRING: "       FreeRADIUS-Total-Acct-Dropped-
Requests = 787"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.18 = STRING: "       FreeRADIUS-Total-Acct-Unknown-
Types = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.19 = STRING: "       FreeRADIUS-Total-Proxy-Access-
Requests = 87580"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.20 = STRING: "       FreeRADIUS-Total-Proxy-Access-
Accepts = 5488"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.21 = STRING: "       FreeRADIUS-Total-Proxy-Access-
Rejects = 8744"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.22 = STRING: "       FreeRADIUS-Total-Proxy-Access-
Challenges = 73018"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.23 = STRING: "       FreeRADIUS-Total-Proxy-Auth-
Responses = 87250"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.24 = STRING: "       FreeRADIUS-Total-Proxy-Auth-
Duplicate-Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.25 = STRING: "       FreeRADIUS-Total-Proxy-Auth-
Malformed-Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.26 = STRING: "       FreeRADIUS-Total-Proxy-Auth-
Invalid-Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.27 = STRING: "       FreeRADIUS-Total-Proxy-Auth-
Dropped-Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.28 = STRING: "       FreeRADIUS-Total-Proxy-Auth-
Unknown-Types = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.29 = STRING: "       FreeRADIUS-Total-Proxy-
Accounting-Requests = 16595"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.30 = STRING: "       FreeRADIUS-Total-Proxy-
Accounting-Responses = 16461"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.31 = STRING: "       FreeRADIUS-Total-Proxy-Acct-
Duplicate-Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.32 = STRING: "       FreeRADIUS-Total-Proxy-Acct-
Malformed-Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.33 = STRING: "       FreeRADIUS-Total-Proxy-Acct-
Invalid-Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.34 = STRING: "       FreeRADIUS-Total-Proxy-Acct-
Dropped-Requests = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.35 = STRING: "       FreeRADIUS-Total-Proxy-Acct-
Unknown-Types = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.36 = STRING: "       FreeRADIUS-Stats-Start-Time =
\"May  6 2014 16:16:36 WEST\""
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.37 = STRING: "       FreeRADIUS-Stats-HUP-Time = \"
May 10 2014 06:25:04 WEST\""
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.38 = STRING: "       FreeRADIUS-Queue-Len-Internal
= 0"
```

```
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.39 = STRING: "        FreeRADIUS-Queue-Len-Proxy = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.40 = STRING: "        FreeRADIUS-Queue-Len-Auth = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.41 = STRING: "        FreeRADIUS-Queue-Len-Acct = 0"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.42 = STRING: "        FreeRADIUS-Queue-Len-Detail =
0"
```

snmpget

Pode-se invocar qualquer das OIDs anteriores individualmente com o comando snmpget. É preciso ter atenção que as OIDs individuais das extensões podem variar de acordo com a configuração local, e se estiverem mais extensões configuradas.

```
#snmpget -v2c -c ciestero localhost iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.13
iso.3.6.1.4.1.8072.1.3.2.4.1.2.7.114.97.100.115.116.97.116.13 = STRING: "        FreeRADIUS-Total-Accounting-
Responses = 220690"
```

radmin

O radmin e o wrapper associado raddebug são bastante interessantes para fazer debugging de questões do freeradius. o radmin dá para enviar comandos directamente, ou simplesmente invocado, abre uma shell que aceita comandos.

Ficam aqui exemplos de uso do radmin, no entanto, recomenda-se o uso do raddebug para fazer despite de problemas de utilizadores.

radmin [**-e** *command*] [**-i** *input_file*] [**-n** *name*] [**-o** *output_file*] [**-q**]

É necessário cautela a invocar certas directivas de radmin, já que existe a possibilidade de crashar o daemon de freeradius.

Fazer rodar logs a partir da v2.2.2:

```
# radmin -e 'hup main.log'
```

Invocar o radmin, e verificar a versão do freeradius a correr:

```
#radmin
radmin> show version
FreeRADIUS Version 2.2.4 (git #14e1ee7), for host x86_64-pc-linux-gnu, built on Jan 16 2014 at 21:25:50
```

E a última vez que arrancou.

```
radmin> show uptime
Up since Sat Oct 19 09:35:59 2013
```

Estatisticas de autenticação do servidor "home" (vários domínios se tal existirem)

```
radmin> stats home_server auth
 requests 94
 responses 80
 accepts 4
 rejects 9
 challenges 67
  dup 0
 invalid 0
 malformed 0
 bad_signature 0
 dropped 0
 unknown_types 0
radmin> stats client auth
 requests 969
 responses 955
 accepts 78
 rejects 35
 challenges 842
 dup 12
 invalid 0
 malformed 0
 bad_signature 0
 dropped 14
 unknown_types 0
radmin> stats client acct
 requests 153
 responses 145
 dup 0
 invalid 0
 malformed 0
 bad_signature 0
 dropped 8
 unknown_types 0
```

Estatisticas de contabilização do servidor "home" (vários domínios se tal existirem)

```
radmin> stats home_server acct
 requests 0
 responses 0
 dup 0
 invalid 0
 malformed 0
 bad_signature 0
 dropped 0
 unknown_types 0
```

Lista de clientes activos:

```
radmin> show client list
 127.0.0.1
 193.136.188.36
 10.10.2.0/24
 193.136.192.43
 193.136.192.44
```

Configuração de cliente:

```
radmin> show client config 193.136.192.43
client 193.136.192.43 {
 nastype = other
 secret =xxxxxx
 shortname = proxyNacional1
 require_message_authenticator = no
}
```

Lista de modulos activo:

```
radmin> show module list
 logintime
 acct_unique
 reject (always)
 ok (always)
 expiration
 ldap
 auth_log (detail)
 reply_log (detail)
 pre_proxy_log (detail)
 post_proxy_log (detail)
 suffix (realm)
 attr_filter.post-proxy (attr_filter)
 attr_filter.pre-proxy (attr_filter)
 attr_filter.access_reject (attr_filter)
 attr_filter.accounting_response (attr_filter)
 preprocess
 expr
 detail
 mschap
 files
 eap
 sql
```

show module methods <module> - lista secções onde módulos são usados:

```
radmin> show module methods eap
 authenticate
 authorize
 post-proxy
show module config eap
eap {
 default_eap_type = "ttls"
 timer_expire = 60
 ignore_unknown_eap_types = no
 cisco_accounting_username_bug = no
 max_sessions = 4096
}
```

Verificar propriedades de um modulo:

```
radmin> show module flags eap
 will-check-config
```

Sintaxe para acrescentar cliente em runtime:

radmin>add client file <filename>

Sintaxe para apagar um cliente em runtime:

radmin>del client ipaddr

Sintaxe para fazer reload das configurações. Pode levar um nome de um modulo à frente.

radmin>hup

Sintaxe para inspeccionar o estado de debugging.
radmin> show debug

show debug condition - Shows current debugging condition.

show debug level - Shows current debugging level.

show debug file - Shows current debugging file.

Para direccionar a saida de logs para um ficheiro:

debug file bob.log

Na directiva debug file, não é permitido colocar caminhos completos, sendo que o ficheiro de log fica em /var/log/freeradius

Para fazer uma condição de fazer tracking de processos de autenticação:

debug condition '(User-Name == bob)'

debug condition '((User-Name == bob) || (Packet-Src-IP-Address == 192.168.1.1))'

Para desactivar o debug:

debug condition Disable debug conditionals.

Ver estatísticas de serviço em FreeRadius 3:

```
radmin> stats socket 10.255.251.2 1812
        requests        645589
        responses       641483
        accepts         359013
        rejects         282470
        challenges      0
        dup             0
        invalid         0
        malformed       0
        bad_authenticator       0
        dropped         3110
        unknown_types   0
        last_packet     1402555332
        elapsed.1us     0
        elapsed.10us    0
        elapsed.100us   0
        elapsed.1ms     0
        elapsed.10ms    229378
        elapsed.100ms   384248
        elapsed.1s      27768
        elapsed.10s     86
```

Para sair do radmin:

quit

Para as directivas de debubbing é preferivel usar o raddebug.
Por vezes, no debug de utilizadores pode aparecer dados de outros utilizadores, este problema já foi solucionado em versões mais recentes de FreeRADIUS do que a que vem com o Debian 7.
é necessário ter cuidado com a directiva debug file, já que esta destrói ficheiros que já existam com o mesmo path em versões mais antigas do FreeRadius.

raddebug

Patch de raddebug

Se foi instalada a versão de freeradius.org, não se recomenda fazer esta alteração. Apenas será feita por quem não se sentir confortável em compilar código, e tenha mantido a versão stock 2.1.12 do Debian 7.

Nota: o raddebug aparenta ter problemas de direitos na versão stock Debian 2.1.12, mas não no patch da última versão de freeradius. Para o usar devidamente com o utilizador root na versão defeito Debian, recomenda-se fazer o patch seguinte, com os comandos seguintes. O dpkg-divert destina-se a garantir que qualquer update que seja realizado pelo sistema não toca no nosso raddebug modificado.

```
dpkg-divert --local /usr/sbin/raddebug
patch -p0 /usr/sbin/raddebug < raddebug.patch
```

raddebug.patch

```
95a96
> chgrp radius $outfile
```

Operações de debugging

Para activar o debug geral durante 1 minuto:

raddebug -t 60

Para fazer debug de todas as transacções de um utilizador para o stdout durante 1 minuto:

Seguir o processo de autenticação de um utilizador:

raddebug -t 60 -u utilizador@iscte.pt

ou de um IP:

raddebug -t 60 -i endereço_IPv4

raddebug -t 60 -l endereço_IPv6

Por último, pode-se usar também o raddebug com condições unlang:

raddebug -t -c condição_unlang

raddedbug -t -c '(Packet-Src-IP-Address == ipv4-address)'

O utilizador que estiver a correr o raddebug tem de ter permissões de escrita em /var/log/freeradius, já que o raddebug cria nesse directório um ficheiro temporário radmin.debug.$PID com o stdout do radmin que invoca.

Para seguir o processo de autenticação completo de um utilizador.

```
#raddebug -u rffro@iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] Received Access-Request packet from host 10.61.10.12 port 58406,
id=12, length=182
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  User-Name = "rffro@iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-IP-Address = 10.61.10.12
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-Port = 2063
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Called-Station-Id = "00-0C-29-4C-B5-4F:EDUROAM_1020"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Calling-Station-Id = "60-C5-47-8B-FF-46"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Framed-MTU = 1250
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-Port-Type = Wireless-802.11
```

```
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Framed-Compression = None
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Connect-Info = "CONNECT Unknown radio"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Chargeable-User-Identity = ""
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  EAP-Message = 0x020100130172666672f4069736374652e7074
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Message-Authenticator = 0x4b8b690a2d208650f005ba6a6ed0f842
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] # Executing section authorize from file /etc/freeradius/sites-
enabled/iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] +- entering group authorize {...}
Tue Nov 12 09:21:34 2013 : Debug: [auth_log]  expand: /var/log/freeradius/radacct/%{Client-IP-Address}/auth-
detail-%Y%m%d -> /var/log/freeradius/radacct/10.61.10.12/auth-detail-20131112
Tue Nov 12 09:21:34 2013 : Debug: [auth_log] /var/log/freeradius/radacct/%{Client-IP-Address}/auth-detail-%Y%m%
d expands to /var/log/freeradius/radacct/10.61.10.12/auth-detail-20131112
Tue Nov 12 09:21:34 2013 : Debug: [auth_log]  expand: %t -> Tue Nov 12 09:21:34 2013
Tue Nov 12 09:21:34 2013 : Debug: ++[auth_log] returns ok
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Looking up realm "iscte.pt" for User-Name = "rffro@iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Found realm "iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Adding Stripped-User-Name = "rffro"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Adding Realm = "iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Authentication realm is LOCAL.
Tue Nov 12 09:21:34 2013 : Debug: ++[suffix] returns ok
Tue Nov 12 09:21:34 2013 : Debug: [eap] EAP packet type response id 1 length 19
Tue Nov 12 09:21:34 2013 : Debug: [eap] No EAP Start, assuming it's an on-going EAP conversation
Tue Nov 12 09:21:34 2013 : Debug: ++[eap] returns updated
Tue Nov 12 09:21:34 2013 : Debug: ++? if (User-name == "radius-teste@iscte.pt" )
Tue Nov 12 09:21:34 2013 : Debug: ? Evaluating (User-name == "radius-teste@iscte.pt" ) -> FALSE
Tue Nov 12 09:21:34 2013 : Debug: ++? if (User-name == "radius-teste@iscte.pt" ) -> FALSE
Tue Nov 12 09:21:34 2013 : Debug: ++? if (!(User-Name =~ /^([^@]*)@(.+)$$/))
Tue Nov 12 09:21:34 2013 : Debug: ?? Evaluating (User-Name =~ /^([^@]*)@(.+)$$/) -> TRUE
Tue Nov 12 09:21:34 2013 : Debug: ? Converting !TRUE -> FALSE
Tue Nov 12 09:21:34 2013 : Debug: ++? if (!(User-Name =~ /^([^@]*)@(.+)$$/)) -> FALSE
Tue Nov 12 09:21:34 2013 : Debug: ++- entering policy filter_username {...}
Tue Nov 12 09:21:34 2013 : Debug: +++? if (User-Name =~ /^ /)
Tue Nov 12 09:21:34 2013 : Debug: ? Evaluating (User-Name =~ /^ /) -> FALSE
Tue Nov 12 09:21:34 2013 : Debug: +++? if (User-Name =~ /^ /) -> FALSE
Tue Nov 12 09:21:34 2013 : Debug: +++? if (User-Name =~ / $$/)
Tue Nov 12 09:21:34 2013 : Debug: ? Evaluating (User-Name =~ / $$/) -> FALSE
Tue Nov 12 09:21:34 2013 : Debug: +++? if (User-Name =~ / $$/) -> FALSE
Tue Nov 12 09:21:34 2013 : Debug: +++? if (User-Name != "%{tolower:%{User-Name}}")
Tue Nov 12 09:21:34 2013 : Debug:  expand: %{User-Name} -> rffro@iscte.pt
Tue Nov 12 09:21:34 2013 : Debug:  expand: %{tolower:%{User-Name}} -> rffro@iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: ? Evaluating (User-Name != "%{tolower:%{User-Name}}") -> FALSE
Tue Nov 12 09:21:34 2013 : Debug: +++? if (User-Name != "%{tolower:%{User-Name}}") -> FALSE
Tue Nov 12 09:21:34 2013 : Debug: ++- policy filter_username returns updated
Tue Nov 12 09:21:34 2013 : Debug: ++? if (Calling-Station-Id =~ /([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]
{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})/i)
Tue Nov 12 09:21:34 2013 : Debug: ? Evaluating (Calling-Station-Id =~ /([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-
9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})/i) -> TRUE
Tue Nov 12 09:21:34 2013 : Debug: ++? if (Calling-Station-Id =~ /([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]
{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})/i) -> TRUE
Tue Nov 12 09:21:34 2013 : Debug: ++- entering if (Calling-Station-Id =~ /([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?
([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})/i) {...}
Tue Nov 12 09:21:34 2013 : Debug:  expand: %{1}:%{2}:%{3}:%{4}:%{5}:%{6} -> 60:C5:47:8B:FF:46
Tue Nov 12 09:21:34 2013 : Debug:  expand: %{toupper:%{1}:%{2}:%{3}:%{4}:%{5}:%{6}} -> 60:C5:47:8B:FF:46
Tue Nov 12 09:21:34 2013 : Debug: +++[request] returns updated
Tue Nov 12 09:21:34 2013 : Debug: ++- if (Calling-Station-Id =~ /([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]
{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})/i) returns updated
Tue Nov 12 09:21:34 2013 : Debug: ++ ... skipping else for request 360: Preceding "if" was taken
Tue Nov 12 09:21:34 2013 : Debug: ++? if ("%{sql: SELECT count(*) FROM banned_list WHERE mac_address = '%
{Calling-Station-Id}' or username = LOWER('%{User-Name}') }" != 0 )
Tue Nov 12 09:21:34 2013 : Debug: sql_xlat
Tue Nov 12 09:21:34 2013 : Debug:  expand: %{User-Name} -> rffro@iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: sql_set_user escaped user --> 'rffro@iscte.pt'
Tue Nov 12 09:21:34 2013 : Debug:  expand:  SELECT count(*) FROM banned_list WHERE mac_address = '%{Calling-
Station-Id}' or username = LOWER('%{User-Name}')  ->  SELECT count(*) FROM banned_list WHERE mac_address = '60:
C5:47:8B:FF:46' or username = LOWER('rffro@iscte.pt')
Tue Nov 12 09:21:34 2013 : Debug: sql_xlat finished
Tue Nov 12 09:21:34 2013 : Debug:  expand: %{sql: SELECT count(*) FROM banned_list WHERE mac_address = '%
{Calling-Station-Id}' or username = LOWER('%{User-Name}') } -> 0
Tue Nov 12 09:21:34 2013 : Debug: ? Evaluating ("%{sql: SELECT count(*) FROM banned_list WHERE mac_address = '%
{Calling-Station-Id}' or username = LOWER('%{User-Name}') }" != 0 ) -> FALSE
Tue Nov 12 09:21:34 2013 : Debug: ++? if ("%{sql: SELECT count(*) FROM banned_list WHERE mac_address = '%
```

```
{Calling-Station-Id}' or username = LOWER('%{User-Name}') }" != 0 ) -> FALSE
Tue Nov 12 09:21:34 2013 : Debug: Found Auth-Type = EAP
Tue Nov 12 09:21:34 2013 : Debug: # Executing group from file /etc/freeradius/sites-enabled/iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: +- entering group authenticate {...}
Tue Nov 12 09:21:34 2013 : Debug: [eap] EAP Identity
Tue Nov 12 09:21:34 2013 : Debug: [eap] processing type tls
Tue Nov 12 09:21:34 2013 : Debug: [tls] Initiate
Tue Nov 12 09:21:34 2013 : Debug: [tls] Start returned 1
Tue Nov 12 09:21:34 2013 : Debug: ++[eap] returns handled
Tue Nov 12 09:21:34 2013 : Debug: Sending Access-Challenge packet to host 10.61.10.12 port 58406, id=12,
length=0
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message = 0x010200061520
Tue Nov 12 09:21:34 2013 : Debug:  Message-Authenticator = 0x00000000000000000000000000000000
Tue Nov 12 09:21:34 2013 : Debug:  State = 0x4bddc0a94bdfd5e9b98e0be69018a521
Tue Nov 12 09:21:34 2013 : Debug: Finished request 360.
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] Received Access-Request packet from host 10.61.10.12 port 58406,
id=13, length=333
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  User-Name = "rffro@iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-IP-Address = 10.61.10.12
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-Port = 2063
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Called-Station-Id = "00-0C-29-4C-B5-4F:EDUROAM_1020"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Calling-Station-Id = "60-C5-47-8B-FF-46"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Framed-MTU = 1250
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-Port-Type = Wireless-802.11
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Framed-Compression = None
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Connect-Info = "CONNECT Unknown radio"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Chargeable-User-Identity = ""
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  EAP-Message =
0x02020098158000000008e160301008901000085030152 81f3200d0080149d0dddce9a45a116b6e8a1fddc4c05eaf1c8f243cb2fee5a0000
4a00ffc024c023c00ac009c007c008c028c027c014c013c011c012c026c025c02ac029c005c004c002c003c00fc00ec00cc00d003d003c00
2f000500040035000a0067006b00330039001601000012000a000800060017001800190000b00020100
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  State = 0x4bddc0a94bdfd5e9b98e0be69018a521
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Message-Authenticator = 0x6c4efcadfe398d9525f8c9fcf34c3d37
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] # Executing section authorize from file /etc/freeradius/sites-
enabled/iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] +- entering group authorize {...}
Tue Nov 12 09:21:34 2013 : Debug: [auth_log]  expand: /var/log/freeradius/radacct/%{Client-IP-Address}/auth-
detail-%Y%m%d -> /var/log/freeradius/radacct/10.61.10.12/auth-detail-20131112
Tue Nov 12 09:21:34 2013 : Debug: [auth_log] /var/log/freeradius/radacct/%{Client-IP-Address}/auth-detail-%Y%m%
d expands to /var/log/freeradius/radacct/10.61.10.12/auth-detail-20131112
Tue Nov 12 09:21:34 2013 : Debug: [auth_log]  expand: %t -> Tue Nov 12 09:21:34 2013
Tue Nov 12 09:21:34 2013 : Debug: ++[auth_log] returns ok
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Looking up realm "iscte.pt" for User-Name = "rffro@iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Found realm "iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Adding Stripped-User-Name = "rffro"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Adding Realm = "iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Authentication realm is LOCAL.
Tue Nov 12 09:21:34 2013 : Debug: ++[suffix] returns ok
Tue Nov 12 09:21:34 2013 : Debug: [eap] EAP packet type response id 2 length 152
Tue Nov 12 09:21:34 2013 : Debug: [eap] Continuing tunnel setup.
Tue Nov 12 09:21:34 2013 : Debug: ++[eap] returns ok
Tue Nov 12 09:21:34 2013 : Debug: Found Auth-Type = EAP
Tue Nov 12 09:21:34 2013 : Debug: # Executing group from file /etc/freeradius/sites-enabled/iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: +- entering group authenticate {...}
Tue Nov 12 09:21:34 2013 : Debug: [eap] Request found, released from the list
Tue Nov 12 09:21:34 2013 : Debug: [eap] EAP/ttls
Tue Nov 12 09:21:34 2013 : Debug: [eap] processing type ttls
Tue Nov 12 09:21:34 2013 : Debug: [ttls] Authenticate
Tue Nov 12 09:21:34 2013 : Debug: [ttls] processing EAP-TLS
Tue Nov 12 09:21:34 2013 : Debug: [ttls] Length Included
Tue Nov 12 09:21:34 2013 : Debug: [ttls] eaptls_verify returned 11

Tue Nov 12 09:21:34 2013 : Debug: [ttls]     (other): before/accept initialization
Tue Nov 12 09:21:34 2013 : Debug: [ttls]     TLS_accept: before/accept initialization
Tue Nov 12 09:21:34 2013 : Debug: [ttls]     TLS_accept: SSLv3 read client hello A
Tue Nov 12 09:21:34 2013 : Debug: [ttls]     TLS_accept: SSLv3 write server hello A
Tue Nov 12 09:21:34 2013 : Debug: [ttls]     TLS_accept: SSLv3 write certificate A
Tue Nov 12 09:21:34 2013 : Debug: [ttls]     TLS_accept: SSLv3 write key exchange A
Tue Nov 12 09:21:34 2013 : Debug: [ttls]     TLS_accept: SSLv3 write server done A
Tue Nov 12 09:21:34 2013 : Debug: [ttls]     TLS_accept: SSLv3 flush data
Tue Nov 12 09:21:34 2013 : Debug: [ttls]     TLS_accept: Need to read more data: SSLv3 read client certificate A
```

```
Tue Nov 12 09:21:34 2013 : Debug: [ttls] eaptls_process returned 13

Tue Nov 12 09:21:34 2013 : Debug: ++[eap] returns handled
Tue Nov 12 09:21:34 2013 : Debug: Sending Access-Challenge packet to host 10.61.10.12 port 58406, id=13,
length=0
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message =
0x0103040015c000000f021603010039020000350301528 1f31e25ad5aa745066085ce675f20994e5efdc8b329b7fe6f4817334f9e6600c0
1400000dff01000100000b000403000102160301 0d660b000d62000d5f00047a308204763082035ea003020102021100afef74658346df71
399fb806aefc0468300d06092a864886f70d0101050500303631 0b30090603550406130 24e4c310f300d060355040a1306544552454e4131
163014060355040313 0d544552454e412053534c204341301e170d3133303731313030303030305a170d3136303731303233353935395a30
423121301f060355040b1318446f6d61696e20436f6e74726f6c2056616c
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message =
0x696461746564311d301b060355040313147261646975733 22e69736374652d69756c2e707430820122300d06092a864886f70d01010105
000382010f003082010a0282010100bb4cb21957b3ad6bbab4a611f77fb6ca20d7bda659391d578c13d8d79f2b9c25d7823d7ffa3fe214a6
7fc9bb9e22bd7912fd721289c8cbe1a4308a7fc3973a1dec39d04058ec279dd4e18301cc22dd615d180a1e776439981043b1e47f980e1da0
a5addb32d92f9cad8f3b6d204fe37c500d77bcc7348647c6802b7240bb9da7111e4110f4daf49b340639211a9930c42689541becd9f855c3
873d073e725ccb34c48a774a0541d6932087f81c13d58b12133c444bb3f4
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message =
0x3368802503a1503f456de418845f22437c3a7c74a0d8bddc8c6de828fa529ef85616077fe6a72642aa2d9cbe2dd46deec888c451ff0360
80ff0fa794f5291cfe5bf678d0a495201fc10203010001a38201713082016d301f0603551d230418301680140cbd93680cf3deaba3496b2b
375747ea90e3b9ed301d0603551d0e04160414a6f953f426a2652a413a02d7c4ef2603a8e7b150300e0603551d0f0101ff0404030205a030
0c0603551d130101ff04023000301d0603551d250416301406082b06010505070301 06082b06010505070302302206035 51d20041b301930
0d060b2b06010401b2310102021d3008060667810c010201303a0603551d
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message =
0x1f04333031302fa02da02b8629687474703a2f2f63726c2e7463732e746572656e612e6f72672f544552454e4153534c43412e63726c30
6d06082b06010505070101046130 5f303506082b06010505073002862968747 4703a2f2f6372742e7463732e746572656e612e6f72672f54
4552454e4153534c43412e637274302606082b06010505073001861a687474703a2f2f6f6373702e7463732e746572656e612e6f7267301f
0603551d1104183016821472616469757 3322e69736374652d69756c2e7074300d06092a864886f70d01010505000382010100049c1e46c1
45a0befb63737b2990a92220be8023984bc30a3b4b7ac71935a5d39191d7
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message = 0x7d82e98fc0e48acd3cffedbb
Tue Nov 12 09:21:34 2013 : Debug:  Message-Authenticator = 0x00000000000000000000000000000000
Tue Nov 12 09:21:34 2013 : Debug:  State = 0x4bddc0a94aded5e9b98e0be69018a521
Tue Nov 12 09:21:34 2013 : Debug: Finished request 362.
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] Received Access-Request packet from host 10.61.10.12 port 58406,
id=14, length=187
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  User-Name = "rffro@iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-IP-Address = 10.61.10.12
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-Port = 2063
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Called-Station-Id = "00-0C-29-4C-B5-4F:EDUROAM_1020"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Calling-Station-Id = "60-C5-47-8B-FF-46"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Framed-MTU = 1250
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-Port-Type = Wireless-802.11
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Framed-Compression = None
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Connect-Info = "CONNECT Unknown radio"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Chargeable-User-Identity = ""
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  EAP-Message = 0x020300061500
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  State = 0x4bddc0a94aded5e9b98e0be69018a521
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Message-Authenticator = 0xbc028034c50751ccecaadb271569011b
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] # Executing section authorize from file /etc/freeradius/sites-
enabled/iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] +- entering group authorize {...}
Tue Nov 12 09:21:34 2013 : Debug: [auth_log]  expand: /var/log/freeradius/radacct/%{Client-IP-Address}/auth-
detail-%Y%m%d -> /var/log/freeradius/radacct/10.61.10.12/auth-detail-20131112
Tue Nov 12 09:21:34 2013 : Debug: [auth_log] /var/log/freeradius/radacct/%{Client-IP-Address}/auth-detail-%Y%m%
d expands to /var/log/freeradius/radacct/10.61.10.12/auth-detail-20131112
Tue Nov 12 09:21:34 2013 : Debug: [auth_log]  expand: %t -> Tue Nov 12 09:21:34 2013
Tue Nov 12 09:21:34 2013 : Debug: ++[auth_log] returns ok
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Looking up realm "iscte.pt" for User-Name = "rffro@iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Found realm "iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Adding Stripped-User-Name = "rffro"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Adding Realm = "iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Authentication realm is LOCAL.
Tue Nov 12 09:21:34 2013 : Debug: ++[suffix] returns ok
Tue Nov 12 09:21:34 2013 : Debug: [eap] EAP packet type response id 3 length 6
Tue Nov 12 09:21:34 2013 : Debug: [eap] Continuing tunnel setup.
Tue Nov 12 09:21:34 2013 : Debug: ++[eap] returns ok
Tue Nov 12 09:21:34 2013 : Debug: Found Auth-Type = EAP
Tue Nov 12 09:21:34 2013 : Debug: # Executing group from file /etc/freeradius/sites-enabled/iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: +- entering group authenticate {...}
Tue Nov 12 09:21:34 2013 : Debug: [eap] Request found, released from the list
Tue Nov 12 09:21:34 2013 : Debug: [eap] EAP/ttls
```

```
Tue Nov 12 09:21:34 2013 : Debug: [eap] processing type ttls
Tue Nov 12 09:21:34 2013 : Debug: [ttls] Authenticate
Tue Nov 12 09:21:34 2013 : Debug: [ttls] processing EAP-TLS
Tue Nov 12 09:21:34 2013 : Debug: [ttls] Received TLS ACK
Tue Nov 12 09:21:34 2013 : Debug: [ttls] ACK handshake fragment handler
Tue Nov 12 09:21:34 2013 : Debug: [ttls] eaptls_verify returned 1

Tue Nov 12 09:21:34 2013 : Debug: [ttls] eaptls_process returned 13

Tue Nov 12 09:21:34 2013 : Debug: ++[eap] returns handled
Tue Nov 12 09:21:34 2013 : Debug: Sending Access-Challenge packet to host 10.61.10.12 port 58406, id=14,
length=0
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message =
0x0104040015c000000f02d8665c367cf6474856dbd062a29c49dd096d01d176519ff4a61d9da18e5b7cab4a0fb3c15c67a5fd1fe843d8bf
72e438e20ccb516df110843e9de6a8e5e436cab80d85605e746e839d5245ff3a9b9208828e1c47614d8bdc0abf64bf6abefaa6f2177669fd
42c834a835570936e81fd134ab6926b349738ab530475ab425a2bc22c7a01e11b6bf710d398bf3538655539b3711a55155c1930a18554118
82d244fc1d127f99064f481bd0327adba0fb07030320820cc23d78311eca83e68389ecb2043f1e2d8a67515aca5065d29ea66b6000049c30
82049830820380a00302010202104bc814032f07fa6aa4f0da29df6179ba
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message =
0x300d06092a864886f70d01010505003081973l0b3009060355040613025553310b3009060355040813025554311730150603550407130e
53616c74204c616b652043697479311e301c060355040a13155468652055534552545255535420 4e6574776f726b3121301f060355040b13
18687474703a2f2f7777772e75736572747275737 42e636f6d311f301d06035504031316555 44e2d5553455246697273742d486172647761
7265301e170d303930353138303030303030305a170d323030353330313034383385a3036310b3009060355040613024e4c310f300d060355
040a1306544552454e4131163014060355040313 0d544552454e41205353
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message =
0x4c204341308201223 00d06092a864886f70d01010105000382010f003082010a0282010100c3e348c42f5cc1cba999fd1ba2835d8a3dad
3ad0e2a4431f4d0efe352530a5691bc4e8e5c18f547ee16aa29a5c5cde3dfc02ce96b85f8f835bcc604090f8e4b63a259c5f1451ecb1e7af
9e50a13155c702bdac528a7f358e82fa84ad15fea27f83103a5553942c01167494546328a3f25b293d94888020e214592119b4a498e160e6
f2eba2808343e0ad68f379198b6843513f8a9b41850c358c5db5f1b6e5a7c383b56b236fd4a5eb50e594f14a5fee274b141215244c0dcf62
8db70021ad3a320f580b5f1e9bd1df9d8ea91935502f41a9ad3bc6e045b2
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message =
0x53397f21bf221a875c34ae526f077da20b4e9f2b79a67d13ddf57f837c2f5a5d77787891a014bf7d0203010001a382013e3082013a301f
0603551d23041830168014a1725f261b289843955d0737d585969d4bd2c345301d0603551d0e041604140cbd93680cf3deaba3496b2b3757
47ea90e3b9ed300e0603551d0f0101ff040403020106301206035 51d130101ff040830060101ff02010030180603551d200411300f300d06
0b2b06010401b2310102021d30440603551d1f043d303b3039a037a0358633687474703a2f2f63726c2e757365727 4727573742e636f6d2f
55544e2d5553455246697273742d486172647761726 5e63726c30740608
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message = 0x2b0601050507010104683066
Tue Nov 12 09:21:34 2013 : Debug:  Message-Authenticator = 0x00000000000000000000000000000000
Tue Nov 12 09:21:34 2013 : Debug:  State = 0x4bddc0a949d9d5e9b98e0be69018a521
Tue Nov 12 09:21:34 2013 : Debug: Finished request 363.
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] Received Access-Request packet from host 10.61.10.12 port 58406,
id=15, length=187
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  User-Name = "rffro@iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-IP-Address = 10.61.10.12
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-Port = 2063
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Called-Station-Id = "00-0C-29-4C-B5-4F:EDUROAM_1020"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Calling-Station-Id = "60-C5-47-8B-FF-46"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Framed-MTU = 1250
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-Port-Type = Wireless-802.11
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Framed-Compression = None
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Connect-Info = "CONNECT Unknown radio"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Chargeable-User-Identity = ""
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  EAP-Message = 0x020400061500
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  State = 0x4bddc0a949d9d5e9b98e0be69018a521
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Message-Authenticator = 0xd3cd78ba61d21401764fb8ab21cf9c6e
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] # Executing section authorize from file /etc/freeradius/sites-
enabled/iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] +- entering group authorize {...}
Tue Nov 12 09:21:34 2013 : Debug: [auth_log]  expand: /var/log/freeradius/radacct/%{Client-IP-Address}/auth-
detail-%Y%m%d -> /var/log/freeradius/radacct/10.61.10.12/auth-detail-20131112
Tue Nov 12 09:21:34 2013 : Debug: [auth_log] /var/log/freeradius/radacct/%{Client-IP-Address}/auth-detail-%Y%m%
d expands to /var/log/freeradius/radacct/10.61.10.12/auth-detail-20131112
Tue Nov 12 09:21:34 2013 : Debug: [auth_log]  expand: %t -> Tue Nov 12 09:21:34 2013
Tue Nov 12 09:21:34 2013 : Debug: ++[auth_log] returns ok
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Looking up realm "iscte.pt" for User-Name = "rffro@iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Found realm "iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Adding Stripped-User-Name = "rffro"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Adding Realm = "iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Authentication realm is LOCAL.
Tue Nov 12 09:21:34 2013 : Debug: ++[suffix] returns ok
Tue Nov 12 09:21:34 2013 : Debug: [eap] EAP packet type response id 4 length 6
```

```
Tue Nov 12 09:21:34 2013 : Debug: [eap] Continuing tunnel setup.
Tue Nov 12 09:21:34 2013 : Debug: ++[eap] returns ok
Tue Nov 12 09:21:34 2013 : Debug: Found Auth-Type = EAP
Tue Nov 12 09:21:34 2013 : Debug: # Executing group from file /etc/freeradius/sites-enabled/iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: +- entering group authenticate {...}
Tue Nov 12 09:21:34 2013 : Debug: [eap] Request found, released from the list
Tue Nov 12 09:21:34 2013 : Debug: [eap] EAP/ttls
Tue Nov 12 09:21:34 2013 : Debug: [eap] processing type ttls
Tue Nov 12 09:21:34 2013 : Debug: [ttls] Authenticate
Tue Nov 12 09:21:34 2013 : Debug: [ttls] processing EAP-TLS
Tue Nov 12 09:21:34 2013 : Debug: [ttls] Received TLS ACK
Tue Nov 12 09:21:34 2013 : Debug: [ttls] ACK handshake fragment handler
Tue Nov 12 09:21:34 2013 : Debug: [ttls] eaptls_verify returned 1

Tue Nov 12 09:21:34 2013 : Debug: [ttls] eaptls_process returned 13

Tue Nov 12 09:21:34 2013 : Debug: ++[eap] returns handled
Tue Nov 12 09:21:34 2013 : Debug: Sending Access-Challenge packet to host 10.61.10.12 port 58406, id=15,
length=0
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message =
0x0105040015c000000f02303d06082b0601050507300286316874747703a2f2f6372742e7573657274727573742e636f6d2f55544e416464
5472757374536572766572 5f43412e637274302506082b0601050507300186196874747703a2f2f6f6373702e7573657274727573742e636f
6d300d06092a864886f70d0101050500038201010 04e23ee489cf6858b71c40a6e739372c03a8e808ad9b3cab2d4019c28cff25c0e214493
0bb61a21e39801940e6749811ebe3d0d4e60daefa0314e95eff3dd7a5a822043b6a16343b3506943624b5662b0348ab913435993ec147988
f34893e89dc9fa87720c6b56a0c3158d68a5871f712de65a6d3c69714004
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message =
0x55dca0439420453878d7bd8ad839c6df09b75a9aa903b8281078cdbf011b5a113e38f4d81b3479cf33d201fdac98cd6d4711904cbbb95b
d870e7d5afb6ccc486e675c09e29b62b0f2aa569020de3e9a2b45dc0f3ce2c6a85387661c64982ab51b382a6b941982898fb6bfe8a16ff31
7e5447a83cdc4326a99b05b79ec034439130d432c3115ae10004403082043c30820324a0030201020210484bacf1aac7d71343d1a2743549
9725300d06092a864886f70d0101050500306f310b3009060355040613025345311430120603550 40a130b4164645472757374204142312 6
3024060355040b131d4164645472757374204578746572 6e616c20545450
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message =
0x204e6574776f726b312230200603550403131941646454727573742045787465726e616c20434120526f6f74301e170d30353036303730
38303931305a170d3230303533303130343833385a308197310b3009060355040613025553310b3009060355040813025554311730150603
550407130e53616c74204c616b652043697479311e301c060355040a13155468652055534552545255354204e6574776f726b3121301f06
0355040b1318687474703a2f2f7777772e7573657274727573742e636f6d311f301d06035504031316555 44e2d5553455246697273742d48
617264776172653082012300d06092a864886f70d01010105000382010f
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message =
0x003082010a0282010100b1f7c3383fb4a87fcf39825167d06d9fd2ff58f3e79f2bec0d895499b9389916f7e0217948c2bb617412961d3c
6a72d53c10673a39ed2b13cd66eb950933a46c97b1e8c6ecc175799c465e8dabd06afdb92a55171054b319f09af6f1b15db6a76dfbe07117
6ba288fb00dffe1a31770c9a017ab132e32b0107386ec3a55e23bc459b7b50c1c9308fdbe52b7ad35bfb33401ea0d59817bc8b87c389d35d
a08eb2aaaaf68e698806c5fa8921f3089d692e09339b290d460f8ccc4934b06951bdf906cd68ad664cbc3eac61bd0a880ec8df3dee7c044c
9d0a5e6b91d6eec7ed288dab4d878973d06ea4d01e168b14e17644037f63
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message = 0xace4cd499cc592f4ab32a148
Tue Nov 12 09:21:34 2013 : Debug:  Message-Authenticator = 0x00000000000000000000000000000000
Tue Nov 12 09:21:34 2013 : Debug:  State = 0x4bddc0a948d8d5e9b98e0be69018a521
Tue Nov 12 09:21:34 2013 : Debug: Finished request 365.
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] Received Access-Request packet from host 10.61.10.12 port 58406,
id=17, length=187
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  User-Name = "rffro@iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-IP-Address = 10.61.10.12
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-Port = 2063
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Called-Station-Id = "00-0C-29-4C-B5-4F:EDUROAM_1020"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Calling-Station-Id = "60-C5-47-8B-FF-46"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Framed-MTU = 1250
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-Port-Type = Wireless-802.11
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Framed-Compression = None
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Connect-Info = "CONNECT Unknown radio"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Chargeable-User-Identity = ""
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  EAP-Message = 0x020500061500
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  State = 0x4bddc0a948d8d5e9b98e0be69018a521
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Message-Authenticator = 0xec1f1b817c34cc3b85c6e0f0e077400f
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] # Executing section authorize from file /etc/freeradius/sites-
enabled/iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] +- entering group authorize {...}
Tue Nov 12 09:21:34 2013 : Debug: [auth_log]  expand: /var/log/freeradius/radacct/%{Client-IP-Address}/auth-
detail-%Y%m%d -> /var/log/freeradius/radacct/10.61.10.12/auth-detail-20131112
Tue Nov 12 09:21:34 2013 : Debug: [auth_log] /var/log/freeradius/radacct/%{Client-IP-Address}/auth-detail-%Y%m%
d expands to /var/log/freeradius/radacct/10.61.10.12/auth-detail-20131112
Tue Nov 12 09:21:34 2013 : Debug: [auth_log]  expand: %t -> Tue Nov 12 09:21:34 2013
Tue Nov 12 09:21:34 2013 : Debug: ++[auth_log] returns ok
```

```
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Looking up realm "iscte.pt" for User-Name = "rffro@iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Found realm "iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Adding Stripped-User-Name = "rffro"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Adding Realm = "iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Authentication realm is LOCAL.
Tue Nov 12 09:21:34 2013 : Debug: ++[suffix] returns ok
Tue Nov 12 09:21:34 2013 : Debug: [eap] EAP packet type response id 5 length 6
Tue Nov 12 09:21:34 2013 : Debug: [eap] Continuing tunnel setup.
Tue Nov 12 09:21:34 2013 : Debug: ++[eap] returns ok
Tue Nov 12 09:21:34 2013 : Debug: Found Auth-Type = EAP
Tue Nov 12 09:21:34 2013 : Debug: # Executing group from file /etc/freeradius/sites-enabled/iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: +- entering group authenticate {...}
Tue Nov 12 09:21:34 2013 : Debug: [eap] Request found, released from the list
Tue Nov 12 09:21:34 2013 : Debug: [eap] EAP/ttls
Tue Nov 12 09:21:34 2013 : Debug: [eap] processing type ttls
Tue Nov 12 09:21:34 2013 : Debug: [ttls] Authenticate
Tue Nov 12 09:21:34 2013 : Debug: [ttls] processing EAP-TLS
Tue Nov 12 09:21:34 2013 : Debug: [ttls] Received TLS ACK
Tue Nov 12 09:21:34 2013 : Debug: [ttls] ACK handshake fragment handler
Tue Nov 12 09:21:34 2013 : Debug: [ttls] eaptls_verify returned 1

Tue Nov 12 09:21:34 2013 : Debug: [ttls] eaptls_process returned 13

Tue Nov 12 09:21:34 2013 : Debug: ++[eap] returns handled
Tue Nov 12 09:21:34 2013 : Debug: Sending Access-Challenge packet to host 10.61.10.12 port 58406, id=17,
length=0
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message =
0x0106032a158000000f025b0203010001a381aa3081a7301f0603551d23041830168014adbd987a34b426f7fac42654ef03bde024cb541a
301d0603551d0e04160414a1725f261b289843955d0737d585969d4bd2c345300e0603551d0f0101ff040403020106300f0603551d130101
ff040530030101ff30440603551d1f043d303b3039a037a0358633687474703a2f2f63726c2e7573657274727573742e636f6d2f41646454
72757374457874657265726e616c4341526f6f742e63726c300d06092a864886f70d0101050500038201010003cec7be0aea30e966d30d785c6d2
685b455a82a6340fb0c992235e116d0811b27409233a352573585ecab97c
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message =
0x28fa47ecf9a0035850b653ef8cdb39e467e9d8ca2846d4a7e0f53875f8e7cb5cbf1d113c6a409b2d4456d3f7ff0528320c15c8644593e8
21248f2dda7a847b4fcfcdb2257c7710d394d10491a8251c09220f7d44351114efaf00fe5eea5f8eb0d99259bafc1396a0180156cedaf628
0bb1afdd5c4f5cb2f38f5a71cfed18ad63881d8e95f7ea95e71fad90b8840847857f222f1a1d4830d64c08d8371967322beb5cd0b2fc6e57
9f04355e90007e11c7de132acda46d4526c78856a0f06af7d8e7fc277e6708d0bdfab6c361020165b9b82fcf5a160301014b0c0001470300
174104f52439fdd5b87722b58c3ebeaf83b335abe7f2627816344d4e9b35
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message =
0x8422eb1b73f4f99a976efcef29229c255891fe8fd7e101c98971c4a2fdb4911e92e69c21540100af41f62f5c0601a28f04fe5c54100e01
861928e396432bb0bebcd7ce085bb65292ade56b40575201b84860910b19d126d66d2fa264991fe6e8cf674eeed7122a12f9b9d73b6ca9ae
98642ea0db8d2a272f1eface725ae2cb7cc86bab7d386ac19f4d29d054bc7f020f7b0fdcca8c3b1c77bcf063d442ba164b622d0a4531fb91
a608931f0c6d2a651773672518bd4b36b019c4b42c237725da934151da3dde5283934fb352e4ed696c04076800334f3dd2fb98ab0cc54819
54f8e2e8ec4b32f0e60dbe73cc4dcc482b2dfec5cce1364c53bee149b947
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message =
0xf145b3b716ba2bee2722327e2f4ce1c347b352aaf2251a8df263abf360ee8c40684b2a06ec6034685126160301000040e000000
Tue Nov 12 09:21:34 2013 : Debug:  Message-Authenticator = 0x00000000000000000000000000000000
Tue Nov 12 09:21:34 2013 : Debug:  State = 0x4bddc0a94fdbd5e9b98e0be69018a521
Tue Nov 12 09:21:34 2013 : Debug: Finished request 368.
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] Received Access-Request packet from host 10.61.10.12 port 58406,
id=18, length=325
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  User-Name = "rffro@iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-IP-Address = 10.61.10.12
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-Port = 2063
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Called-Station-Id = "00-0C-29-4C-B5-4F:EDUROAM_1020"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Calling-Station-Id = "60-C5-47-8B-FF-46"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Framed-MTU = 1250
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-Port-Type = Wireless-802.11
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Framed-Compression = None
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Connect-Info = "CONNECT Unknown radio"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Chargeable-User-Identity = ""
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  EAP-Message =
0x020600901580000000861603010046100000424104 89c86de0667ea943c87221ef12abc060dfd8796f806900e699d8bf6818c4387093e7
7c221651072a2ae63157bd6f7eccb4d6a576d1d8280f3e1e9a9fe0a6066714030100010116030100 30ed1aa3048abae8da8a04a3083d3541
a652f486a6a150e2aac3317df3c8e9b5349d80c94a6b7263e94c9ba42aaaa2c0d7
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  State = 0x4bddc0a94fdbd5e9b98e0be69018a521
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Message-Authenticator = 0x149694d3d238dbc5d7430dde3f1ac062
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] # Executing section authorize from file /etc/freeradius/sites-
enabled/iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] +- entering group authorize {...}
Tue Nov 12 09:21:34 2013 : Debug: [auth_log]  expand: /var/log/freeradius/radacct/%{Client-IP-Address}/auth-
```

```
detail-%Y%m%d -> /var/log/freeradius/radacct/10.61.10.12/auth-detail-20131112
Tue Nov 12 09:21:34 2013 : Debug: [auth_log] /var/log/freeradius/radacct/%{Client-IP-Address}/auth-detail-%Y%m%
d expands to /var/log/freeradius/radacct/10.61.10.12/auth-detail-20131112
Tue Nov 12 09:21:34 2013 : Debug: [auth_log]  expand: %t -> Tue Nov 12 09:21:34 2013
Tue Nov 12 09:21:34 2013 : Debug: ++[auth_log] returns ok
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Looking up realm "iscte.pt" for User-Name = "rffro@iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Found realm "iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Adding Stripped-User-Name = "rffro"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Adding Realm = "iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Authentication realm is LOCAL.
Tue Nov 12 09:21:34 2013 : Debug: ++[suffix] returns ok
Tue Nov 12 09:21:34 2013 : Debug: [eap] EAP packet type response id 6 length 144
Tue Nov 12 09:21:34 2013 : Debug: [eap] Continuing tunnel setup.
Tue Nov 12 09:21:34 2013 : Debug: ++[eap] returns ok
Tue Nov 12 09:21:34 2013 : Debug: Found Auth-Type = EAP
Tue Nov 12 09:21:34 2013 : Debug: # Executing group from file /etc/freeradius/sites-enabled/iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: +- entering group authenticate {...}
Tue Nov 12 09:21:34 2013 : Debug: [eap] Request found, released from the list
Tue Nov 12 09:21:34 2013 : Debug: [eap] EAP/ttls
Tue Nov 12 09:21:34 2013 : Debug: [eap] processing type ttls
Tue Nov 12 09:21:34 2013 : Debug: [ttls] Authenticate
Tue Nov 12 09:21:34 2013 : Debug: [ttls] processing EAP-TLS
Tue Nov 12 09:21:34 2013 : Debug: [ttls] Length Included
Tue Nov 12 09:21:34 2013 : Debug: [ttls] eaptls_verify returned 11

Tue Nov 12 09:21:34 2013 : Debug: [ttls]     TLS_accept: SSLv3 read client key exchange A
Tue Nov 12 09:21:34 2013 : Debug: [ttls]     TLS_accept: SSLv3 read finished A
Tue Nov 12 09:21:34 2013 : Debug: [ttls]     TLS_accept: SSLv3 write change cipher spec A
Tue Nov 12 09:21:34 2013 : Debug: [ttls]     TLS_accept: SSLv3 write finished A
Tue Nov 12 09:21:34 2013 : Debug: [ttls]     TLS_accept: SSLv3 flush data
Tue Nov 12 09:21:34 2013 : Debug: [ttls]     (other): SSL negotiation finished successfully
Tue Nov 12 09:21:34 2013 : Debug: [ttls] eaptls_process returned 13

Tue Nov 12 09:21:34 2013 : Debug: ++[eap] returns handled
Tue Nov 12 09:21:34 2013 : Debug: Sending Access-Challenge packet to host 10.61.10.12 port 58406, id=18,
length=0
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message =
0x0107004515800000003b1403010001011603010030adce228b69e5079729978735f2d05190c5f8b0d4e7454fffb7e397185850386b48cd
b3fe688b8cbd34b03d9b4ba63ef3
Tue Nov 12 09:21:34 2013 : Debug:  Message-Authenticator = 0x00000000000000000000000000000000
Tue Nov 12 09:21:34 2013 : Debug:  State = 0x4bddc0a94edad5e9b98e0be69018a521
Tue Nov 12 09:21:34 2013 : Debug: Finished request 371.
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] Received Access-Request packet from host 10.61.10.12 port 58406,
id=19, length=340
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  User-Name = "rffro@iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-IP-Address = 10.61.10.12
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-Port = 2063
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Called-Station-Id = "00-0C-29-4C-B5-4F:EDUROAM_1020"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Calling-Station-Id = "60-C5-47-8B-FF-46"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Framed-MTU = 1250
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-Port-Type = Wireless-802.11
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Framed-Compression = None
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Connect-Info = "CONNECT Unknown radio"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Chargeable-User-Identity = ""
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  EAP-Message =
0x0207009f1580000000951703010090 9fce18abd32eb3d8a4bdcfc6563b3fd67828d155ef2752dfa80135f2e95b0d99d6052d72f4f9cd34
9832ee105c77a42bccf6e91e17c60679381432f6e5ec22ba9432e56c456a4e44888cc6b9f3c582aa81ea3a8eef7d13520dee9e787c4f78cd
67f6ca6b458efea37aea69f1cffa240e3b2d333b19b12f3cfda440309ce2fab3c7ef2e66f96d318fac7b807a4e6c505c
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  State = 0x4bddc0a94edad5e9b98e0be69018a521
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Message-Authenticator = 0x2731026aebed1008c274612d55553bb3
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] # Executing section authorize from file /etc/freeradius/sites-
enabled/iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] +- entering group authorize {...}
Tue Nov 12 09:21:34 2013 : Debug: [auth_log]  expand: /var/log/freeradius/radacct/%{Client-IP-Address}/auth-
detail-%Y%m%d -> /var/log/freeradius/radacct/10.61.10.12/auth-detail-20131112
Tue Nov 12 09:21:34 2013 : Debug: [auth_log] /var/log/freeradius/radacct/%{Client-IP-Address}/auth-detail-%Y%m%
d expands to /var/log/freeradius/radacct/10.61.10.12/auth-detail-20131112
Tue Nov 12 09:21:34 2013 : Debug: [auth_log]  expand: %t -> Tue Nov 12 09:21:34 2013
Tue Nov 12 09:21:34 2013 : Debug: ++[auth_log] returns ok
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Looking up realm "iscte.pt" for User-Name = "rffro@iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Found realm "iscte.pt"
```

```
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Adding Stripped-User-Name = "rffro"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Adding Realm = "iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Authentication realm is LOCAL.
Tue Nov 12 09:21:34 2013 : Debug: ++[suffix] returns ok
Tue Nov 12 09:21:34 2013 : Debug: [eap] EAP packet type response id 7 length 159
Tue Nov 12 09:21:34 2013 : Debug: [eap] Continuing tunnel setup.
Tue Nov 12 09:21:34 2013 : Debug: ++[eap] returns ok
Tue Nov 12 09:21:34 2013 : Debug: Found Auth-Type = EAP
Tue Nov 12 09:21:34 2013 : Debug: # Executing group from file /etc/freeradius/sites-enabled/iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: +- entering group authenticate {...}
Tue Nov 12 09:21:34 2013 : Debug: [eap] Request found, released from the list
Tue Nov 12 09:21:34 2013 : Debug: [eap] EAP/ttls
Tue Nov 12 09:21:34 2013 : Debug: [eap] processing type ttls
Tue Nov 12 09:21:34 2013 : Debug: [ttls] Authenticate
Tue Nov 12 09:21:34 2013 : Debug: [ttls] processing EAP-TLS
Tue Nov 12 09:21:34 2013 : Debug: [ttls] Length Included
Tue Nov 12 09:21:34 2013 : Debug: [ttls] eaptls_verify returned 11
Tue Nov 12 09:21:34 2013 : Debug: [ttls] eaptls_process returned 7
Tue Nov 12 09:21:34 2013 : Debug: [ttls] Session established.  Proceeding to decode tunneled attributes.
Tue Nov 12 09:21:34 2013 : Debug: # Executing section authorize from file /etc/freeradius/sites-enabled/inner-
tunnel
Tue Nov 12 09:21:34 2013 : Debug: +- entering group authorize {...}
Tue Nov 12 09:21:34 2013 : Debug: ++? if (!(User-Name =~ /^([^@]*)@(.+)$$/))
Tue Nov 12 09:21:34 2013 : Debug: ?? Evaluating (User-Name =~ /^([^@]*)@(.+)$$/) -> TRUE
Tue Nov 12 09:21:34 2013 : Debug: ? Converting !TRUE -> FALSE
Tue Nov 12 09:21:34 2013 : Debug: ++? if (!(User-Name =~ /^([^@]*)@(.+)$$/)) -> FALSE
Tue Nov 12 09:21:34 2013 : Debug: [mschap] Found MS-CHAP attributes.  Setting 'Auth-Type  = mschap'
Tue Nov 12 09:21:34 2013 : Debug: ++[mschap] returns ok
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Looking up realm "iscte.pt" for User-Name = "rffro@iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Found realm "iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Adding Stripped-User-Name = "rffro"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Adding Realm = "iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Authentication realm is LOCAL.
Tue Nov 12 09:21:34 2013 : Debug: ++[suffix] returns ok
Tue Nov 12 09:21:34 2013 : Debug: ++[control] returns ok
Tue Nov 12 09:21:34 2013 : Debug: [eap] No EAP-Message, not doing EAP
Tue Nov 12 09:21:34 2013 : Debug: ++[eap] returns noop
Tue Nov 12 09:21:34 2013 : Debug: [ldap] performing user authorization for rffro
Tue Nov 12 09:21:34 2013 : Debug: [ldap]  expand: %{Stripped-User-Name} -> rffro
Tue Nov 12 09:21:34 2013 : Debug: [ldap]  expand: (sAMAccountName=%{%{Stripped-User-Name}:-%{User-Name}}) ->
(sAMAccountName=rffro)
Tue Nov 12 09:21:34 2013 : Debug: [ldap]  expand: CN=Users,DC=wiscte,DC=wfarm -> CN=Users,DC=wiscte,DC=wfarm
Tue Nov 12 09:21:34 2013 : Debug: [ldap] No default NMAS login sequence
Tue Nov 12 09:21:34 2013 : Debug: [ldap] looking for check items in directory...
Tue Nov 12 09:21:34 2013 : Debug: [ldap] looking for reply items in directory...
Tue Nov 12 09:21:34 2013 : Debug: [ldap] user rffro authorized to use remote access
Tue Nov 12 09:21:34 2013 : Debug: ++[ldap] returns ok
Tue Nov 12 09:21:34 2013 : Debug: [files]  expand: CN=Users,DC=wiscte,DC=wfarm -> CN=Users,DC=wiscte,DC=wfarm
Tue Nov 12 09:21:34 2013 : Debug: [files]  expand: %{Stripped-User-Name} -> rffro
Tue Nov 12 09:21:34 2013 : Debug: [files]  expand: (sAMAccountName=%{%{Stripped-User-Name}:-%{User-Name}}) ->
(sAMAccountName=rffro)
Tue Nov 12 09:21:34 2013 : Debug: [files] users: Matched entry DEFAULT at line 2
Tue Nov 12 09:21:34 2013 : Debug: ++[files] returns ok
Tue Nov 12 09:21:34 2013 : Debug: Found Auth-Type = MSCHAP
Tue Nov 12 09:21:34 2013 : Debug: # Executing group from file /etc/freeradius/sites-enabled/inner-tunnel
Tue Nov 12 09:21:34 2013 : Debug: +- entering group MS-CHAP {...}
Tue Nov 12 09:21:34 2013 : Debug: [mschap] Creating challenge hash with username: rffro@iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: [mschap] Told to do MS-CHAPv2 for rffro@iscte.pt with NT-Password
Tue Nov 12 09:21:34 2013 : Debug: [mschap]  expand: %{Stripped-User-Name} -> rffro
Tue Nov 12 09:21:34 2013 : Debug: [mschap]  expand: --username=%{%{Stripped-User-Name}:-%{%{User-Name}:-None}} -
> --username=rffro
Tue Nov 12 09:21:34 2013 : Debug: [mschap] Creating challenge hash with username: rffro@iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: [mschap]  expand: %{mschap:Challenge} -> a4f6f5ef0493bb34
Tue Nov 12 09:21:34 2013 : Debug: [mschap]  expand: --challenge=%{%{mschap:Challenge}:-00} -> --
challenge=a4f6f5ef0493bb34
Tue Nov 12 09:21:34 2013 : Debug: [mschap]  expand: %{mschap:NT-Response} ->
a31dd20f06dcfb9e3fa5e52a9193f90aba1604456dd9e558
Tue Nov 12 09:21:34 2013 : Debug: [mschap]  expand: --nt-response=%{%{mschap:NT-Response}:-00} -> --nt-
response=a31dd20f06dcfb9e3fa5e52a9193f90aba1604456dd9e558
Tue Nov 12 09:21:34 2013 : Debug: [mschap] adding MS-CHAPv2 MPPE keys
Tue Nov 12 09:21:34 2013 : Debug: ++[mschap] returns ok
```

```
Tue Nov 12 09:21:34 2013 : Debug:   WARNING: Empty post-auth section.  Using default return values.
Tue Nov 12 09:21:34 2013 : Debug: # Executing section post-auth from file /etc/freeradius/sites-enabled/inner-
tunnel
Tue Nov 12 09:21:34 2013 : Debug: [ttls] Got tunneled Access-Accept
Tue Nov 12 09:21:34 2013 : Debug: [ttls] Got MS-CHAP2-Success, tunneling it to the client in a challenge.
Tue Nov 12 09:21:34 2013 : Debug: ++[eap] returns handled
Tue Nov 12 09:21:34 2013 : Debug: Sending Access-Challenge packet to host 10.61.10.12 port 58406, id=19,
length=0
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message =
0x0108005f158000000055170301005014cc8bf1a1b3a126285fa232691b6963878632737363 48fb2611741590210fe58147fe91ca3904d1
43c7c5880a2c7b5db2a6c07fc5badabde2d43af260f641a07199df09662bce65d687443f25bfbe30
Tue Nov 12 09:21:34 2013 : Debug:  Message-Authenticator = 0x00000000000000000000000000000000
Tue Nov 12 09:21:34 2013 : Debug:  State = 0x4bddc0a94dd5d5e9b98e0be69018a521
Tue Nov 12 09:21:34 2013 : Debug: Finished request 373.
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] Received Access-Request packet from host 10.61.10.12 port 58406,
id=20, length=187
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  User-Name = "rffro@iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-IP-Address = 10.61.10.12
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-Port = 2063
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Called-Station-Id = "00-0C-29-4C-B5-4F:EDUROAM_1020"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Calling-Station-Id = "60-C5-47-8B-FF-46"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Framed-MTU = 1250
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  NAS-Port-Type = Wireless-802.11
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Framed-Compression = None
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Connect-Info = "CONNECT Unknown radio"
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Chargeable-User-Identity = ""
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  EAP-Message = 0x020800061500
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  State = 0x4bddc0a94dd5d5e9b98e0be69018a521
Tue Nov 12 09:21:34 2013 : Debug: [<thread>]  Message-Authenticator = 0x61f258b1a64a5aaee3c0ff83fd94cd0c
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] # Executing section authorize from file /etc/freeradius/sites-
enabled/iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: [<thread>] +- entering group authorize {...}
Tue Nov 12 09:21:34 2013 : Debug: [auth_log]  expand: /var/log/freeradius/radacct/%{Client-IP-Address}/auth-
detail-%Y%m%d -> /var/log/freeradius/radacct/10.61.10.12/auth-detail-20131112
Tue Nov 12 09:21:34 2013 : Debug: [auth_log] /var/log/freeradius/radacct/%{Client-IP-Address}/auth-detail-%Y%m%
d expands to /var/log/freeradius/radacct/10.61.10.12/auth-detail-20131112
Tue Nov 12 09:21:34 2013 : Debug: [auth_log]  expand: %t -> Tue Nov 12 09:21:34 2013
Tue Nov 12 09:21:34 2013 : Debug: ++[auth_log] returns ok
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Looking up realm "iscte.pt" for User-Name = "rffro@iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Found realm "iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Adding Stripped-User-Name = "rffro"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Adding Realm = "iscte.pt"
Tue Nov 12 09:21:34 2013 : Debug: [suffix] Authentication realm is LOCAL.
Tue Nov 12 09:21:34 2013 : Debug: ++[suffix] returns ok
Tue Nov 12 09:21:34 2013 : Debug: [eap] EAP packet type response id 8 length 6
Tue Nov 12 09:21:34 2013 : Debug: [eap] Continuing tunnel setup.
Tue Nov 12 09:21:34 2013 : Debug: ++[eap] returns ok
Tue Nov 12 09:21:34 2013 : Debug: Found Auth-Type = EAP
Tue Nov 12 09:21:34 2013 : Debug: # Executing group from file /etc/freeradius/sites-enabled/iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: +- entering group authenticate {...}
Tue Nov 12 09:21:34 2013 : Debug: [eap] Request found, released from the list
Tue Nov 12 09:21:34 2013 : Debug: [eap] EAP/ttls
Tue Nov 12 09:21:34 2013 : Debug: [eap] processing type ttls
Tue Nov 12 09:21:34 2013 : Debug: [ttls] Authenticate
Tue Nov 12 09:21:34 2013 : Debug: [ttls] processing EAP-TLS
Tue Nov 12 09:21:34 2013 : Debug: [ttls] Received TLS ACK
Tue Nov 12 09:21:34 2013 : Debug: [ttls] ACK handshake is finished
Tue Nov 12 09:21:34 2013 : Debug: [ttls] eaptls_verify returned 3

Tue Nov 12 09:21:34 2013 : Debug: [ttls] eaptls_process returned 3

Tue Nov 12 09:21:34 2013 : Debug: [ttls] Using saved attributes from the original Access-Accept
Tue Nov 12 09:21:34 2013 : Debug: [eap] Freeing handler
Tue Nov 12 09:21:34 2013 : Debug: ++[eap] returns ok
Tue Nov 12 09:21:34 2013 : Debug: # Executing section post-auth from file /etc/freeradius/sites-enabled/iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: +- entering group post-auth {...}
Tue Nov 12 09:21:34 2013 : Debug: [reply_log]  expand: /var/log/freeradius/radacct/%{Client-IP-Address}/reply-
detail-%Y%m%d -> /var/log/freeradius/radacct/10.61.10.12/reply-detail-20131112
Tue Nov 12 09:21:34 2013 : Debug: [reply_log] /var/log/freeradius/radacct/%{Client-IP-Address}/reply-detail-%Y%
m%d expands to /var/log/freeradius/radacct/10.61.10.12/reply-detail-20131112
Tue Nov 12 09:21:34 2013 : Debug: [reply_log]  expand: %t -> Tue Nov 12 09:21:34 2013
```

```
Tue Nov 12 09:21:34 2013 : Debug: ++[reply_log] returns ok
Tue Nov 12 09:21:34 2013 : Debug: ++? if (User-Name != "radius_user@iscte.pt" )
Tue Nov 12 09:21:34 2013 : Debug: ? Evaluating (User-Name != "radius_user@iscte.pt" ) -> TRUE
Tue Nov 12 09:21:34 2013 : Debug: ++? if (User-Name != "radius_user@iscte.pt" ) -> TRUE
Tue Nov 12 09:21:34 2013 : Debug: ++- entering if (User-Name != "radius_user@iscte.pt" ) {...}
Tue Nov 12 09:21:34 2013 : Debug: [sql]  expand: %{User-Name} -> rffro@iscte.pt
Tue Nov 12 09:21:34 2013 : Debug: [sql] sql_set_user escaped user --> 'rffro@iscte.pt'
Tue Nov 12 09:21:34 2013 : Debug: [sql]  expand: %{User-Password} ->
Tue Nov 12 09:21:34 2013 : Debug: [sql]  ... expanding second conditional
Tue Nov 12 09:21:34 2013 : Debug: [sql]  expand: %{Chap-Password} ->
Tue Nov 12 09:21:34 2013 : Debug: [sql]  expand: INSERT INTO radpostauth                          (username,
pass, reply, authdate)                          VALUES (                          '%{User-
Name}',                          '%{%{User-Password}:-%{Chap-Password}}',                          '%{reply:
Packet-Type}', '%S') -> INSERT INTO radpostauth                          (username, pass, reply,
authdate)                          VALUES (                          'rffro@iscte.
pt',                          '',                          'Access-Accept', '2013-11-12 09:21:34')
Tue Nov 12 09:21:34 2013 : Debug: +++[sql] returns ok
Tue Nov 12 09:21:34 2013 : Debug: ++- if (User-Name != "radius_user@iscte.pt" ) returns ok
Tue Nov 12 09:21:34 2013 : Debug: Sending Access-Accept packet to host 10.61.10.12 port 58406, id=20, length=0
Tue Nov 12 09:21:34 2013 : Debug:  Service-Type = Framed-User
Tue Nov 12 09:21:34 2013 : Debug:  Reply-Message = "Eduroam ISCTE"
Tue Nov 12 09:21:34 2013 : Debug:  Framed-MTU = 1300
Tue Nov 12 09:21:34 2013 : Debug:  Tunnel-Type:0 = VLAN
Tue Nov 12 09:21:34 2013 : Debug:  Tunnel-Medium-Type:0 = IEEE-802
Tue Nov 12 09:21:34 2013 : Debug:  Tunnel-Private-Group-Id:0 = "203"
Tue Nov 12 09:21:34 2013 : Debug:  MS-MPPE-Recv-Key =
0x88656553bdf8ba1f5fa28f3e18a7afa61053c5f04540c04653a91c608c6e5749
Tue Nov 12 09:21:34 2013 : Debug:  MS-MPPE-Send-Key =
0xae254369a6a2420794fb7381e56010c0082d32de4aaa5dc0b4b0d9027f655e5f
Tue Nov 12 09:21:34 2013 : Debug:  EAP-MSK =
0x88656553bdf8ba1f5fa28f3e18a7afa61053c5f04540c04653a91c608c6e5749ae254369a6a2420794fb7381e56010c0082d32de4aaa5d
c0b4b0d9027f655e5f
Tue Nov 12 09:21:34 2013 : Debug:  EAP-EMSK =
0x62a820f0fc55bfccb8bcea7b4ed34ac70c93b889772b797ecf94be4490b8dd4d3c9f4a46985b7cd388be7e98299d9d6d345aaeebc614c6
9a2d0578c8049258b0
Tue Nov 12 09:21:34 2013 : Debug:  EAP-Message = 0x03080004
Tue Nov 12 09:21:34 2013 : Debug:  Message-Authenticator = 0x00000000000000000000000000000000
Tue Nov 12 09:21:34 2013 : Debug:  User-Name = "rffro"
Tue Nov 12 09:21:34 2013 : Debug: Finished request 378.
Tue Nov 12 09:21:39 2013 : Debug: Cleaning up request 360 ID 12 with timestamp +33
Tue Nov 12 09:21:39 2013 : Debug: Cleaning up request 362 ID 13 with timestamp +33
Tue Nov 12 09:21:39 2013 : Debug: Cleaning up request 363 ID 14 with timestamp +33
Tue Nov 12 09:21:39 2013 : Debug: Cleaning up request 365 ID 15 with timestamp +33
Tue Nov 12 09:21:39 2013 : Debug: Cleaning up request 368 ID 17 with timestamp +33
Tue Nov 12 09:21:39 2013 : Debug: Cleaning up request 371 ID 18 with timestamp +33
Tue Nov 12 09:21:39 2013 : Debug: Cleaning up request 373 ID 19 with timestamp +33
Tue Nov 12 09:21:39 2013 : Debug: Cleaning up request 378 ID 20 with timestamp +33
```

Mensagem retornada em caso de utilizador bloqueado:

```
Mon Nov 11 18:38:44 2013 : Debug: Sending Access-Reject packet to host 10.61.10.12 port 57950, id=116, length=0
Mon Nov 11 18:38:44 2013 : Debug: Reply-Message = "quarantined, contact ISCTE"
Mon Nov 11 18:38:44 2013 : Debug: Finished request 65.
```

radsniff

Para escutar o tráfego de radius, o radsniff faz sniffing de trafego com a biblioteca libpcap, tal como o tcpdump, e em consequência, aceita parâmetros muito similares ao tcpdump. Lê e usa os atributos RADIUS configurados para descodificar mensagens RADIUS. Pode-se filtrar as mensagens a escutar por filtros BPF (tcpdump), por atributos RADIUS, ou até mesmo definir qual o secret do RADIUS para ser capaz de interpretar mais dados.

O comportamento desde comando mudou do FR2 para o Freeradius 3. Em FR2 o defeito é mostrar todos os cabeçalhos, em FR3 não mostra excepto se se usar a opção -x /debug. Ou seja, o comportamento por defeito em FR3 é o equivalente a usar a opção -m em FR2.

Escutar 3 pacotes RADIUS

```
# radsniff -xc 3 (FR3)  ou radsniff -c 3 (FR2)
Access-Request Id 187 10.61.10.11:54805 -> 193.136.188.36:1812 +0.000
 User-Name = "rpcfe@iscte.pt"
 NAS-IP-Address = 10.61.10.11
 NAS-Port = 2086
 Called-Station-Id = "00-50-56-80-36-73:EDUROAM_1020"
 Calling-Station-Id = "18-87-96-61-3E-01"
 Framed-MTU = 1250
 NAS-Port-Type = Wireless-802.11
 Framed-Compression = None
 Connect-Info = "CONNECT Unknown radio"
 Chargeable-User-Identity = ""
 EAP-Message = 0x02010017017270636665406973637465 2d69756c2e7074
 Message-Authenticator = 0xce8c60c34d4bd6762e3e441a60235006

Access-Request Id 79 193.136.188.36:1814 -> 193.136.192.43:1812 +0.001
 User-Name = "rpcfe@iscte.pt"
 NAS-IP-Address = 193.136.188.36
 Calling-Station-Id = "18-87-96-61-3E-01"
 NAS-Port-Type = Wireless-802.11
 EAP-Message = 0x02010017017270636665406973637465 2d69756c2e7074
 Message-Authenticator = 0x2b760236ef7d4aadbcf7a6d3fb872fad
 Proxy-State = 0x313837
 Operator-Name = "1iscte.pt"

Access-Reject Id 79 193.136.192.43:1812 -> 193.136.188.36:1814 +0.016
 Reply-Message = "Request Denied"
 Proxy-State = 0x313837
```

Imprimir os cabeçalhos de 10 pacotes

```
# radsniff -c 10 (FR3) ou radsniff -c 10 -m (FR2)
Accounting-Request Id 79 10.61.10.11:53162 -> 193.136.188.36:1813 +0.000
Accounting-Response Id 79 193.136.188.36:1813 -> 10.61.10.11:53162 +0.003
Accounting-Request Id 80 10.61.10.11:53162 -> 193.136.188.36:1813 +0.061
Accounting-Response Id 80 193.136.188.36:1813 -> 10.61.10.11:53162 +0.063
Accounting-Request Id 81 10.61.10.11:53162 -> 193.136.188.36:1813 +0.089
Accounting-Response Id 81 193.136.188.36:1813 -> 10.61.10.11:53162 +0.092
Access-Request Id 130 10.10.66.5:32770 -> 193.136.188.36:1812 +0.610
Access-Request Id 101 193.136.188.36:1814 -> 193.136.192.43:1812 +0.612
Access-Challenge Id 101 193.136.192.43:1812 -> 193.136.188.36:1814 +0.624
Access-Challenge Id 130 193.136.188.36:1812 -> 10.10.66.5:32770 +0.625
```

Escutar os próximos 3 pacotes enviados para um dos servidores da federação PT.

```
radsniff -xc 3 -f "host 193.136.192.43" (FR3) ou radsniff -c 3 -f "host 193.136.192.43" (FR2)
Access-Request Id 46 193.136.188.36:1814 -> 193.136.192.43:1812 +0.000
 User-Name = "358921fp@eur.nl"
 NAS-IP-Address = 193.136.188.36
 Calling-Station-Id = "30-39-26-DE-F4-51"
 NAS-Port-Type = Wireless-802.11
 EAP-Message = 0x020100140133353839323166704065757 22e6e6c
 Message-Authenticator = 0x63ee3e99287bc54e79759bd21e44f909
 Proxy-State = 0x313534
 Operator-Name = "1iscte.pt"

Access-Challenge Id 46 193.136.192.43:1812 -> 193.136.188.36:1814 +0.128
 EAP-Message = 0x010200061520
 Message-Authenticator = 0xc06f1ed1ec343dbb646e830e3208a35f
 Proxy-State = 0x313534

Access-Request Id 105 193.136.188.36:1814 -> 193.136.192.43:1812 +0.144
 User-Name = "358921fp@eur.nl"
 NAS-IP-Address = 193.136.188.36
 Calling-Station-Id = "30-39-26-DE-F4-51"
 NAS-Port-Type = Wireless-802.11
 EAP-Message = 0x020200060319
 Message-Authenticator = 0x17f12e046d682b6fe011542e501518fc
 Proxy-State = 0x313535
 Operator-Name = "1iscte.pt"
```

Fazer sniffing da ligação à federação

```
 #radsniff -xc 3 -f "host 193.136.192.43" -s secret (FR3) ou radsniff -c 3 -f "host 193.136.192.43" (FR2)
Access-Challenge Id 40 193.136.192.43:1812 -> 193.136.188.36:1814 +0.000
 Session-Timeout = 30
 EAP-Message = 0x010200061920
 State = 0x42a004ce0000013700010200c188ba7000000000000000000000000000000041c92b5b8
 Message-Authenticator = 0x8a723148d9a4966afe946551c0cbe627
 Proxy-State = 0x313136

Access-Request Id 101 193.136.188.36:1814 -> 193.136.192.43:1812 +0.095
 User-Name = "11136910@lis.ulusiada.pt"
 NAS-IP-Address = 193.136.188.36
 Calling-Station-Id = "94-CE-2C-37-C1-80"
 NAS-Port-Type = Wireless-802.11
 EAP-Message =
0x020200d01980000000c616030100c1010000bd0301527964ca506fb39e3e00e1751fca6cf1d998cb24b97f0fb5165f1a2a3724a8840000
54c014c00ac022c02100390038c00fc0050035c012c008c01cc01b00160013c00dc003000ac013c009c01fc01e00330032c00ec004002fc0
11c007c00cc00200050004001500120009001400110008000600030 0ff01000040000b00040300010 2000a00340032000e000d0019000b00
0c00180009000a00160017000800060007001400150004000500120013000100020003000f00100011
 State = 0x42a004ce0000013700010200c188ba7000000000000000000000000000000041c92b5b8
 Message-Authenticator = 0x9bcdc266da5dc98f5a3e0ea4c48e6f65
 Proxy-State = 0x313139
 Operator-Name = "1iscte.pt"

Access-Request Id 37 193.136.192.43:59017 -> 193.136.188.36:1812 +0.175
 User-Name = "sfmco@iscte.pt"
 Framed-MTU = 1400
 Called-Station-Id = "E8-BA-70-C2-70-A0:eduroam"
 Calling-Station-Id = "742f.6894.08a2"
 Service-Type = Login-User
 Message-Authenticator = 0x4b8fc95675c416928108024022140da6
 EAP-Message = 0x020100130173666d636f4069736374652e7074
 NAS-Port-Type = Wireless-802.11
 NAS-Port = 100667
 NAS-Port-Id = "100667"
 NAS-IP-Address = 10.0.2.26
 NAS-Identifier = "CIVIL_Piso0_V008"
 NAS-Identifier = ".UTL"
 Operator-Name = "1utl.pt"
 Vendor-25178-Attr-10 = 0x5054
 Proxy-State = 0x4f53432d457874656e6465642d49643d35363639
```

Escutar com filtros de atributos:

#radsniff -r 'Operator-Name=="1utl.pt"'

#radsniff -r 'User-Name=="radius_user@iscte.pt"'

Há quem use o radsniff como base para estatísticas como se pode ver nesta página. http://wiki.freeradius.org/guide/stats-with-radsniff ; recomendamos no entanto extrair estatísticas internas através do radclient, já que é menos intensivo do ponto de vista de recursos.

Ler captura de ficheiro

```
$radsniff -xI radius-outbound-com-operator-name.pcap.pcapng (FR3) ou  radsniff -I radius-outbound-com-operator-name.pcap.pcapng (FR2)
Logging all events
Sniffing on (radius-outbound-com-operator-name.pcap.pcapng)
2015-01-23 17:09:24.632789 (1) Access-Request Id 164 radius-outbound-com-operator-name.pcap.pcapng:2001:690:2008::100:3001:51694 -> 2001:690:a00:4001::43:1812 +0.000
        User-Name = 'lmeoliveira@fc.ul.pt'
        NAS-IP-Address = 10.2.7.6
        NAS-Port = 39736
        Service-Type = Login-User
        Framed-MTU = 1400
        Called-Station-Id = '00146a3d9a90'
        Calling-Station-Id = 'a8bbcf240c8c'
        NAS-Identifier = '.IPL.PT'
        Proxy-State = 0x3838
        NAS-Port-Type = Wireless-802.11
        Connect-Info = '10.2.7.6 192.104.48.112'
        EAP-Message = 0x02010019016c6d656f6c697665697261406663 2e756c2e7074
        Message-Authenticator = 0x4fa03d798b86b9d982ea2ca51b866b75
        Eduroam-SP-Country = 'PT'
        WISPr-Location-ID = 'isocc=PT,cc=351,ac=210,network=eduroam'
        WISPr-Location-Name = 'IPL-ISEL-EdC-P0-ZonaC0.14'
        Operator-Name = '1ipl.pt'
        Authenticator-Field = 0x457f7869cb07f83c63ea33dae07d7a8d
Done reading packets (radius-outbound-com-operator-name.pcap.pcapng)
Done sniffing
```

radtee

<a desenvolver>

https://github.com/redBorder/freeradius/blob/master/scripts/radtee

eapol_test

Existe um comando bastante interessante para testar o serviço eduroam, que é o eapol_test. Este pequeno utilitário simula ligações EAP ao nível da linha de comando.

Infelizmente no Debian, não é possível instalar automaticamente a partir do APT, pelo que se torna necessário obter a source. Esta pode ser obtida da página http://hostap.epitest.fi/wpa_supplicant/ e à data de escrita deste documento, é o ficheiro wpa_supplicant-2.3.tar.gz

A v2.1 tem erros conhecidos no tratamento de certificados, e não se recomenda. http://lists.shmoo.com/pipermail/hostap/2014-February/029517.html

Portanto, para o instalar:

```
sudo aptitude install libnl-dev libssl-dev apt-src
wget http://hostap.epitest.fi/releases/wpa_supplicant-2.3.tar.gz
tar -zxvf wpa_supplicant-2.3.tar.gz
cd wpa_supplicant-2.3
cd wpa_supplicant
cp defconfig .config
make eapol_test
sudo cp eapol_test /opt/bin/eapol_test
```

Não retirar comentário de CONFIG_EAPOL_TEST como se encontra nalgumas instruções.

Em seguida, criar um ficheiro como input para este comando, a definir o utilizador, a password, e dados dos protocolos a usar na simulação da ligação wireless.

ttls-eap-mschapv2.conf

```
network={
ssid="eduroam"
key_mgmt=WPA-EAP
eap=TTLS
identity="radius_test@iscte.pt"
anonymous_identity="radius_test@iscte.pt"
password="password"
phase2="auth=MSCHAPv2"
}
```

E por último, corre-se o comando: (onde testing123 é a password definida no clients.conf do IP a partir do qual estamos a fazer este teste)

```
/opt/bin/eapol_test -c ttls-eap-mschapv2.conf -s testing123 -a radius.iscte.pt
```

A opção -o também é bastante útil, para obter o certificado dado pelo servidor (radius), para verificar se este está bem.

```
/opt/bin/eapol_test -c ttls-eap-mschapv2.conf -s testing123 -a radius.iscte.pt -o certificado.txt
```

O eapol_test tem também uma opção -N para passar atributos RADIUS. (-N "64:d:13" Tunnel Type 13 - VLAN)

Exemplo de ficheiro para testar PEAP-MSCHAPv2

peap-mschapv2.conf

```
#   eapol_test -c peap-mschapv2.conf -s testing123
network={
        ssid="eduroam"
            key_mgmt=IEEE8021X
        eap=PEAP
        proto=WPA2
        identity="radius@iscte.pt"
        anonymous_identity="radius@iscte.pt"
        password="xxxxx"
        phase2="autheap=MSCHAPv2"
}
```

Medição de tempos de pedidos

Necessitávamos de uma forma de contabilizar o tempo de processamento de pedidos de autenticação ao FreeRadius fazendo o túnel EAP para testar a solução com os protocolos usados pelos clientes. Nos scripts a invocar o eapol_test não se conseguia medir devidamente o tempo, dado o tempo gasto para invocar binários, pipes e processar ficheiros de configurações (não) ser contabilizado. Decidimos então fazer uma patch ao eapol_test.

eapol.patch - Patch eapol_test

```
1259a1260,1264
>         {
>         #include <time.h>
>
>         clock_t t;
>         t = clock();
1278c1283,1285
<
---
>         t= clock() - t;
>         printf("FreeRADIUS: time %.3f seconds\n", ((float)t)/CLOCKS_PER_SEC);
>         }
1300a1308
>
```

Para aplicar o patch, fazer no directório descrito nos passos para compilar o eapol_test, e correr o comandos:

```
cd wpa_supplicant-2.0/wpa_supplicant
patch eapol_test.c < eapol.patch
make eapol_test
strip eapol_test
sudo cp eapol_test /opt/bin
```

Aplicando este patch, o output do eapol_test fica com uma linha extra:

EAPOL: SUPP_BE entering state IDLE eapol_sm_cb: success=1 **FreeRADIUS: time 0.010 seconds** EAPOL: Successfully fetched key (len=32) PMK from EAPOL - hexdump(len=32): fa 65 9a 9f 9a 2f 45 f3 44 f6 53 25 f4 f3 26 16 51 aa 2f 73 40 0f 9e 80 90 a9 08 80 8f d7 6d a3 EAP: deinitialize previously used EAP method (25, PEAP) at EAP deinit ENGINE: engine deinit MPPE keys OK: 1 mismatch: 0 SUCCESS

a resolução do timer são incrementos de 10ms; ou seja neste caso sabemos que demorou entre 10ms a 20ms.
Esta necessidade do patch advém do radtest não suportar nem MSCHAPv2, nem PEAP ou EAP-TTLS.

rad_eap_test

É um script wrapper para o eapol_test, cuja source pode ser encontra aqui: http://www.eduroam.cz/rad_eap_test/

De momento, para fazer download, basta fazer:

```
wget http://www.eduroam.cz/rad_eap_test/rad_eap_test-0.23.tar.bz2
```

O ficheiro vem com diversos componentes, e patches para o eapol_test, que não é necessário aplicar nas últimas versões. Basta fazer:

```
tar -jxvf rad_eap_test-0.23.tar.bz2
cd rad_eap_test-0.23
sudo cp rad_eap_test /opt/bin
sudo mkdir -p /usr/local/share/man/man1
sudo cp doc/rad_eap_test.1 /usr/local/share/man/man1/
```

A sintaxe para testar o radius é:

```
/opt/bin/rad_eap_test -H radius2.iscte.pt -P 1812 -S xxxxxx -m WPA-EAP -e PEAP -s eduroam -M 00:00:00:00:00:00 -
i 'Roaming Test NAGIOS ISCTE.PT' -u radius_user@iscte.pt -p password
```

time

E para ter uma ideia de timings da autenticação:

```
time /usr/bin/ntlm_auth --request-nt-key --username=teste --domain=ISCTE --password=xxxpassword
NT_STATUS_OK: Success (0x0)
real 0m0.013s
user 0m0.000s
sys 0m0.004s
```

```
time radtest -t mschap teste@iscte.pt 6ziFgmD0wVbnXnK radius2.iscte.pt:1812 0 xxxxxxx > /dev/null
real 0m0.162s
user 0m0.020s
sys 0m0.016s
```

```
time ( /opt/bin/eapol_test -c conf/peap-mschapv2.conf -s testing123 -a 193.136.188.36 > /dev/null )
real 0m0.208s
user 0m0.008s
sys 0m0.008s
```

O eapol_test tem também a opção para fazer vários pedidos. A partir de 70 iterações começamos a ter erros, pelo que esta ferramenta como analise de performance tem as suas limitações.

```
/opt/bin/eapol_test -c conf/peap-mschapv2.conf -s wirelessiscte -a 193.136.188.36 -r 70 > /dev/null
real        0m25.959s
user        0m0.324s
sys        0m0.324s
```

O timing de ferramentas complexas como o radtest ou o eapol_test tomam também o seu tempo, e distorcem o valor real dos acontecimentos. Testando de forma independente, com um patch ao eapol_test em C, uma conexão EAP interna ao servidor freeradius, esta não demora 208ms como sugere o time do eapol_test mas sim, entre 10 a 20ms, o que é uma valor mais dentro dos parâmetros normais de serviço (>200ms no próprio servidor/serviço indicaria problemas algures num servidor ou na infra-estrutura). Como sempre, é necessário cuidado em balancear os dados que conhecemos para interpretar os outputs das ferramentas que se encontram ao nosso alcance. Ou seja, os valores destas ferramentas devem ser tomados como uma referência padrão quando o serviço está a operar devidamente para mais tarde permitir detectar problemas/desvios ao padrão, mas não devem ser tomados literalmente como os tempos correctos das operações subjacentes a ser medidas. Ver o patch para eapol_test que desenvolvemos para ter uma medida mais correcta do tempo de autenticação. Obviamente que fazendo mais pedidos, o atraso do tempo de setup dilui-se e deixa de ser uma consideração.

Evolynx

Para fazer tests de performance/stress no FreedRadius, pode-se usar em Windows, o útilitário da Evolynx.

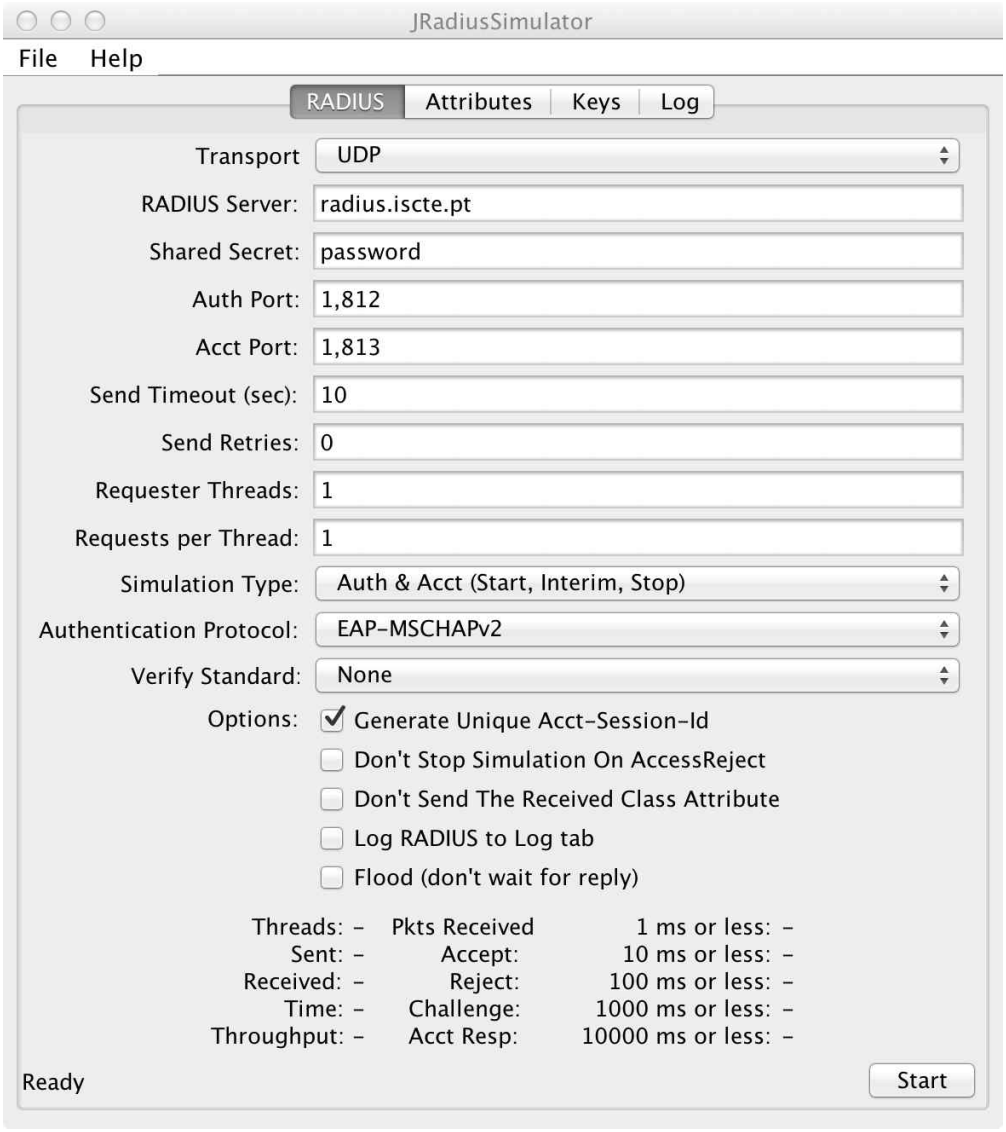
O URL de download é este: https://www.evolynx.com/radius/dl_loadtest.aspx

JRadius

Para testar/auditar o FreeRADIUS também se pode usar o JRadius em http://www.coova.org/JRadius/Simulator

O JRadius é uma aplicação opensource que foi desanhada para testes de RADIUS e servidores, gerando trafego FreeRADIUS.

Pode-se fazer download deste na versão corrente http://coova-dev.s3.amazonaws.com/mvn/net/jradius/jradius-client/1.1.4/jradius-client-1.1.4-release.zip e correr localmente ou pode se invocar o JRadius directamente a partir deste link https://coova-desktop.s3.amazonaws.com/simulator.jnlp, no entanto o browser tem de suportar este tipo de configurações como por exemplo, o FireFox.



openssl

```
$openssl verify  -CAfile ca.pem server.pem
server.pem: OK
```

```
$openssl x509 -in /etc/freeradius/certs/server.pem -text -noout
Certificate:
```

```
Data:
    Version: 3 (0x2)
    Serial Number:
        af:ef:74:65:83:46:df:71:39:9f:b8:06:ae:fc:04:68
Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=NL, O=TERENA, CN=TERENA SSL CA
    Validity
        Not Before: Jul 11 00:00:00 2013 GMT
        Not After : Jul 10 23:59:59 2016 GMT
    Subject: OU=Domain Control Validated, CN=radius2.iscte.pt
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:bb:4c:b2:19:57:b3:ad:6b:ba:b4:a6:11:f7:7f:
                b6:ca:20:d7:bd:a6:59:39:1d:57:8c:13:d8:d7:9f:
                2b:9c:25:d7:82:3d:7f:fa:3f:e2:14:a6:7f:c9:bb:
                9e:22:bd:79:12:fd:72:12:89:c8:cb:e1:a4:30:8a:
                7f:c3:97:3a:1d:ec:39:d0:40:58:ec:27:9d:d4:e1:
                83:01:cc:22:dd:61:5d:18:0a:1e:77:64:39:98:10:
                43:b1:e4:7f:98:0e:1d:a0:a5:ad:db:32:d9:2f:9c:
                ad:8f:3b:6d:20:4f:e3:7c:50:0d:77:bc:c7:34:86:
                47:c6:80:2b:72:40:bb:9d:a7:11:1e:41:10:f4:da:
                f4:9b:34:06:39:21:1a:99:30:c4:26:89:54:1b:ec:
                d9:f8:55:c3:87:3d:07:3e:72:5c:cb:34:c4:8a:77:
                4a:05:41:d6:93:20:87:f8:1c:13:d5:8b:12:13:3c:
                44:4b:b3:f4:33:68:80:25:03:a1:50:3f:45:6d:e4:
                18:84:5f:22:43:7c:3a:7c:74:a0:d8:bd:dc:8c:6d:
                e8:28:fa:52:9e:f8:56:16:07:7f:e6:a7:26:42:aa:
                2d:9c:be:2d:d4:6d:ee:c8:88:c4:51:ff:03:60:80:
                ff:0f:a7:94:f5:29:1c:fe:5b:f6:78:d0:a4:95:20:
                1f:c1
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Authority Key Identifier:
            keyid:0C:BD:93:68:0C:F3:DE:AB:A3:49:6B:2B:37:57:47:EA:90:E3:B9:ED

        X509v3 Subject Key Identifier:
            A6:F9:53:F4:26:A2:65:2A:41:3A:02:D7:C4:EF:26:03:A8:E7:B1:50
        X509v3 Key Usage: critical
            Digital Signature, Key Encipherment
        X509v3 Basic Constraints: critical
            CA:FALSE
        X509v3 Extended Key Usage:
            TLS Web Server Authentication, TLS Web Client Authentication
        X509v3 Certificate Policies:
            Policy: 1.3.6.1.4.1.6449.1.2.2.29
            Policy: 2.23.140.1.2.1

        X509v3 CRL Distribution Points:

            Full Name:
              URI:http://crl.tcs.terena.org/TERENASSLCA.crl

        Authority Information Access:
            CA Issuers - URI:http://crt.tcs.terena.org/TERENASSLCA.crt
            OCSP - URI:http://ocsp.tcs.terena.org

        X509v3 Subject Alternative Name:
            DNS:radius2.iscte.pt
Signature Algorithm: sha1WithRSAEncryption
     04:9c:1e:46:c1:45:a0:be:fb:63:73:7b:29:90:a9:22:20:be:
     80:23:98:4b:c3:0a:3b:4b:7a:c7:19:35:a5:d3:91:91:d7:7d:
     82:e9:8f:c0:e4:8a:cd:3c:ff:ed:bb:d8:66:5c:36:7c:f6:47:
     48:56:db:d0:62:a2:9c:49:dd:09:6d:01:d1:76:51:9f:f4:a6:
     1d:9d:a1:8e:5b:7c:ab:4a:0f:b3:c1:5c:67:a5:fd:1f:e8:43:
     d8:bf:72:e4:38:e2:0c:cb:51:6d:f1:10:84:3e:9d:e6:a8:e5:
     e4:36:ca:b8:0d:85:60:5e:74:6e:83:9d:52:45:ff:3a:9b:92:
     08:82:8e:1c:47:61:4d:8b:dc:0a:bf:64:bf:6a:be:fa:a6:f2:
     17:76:69:fd:42:c8:34:a8:35:57:09:36:e8:1f:d1:34:ab:69:
     26:b3:49:73:8a:b5:30:47:5a:b4:25:a2:bc:22:c7:a0:1e:11:
```

```
        b6:bf:71:0d:39:8b:f3:53:86:55:53:9b:37:11:a5:51:55:c1:
        93:0a:18:55:41:18:82:d2:44:fc:1d:12:7f:99:06:4f:48:1b:
        d0:32:7a:db:a0:fb:07:03:03:20:82:0c:c2:3d:78:31:1e:ca:
        83:e6:83:89:ec:b2:04:3f:1e:2d:8a:67:51:5a:ca:50:65:d2:
        9e:a6:6b:60
```

Outras ferramentas de medição de performance

blktrace

```
sudo blktrace -w 3 /dev/sda
=== sda ===
  CPU  0:                   67 events,        4 KiB data
  CPU  1:                   19 events,        1 KiB data
  Total:                    86 events (dropped 0),        5 KiB data
```

free

free -m - visualizar memória livre

```
$ free -m
             total       used       free     shared    buffers     cached
Mem:           502         61        440          0          0         17
-/+ buffers/cache:         44        458
Swap:         1063          0       1063
```

top

top/htop - ocupação de recursos/processos

```
$top
top - 02:29:51 up 7 days,  2:43,  1 user,  load average: 0.02, 0.03, 0.05
Tasks:  76 total,   1 running,  75 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.0 sy,  0.0 ni, 96.8 id,  3.2 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem:    514328 total,    73444 used,   440884 free,      640 buffers
KiB Swap:  1089532 total,        0 used,  1089532 free,    28440 cached

  PID USER      PR  NI  VIRT  RES  SHR S  %CPU %MEM    TIME+  COMMAND
    9 root      20   0     0    0    0 S   0.3  0.0   0:05.28 kworker/1:0
 1657 root      20   0 28152 3196 2564 S   0.3  0.6   8:08.18 vmtoolsd
 7404 rui       20   0  4384 1292 1012 R   0.3  0.3   0:00.01 top
    1 root      20   0  2280  688  584 S   0.0  0.1   0:08.35 init
    2 root      20   0     0    0    0 S   0.0  0.0   0:00.00 kthreadd
    3 root      20   0     0    0    0 S   0.0  0.0   0:32.41 ksoftirqd/0
    5 root      20   0     0    0    0 S   0.0  0.0   0:00.00 kworker/u:0
    6 root      rt   0     0    0    0 S   0.0  0.0   0:02.00 migration/0
    7 root      rt   0     0    0    0 S   0.0  0.0   0:04.81 watchdog/0
    8 root      rt   0     0    0    0 S   0.0  0.0   0:02.92 migration/1
   10 root      20   0     0    0    0 S   0.0  0.0   0:18.60 ksoftirqd/1
   12 root      rt   0     0    0    0 S   0.0  0.0   0:03.08 watchdog/1
   13 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 cpuset
   14 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 khelper
```

```
   15 root      20   0     0    0    0 S   0.0  0.0   0:00.00 kdevtmpfs
   16 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 netns
   17 root      20   0     0    0    0 S   0.0  0.0   0:02.37 sync_supers
   18 root      20   0     0    0    0 S   0.0  0.0   0:00.05 bdi-default
   19 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 kintegrityd
   20 root       0 -20     0    0    0 S   0.0  0.0   0:00.06 kblockd
   21 root      20   0     0    0    0 S   0.0  0.0   0:00.16 khungtaskd
   22 root      20   0     0    0    0 S   0.0  0.0   0:11.81 kswapd0
   23 root      25   5     0    0    0 S   0.0  0.0   0:00.00 ksmd
   24 root      20   0     0    0    0 S   0.0  0.0   0:00.00 fsnotify_mark
   25 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 crypto
  108 root      20   0     0    0    0 S   0.0  0.0   0:00.00 scsi_eh_0
  119 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 vmw_pvscsi_wq_0
  143 root      20   0     0    0    0 S   0.0  0.0   0:00.00 kworker/u:1
  157 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 kdmflush
  165 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 kdmflush
  180 root      20   0     0    0    0 S   0.0  0.0   0:02.60 kjournald
  305 root      20   0  2712 1112  644 S   0.0  0.2   0:00.05 udevd
  398 root      20   0  2712  700  224 S   0.0  0.1   0:00.00 udevd
  400 root      20   0  2712  780  304 S   0.0  0.2   0:00.00 udevd
  562 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 kdmflush
  564 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 kdmflush
  566 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 kdmflush
  567 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 kdmflush
 1160 root      20   0     0    0    0 S   0.0  0.0   0:36.84 kjournald
 1161 root      20   0     0    0    0 S   0.0  0.0   0:00.67 kjournald
 1162 root      20   0     0    0    0 S   0.0  0.0   0:00.33 kjournald
 1163 root      20   0     0    0    0 S   0.0  0.0   0:09.85 kjournald
 1583 root      20   0  3996  376  176 S   0.0  0.1   0:00.00 syslog-ng
 1584 root      20   0  8084 3644 2256 S   0.0  0.7   0:17.36 syslog-ng
 1618 root      20   0  9936 1100  644 S   0.0  0.2   0:25.39 nmbd
 1638 root      20   0 20924 3336 2528 S   0.0  0.6   0:08.67 smbd
 1684 root      20   0 19700 1248  520 S   0.0  0.2   0:00.24 smbd
 1685 root      20   0  3840  980  776 S   0.0  0.2   0:01.82 cron
 1758 snmp      20   0 10020 3400 1720 S   0.0  0.7   1:29.62 snmpd
 1796 www-data  20   0  7104 2824 1640 S   0.0  0.5   0:21.40 lighttpd
 1840 root      20   0  6464 1088  656 S   0.0  0.2   0:09.22 sshd
 1935 root      20   0  2592  768  604 S   0.0  0.1   0:00.00 xinetd
 2032 root      20   0  3784  812  684 S   0.0  0.2   0:00.00 getty
 2633 root      20   0     0    0    0 S   0.0  0.0   0:06.66 flush-254:3
 5306 root      20   0     0    0    0 S   0.0  0.0   0:04.37 flush-254:5
 7187 freerad   20   0 55324 5728 2672 S   0.0  1.1   0:00.29 freeradius
 7260 root      20   0  9264 2960 2372 S   0.0  0.6   0:00.04 sshd
 7262 rui       20   0  9264 1380  792 S   0.0  0.3   0:00.01 sshd
 7263 rui       20   0  6356 3572 1580 S   0.0  0.7   0:00.19 bash
 7402 rui       20   0  6356 2324  332 S   0.0  0.5   0:00.00 bash
 7403 rui       20   0  3356  616  540 S   0.0  0.1   0:00.00 logger
15337 root      20   0     0    0    0 S   0.0  0.0   0:12.88 kworker/0:0
16777 root      20   0  4772  792  380 S   0.0  0.2   0:00.00 bash
16778 root      20   0  3356  620  540 S   0.0  0.1   0:00.00 logger
16817 root      20   0 21772 6228 5468 S   0.0  1.2   0:50.17 winbindd
16830 root      20   0 21880 7652 6716 S   0.0  1.5   1:04.94 winbindd
17008 root      20   0     0    0    0 S   0.0  0.0   0:15.65 kworker/1:2
18477 root      20   0     0    0    0 S   0.0  0.0   0:03.02 kworker/0:2
26174 root      20   0 22924 1872 1096 S   0.0  0.4   0:00.00 winbindd
26661 root      20   0     0    0    0 S   0.0  0.0   0:01.93 flush-254:0
27870 root      20   0     0    0    0 S   0.0  0.0   0:00.09 flush-254:2
29147 root      20   0  4772  792  380 S   0.0  0.2   0:00.00 bash
29148 root      20   0  3356  620  540 S   0.0  0.1   0:00.00 logger
29185 nagios    20   0  4392  900  620 S   0.0  0.2   0:17.02 nrpe
29428 root      20   0     0    0    0 S   0.0  0.0   0:00.21 flush-254:4
30604 root      20   0  5392 1400  960 S   0.0  0.3   0:47.95 monit
```

htop

```
$htop
  1  [                          0.0%]     Tasks: 32, 5 thr; 1 running
  2  [|                         0.7%]     Load average: 0.00 0.01 0.05
  Mem[||||||||               44/502MB]     Uptime: 7 days, 02:46:18
  Swp[                       0/1063MB]

  PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
30604 root       20   0  5392  1400   960 S  0.0  0.3  0:47.98 /usr/bin/monit -c
 7494 rui        20   0  4584  1716  1280 R  0.0  0.3  0:00.05 htop
    1 root       20   0  2280   688   584 S  0.0  0.1  0:08.34 init [2]
  305 root       20   0  2712  1112   644 S  0.0  0.2  0:00.05 udevd --daemon
  398 root       20   0  2712   700   224 S  0.0  0.1  0:00.00 udevd --daemon
  400 root       20   0  2712   780   304 S  0.0  0.2  0:00.00 udevd --daemon
 1583 root       20   0  3996   376   176 S  0.0  0.1  0:00.00 supervising syslo
 1584 root       20   0  8084  3644  2256 S  0.0  0.7  0:17.37 /usr/sbin/syslog-
 1618 root       20   0  9936  1100   644 S  0.0  0.2  0:25.40 /usr/sbin/nmbd -D
 1638 root       20   0 20924  3336  2528 S  0.0  0.6  0:08.66 /usr/sbin/smbd -D
 1657 root       20   0 28152  3196  2564 S  0.0  0.6  8:08.31 /usr/bin/vmtoolsd
 1684 root       20   0 19700  1248   520 S  0.0  0.2  0:00.23 /usr/sbin/smbd -D
 1685 root       20   0  3840   980   776 S  0.0  0.2  0:01.82 /usr/sbin/cron
 1758 snmp       20   0 10020  3400  1720 S  0.0  0.7  1:29.65 /usr/sbin/snmpd -
 1796 www-data   20   0  7104  2824  1640 S  0.0  0.5  0:21.41 /usr/sbin/lighttp
 1840 root       20   0  6464  1088   656 S  0.0  0.2  0:09.23 /usr/sbin/sshd
 1935 root       20   0  2592   768   604 S  0.0  0.1  0:00.00 /usr/sbin/xinetd
 2032 root       20   0  3784   812   684 S  0.0  0.2  0:00.00 /sbin/getty 38400
 7260 root       20   0  9264  2960  2372 S  0.0  0.6  0:00.04 sshd: rui [priv]
 7262 rui        20   0  9264  1380   792 S  0.0  0.3  0:00.02 sshd: rui@pts/1
 7263 rui        20   0  6356  3572  1580 S  0.0  0.7  0:00.20 -bash
 7438 freerad    20   0 55340  5560  2600 S  0.0  1.1  0:00.04 /usr/sbin/freerad
F1Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

iftop

iftop - visualização gráfica/curses de ocupação de rede

```
#iftop
                12.5kb          25.0kb          37.5kb          50.0kb    62.5kb

radius2.iscte.pt       => horus2.wiscte.wfarm           0b   4.00kb  4.00kb
                           <=                               0b   3.40kb  3.40kb
radius2.iscte.pt       => dns2.iscte.pt              1.38kb  2.07kb  2.07kb
                           <=                           2.98kb  4.63kb  4.63kb
radius2.iscte.pt       => a79-169-248-181.cpe.netca  4.27kb  5.31kb  5.31kb
                           <=                            208b    516b    516b
radius2.iscte.pt       => nagios3.srv.rede              0b   1.27kb  1.27kb
                           <=                               0b   1.27kb  1.27kb
radius2.iscte.pt       => jord.iscte.intranet           0b   1.71kb  1.71kb
                           <=                               0b    274b    274b
radius2.iscte.pt       => syslog.iscte.intranet         0b    821b    821b
                           <=                               0b      0b      0b
255.255.255.255            => rede34-166.iscte.intranet     0b      0b      0b
                           <=                            2.88kb   736b    736b
radius2.iscte.pt       => ap-meruc.rede                 0b    336b    336b
                           <=                               0b    336b    336b
radius2.iscte.pt       => p-merumc1550v.rede            0b     96b     96b
                           <=                               0b    490b    490b
255.255.255.255            => rede34-186.iscte.intranet     0b      0b      0b
                           <=                               0b    428b    428b
broadcast.iscte.intranet   => rede34-166.iscte.intranet     0b      0b      0b
                           <=                            1.44kb   368b    368b
broadcast.iscte.intranet   => rede33-5.iscte.intranet       0b      0b      0b
                           <=                               0b    314b    314b

TX:             cum:   15.6kB   peak:   39.7kb  rates:   5.64kb  15.6kb  15.6kb
RX:                    17.0kB           37.5kb           11.3kb  17.0kb  17.0kb
TOTAL:                 32.6kB           77.2kb           17.0kb  32.6kb  32.6kb
```

iotop

iotop - visual gráfica/curses de uso de disco

```
#iotop
Total DISK READ:       0.00 B/s | Total DISK WRITE:       0.00 B/s
  TID  PRIO  USER     DISK READ  DISK WRITE  SWAPIN     IO>    COMMAND
 7439 be/4 freerad     0.00 B/s    3.92 K/s  0.00 %  0.00 % freeradius
 7441 be/4 freerad     0.00 B/s   11.77 K/s  0.00 %  0.00 % freeradius
 7442 be/4 freerad     0.00 B/s    3.92 K/s  0.00 %  0.00 % freeradius
    1 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % init [2]
    2 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kthreadd]
    3 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [ksoftirqd/0]
    5 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kworker/u:0]
    6 rt/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [migration/0]
    7 rt/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [watchdog/0]
    8 rt/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [migration/1]
    9 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kworker/1:0]
   10 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [ksoftirqd/1]
   12 rt/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [watchdog/1]
   13 be/0 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [cpuset]
   14 be/0 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [khelper]
   15 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kdevtmpfs]
   16 be/0 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [netns]
   17 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [sync_supers]
   18 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [bdi-default]
   19 be/0 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kintegrityd]
   20 be/0 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kblockd]
   21 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [khungtaskd]
   22 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kswapd0]
   23 be/5 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [ksmd]
   24 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [fsnotify_mark]
   25 be/0 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [crypto]
26661 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [flush-254:0]
18477 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kworker/0:2]
```

nicstat

```
$ nicstat -nx
13:44:57      RdKB    WrKB   RdPkt   WrPkt   IErr  OErr  Coll  NoCP Defer  %Util
eth0          4.53    2.98   30.33   13.26   0.00  0.00  0.00  0.00  0.00   0.00
```

vmstat

```
# vmstat
procs -----------memory---------- ---swap-- -----io---- -system-- ----cpu----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa
 0  0      0 423120   2332  42812    0    0     1    11   14    3  1  0 98  1
```

Ferramentas de monitorização de sistema/mensagens

strace

Para usar trace o aconselhado é correr em foreground com freeradius -f

sysdig

linux-tools package? sysstat package

MySQL

Para fazer debug ao freeradius/autenticações, pode-se editar a BD quer com o PHPMyadmin, ou fazer queries directamente.

Para fazer a ligação ao mysql:

```
mysql -u radius -p password  radius --host=db1.iscte.local
```

```
mysql> use radius
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
```

```
mysql> show tables;
+------------------+
| Tables_in_radius |
+------------------+
| radacct          |
| radpostauth      |
+------------------+
2 rows in set (0.00 sec)
```

```
mysql> describe radpostauth;
+----------+-------------+------+-----+-------------------+-----------------------------+
| Field    | Type        | Null | Key | Default           | Extra                       |
+----------+-------------+------+-----+-------------------+-----------------------------+
| id       | int(11)     | NO   | PRI | NULL              | auto_increment              |
| username | varchar(64) | NO   |     |                   |                             |
| pass     | varchar(64) | NO   |     |                   |                             |
| reply    | varchar(32) | NO   |     |                   |                             |
| authdate | timestamp   | NO   |     | CURRENT_TIMESTAMP | on update CURRENT_TIMESTAMP |
+----------+-------------+------+-----+-------------------+-----------------------------+
5 rows in set (0.00 sec)
```

Ultimos dez logins:

```
mysql> select * from radpostauth order by id desc limit 10;
+---------+-----------------+------+---------------+---------------------+
| id      | username        | pass | reply         | authdate            |
+---------+-----------------+------+---------------+---------------------+
| 1200255 | cebp@iscte.pt   |      | Access-Accept | 2013-10-16 08:43:39 |
| 1200254 | host/SWARLOS    |      | Access-Reject | 2013-10-16 08:43:35 |
| 1200253 | aclsa@iscte.pt  |      | Access-Accept | 2013-10-16 08:43:34 |
| 1200252 | ymaiu@iscte.pt  |      | Access-Accept | 2013-10-16 08:43:30 |
| 1200251 | ymaiu@iscte.pt  |      | Access-Accept | 2013-10-16 08:43:30 |
| 1200250 | prfcs1@iscte.pt |      | Access-Accept | 2013-10-16 08:43:26 |
| 1200249 | mjcle@iscte.pt  |      | Access-Accept | 2013-10-16 08:43:26 |
| 1200248 | cebp@iscte.pt   |      | Access-Accept | 2013-10-16 08:43:25 |
| 1200247 | cmara1@iscte.pt |      | Access-Accept | 2013-10-16 08:43:25 |
| 1200246 | cmara1@iscte.pt |      | Access-Accept | 2013-10-16 08:43:25 |
+---------+-----------------+------+---------------+---------------------+
10 rows in set (0.00 sec)
```

Ultimos dez logins de um utilizador:

```
mysql> select * from radpostauth where username="radius-teste@iscte.pt" order by id limit 10;
+-------+----------------------+-------------+---------------+---------------------+
| id    | username             | pass        | reply         | authdate            |
+-------+----------------------+-------------+---------------+---------------------+
| 40777 | radius-teste@iscte.pt | radius-teste | Access-Reject | 2013-08-27 15:20:26 |
| 40936 | radius-teste@iscte.pt | radius-teste | Access-Reject | 2013-08-27 15:35:26 |
| 41090 | radius-teste@iscte.pt | radius-teste | Access-Reject | 2013-08-27 15:50:25 |
| 41217 | radius-teste@iscte.pt | radius-teste | Access-Reject | 2013-08-27 16:05:26 |
| 41311 | radius-teste@iscte.pt | radius-teste | Access-Reject | 2013-08-27 16:20:36 |
| 41428 | radius-teste@iscte.pt | radius-teste | Access-Reject | 2013-08-27 16:35:26 |
| 41514 | radius-teste@iscte.pt | radius-teste | Access-Reject | 2013-08-27 16:50:36 |
| 41632 | radius-teste@iscte.pt | radius-teste | Access-Reject | 2013-08-27 17:05:25 |
| 41738 | radius-teste@iscte.pt | radius-teste | Access-Reject | 2013-08-27 17:20:26 |
| 41840 | radius-teste@iscte.pt | radius-teste | Access-Reject | 2013-08-27 17:35:27 |
+-------+----------------------+-------------+---------------+---------------------+
10 rows in set (0.04 sec)
```

Últimos dez logins sem sucesso:

```
mysql> select * from radpostauth where reply like "%Reject%" order by id desc limit 10;
+---------+----------------------+------+---------------+---------------------+
| id      | username             | pass | reply         | authdate            |
+---------+----------------------+------+---------------+---------------------+
| 1200294 | host/RitaSequeira-PC |      | Access-Reject | 2013-10-16 08:44:52 |
| 1200256 | Pedro                |      | Access-Reject | 2013-10-16 08:43:41 |
| 1200254 | host/SWARLOS         |      | Access-Reject | 2013-10-16 08:43:35 |
| 1200220 | 26Novembro           |      | Access-Reject | 2013-10-16 08:42:40 |
| 1200217 | 26Novembro           |      | Access-Reject | 2013-10-16 08:42:38 |
| 1200216 | 26Novembro           |      | Access-Reject | 2013-10-16 08:42:36 |
| 1200215 | 26Novembro           |      | Access-Reject | 2013-10-16 08:42:35 |
| 1200214 | 26Novembro           |      | Access-Reject | 2013-10-16 08:42:32 |
| 1200211 | 26Novembro           |      | Access-Reject | 2013-10-16 08:42:31 |
| 1200210 | 26Novembro           |      | Access-Reject | 2013-10-16 08:42:28 |
+---------+----------------------+------+---------------+---------------------+
10 rows in set (0.00 sec)
```

Número de IPs por mês:

```
SELECT MONTH(DATE(Acctstoptime)) AS Month, COUNT(DISTINCT framedipaddress),   COUNT(framedipaddress) FROM
radacct WHERE (Acctstoptime BETWEEN DATE_SUB(NOW(), INTERVAL 12 MONTH) AND NOW()) GROUP BY Month ORDER BY Month;
+-------+---------------------------------+-----------------------+
| Month | COUNT(DISTINCT framedipaddress) | COUNT(framedipaddress) |
+-------+---------------------------------+-----------------------+
|     9 |                            5516 |                136995 |
|    10 |                            6314 |                183838 |
+-------+---------------------------------+-----------------------+
4 rows in set (0.46 sec)
```

Utilizadores vs autenticações:

```
mysql> SELECT MONTH(DATE(authdate)) AS Month, COUNT(DISTINCT username),   COUNT(username) FROM radpostauth
WHERE (authdate BETWEEN DATE_SUB(NOW(), INTERVAL 12 MONTH) AND NOW()) GROUP BY Month ORDER BY Month;
+-------+--------------------------+-----------------+
| Month | COUNT(DISTINCT username) | COUNT(username) |
+-------+--------------------------+-----------------+
|     9 |                     6352 |          488981 |
|    10 |                     8018 |          652889 |
+-------+--------------------------+-----------------+
4 rows in set (3.43 sec)
```

Utilizadores em roaming:

```
mysql> select * from radpostauth where username not like "%@iscte.pt" and reply like "%Accept" group by
username order by id limit 10;
+------+-----------------------------+------+---------------+---------------------+
| id   | username                    | pass | reply         | authdate            |
+------+-----------------------------+------+---------------+---------------------+
| 4672 | cgalmeida@ics.ul.pt         |      | Access-Accept | 2013-08-13 09:51:33 |
| 4788 | 136310003@fch.lisboa.ucp.pt |      | Access-Accept | 2013-08-13 10:41:25 |
| 4934 | b5847@ics.uminho.pt         |      | Access-Accept | 2013-08-13 11:22:59 |
| 5120 | 10419519@uva.nl             |      | Access-Accept | 2013-08-13 12:25:20 |
| 5280 | b5847@scom.uminho.pt        |      | Access-Accept | 2013-08-13 12:47:01 |
| 5281 | a25245@ubi.pt               |      | Access-Accept | 2013-08-13 12:47:03 |
| 5312 | hb11197@pclan.umac.mo       |      | Access-Accept | 2013-08-13 12:50:42 |
| 5549 | mliberato@campus.ul.pt      |      | Access-Accept | 2013-08-13 13:19:24 |
| 5633 | hmertens@uni-klu.ac.at      |      | Access-Accept | 2013-08-13 13:34:21 |
| 5696 | as1@campus.ul.pt            |      | Access-Accept | 2013-08-13 13:42:46 |
+------+-----------------------------+------+---------------+---------------------+
10 rows in set (0.71 sec)
```

Utilizadores mal configurados - neste exemplo tínhamos esquecido de bloquear o domínio NULL em /etc/freeradius/users

```
mysql> select * from radpostauth where username not like "%@%" and reply like "%Accept" group by username order
by id limit 20;
+---------+----------+------+---------------+---------------------+
| id      | username | pass | reply         | authdate            |
+---------+----------+------+---------------+---------------------+
| 1173575 | mmraa1   |      | Access-Accept | 2013-10-15 16:09:02 |
| 1174561 | ngfsl    |      | Access-Accept | 2013-10-15 16:20:10 |
| 1175387 | rmlpo    |      | Access-Accept | 2013-10-15 16:32:51 |
| 1175810 | rmrca1   |      | Access-Accept | 2013-10-15 16:38:55 |
| 1175874 | jpgsa11  |      | Access-Accept | 2013-10-15 16:40:04 |
| 1175876 | joao     |      | Access-Accept | 2013-10-15 16:40:04 |
| 1176740 | iscte    |      | Access-Accept | 2013-10-15 16:52:12 |
| 1179201 | jtnto    |      | Access-Accept | 2013-10-15 17:24:34 |
| 1179744 | bsmgl    |      | Access-Accept | 2013-10-15 17:31:42 |
| 1186722 | eraoa    |      | Access-Accept | 2013-10-15 18:54:10 |
| 1186864 | jppac    |      | Access-Accept | 2013-10-15 18:56:28 |
| 1186977 | mccsa1   |      | Access-Accept | 2013-10-15 18:58:25 |
| 1187847 | tmsmc    |      | Access-Accept | 2013-10-15 19:17:17 |
| 1192512 | bmemo    |      | Access-Accept | 2013-10-15 20:47:15 |
| 1194124 | jpomb    |      | Access-Accept | 2013-10-15 21:27:40 |
| 1197381 | vbmba    |      | Access-Accept | 2013-10-16 07:30:17 |
| 1197947 | dbrse    |      | Access-Accept | 2013-10-16 08:00:41 |
| 1198048 | pmncm    |      | Access-Accept | 2013-10-16 08:03:22 |
| 1198449 | frlrs    |      | Access-Accept | 2013-10-16 08:10:44 |
| 1199943 | jmsms11  |      | Access-Accept | 2013-10-16 08:36:03 |
+---------+----------+------+---------------+---------------------+
20 rows in set (0.60 sec)
```

Utilizadores com eduroam mal configurada - não seleccionaram utilizador na configuração

```
mysql> select * from radpostauth where username not like "%@%" and reply like "%Reject" group by username order
by id limit 20;
+-------+--------------------------------+------+---------------+---------------------+
| id    | username                       | pass | reply         | authdate            |
+-------+--------------------------------+------+---------------+---------------------+
|  4677 | d3663                          |      | Access-Reject | 2013-08-13 09:52:42 |
|  5090 | Rafael-PC=5CRafael             |      | Access-Reject | 2013-08-13 12:22:22 |
|  5154 | host/Teodosio-PC               |      | Access-Reject | 2013-08-13 12:31:42 |
|  5382 | b5847                          |      | Access-Reject | 2013-08-13 12:58:38 |
|  5897 | 53617                          |      | Access-Reject | 2013-08-13 14:14:30 |
|  6158 | host/chico-PC                  |      | Access-Reject | 2013-08-13 14:47:20 |
|  6279 | ist163317                      |      | Access-Reject | 2013-08-13 15:03:36 |
|  6374 | host/WJNJPTL3ABY2V.wks.jnj.com |      | Access-Reject | 2013-08-13 15:16:38 |
|  7082 | Joana2cris                     |      | Access-Reject | 2013-08-13 17:34:49 |
|  7403 | INETPSA=5CU265946              |      | Access-Reject | 2013-08-13 19:36:23 |
|  8064 | fm.ul.pt                       |      | Access-Reject | 2013-08-14 11:09:01 |
|  8162 | host/WingH-THINK               |      | Access-Reject | 2013-08-14 11:19:33 |
|  9190 | Marta-PC=5CMarta               |      | Access-Reject | 2013-08-14 12:28:35 |
|  9400 | d4808                          |      | Access-Reject | 2013-08-14 12:42:06 |
|  9664 | encoa                          |      | Access-Reject | 2013-08-14 12:54:05 |
| 10166 | ist170275                      |      | Access-Reject | 2013-08-14 13:51:24 |
| 10240 | host/FRC                       |      | Access-Reject | 2013-08-14 13:56:22 |
| 10400 | ist166941                      |      | Access-Reject | 2013-08-14 14:06:50 |
| 10562 | host/Emanuel-VAIO              |      | Access-Reject | 2013-08-14 14:17:05 |
| 11154 | GLINTT=5Candreia.miguel        |      | Access-Reject | 2013-08-14 14:45:59 |
+-------+--------------------------------+------+---------------+---------------------+
20 rows in set (3.35 sec)
```

Fazer uma query de x a x data.

select * from radpostauth where authdate between FROM_UNIXTIME(1382778000) AND FROM_UNIXTIME(1382846400);

mysql> select SUM(acctoutputoctets) from radacct where acctstarttime > FROM_UNIXTIME(1382778000) AND acctstoptime < FROM_UNIXTIME (1382846400);

```
+-----------------------+
| SUM(acctoutputoctets) |
+-----------------------+
|          121673366254 |
+-----------------------+
1 row in set (0.02 sec)
```

mysql> select SUM(acctinputoctets) from radacct where acctstarttime > FROM_UNIXTIME(1382778000) AND acctstoptime < FROM_UNIXTIME (1382846400);

```
+----------------------+
| SUM(acctinputoctets) |
+----------------------+
|          67672784429 |
+----------------------+
1 row in set (0.02 sec)
```

Detectar NAS mal configurados que enviam IP em vez de MAC no campo CallingStationId.

```
mysql> use radius
mysql> select  distinct(nasipaddress) from radacct where callingstationid like "%.%.%.%" order by radacctid;
+-----------------+
| nasipaddress    |
+-----------------+
| 10.10.66.5      |
| 10.99.4.111     |
| 10.99.4.211     |
| 10.99.4.121     |
| 163.117.43.3    |
| 172.17.248.20   |
| 10.200.24.13    |
| 164.8.109.4     |
| 10.2.0.69       |
| 10.2.0.68       |
| 130.208.165.248 |
| 10.99.4.221     |
| 172.17.248.22   |
| 10.200.24.43    |
| 10.90.0.40      |
| 10.90.0.29      |
| 10.90.0.47      |
| 10.90.0.62      |
| 10.90.0.39      |
| 10.90.0.25      |
+-----------------+
20 rows in set (45.00 sec)
```

Logins distintos com sucesso nas últimas 24h:

```
mysql> select count(distinct(username)) from radpostauth where reply like "%Accept" and authdate > now() -
interval 1 day;
+--------------------------+
| count(distinct(username)) |
+--------------------------+
|                     1455 |
+--------------------------+
1 row in set (8.59 sec)
```

Logins distintos com sucesso na última semana:

```
mysql> select count(distinct(username)) from radpostauth where reply like "%Accept" and authdate > now() -
interval 1 week;
+--------------------------+
| count(distinct(username)) |
+--------------------------+
|                     3428 |
+--------------------------+
1 row in set (8.46 sec)
```

Logins distintos com sucesso no último mês:

```
mysql> select count(distinct(username)) from radpostauth where reply like "%Accept" and authdate > now() -
interval 1 month;
+--------------------------+
| count(distinct(username)) |
+--------------------------+
|                     6375 |
+--------------------------+
1 row in set (8.59 sec)
```

Logins distintos com sucesso no último ano:

```
mysql> select count(distinct(username)) from radpostauth where reply like "%Accept" and authdate > now() -
interval 1 year;
+--------------------------+
| count(distinct(username)) |
+--------------------------+
|                    19681 |
+--------------------------+
1 row in set (12.44 sec)
```

Logins por mês do ano de 2014:

```
 SELECT MONTH(DATE(authdate)) AS Month, COUNT(DISTINCT username),   COUNT(username) FROM radpostauth WHERE YEAR
(DATE(authdate))=2014 GROUP BY Month ORDER BY Month;
+-------+--------------------------+-----------------+
| Month | COUNT(DISTINCT username) | COUNT(username) |
+-------+--------------------------+-----------------+
|     1 |                     8812 |          712702 |
|     2 |                     9326 |          857004 |
|     3 |                    10291 |          929629 |
|     4 |                     9345 |          633058 |
|     5 |                    10629 |          908908 |
|     6 |                     8234 |         1170513 |
|     7 |                     5387 |          423632 |
|     8 |                     2620 |          158626 |
|     9 |                     9299 |          672461 |
|    10 |                    13793 |         1137179 |
|    11 |                    12133 |          999273 |
|    12 |                    10539 |          690671 |
+-------+--------------------------+-----------------+

12 rows in set (29.88 sec)
```

Consumos do ano por mês.

```
SELECT MONTH(DATE(acctupdatetime)) AS Month, SUM(acctinputoctets), SUM(acctoutputoctets) FROM radacct WHERE YEAR
(DATE(acctupdatetime))=2014  GROUP BY Month ORDER BY Month;
```

Dominios em roaming

```
SELECT distinct(SUBSTRING_INDEX(username, '@', -1)) from radpostauth where username like "%@%" and username not
like "%@iscte.pt" and reply like "%Accept";
```

Tops roaming

```
SELECT SUBSTRING_INDEX(username, '@', -1) as Domain,count(*) as Hits from radpostauth where username like "%@%"
and username not like "%@iscte.pt" and reply like "%Accept" group by Domain order by Hits;
```

Tops TLDs

```
mysql>SELECT SUBSTRING_INDEX(username, '.', -1) as Domain,count(*) * 100 / 500233 as Hits from radpostauth
where username like "%@%" and username not like "%@iscte.pt" and username not like "%@iscte-iul.pt" and reply
like "%Accept" group by Domain order by Hits;
+--------+---------+

| Domain | Hits    |

+--------+---------+
| cy     |  0.0002 |
| is     |  0.0002 |
| il     |  0.0018 |
| sk     |  0.0026 |
| ro     |  0.0030 |
| eu     |  0.0030 |
| gr     |  0.0042 |
| ie     |  0.0060 |
| iscte  |  0.0076 |
| cat    |  0.0168 |
| hr     |  0.0174 |
| tr     |  0.0176 |
| sg     |  0.0188 |
| au     |  0.0214 |
| hk     |  0.0260 |
| rs     |  0.0314 |
| fr     |  0.0448 |
| za     |  0.0450 |
| lt     |  0.0494 |
| lu     |  0.0550 |
| ca     |  0.0598 |
| pl     |  0.0676 |
| ch     |  0.0716 |
| si     |  0.0884 |
| br     |  0.0912 |
| no     |  0.1077 |
| edu    |  0.2425 |
| fi     |  0.2631 |
| at     |  0.2789 |
| be     |  0.3019 |
| it     |  0.4852 |
| se     |  0.5320 |
| dk     |  0.5679 |
| cz     |  0.5967 |
| mo     |  0.6403 |
| uk     |  1.0709 |
| es     |  1.4655 |
| nl     |  2.4944 |
| de     |  2.8537 |
| pt     | 87.3489 |
+--------+---------+
40 rows in set (10.33 sec)
```

Queriy utilizadores iscte.pt locais.

```
mysql> select MONTH(acctstoptime) AS Month, count(distinct(username)) from radacct where  realm= "iscte.pt" and
year(acctstoptime)=2014 and (nasipaddress like "10.61.10.1%" or nasipaddress like "10.10.65.%") group by month
order by month;;

+-------+--------------------------+

| Month | count(distinct(username)) |

+-------+--------------------------+
|     1 |                     3685 |
|     2 |                     3956 |
|     3 |                     4068 |
|     4 |                     3901 |
|     5 |                     4054 |
|     6 |                     3256 |

|     8 |                      200 |
|     9 |                     3364 |
|    10 |                     4550 |
|    11 |                     4585 |
|    12 |                     4286 |
+-------+--------------------------+

11 rows in set (32.30 sec)
```

Query utilizadores iscte.pt em roaming.

```
mysql> select MONTH(acctstoptime) AS Month, count(distinct(username)) from radacct where  realm= "iscte.pt" and
year(acctstoptime)=2014 and nasipaddress not like "10.61.10.1%" and nasipaddress not like "10.10.65.%" group by
month order by month;
+-------+--------------------------+
| Month | count(distinct(username)) |
+-------+--------------------------+
|     1 |                     2171 |
|     2 |                     2511 |
|     3 |                     2879 |
|     4 |                     2765 |
|     5 |                     3076 |
|     6 |                     2408 |
|     8 |                      228 |
|     9 |                     2711 |
|    10 |                     3525 |
|    11 |                     3473 |
|    12 |                     3243 |
+-------+--------------------------+
11 rows in set (13.34 sec)
```

/var/log/syslog

Logs enviado pelo AP com clientes a tentar demasiadas vezes autenticações erradas (bloqueio temporário).

```
syslog:/var/log# grep 10.10.66.5 syslog | grep "Max EAP identity"
Apr 28 09:13:19 10.10.66.5 1x_auth_pae.c:2488 DOT1X-3-MAX_EAP_RETRIES: Max EAP identity request retries (21) exceeded for client 28:18:78:5a:79:51
Apr 28 09:13:49 10.10.66.5 1x_auth_pae.c:2488 DOT1X-3-MAX_EAP_RETRIES: Max EAP identity request retries (21) exceeded for client d0:df:9a:5d:ee:cd
Apr 28 09:15:58 10.10.66.5 1x_auth_pae.c:2488 DOT1X-3-MAX_EAP_RETRIES: Max EAP identity request retries (21) exceeded for client 44:d8:84:4c:c8:d2
Apr 28 09:16:12 10.10.66.5 1x_auth_pae.c:2488 DOT1X-3-MAX_EAP_RETRIES: Max EAP identity request retries (21) exceeded for client d0:df:9a:5d:ee:cd
Apr 28 09:16:41 10.10.66.5 1x_auth_pae.c:2488 DOT1X-3-MAX_EAP_RETRIES: Max EAP identity request retries (21) exceeded for client 2c:b4:3a:eb:38:af
Apr 28 09:17:43 10.10.66.5 1x_auth_pae.c:2488 DOT1X-3-MAX_EAP_RETRIES: Max EAP identity request retries (21) exceeded for client d0:17:6a:fc:7f:eb
```

Grep com debugging activo de logs. Detecção de erro em filtro de dominios.

```
$grep 193.136.188.36 syslog | grep meru | grep 3gp

Jan 21 19:03:30 193.136.188.36 freeradius[19558]: (3807) Invalid user: [1268069614894544@wlan.mnc006.mcc268.3gppnetwork.org] (from client meruc port 2049 cli D0-7A-B5-9B-5F-3D)

Jan 21 19:03:32 193.136.188.36 freeradius[19558]: (3809) Invalid user: [1268069614894544@wlan.mnc006.mcc268.3gppnetwork.org] (from client meruc port 2049 cli D0-7A-B5-9B-5F-3D)

Jan 21 19:03:34 193.136.188.36 freeradius[19558]: (3811) Invalid user: [1268069614894544@wlan.mnc006.mcc268.3gppnetwork.org] (from client meruc port 2049 cli D0-7A-B5-9B-5F-3D)

Jan 21 19:03:36 193.136.188.36 freeradius[19558]: (3815) Invalid user: [1268069614894544@wlan.mnc006.mcc268.3gppnetwork.org] (from client meruc port 2049 cli D0-7A-B5-9B-5F-3D)

Jan 21 19:03:38 193.136.188.36 freeradius[19558]: (3825) Invalid user: [1268069614894544@wlan.mnc006.mcc268.3gppnetwork.org] (from client meruc port 2049 cli D0-7A-B5-9B-5F-3D)

Jan 21 19:03:40 193.136.188.36 freeradius[19558]: (3841) Invalid user: [1268069614894544@wlan.mnc006.mcc268.3gppnetwork.org] (from client meruc port 2049 cli D0-7A-B5-9B-5F-3D)

Jan 21 19:03:42 193.136.188.36 freeradius[19558]: (3847) Invalid user: [1268069614894544@wlan.mnc006.mcc268.3gppnetwork.org] (from client meruc port 2049 cli D0-7A-B5-9B-5F-3D)

Jan 21 19:03:44 193.136.188.36 freeradius[19558]: (3849) Invalid user: [1268069614894544@wlan.mnc006.mcc268.3gppnetwork.org] (from client meruc port 2049 cli D0-7A-B5-9B-5F-3D)

Jan 21 19:04:30 193.136.188.36 freeradius[19558]: (4002) Invalid user: [1268069614894544@wlan.mnc006.mcc268.3gppnetwork.org] (from client meruc port 2049 cli D0-7A-B5-9B-5F-3D)

Jan 21 19:04:32 193.136.188.36 freeradius[19558]: (4004) Invalid user: [1268069614894544@wlan.mnc006.mcc268.3gppnetwork.org] (from client meruc port 2049 cli D0-7A-B5-9B-5F-3D)

Jan 21 19:04:34 193.136.188.36 freeradius[19558]: (4026) Invalid user: [1268069614894544@wlan.mnc006.mcc268.3gppnetwork.org] (from client meruc port 2049 cli D0-7A-B5-9B-5F-3D)

Jan 21 19:04:36 193.136.188.36 freeradius[19558]: (4044) Invalid user: [1268069614894544@wlan.mnc006.mcc268.3gppnetwork.org] (from client meruc port 2049 cli D0-7A-B5-9B-5F-3D)

Jan 21 19:05:28 193.136.188.36 freeradius[19558]: (4157) Invalid user: [1268069614894544@wlan.mnc006.mcc268.3gppnetwork.org] (from client meruc port 2049 cli D0-7A-B5-9B-5F-3D)

Jan 21 19:11:08 193.136.188.36 freeradius[19558]: (5056) Invalid user: [1268069614894544@wlan.mnc006.mcc268.3gppnetwork.org] (from client meruc port 2105 cli D0-7A-B5-9B-5F-3D)

Jan 21 19:11:14 193.136.188.36 freeradius[19558]: (5062) Invalid user: [1268069614894544@wlan.mnc006.mcc268.3gppnetwork.org] (from client meruc port 2054 cli D0-7A-B5-9B-5F-3D
```

Logs de autenticações na federação.

Jan 21 06:34:21 193.136.188.36 freeradius[30263]: (7818) Login OK: [imaaf@iscte.pt] (from client proxyNacional1 port 29 cli 38-aa-3c-6e-d2-ff via TLS tunnel)

Jan 21 06:34:21 193.136.188.36 freeradius[30263]: (7819) Login OK: [imaaf@iscte.pt] (from client proxyNacional1 port 29 cli 38-aa-3c-6e-d2-ff)

Jan 21 06:35:22 193.136.188.36 freeradius[30263]: (7823) Invalid user: [radius-teste@iscte.pt] (from client proxyNacional2 port 0)

Jan 21 06:36:37 193.136.188.36 freeradius[30263]: (7832) Login OK: [mjsr@iscte.pt] (from client proxyNacional1 port 1 cli C8-BC-C8-EF-D4-13 via TLS tunnel)

Jan 21 06:36:38 193.136.188.36 freeradius[30263]: (7833) Login OK: [mjsr@iscte.pt] (from client proxyNacional1 port 1 cli C8-BC-C8-EF-D4-13)

Jan 21 06:39:25 193.136.188.36 freeradius[30263]: (7873) Login OK: [imaaf@iscte.pt] (from client proxyNacional1 port 29 cli 38-aa-3c-6e-d2-ff via TLS tunnel)

Jan 21 06:39:25 193.136.188.36 freeradius[30263]: (7874) Login OK: [imaaf@iscte.pt] (from client proxyNacional1 port 29 cli 38-aa-3c-6e-d2-ff)

Jan 21 06:41:47 193.136.188.36 freeradius[30263]: (7881) Login OK: [imaaf@iscte.pt] (from client proxyNacional1 port 29 cli 38-aa-3c-6e-d2-ff)

Jan 21 06:47:27 193.136.188.36 freeradius[30263]: (7950) Login OK: [kehaa@iscte.pt] (from client proxyNacional1 port 8898 cli 7C-D1-C3-8D-0B-C2 via TLS tunnel)

Cliente mal configurado.

Mar 3 11:45:00 193.136.188.36 freeradius[28574]: (12207) Login incorrect (eap: No mutually acceptable types found): [iovoa@iscte.pt] (from client meruc port 2067 cli D0:7A:B5:71:98:61)

FreeRadius not compiled to talk directly with SAMBA.

rlm_mschap (mschap): 'winbind' auth not enabled at compiled time

/etc/freeradius/mods-enabled/mschap[10]: Instantiation failed for module "mschap"

Certificado assinado por uma CA não conhecida por freeradius e não instalada em certs

Wed May 27 00:10:44 2015 : Debug: (89) eap_tls: <<< TLS 1.0 Alert [length 0002], fatal unknown_ca
Wed May 27 00:10:44 2015 : ERROR: (89) eap_tls: TLS Alert read:fatal:unknown CA
Wed May 27 00:10:44 2015 : ERROR: (89) eap_tls: TLS_accept: Failed in SSLv3 read client certificate A

/var/log/freeradius/radius.log

O FreeRadius envia para o syslog mensagens de diagnóstico de operação normal.

Mensagem normal de arranque de saída do FreeRadius.

Sun Nov 3 07:00:05 2013 : Info: Ready to process requests.

Sun Nov 3 07:10:01 2013 : Info: Signalled to terminate

Sun Nov 3 07:10:01 2013 : Info: Exiting normally.

Mensagem de arranque normal do daemon FreeRadius

```
Sun Nov  3 07:40:01 2013 : Info: rlm_sql_mysql: Starting connect to MySQL server for #19
Sun Nov  3 07:40:01 2013 : Info: rlm_sql (sql): Connected new DB handle, #19
Sun Nov  3 07:40:01 2013 : Info: Loaded virtual server <default>
Sun Nov  3 07:40:01 2013 : Info: Loaded virtual server inner-tunnel
Sun Nov  3 07:40:01 2013 : Info:  ... adding new socket proxy address * port 46906
Sun Nov  3 07:40:01 2013 : Info:  ... adding new socket proxy address * port 42864
Sun Nov  3 07:40:01 2013 : Info:  ... adding new socket proxy address * port 51203
Sun Nov  3 07:40:01 2013 : Info:  ... adding new socket proxy address * port 53214
Sun Nov  3 07:40:01 2013 : Info: Ready to process requests.
```

Se se tentar levantar o freeradius com ele já em cima, ver-se-á a seguinte mensagem. Caso seja realmente o pretendido, dever-se-á matar a cópia anterior.

```
Failed binding to authentication address * port 1645: Address already in use
> /etc/freeradius/radiusd.conf[xx]: Error binding to port for 0.0.0.0 port 1812
```

Erro no shared secret.

```
Fri Aug 2 16:45:38 2013 : Debug: WARNING: Unprintable characters in the password. Double-check the shared secret on the server and the NAS!
```

Erro de deadlock de transacções. Não é fatal. Antes do 2.2.4 estas situações implicavam fazer restart ao freeradius.

```
Sat Jan 18 09:22:26 2014 : Error: [sql] Couldn't insert SQL accounting START record - Deadlock found when trying to get lock; try restarting transaction
Sat Jan 18 10:29:24 2014 : Error: [sql] Couldn't update SQL accounting STOP record - Deadlock found when trying to get lock; try restarting transaction
Sat Jan 18 10:29:24 2014 : Error: rlm_sql_mysql: MySQL error 'Deadlock found when trying to get lock; try restarting transaction'
```

Mensagem em caso de erros de ligação ao MySQL; pode acontecer quando o max_servers ser maior que sql_num_socks, ao contrário do que é aconselhado de serem idênticos.

```
Thu Nov  7 18:32:09 2013 : Error: rlm_sql (sql): Failed to connect DB handle #17
Thu Nov  7 18:32:09 2013 : Error: rlm_sql (sql): Failed to connect DB handle #16
Thu Nov  7 18:32:09 2013 : Error: rlm_sql (sql): Failed to connect DB handle #19
Thu Nov  7 18:32:09 2013 : Error: rlm_sql (sql): Failed to connect DB handle #1
Thu Nov  7 18:32:10 2013 : Error: rlm_sql (sql): There are no DB handles to use! skipped 20, tried to connect 0
Thu Nov  7 18:32:11 2013 : Error: rlm_sql (sql): There are no DB handles to use! skipped 20, tried to connect 0
Thu Nov  7 18:32:12 2013 : Error: rlm_sql (sql): There are no DB handles to use! skipped 20, tried to connect 0
Thu Nov  7 18:32:13 2013 : Error: rlm_sql (sql): There are no DB handles to use! skipped 20, tried to connect 0
```

No caso de cliente tentar usar CA/certificado errado para falar com o freeradius:

```
rlm_eap: SSL error error:14094418:SSL routines:SSL3_READ_BYTES:tlsv1 alert unknown ca
```

/var/log/freeradius/radacct

O FreeRADIUS com o accounting detalhado coloca logs debaixo deste directório, organizado por em directórios por IP (normalmente os APs e os proxies nacionais).

```
# ls
193.136.192.43 193.136.192.44 193.136.188.36
```

Debaixo de cada directório, são criados um ficheiro por dia, com a data no final, para várias fases do processo de funcionamento do freeradius (-AAAAMMDD).

A freqüência pode ser mudada, para por exemplo, criar ficheiros por hora.

Uma vez que estes ficheiros estão ordenados por IP, são bastante úteis para fazer despistar problemas de utilizadores.

Os ficheiros são:

- auth-detail
- detail
- reply-detail
- pre-proxy-detail
- post-proxy-detail

auth-detail

Este ficheiro fica com o log detalhado da secção authorize.

```
Tue Aug 27 15:10:20 2013
Packet-Type = Access-Request
User-Name = "fccn-eduroamteste@iscte.pt"
Framed-MTU = 1400
Called-Station-Id = "0c85.2567.ce50"
Calling-Station-Id = "6067.20b1.8370"
Cisco-AVPair = "ssid=eduroam"
WISPr-Location-Name = "FCCN - Edificio Central (piso 0)"
Service-Type = Login-User
Message-Authenticator = 0x0ef35e88e202f53675dafb271accc165
EAP-Message = 0x020c002b1900170301002066bb9b8abd4750b21b02933fc84e7eb6f7
7e81844ab3d7bf5d271eff15b9e0f5
NAS-Port-Type = Wireless-802.11
NAS-Port = 917
NAS-Port-Id = "917"
State = 0x609cc6fe6990dfee60dce4a71b8fbf60
NAS-IP-Address = 10.0.11.2
Operator-Name = "1fcc"
Vendor-25178-Attr-10 = 0x5054
Operator-Name = "1fccn.pt"
Proxy-State = 0x4f53432d457874656e6465642d49643d31
```

detail

```
Tue Aug 27 15:10:20 2013
Acct-Session-Id = "00005F46"
Called-Station-Id = "0c85.2567.ce50"
Calling-Station-Id = "6067.20b1.8370"
Cisco-AVPair = "ssid=eduroam"
Cisco-AVPair = "vlan-id=12"
Cisco-AVPair = "nas-location=FCCN - Edificio Central (piso 0)"
WISPr-Location-Name = "FCCN - Edificio Central (piso 0)"
User-Name = "fccn-eduroamteste@iscte.pt"
Cisco-AVPair = "connect-progress=Call Up"
Acct-Authentic = RADIUS
Acct-Status-Type = Start
NAS-Port-Type = Wireless-802.11
NAS-Port = 917
NAS-Port-Id = "917"
Service-Type = Framed-User
NAS-IP-Address = 10.0.11.2
Acct-Delay-Time = 0
Operator-Name = "1fcc"
Vendor-25178-Attr-10 = 0x5054
Attr-103 = 0x521cb34c
Operator-Name = "1fccn.pt"
Proxy-State = 0x4f53432d457874656e6465642d49643d31
FreeRADIUS-Acct-Session-Start-Time = "Aug 27 2013 15:10:20 WEST"
Acct-Unique-Session-Id = "7385715713ee0773"
Stripped-User-Name = "fccn-eduroamteste"
Realm = "iscte.pt"
Timestamp = 1377612620
```

reply-detail

Este ficheiro tem os logs detalhados das respostas às mensagens RADIUS.

```
/var/log/freeradius/rad~/reply-detail-20130827 1045/108K 0%
Tue Aug 27 15:10:20 2013
Packet-Type = Access-Accept
User-Name = "fccn-eduroamteste@iscte.pt"
Service-Type = Framed-User
Reply-Message = "Eduroam Alunos"
Framed-MTU = 1300
Tunnel-Type:0 = VLAN
Tunnel-Medium-Type:0 = IEEE-802
Tunnel-Private-Group-Id:0 = "200"
MS-MPPE-Recv-Key = 0xec495557b5eb65b1eeb26ed40dc8b2d8dd310cb0b949ad9bbed
76f6b89e9030f
MS-MPPE-Send-Key = 0x7ff07aecb36dfd6117e696c7c332b7012b79d63d3c513f20068
adcad45d514cd
EAP-MSK = 0xec495557b5eb65b1eeb26ed40dc8b2d8dd310cb0b949ad9bbed76f6b89e9
030f7ff07aecb36dfd6117e696c7c332b7012b79d63d3c513f20068adcad45d514cd
EAP-EMSK = 0x42ae50bfdf2807f030b5f80d0ae268f5932c8c06eddf47602626bf05263
5b1dc8bf0c3f02952468d7dd43b71e44b3273071933f4c3adc46da3a46ecca993ee9e
EAP-Message = 0x030c0004
Message-Authenticator = 0x00000000000000000000000000000000
```

pre-proxy-detail

Este ficheiro têm o log detalhado das transacções a dos pedidos de autenticação que irão fazer roaming no ambiente EDUROAM.

```
Wed Sep 11 10:29:25 2013
Packet-Type = Access-Challenge
Filter-Id = "Aluno"
EAP-Message = 0x010600160410eda2b75a094e5e31b54f66c03fdf776c
Message-Authenticator = 0xd5226614db45247be1d15ce2e1309dc2
State = 0xd2ff20ead2f92454149d8c50c74fab8a
Proxy-State = 0x34
Wed Sep 11 10:29:25 2013
Packet-Type = Access-Challenge
Filter-Id = "Aluno"
EAP-Message = 0x010700061920
Message-Authenticator = 0x8f1392c474b1fd60c03f19f592aee00b
State = 0xd2ff20ead3f83954149d8c50c74fab8a
Proxy-State = 0x35

Wed Sep 11 10:29:25 2013
Packet-Type = Access-Challenge
EAP-Message = 0x0108040019c00000120c16030100310200002d0301523037f52b5cc5
a91a6d9a7d11fb4195d77f912cdab3f8e751f7b1e3f9c7a99100002f000005ff0100010016030111
c80b0011c40011c100049f3082049b30820383a00302010202105971c895fff248dd886a328a7b80
e427300d06092a864886f70d01010505003036310b300906035504061302e4c310f300d06035504
0a1306544552454e4131163014060355040313130d544552454e412053534c204341301e170d313330
353233303030303030305a170d3136303532323233353935395a30403121301f060355040b1318446f
6d61696e20436f6e74726f6c2056616c696461746564311b30
EAP-Message = ……
EAP-Message = 0x63848f5084214f6ef696cc30
Message-Authenticator = 0xe942b38614d5f7dce5219db83831e5f6
State = 0xd2ff20ead0f73954149d8c50c74fab8a
Proxy-State = 0x36
Wed Sep 11 10:29:25 2013
Packet-Type = Access-Challenge
EAP-Message = 0x01…
EAP-Message = 0x5345524669727374
Message-Authenticator = 0x43fae53f38deffc82ffc3fab2e87162d
State = 0xd2ff20ead1f63954149d8c50c74fab8a
Proxy-State = 0x38
ed Sep 11 10:29:25 2013
Packet-Type = Access-Challenge
EAP-Message = 0x010a03fc…
EAP-Message = 0xd6eec7ed288dab4d
Message-Authenticator = 0xb13a5f110a1f549c456ce3562b9c2044
State = 0xd2ff20ead6f53954149d8c50c74fab8a
Proxy-State = 0x3130
Wed Sep 11 10:29:25 2013
EAP-Message = 0x3134….0x3135….0x3137…0x3231…0x3232…0x3233…0x3234….
Wed Sep 11 10:29:25 2013
Packet-Type = Access-Accept
Filter-Id = "EDUROAM_31"
MS-MPPE-Recv-Key = 0x42d43bd166fca13939f2c53781e801bc730dfc07243b6788a2d
042d1f15bb603
MS-MPPE-Send-Key = 0xfed6d8c6c45d49474da801cdd4c1d7cdc84ffc01519417f9deb
8a5d0ec4b98c0
EAP-Message = 0x03110004
Message-Authenticator = 0xb1c3557bcf786ebd5a3664020c239b91
Proxy-State = 0x3235
Wed Sep 11 10:29:30 2013
Packet-Type = Accounting-Response
Proxy-State = 0x3337
Wed Sep 11 10:34:31 2013
Packet-Type = Accounting-Response
Proxy-State = 0x3437
Wed Sep 11 10:34:42 2013
Packet-Type = Accounting-Response
Proxy-State = 0x3439
```

post-proxy-detail

Este ficheiro têm o log detalhado das transacções que fizeram roaming no ambiente EDUROAM.

```
Thu Sep 12 09:14:08 2013
Packet-Type = Access-Challenge
Reply-Message = "DA"
Tunnel-Private-Group-Id:0 = "\0002"
Tunnel-Medium-Type:0 = IEEE-802
Tunnel-Type:0 = VLAN
Filter-Id = "e-U"
Framed-IP-Netmask = 255.255.255.0
Framed-IP-Address = 172.18.120.3
EAP-Message = 0x010200061520
Message-Authenticator = 0x0544712c30548917303e53a25c90cc63
State = 0xf9e1f2a0b054885c2a
hu Sep 12 09:30:52 2013
Packet-Type = Access-Accept
MS-CHAP-Domain = "0UMINHO"
MS-MPPE-Encryption-Policy = 0x00000002
MS-MPPE-Encryption-Types = 0x0000000e
Framed-IP-Address = 255.255.255.255
Reply-Message = "Group_ALFA:no;"
User-Name = "id2496@alunos.uminho.pt"
MS-MPPE-Send-Key = 0x5ad6fad31e7d0861204c21ad17a55cc726b4de91ef7e9671eac
1891a6207498a
MS-MPPE-Recv-Key = 0x1f9161a935bc8bbef553228dc7cb924576c3657084ac7d919ca
5723cc0aeb992
EAP-Message = 0x03080004
Message-Authenticator = 0xa110ed9c52d5c93772644ed80cd2ff4f
Proxy-State = 0x3331
Fri Sep 13 10:04:42 2013
Packet-Type = Access-Accept
Reply-Message = "DA"
Tunnel-Private-Group-Id:0 = "\0002"
Tunnel-Medium-Type:0 = IEEE-802
Tunnel-Type:0 = VLAN
Filter-Id = "e-U"
Framed-IP-Netmask = 255.255.255.0
Framed-IP-Address = 172.18.120.3
MS-MPPE-Recv-Key = 0x340a189564981e940f490d72c34757a1a2822cd1b9e108ff40f
e768b2e8e6cb3
MS-MPPE-Send-Key = 0x2ec547e0d54e2cac4698379644ab0122aa86706418c88beeb4c
87b1ce61f1ae3
EAP-Message = 0x03050004
Message-Authenticator = 0x995ed805ccedba004d1c67efd69f35b9
User-Name = "ilobo@ual.pt"
Proxy-State = 0x3830

Fri Sep 13 10:05:12 2013
Packet-Type = Accounting-Response
Proxy-State = 0x3835
```

Listar accounting de utilizador

```
mysql> select * from radacct where username like "rffro%" order by radacctid desc limit 5;
+-----------+------------------+------------------+----------+-----------+-------+-------------+-----------
+-----------------+--------------------+--------------------+-----------------+--------------
+----------------------+----------------------+-----------------+------------------
+--------------------------------+------------------+--------------------+-------------+----------------
+-----------------+----------------+---------------+----------------------+
| radacctid | acctsessionid     | acctuniqueid     | username | groupname | realm | nasipaddress | nasportid |
nasporttype     | acctstarttime       | acctstoptime        | acctsessiontime | acctauthentic |
connectinfo_start     | connectinfo_stop      | acctinputoctets | acctoutputoctets |
calledstationid               | callingstationid  | acctterminatecause | servicetype | framedprotocol |
framedipaddress | acctstartdelay | acctstopdelay | xascendsessionsvrkey |
+-----------+------------------+------------------+----------+-----------+-------+-------------+-----------
+-----------------+--------------------+--------------------+-----------------+--------------
+-------------------+-------------------+--------------------+-----------------
+--------------------------------+------------------+--------------------+-------------+----------------
+-----------------+----------------+---------------+----------------------+
|   1100528 | 52820D0C-00000F2E | 3357c929bb9fbc7e | rffro    |           |       | 10.61.10.12  | 2063      |
Wireless-802.11 | 2013-11-12 14:53:51 | NULL               |              0 | RADIUS        | CONNECT Unknown
radio |                      |              0 |               0 | 00-0C-29-4C-B5-4F:EDUROAM_1020 | 60-C5-47-
8B-FF-46 |                      |             |                |                 |             0 |             0
|                     |
|   1100477 | 52820D0C-00000F1B | 9a17027a1ef38101 | rffro    |           |       | 10.61.10.12  | 2103      |
Wireless-802.11 | 2013-11-12 14:53:09 | NULL               |              0 | RADIUS        | CONNECT Unknown
radio |                      |              0 |               0 | 00-0C-29-4C-B5-4F:EDUROAM_1020 | 1C-AB-A7-
A2-71-A5 |                      |             |                |                 |             0 |             0
|                     |
|   1100356 | 52820D0C-00000EF8 | 287934071c2f8815 | rffro    |           |       | 10.61.10.12  | 2063      |
Wireless-802.11 | 2013-11-12 14:51:41 | 2013-11-12 14:53:50 |            128 | RADIUS        | CONNECT Unknown
radio | CONNECT Unknown radio |           16918 |             8902 | 00-0C-29-4C-B5-4F:EDUROAM_1020 | 60-C5-47-
8B-FF-46 | User-Request       |             |                |                 |             0 |             0
|                     |
|   1099855 | 52820D0C-00000E6D | f344ef805d3e4401 | rffro    |           |       | 10.61.10.12  | 2063      |
Wireless-802.11 | 2013-11-12 14:45:50 | 2013-11-12 14:46:14 |             24 | RADIUS        | CONNECT Unknown
radio | CONNECT Unknown radio |            8495 |             5164 | 00-0C-29-4C-B5-4F:EDUROAM_1020 | 60-C5-47-
8B-FF-46 | User-Request       |             |                |                 |             0 |             0
|                     |
|   1099674 | 52820D0C-00000E2D | f3d812e79229805b | rffro    |           |       | 10.61.10.12  | 2220      |
Wireless-802.11 | 2013-11-12 14:43:56 | 2013-11-12 14:44:31 |             34 | RADIUS        | CONNECT Unknown
radio | CONNECT Unknown radio |            2136 |             4828 | 00-0C-29-4C-B5-4F:EDUROAM_1020 | 1C-AB-A7-
A2-71-A5 | User-Request       |             |                |                 |             0 |             0
|                     |
+-----------+------------------+------------------+----------+-----------+-------+-------------+-----------
+-----------------+--------------------+--------------------+-----------------+--------------
+----------------------+----------------------+-----------------+------------------
+--------------------------------+------------------+--------------------+-------------+----------------
+-----------------+----------------+---------------+----------------------+
5 rows in set (0.01 sec)
```

Instalação de equipamento

NAS/APs

Existe bastantes clientes do protocolo RADIUS, mesmo em routers de nível residencial e open source, o problema é que nem todos suportam VLANs. Obviamente que para níveis de serviço se aconselha equipamento de qualidade profissional, mas para testes há que ter em atenção esse detalhe. A configuração normalmente é feita nos APs ou nos seus controladores, quer por interfaces web, quer em linha de comando.

Normalmente, os equipamentos têm a entrada para dois servidores RADIUS, em que se configura o servidor de RADIUS de serviço, e as portas a usar, e opcionalmente, um segundo para quando o primeiro fica fora de serviço.

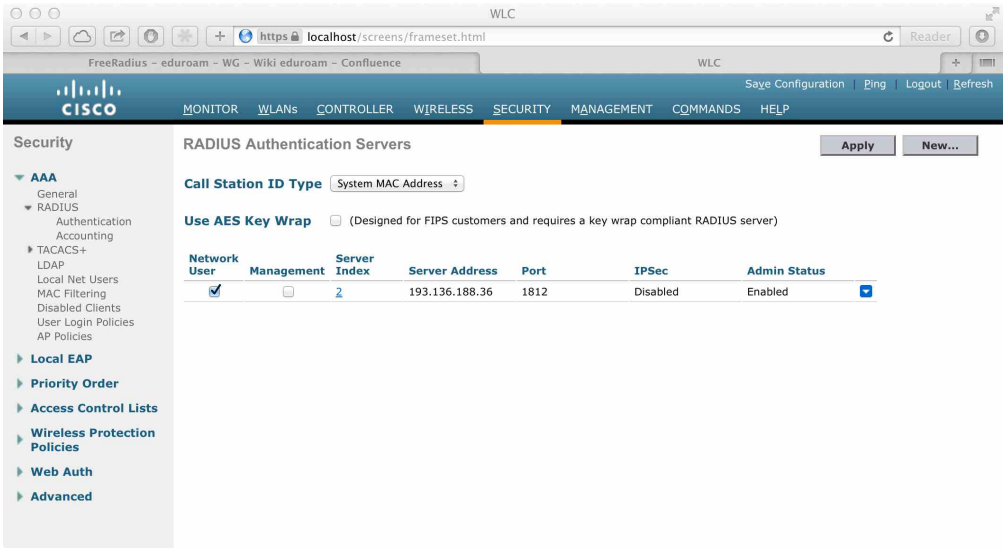
No caso do ISCTE, usamos Xirrus, Cisco e Meru, e durante a fase de piloto do freeradius, fizemos testes com Airport Express e Cisco.

Cisco WLC

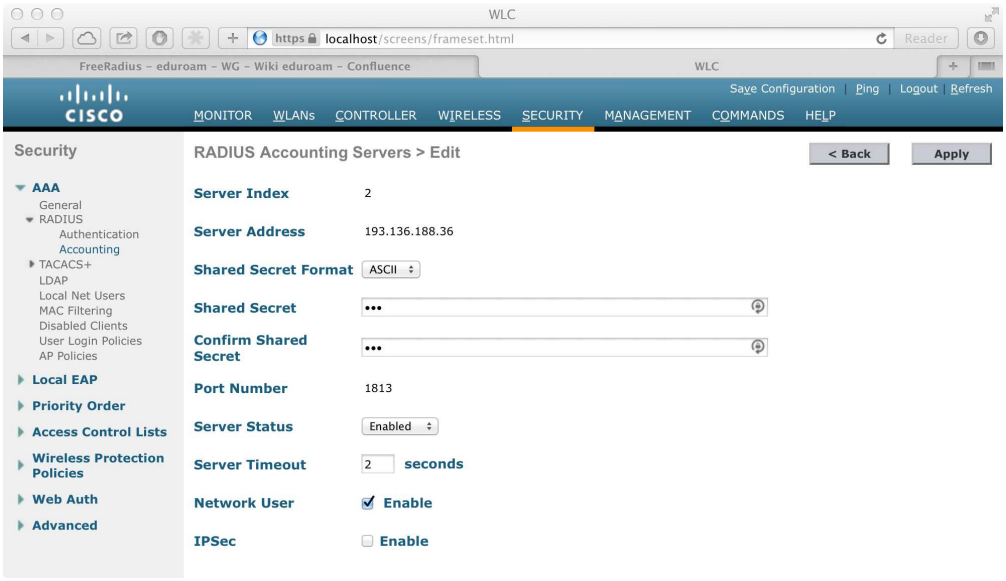
Do lado do Cisco, aqui ficam as configurações para a EDUROAM. De notar que no CallStation ID type, tem-se de seleccionar System MAC Address para os MACs dos clientes aparecerem no campo CallingStationID, ou na linha de comando do WLC:

Cisco Controller) >config radius macaddr

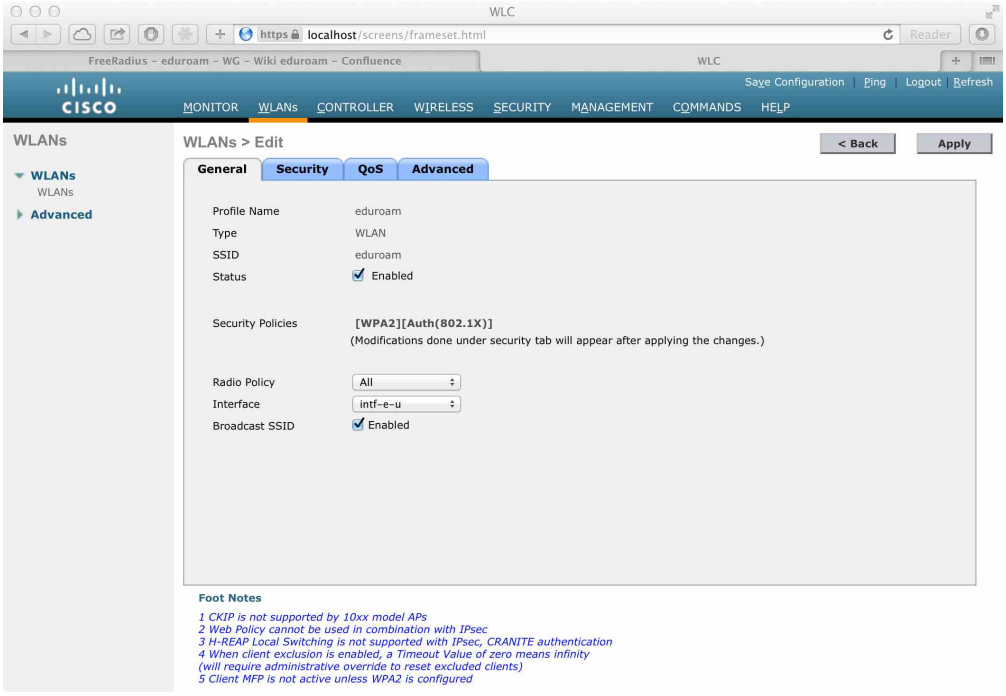
Em seguida, criar a entrada para o servidor freeradius na página de servidores de Autenticação:

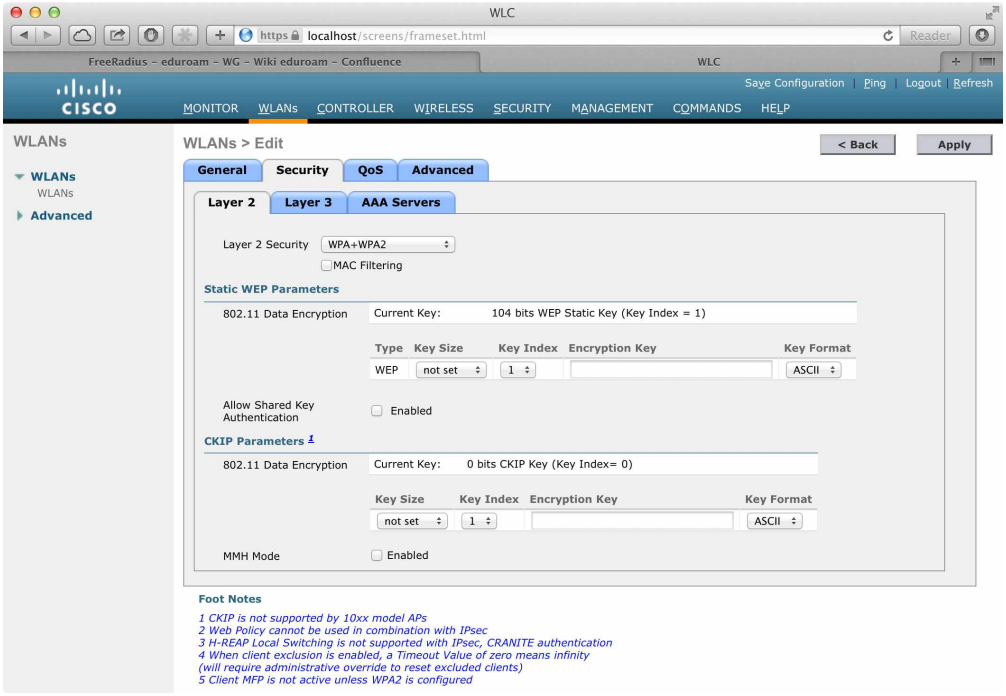


Criar a mesma entrada na página de servidores de Accounting:

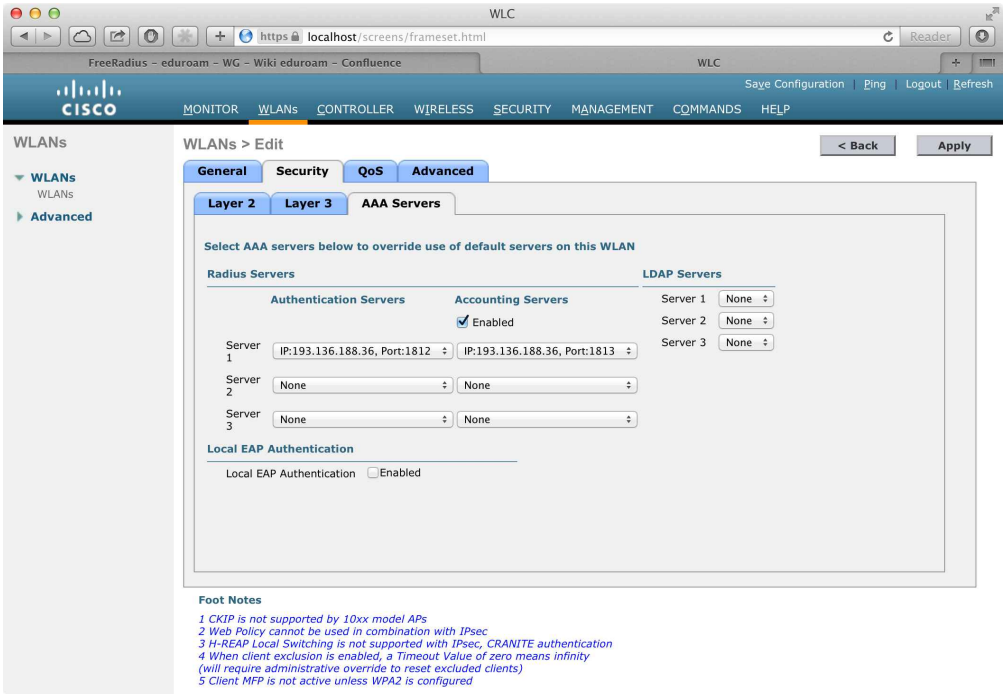


Carateristicas de WLAN:



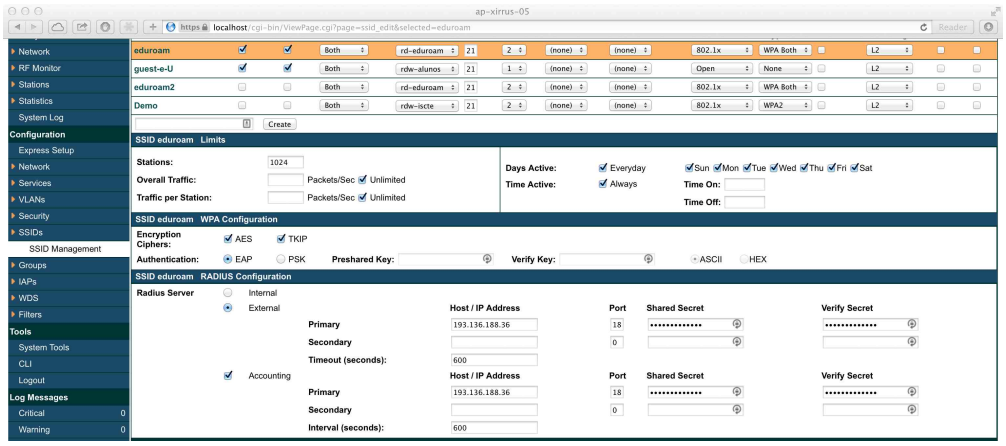


Servidores a ser usados na rede wireless. Colocar no 1 o principal e caso este exista, no 2 o secundário, que será usado no caso do primário falhar.



Xirrus

No equipamento Xirrus, a configuração para EDUROAM corrente é a apresentada.



Meru

No Meru, para configurar EDUROAM mexer nos seguintes quadros:

Cisco Catalyst

O 802.1X não é apenas para redes Wireless. Também o usamos em switches Cisco.

Na configuração actual só autoriza e não define VLANs dinâmicas. A configuração do radius de futuro terá de levar mexidas para acomodar estar a ser inquirida de cisco catalysts, a começar por não devolver VLANs dinâmicas, a organizar por grupos e a fazer o parsing de atributos radius.

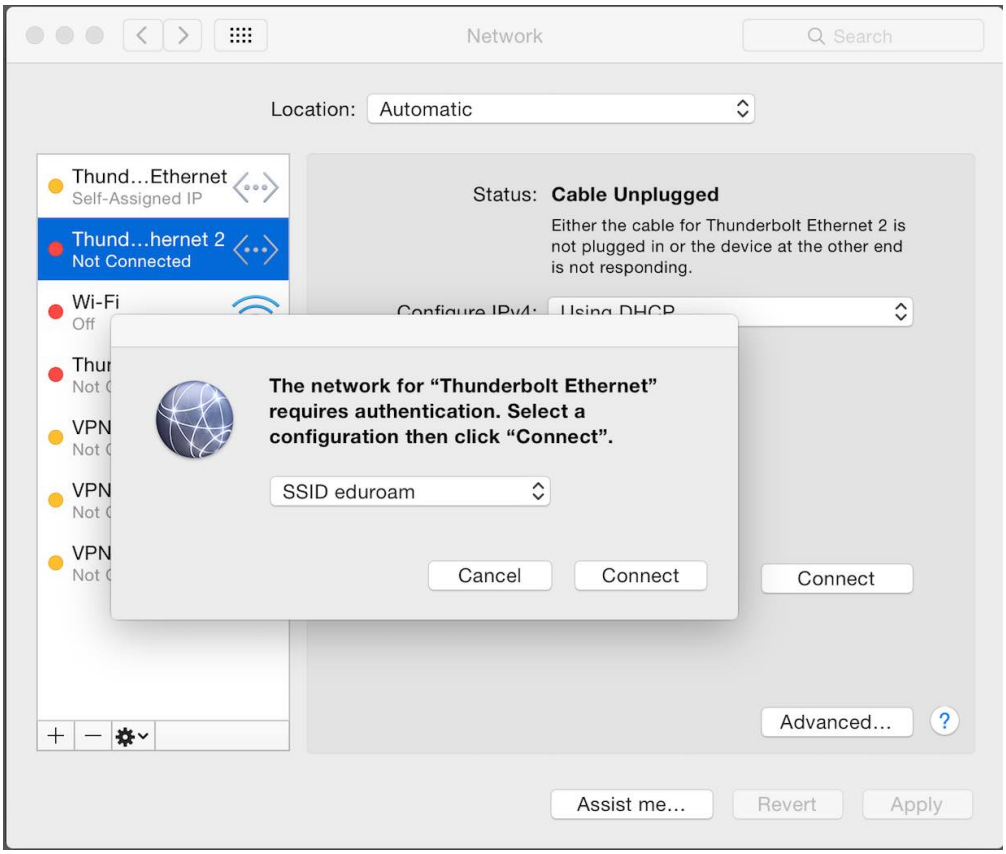
Sugere-se que se crie uma VLAN restrita para configurar a EDUROAM. Esta apenas deve deixar falar com os servidores do serviço DNS, DHCP, e porta 80 para um servidor a definir.

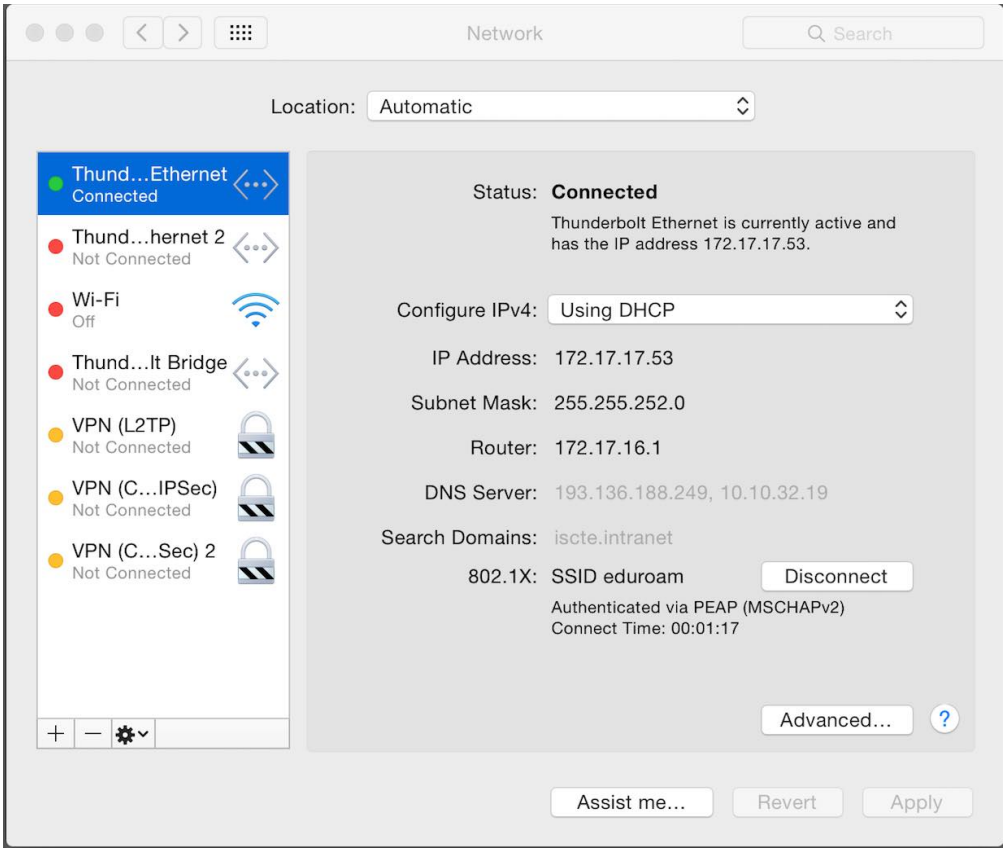
Também definimos uma configuração embrionário de portal "captivo" no BIND/DNS. Tudo o que for pedido é encaminhado para um servidor a definir, e só aceita o cat.eduroam.org. Apontamos para um site/servidor que só tenha manuais/instruções da EDUROAM. Não conseguimos apontar para os sites existentes porque o que vai aparecer é o endereço "original" pedido pelo utilizador (i.e. www.xxxx.com)

Para configurar, fazer:

```
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
radius-server host 193.136.188.36 auth-port 1812 acct-port 1813 key chave
radius-server retransmit 3
interface range f1 - 24
 description 802.1X
switchport mode access
 dot1x port-control auto
 dot1x timeout quiet-period 15
 dot1x max-req 4
 dot1x auth-fail vlan 666
 no cdp enable
 spanning-tree portfast
!
```

A VLAN 112 é um portal captivo que tem acesso ao CAT e aos manuais de instalação da EDUROAM.


Network
Search
Location: Automatic
Thund…Ethernet
Self-Assigned IP
Thund…hernet 2
Not Connected
Wi-Fi
Off
VPN
VPN
VPN
Status: Cable Unplugged
Either the cable for Thunderbolt Ethernet 2 is not plugged in or the device at the other end is not responding.
Configure IPv4: Using DHCP
The network for "Thunderbolt Ethernet" requires authentication. Select a configuration then click "Connect".
SSID eduroam
Cancel
Connect
Connect
Advanced…
Assist me…
Revert
Apply


Network
Search
Location: Automatic
Thund…Ethernet
Connected
Thund…hernet 2
Not Connected
Wi-Fi
Off
Thund…lt Bridge
Not Connected
VPN (L2TP)
Not Connected
VPN (C…IPSec)
Not Connected
VPN (C…Sec) 2
Not Connected
Status: Connected
Thunderbolt Ethernet is currently active and has the IP address 172.17.17.53.
Configure IPv4: Using DHCP
IP Address: 172.17.17.53
Subnet Mask: 255.255.252.0
Router: 172.17.16.1
DNS Server: 193.136.188.249, 10.10.32.19
Search Domains: iscte.intranet
802.1X: SSID eduroam
Disconnect
Authenticated via PEAP (MSCHAPv2)
Connect Time: 00:01:17
Advanced…
Assist me…
Revert
Apply

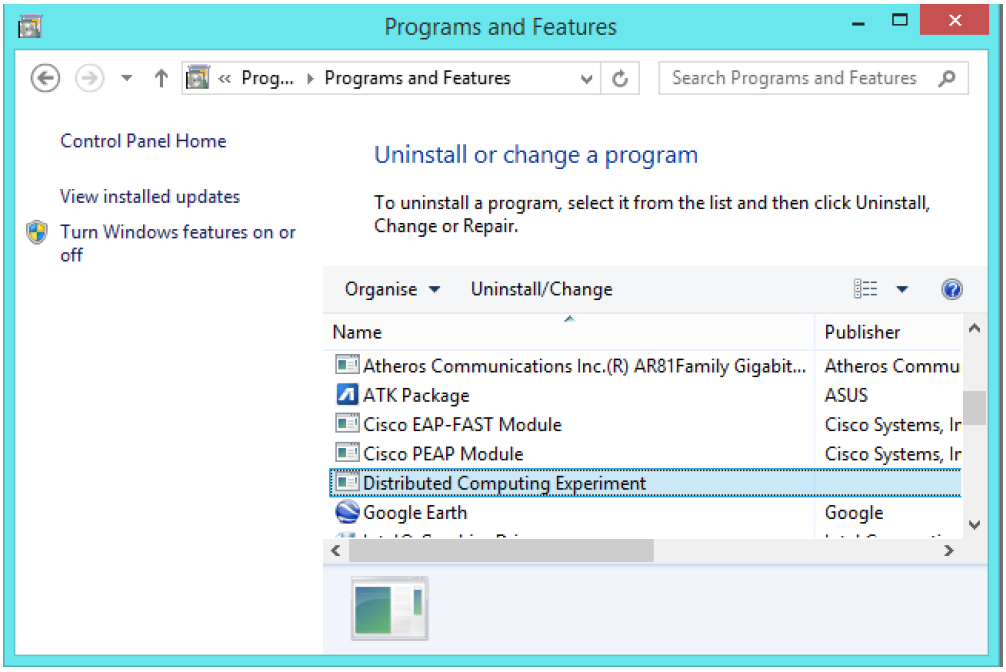
Suporte de protocolos

De acordo com testes realizados, nos sistemas operativos e no CAT, o suporte para protocolos de vários sistemas operativos, no momento é o apresentado na tabela seguinte:

	PEAP	TTLS	MSCHAPv2	PAP	perfis
Windows 8	ok	ok - não no CAT	ok		
Windows 7	ok	n.d.	ok		
Vista	ok	n.d	ok		
XP	ok	n.d	?	?	
OS/X 10.10	ok	ok	ok		ok
OS/X 10.9	ok	ok	ok	ok	ok
OS/X 10.8	ok	ok	ok	ok	ok
OS/X 10.7	ok	ok	ok	ok	ok
OS/X 10.6	ok	ok	ok	ok	
iOS	ok	ok	ok	ok	ok
Android > 2.2	ok	ok	ok	?	

No Surface RT, seleccionando a configuração de Windows 8, constata-se que a configuração automática do CAT não trabalha. No Surface pro, basta instalar o perfil do Windows 8.

Em alguns sistemas de Windows, o suporte para os protocolos está instalado à parte, e será necessário ter atenção a isso ao fazer debugging de problemas. Como exemplo, segue uma imagem capturada de Control Panel/Software Instalado num Windows 8.1 com uma ralink em wifi e Atheros em Ethernet, com os módulos/drivers de EAP/PEAP à parte.

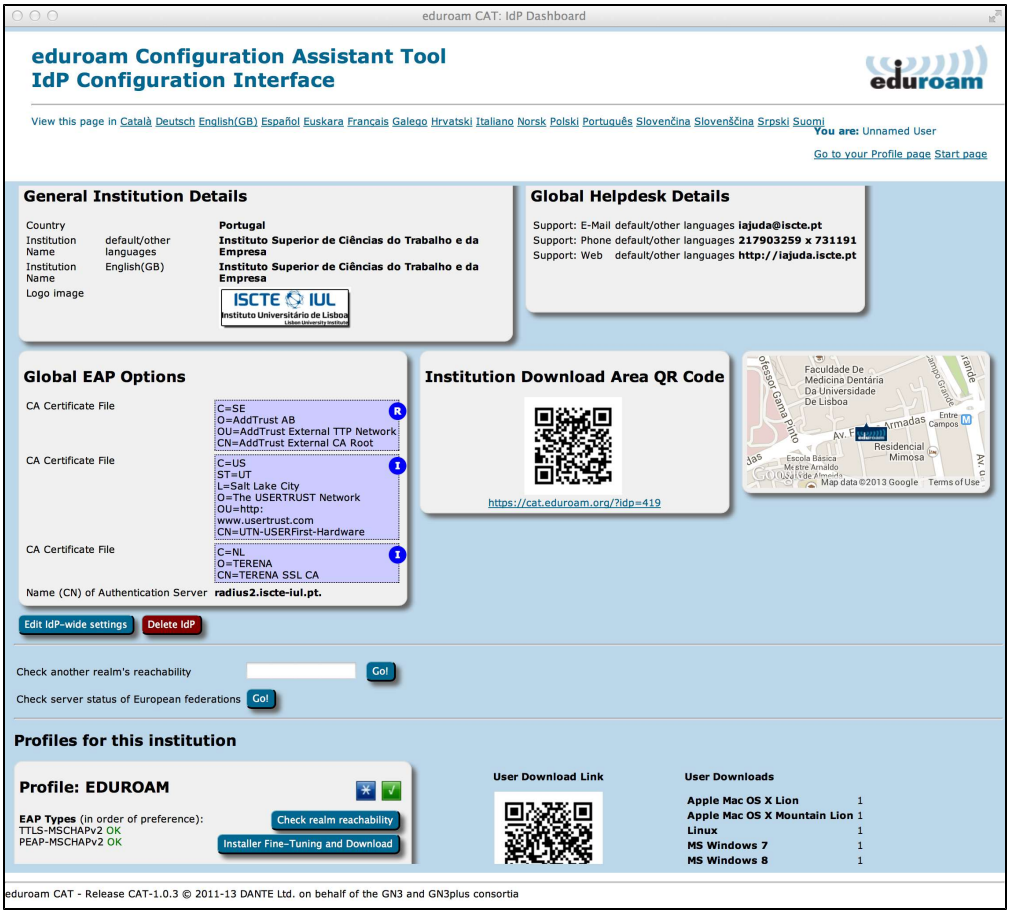


CAT

O EDUROAM Configuration Assistant Tool é uma ferramenta interessante para criar perfis de instalação automáticos para a comunidade EDUROAM, gerando XML para dispositivos da família Apple como profiles, e pacotes de instalação para Windows que trazem software acrescentado para fazer o tratamento de EAP e TTLS (netsh no caso de PEAP, SecureW2 para TTLS https://www.securew2.com/products/enterpriseclient/).

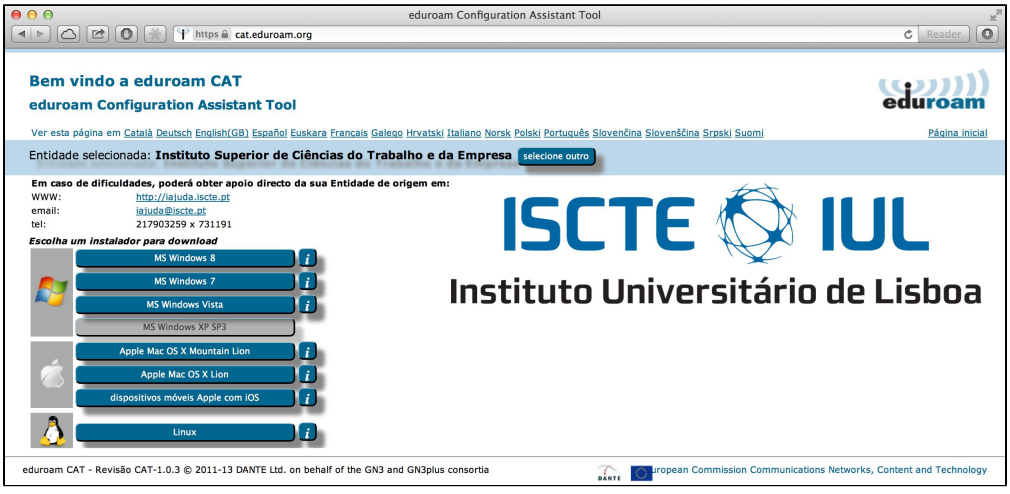
Para criar configurações automáticas de clientes, solicite um convite de membro do http://cat.eduroam.org como gestor do seu dominio ao gestor da sua federação EDUROAM (o seu FLR), no nosso caso FCCN. Ver CAT - eduroam Configuration Assistant Tool, http://www.terena.org/activities/tf-mobility/meetings/24/tf-mobility-cat.pdf e https://www.securew2.com para mais detalhes.

Em Junho de 2014, na federação portuguesa, 19 instituições já usavam o CAT.



Para usar o CAT, ou se entra pela opção eduroam admin sendo o gestor de domínio, ou seleccionado eduroam user caso se seja um utilizador.

Depois de seleccionar eduroam user, aparece um mapa com informação de geoIP/localização geográfica que indica a instituição mais perto. Seleccionado a nossa instituição, o utilizador é presenteado com uma escolha de sistemas operativos, para realizar o donwload do configurador automático.



Foi lançado recentemente um serviço similar, com a mesma interface web, para uso profissional, em https://802.1x-config.org . Este serviço fornece perfis grátis e perfis pagos com branding, à semelhança do CAT para a EDUROAM.
No caso dos certificados que estamos a usar correntemente de Terena, que frequentemente nem estão nos de sistema, têm de meter no CAT/profile a CA de suporte (AddTrust+UTN_USER First-Hardware+TERENA SSL CA)

Configurações manuais

Android

- EAP method: TTLS
- Phase 2 authentication: MSCHAPv2
- Identity: login_de_utilizador@dominio (user@iscte.pt)
- Anonymous: Nesta configuração de freeradius não é necessária (por exemplo, na configuração IAS anterior, tinha de ser preenchido em Android e Linux com anonymous@iscte.pt ou user@iscte.pt). Se estiver em branco, é assumido por defeito o login em Identity.
- Password: palavra-chave do utilizador

O anonymous é processado/usado no outer tunnel e é visto em roaming. O identity é usado/processado no inner_tunnel e é processado pelo instituto de origem.

Conclusão

Em termos de know-how foi extremamente interessante levar a bom termo este projecto, e bastante gratificante acabar por ver este documento tomar forma. Gostaria de agradecer a todas as pessoas, colegas e em particular aos elementos da FCCN e ao Pedro Simões que tornaram possível a existência deste documento. Agradece-se também ao leitor para enviar sugestões/correcções para rui.ribeiro@iscte.pt ou ruyrybeyro@gmail.com

Evoluções futuras

Estas configurações tem várias possibilidades de evolução:

- Gráficos gerados a partir de queries SQL de largura de banda, e uso de IPs/utilizadores (trabalho em curso);
- Servir gz descomprimidos on-the-fly à FCCN na recolha de estatísticas mensais para poupar espaço em disco;
- Configurar comunicação RADSEC com os proxies nacionais;
- Criar um script para recolha de estatísticas a partir da tabela MySQL radacct ao invés dos logs detalhados em /var/log/radacct;
- Configurar o CUI (Chargeable User Identity) ao nível da federação.
- Configurar remote logging para syslog central (suportado nativamente na v3);
- Configuração em redundância/cluster de alta disponibilidade;
- Gestão de BD SQL em relação ao desempenho/ocupação. Considerar a possibilidade da BD operacional ter os últimos dois meses, e todo o resto do histórico estar numa BD à parte;
- Seguir autenticações simultâneas de uma forma mais fiável com o modulo redis.

Anexos

Migração de FreeRadius 2.2.x para 3.x

Esta secção pretende de uma forma ligeira a migração/adaptação de ficheiros que efectuamos de v2.2 para 3.x. No nosso caso, de 2.2.5 para 3.0.3.

O documento oficial de migração está em https://github.com/FreeRADIUS/freeradius-server/blob/v3.0.x/raddb/README.rst

Depois de fazer um backup do directório /etc/freeradius, apagamos os pacotes de freeradius.

dpkg --purge freeradius freeradius-common freeradius-ldap freeradius-mysql freeradius-utils libfreeradius2

Depois da primeira tentativa de instalação dos novos pacotes, criados com as instruções deste documento, tivemos este erro:

dpkg: unrecoverable fatal error, aborting:
syntax error: unknown user 'freerad' in statoverride file

Pelo que tivemos de apagar no ficheiro /var/lib/dpkg/statoverride todas as linhas com o utilizador/string freerad

Em seguida, instalamos os novos pacotes com a seguinte linha de um repositório local: (para ver como fazer com debs, consultar o capitulo de instalação)

dpkg -i freeradius freeradius-common freeradius-ldap freeradius-mysql freeradius-utils libfreeradius3

Em seguida, restauramos os certs do backup no directório certs

Os ficheiros clientes.conf e proxy.conf, /etc/freeradius/sites-available/control-socket, etc/freeradius/sites-available/status, são idênticos à v2.2 e foram copiados.

Os ficheiros modules/f_ticks e modules/mschap foram movidos respectivamente para mods-enabled/f_ticks e mods-enabled/mschap

No dictionary.conf cortamos a linha do INCLUDE. (depois da versão que migramos este ficheiro já serviu diversas correcções)

nos hints cortamos o INCLUDE. (correntemente já não usamos o ficheiro de hints)

movemos também o ficheiro users para /etc/freeradius/mods-config/files. No entanto hoje em dia, já não usamos o ficheiro users, e fazemos todas estas operações em unlang.
Movemos também o ficheiro preproxy_users para mods-config/files/pre-proxy
e o attrs.pre-proxy para mods-config/attr_filter/pre-proxy
e o attrs para mods-config/attr_filter/post-proxy

Na altura, tivemos um sucesso moderado a mover o eap.conf para mods_available/eap, no entanto, dado as mudanças significativas deste ficheiro ao longo da evolução do FreeRadius, aconselha-se mudar as configurações manualmente de acordo com este documento.

Apagamos os links de /etc/freeradius/mods-enabled
chap
dhcp
digest
echo
exec
expiration
dynamic_clients
logintime
pap
passwd
radutmp
replicate
soh
sradutmp
unix

o sites-available/default necessita dos wrapers/listeners para escutar as portas, pelo que tivemos de as acrescentar na nossa configuração.

no radiusd.conf tivemos de acrescentar a directiva seguinte. No entanto, esta depende de como o freeradius é compilado e pode não ser realmente necessária.
allow_vulnerable_openssl = yes

No ficheiro clientes.conf tivemos de mudar nastype para nas_type
sed -i "s/nastype/nas_type/g" clients.conf
sed -i "s/CA_path/ca_path/g" /etc/freeradius/mods-enabled/eap
sed -i "s/CA_file/ca_file/g" /etc/freeradius/mods-enabled/eap

Tivemos também de mudar as permissões em /etc/freeradius/mods-config/files

radius1:/etc/freeradius/mods-config/files# chmod 444 *
radius1:/etc/freeradius/mods-config/files# chown root.root *
radius1:/etc/freeradius/mods-config/files

Em /etc/group, tivemos de acrescentar o utilizador freerad ao grupo winbindd_priv

winbindd_priv:x:107:freerad

O ficheiro /etc/freeradius/mods-enabled/ldap tem de ser editado devido a ser substancialmente diferente da v2 (de acordo com este documento e a configuração local)

e em seguida ln -s /etc/freeradius/mods-available/ldap /etc/freeradius/mods-enabled/ldap

vi /etc/freeradius/policy.d/local_blacklist

```
local_blacklist {
        # Reject Calling-Station-Id-less authentications
        if (!(Calling-Station-Id)) {
          update reply {
            Reply-Message := "No Calling-Station-Id"
          }
          reject
        }
```

```
        if (!(User-Name)) {
          update reply {
            Reply-Message := "No User-Name"
          }
          reject
        }
        filter_username
        if (Calling-Station-Id =~ /([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})/i){
          update request {
            Calling-Station-Id := "%{toupper:%{1}:%{2}:%{3}:%{4}:%{5}:%{6}}"
          }
        }
        else {
          noop
        }
#         if ( "%{sql: SELECT count(*) FROM banned_list WHERE mac_address = '%{Calling-Station-Id}' or username = LOWER('%{User-Name}') }" != 0
) {
#           update reply {
#             Reply-Message = "quarantined, contact ISCTE"
#           }
#         reject
#         }
}
```

Para migrar a BD para FreeRadius 3, fazer:

alter table radacct add acctinterval int(12) default NULL;

alterar

/etc/freeradius/mods-available/sql

```
sql {
driver = "rlm_sql_mysql
server = "localhost"
login = "radius"
password = "radpass"

radius_db = "radius"
```

no radiusd.conf

já não é preciso $INCLUDE sql.conf

É no entanto necessário fazer: /etc/freeradius/mods-enabled# ln -s ../mods-available/sql

Saliente-se que também nos ficheiros de log de detail deixou de ser " para ser ' na versão 3, o que poderá colocar problemas em scripts de análises de logs.

Logs em syslog

Para enviar os logs para syslog em vez do ficheiro por defeito /var/log/freeradius/radius.log, mudar em /etc/freeradius/radius.conf em v3.x:

/etc/freeradius/radiusd.conf

log_destination = syslog

.....

log {

destination = **syslog**

#**f**ile = ${logdir}/radius.log

Log authentication requests to the log file.

auth = **yes**

}

E em seguida, fazer restart ao freeradius.

No nosso caso, nós enviamos isto para o daemon syslog de forma a enviar estas mensagens para o nosso servidor central de logs/syslog.

A plataforma Apple

Os ficheiros de profiles para esta plataforma são ficheiros de texto em formato XML.

iOS

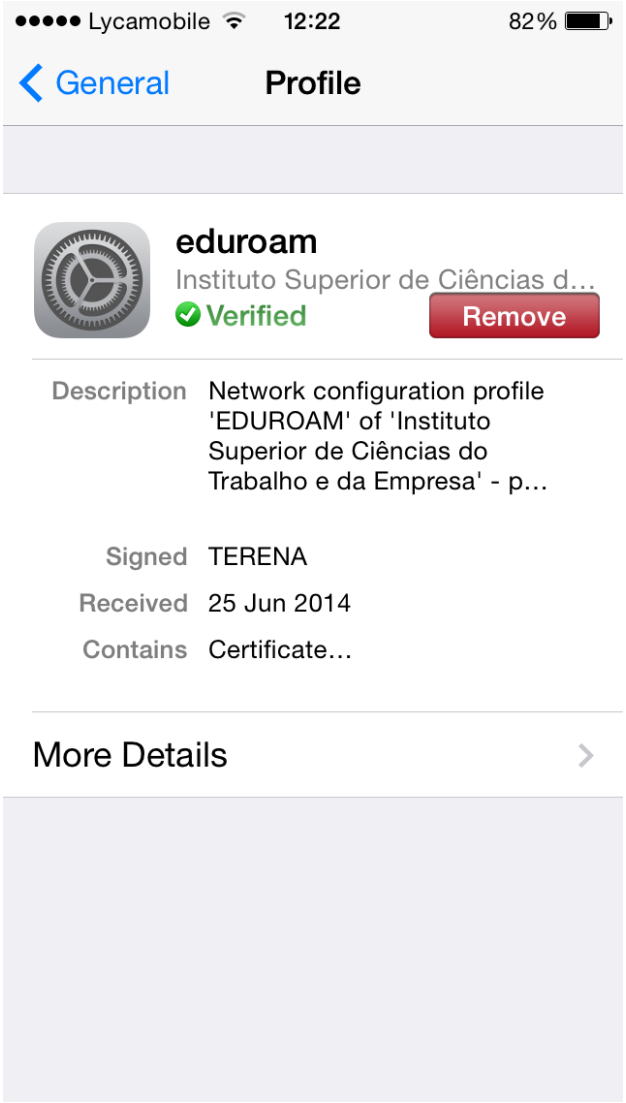
iOS with wireless problems >= 8.0 <= 8.1

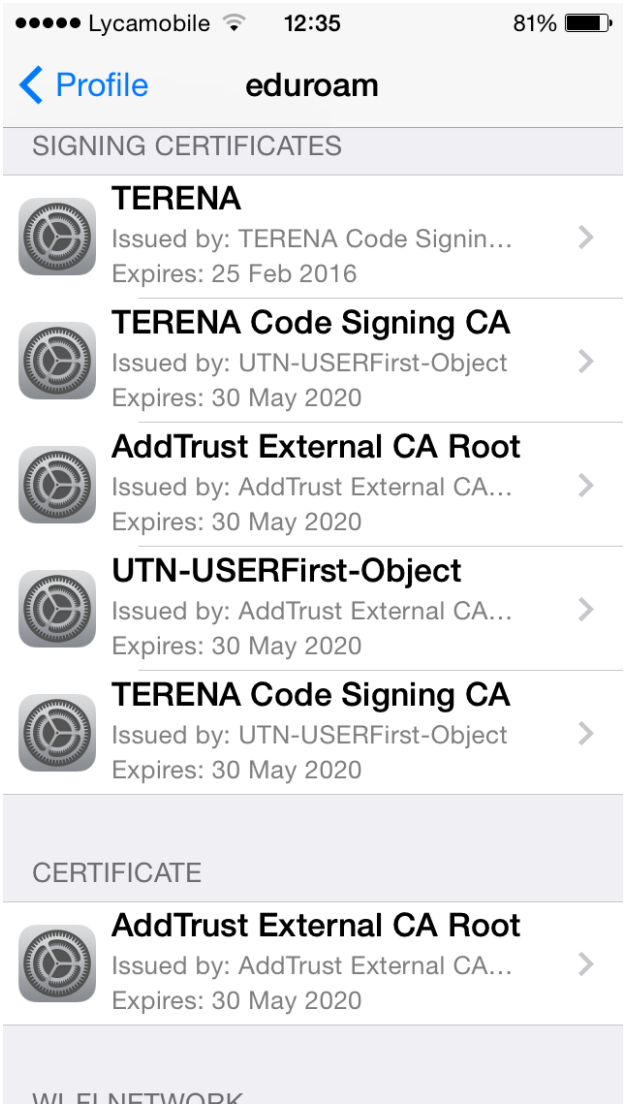
Versão 8 de iOS dá erros de autenticação, para erros que são de conectividade/rede.

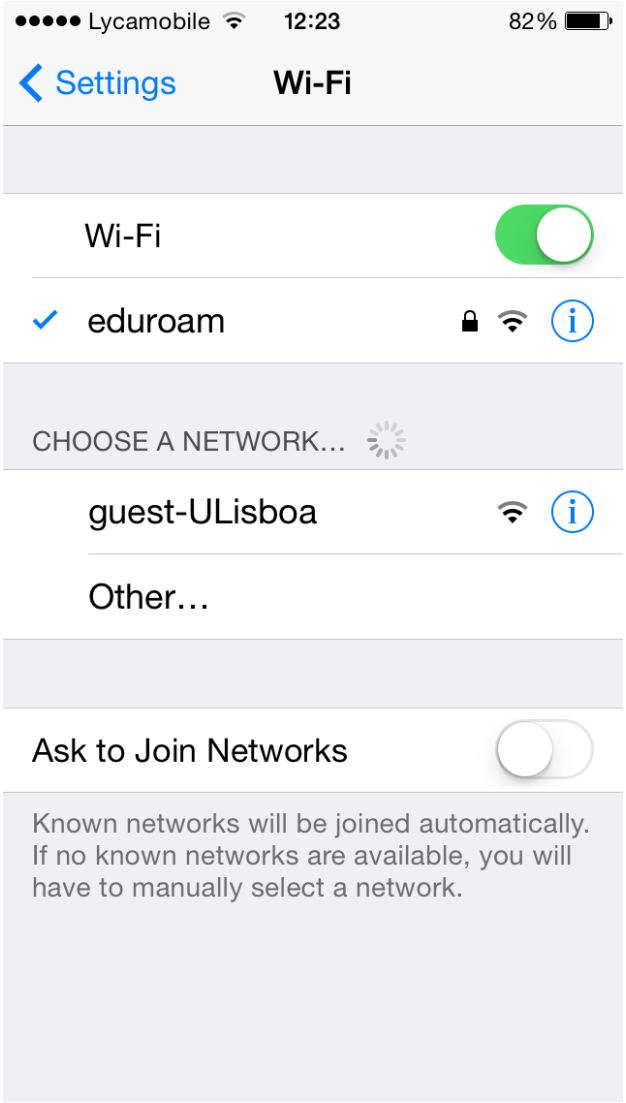
A partir da versão 7 de iOS o SO verifica acesso a www.apple.com, www.appleiphonecell.com e captive.apple.com. Se não tiver acesso a estes sites, o wifi não sobe. http://www.cadinc.com/why-your-apple-ios-7-device-wont-connect-to-the-wifi-network http://blog.erratasec.com/2010/09/apples-secret-wispr-request.html http://stackoverflow.com/questions/19055502/facebook-com-and-the-ios7-captive-portal-detection, http://stackoverflow.com/questions/18891706/ios7-and-captive-portals-changes-to-apple-request-url , e http://forum.mikrotik.com/viewtopic.php?f=2&t=77456 . Na pratica isto significa que não se consegue usar iPhones em redes wifi sem acesso à Internet.

Nota: necessidade de usar Safari para instalação de profile

Optimização de apagar o profile da FON/ZON/Nós


●●●●● Lycamobile
12:22
82%
General
Profile
eduroam
Instituto Superior de Ciências d…
Verified
Remove
Description
Network configuration profile 'EDUROAM' of 'Instituto Superior de Ciências do Trabalho e da Empresa' - p…
Signed
TERENA
Received
25 Jun 2014
Contains
Certificate…
More Details

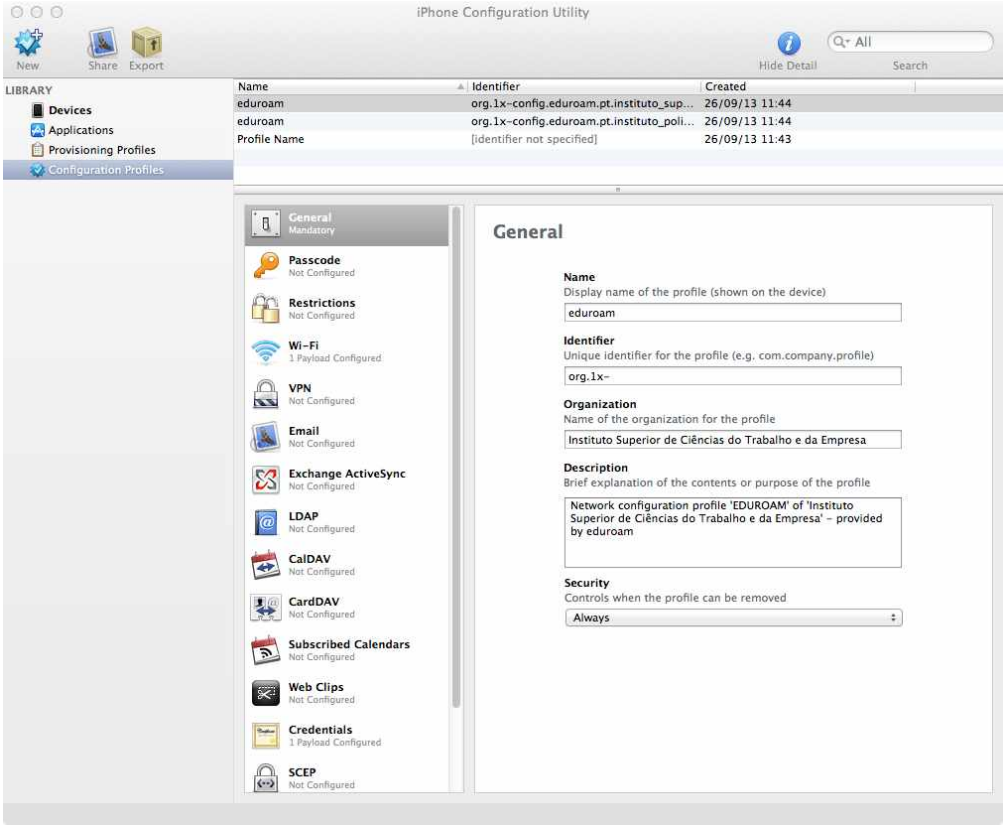

Lycamobile
12:35
81%
Profile
eduroam
SIGNING CERTIFICATES
TERENA
Issued by: TERENA Code Signin…
Expires: 25 Feb 2016
TERENA Code Signing CA
Issued by: UTN-USERFirst-Object
Expires: 30 May 2020
AddTrust External CA Root
Issued by: AddTrust External CA…
Expires: 30 May 2020
UTN-USERFirst-Object
Issued by: AddTrust External CA…
Expires: 30 May 2020
TERENA Code Signing CA
Issued by: UTN-USERFirst-Object
Expires: 30 May 2020
CERTIFICATE
AddTrust External CA Root
Issued by: AddTrust External CA…
Expires: 30 May 2020



Iphone Configuration Utility

No mundo Apple, existe um utilitário extremamente interessante para visualizar/criar profiles de utilização. O iPhone Configuration Utility permite gerir perfis de OS/X e iOS, desde iPads, iPhones, até iMacs e MacBooks Pro.

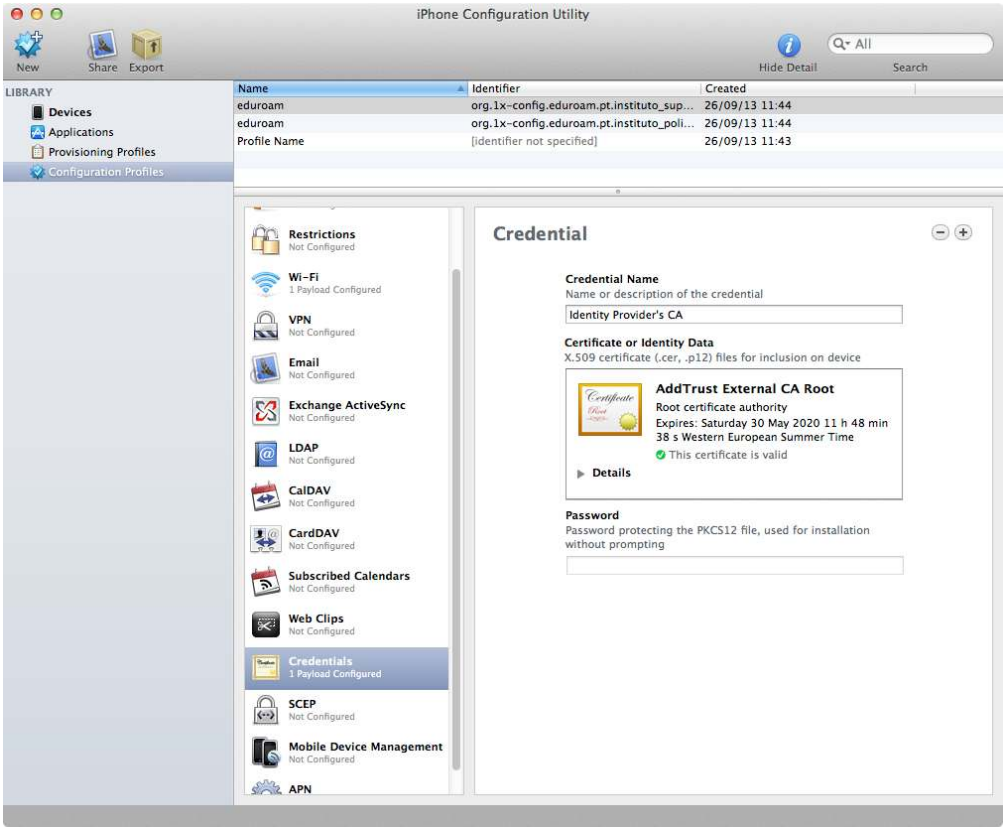
Usando este utilitário, pode se editar o profile eduroam. Desde que este não esteja assinado, pode se fazer mudanças, ou destruir e criar um com um perfil similar.



Visualizando as propriedades de Wifi:



E o certificado que usamos:



O IPhone configurator foi descontinuado oficialmente a partir do Mavericks, e já não se encontra na Apple Store. Também não conhece os certificados da Apple dos equipamentos mais recentes; ia reconhecendo algumas das opções em iOS 7, e já não tem qualquer utilidade em iOS 8. O binário ainda trabalha, e encontra-se para download em http://support.apple.com/kb/DL1465 para OS/X e http://support.apple.com/kb/DL1466 para Windows. No seu lugar é aconselhado o uso do Organizer do XCode e do Apple Configurator, que é usado para fazer provisioning de devices. O Apple Configurator já está disponível na appstore portuguesa, mas no entanto, os servidores da Apple/MDM que permitem definir uma configuração global não estão acessíveis a partir de Portugal. Ver iPhone in Business https://www.apple.com/iphone/business/it/management.html e Apple Deployment Programs https://deploy.apple.com/qforms/open/register/index/avs. O Apple configurator 2, disponível a partir do El Capitan 10.11, permite ver a informação de logs.

Apple Configurator 2

Disponível a partir do El Capital 10.11, permite fazer provisioning empresarial do dispositivos iOS localmente no Mac ou no serviço MDM, e ver logs de debugging sem usar XCode. Permite também carregar profiles directamente de ficheiros XML locais.

Activação de modo developer em iOS

Em iPhones ou iPads pode se efectuar um troubleshooting mais aprofundado, activando as capacidades de developer do mesmo. Isso permite consultar os logs de actividade do sistema em geral.

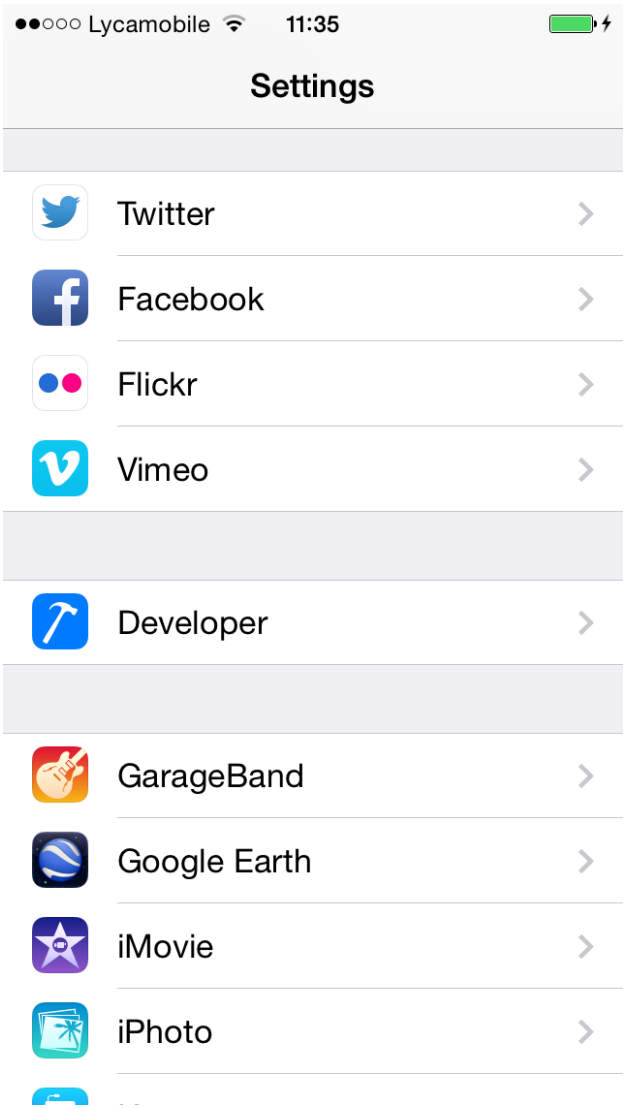
Para tal, é necessário ter uma Apple ID com estatuto de Developer (não tem custos) e instalar o XCode em OS/X.

Nota, o iPhone configurator dá para ver logs sem conta de developer. No entanto, foi descontinuado e não existem garantias durante quanto tempo funcionará.

Depois de o instalar conecta-se o equipamento por um cabo ao Mac, invoca-se o XCode, e escolha-se a opção Window->Organizer.

Depois de escolher Window organizer, no menú seguinte, onde aparece o nome do equipamento, escolher "Use for development". Embora dê mais opções, e erros se não tiver a versão paga da Apple ID Developer, vai activar o modo de developper na mesma.

Para verificar que foi activado, no telefone, seleccionar setting e verificar que apareceu uma nova opção "Developer".



Em seguida, no organizar, carregando no nome do equipamento, desdobra várias opções. Seleccionando a opção Console com o cabo ligado dá para ver os logs. Para limpar os logs existentes, fazer "Clear".

Logs de iPhone com iOS 7 a entrar na eduroam

Mar 25 12:18:40 Rui-Ribeiros-iPhone Preferences[793] <Warning>: -[WiFiManager setEnabled:]:(2014-03-25 12:18:40 +0000) Requested wifi power change to ON
Mar 25 12:18:40 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016182.618000 wlan.N[4341] AppleBCMWLANCore::setPOWER(): [wifid]: Setting power state to 1. stateFlags(20001)
Mar 25 12:18:40 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016182.618013 wlan.N[4342] AppleBCMWLANCore::powerOn(): stateFlags(21001)
Mar 25 12:18:40 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016182.643203 wlan.C[4343] AppleBCMWLANPacketTransmitter::enablePropTxStatus(): Proptx state 1
Mar 25 12:18:40 Rui-Ribeiros-iPhone wifid[40] <Error>: _dispatchDriverAvailable: available 1, reason -528345085, subreason 0
Mar 25 12:18:40 Rui-Ribeiros-iPhone Preferences[793] <Warning>: -[WiFiManager(Private) _powerChanged]:(2014-03-25 12:18:40 +0000) power changed callback, power is now: ON
Mar 25 12:18:40 Rui-Ribeiros-iPhone configd[42] <Notice>: network changed: Proxy

Mar 25 12:18:40 Rui-Ribeiros-iPhone profiled[795] <Notice>: (Note) profiled: Service stopping.
Mar 25 12:18:41 Rui-Ribeiros-iPhone Preferences[793] <Warning>: -[VPNConnectionStore reloadVPN]: The active VPN configuration has changed from (null) to (null)
Mar 25 12:18:41 Rui-Ribeiros-iPhone Preferences[793] <Warning>: -[VPNBundleController _vpnConfigurationChanged:] (0x17808b130: <VPNBundleController: 0x17808b130>): _serviceCount(0), serviceCount(0), toggleInRootMenu(0), RootMenuItem(1)
Mar 25 12:18:41 Rui-Ribeiros-iPhone eapolclient[798] <Notice>: en0 START uid 501 gid 501
Mar 25 12:18:41 Rui-Ribeiros-iPhone Preferences[793] <Warning>: -[WiFiManager(Private) _linkChangedWithDict:]: linkdown(0), associating(0)
Mar 25 12:18:41 Rui-Ribeiros-iPhone Preferences[793] <Warning>: -[APNetworksController isVisible]: _visible(1), _formSheetVisibile(0)
Mar 25 12:18:41 Rui-Ribeiros-iPhone Preferences[793] <Warning>: -[APNetworksController updateCurrentNetworkUI]: currentTrackedNetworkSSID ((null)), currentNetworkSSID(eduroam)
Mar 25 12:18:41 Rui-Ribeiros-iPhone Preferences[793] <Warning>: -[APNetworksController updateCurrentNetworkUI]: Moving "new" current (eduroam) to the top, specifier(eduroam ID:eduroam 0x170168700 target:<APNetworksController 0x15f81b800: navItem <UINavigationItem: 0x1701d6bc0>, view <UITableView: 0x15f81f000; frame = (0 0; 320 568); clipsToBounds = YES; autoresize = W+H; gestureRecognizers = <NSArray: 0x1700597a0>; layer = <CALayer: 0x170221b40>; contentOffset: {0, -64}>>)
Mar 25 12:18:41 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016184.285199 wlan.N[4344] AppleBCMWLANCore::setASSOCIATE(): [wifid]: lowerAuth = AUTHTYPE_OPEN, upperAuth = AUTHTYPE_WPA2_8021X, key = CIPHER_NONE , don't disassociate , 802.1X .
Mar 25 12:18:41 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016184.300756 wlan.N[4345] AppleBCMWLANCore::resetAutoCountry(): EnhancedLocaleEnabled: 1, HostCountry:0, fDefaultCountryCode:XZ, fCurrentHostCountryCode:
Mar 25 12:18:41 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016184.311914 wlan.N[4346] AppleBCMWLANJoinManager::join Beacon Info: @0xfffffff8001b4f000 BSSID=00:0c:e6:6a:34:9a rssi=-70 noise=-90 snr= 17 cca= 1 rate=54 (100%) channel=36 encryption=0x8 ap=1 failures= 0 age=0 ssid[7]='eduroam'
Mar 25 12:18:41 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016184.313775 wlan.N[4347] AppleBCMWLANJoinManager::join Beacon Info: @0xfffffff8001414000 BSSID=00:0c:e6:6a:6e:bf rssi=-72 noise=-95 snr= 15 rate=54 (100%) channel= 1 encryption=0x8 ap=1 failures= 0 age=1 ssid[7]='eduroam'
Mar 25 12:18:41 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016184.335055 wlan.A[4348] Active Ports:
Mar 25 12:18:41 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016184.335080 wlan.A[4349] AppleBCMWLANCore::deleteAllPktFilters(): Deleted IPv4/IPv6 and Magic packet filters
Mar 25 12:18:41 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016184.335095 wlan.A[4350] AppleBCMWLANNetManager::prepareToBringUpLink(): Delaying powersave entry in order to get an IP address
Mar 25 12:18:41 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016184.335109 wlan.N[4351] [bringUpLink] AppleBCMWLAN Joined BSS: @0xfffffff8001b4f000 BSSID=00:0c:e6:6a:34:9a rssi=-70 noise=-89 snr= 17 cca= 2 rate=54 (100%) channel=36 encryption=0x8 ap=1 failures= 0 age=0 ssid[7]='eduroam'
Mar 25 12:18:41 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016184.335129 wlan.A[4352] AppleBCMWLANNetManager::updateLinkQualityMetrics(): Report LQM to User Land 50, fAverageRSSI -85
Mar 25 12:18:41 Rui-Ribeiros-iPhone kernel[0] <Debug>: AirPort: Link Up on en0
Mar 25 12:18:41 Rui-Ribeiros-iPhone kernel[0] <Debug>: en0::startOutputQueues (0)
Mar 25 12:18:41 Rui-Ribeiros-iPhone kernel[0] <Debug>: en0: BSSID changed to 00:0c:e6:6a:34:9a
Mar 25 12:18:41 Rui-Ribeiros-iPhone kernel[0] <Debug>: en0::IO80211Interface::postMessage bssid changed
Mar 25 12:18:41 Rui-Ribeiros-iPhone kernel[0] <Debug>: en0: BSSID changed to 00:0c:e6:6a:34:9a
Mar 25 12:18:41 Rui-Ribeiros-iPhone kernel[0] <Debug>: en0::IO80211Interface::postMessage bssid changed
Mar 25 12:18:42 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016184.384722 wlan.A[4353] AppleBCMWLANCore::setProperties(): Active during sleep supported (true)
Mar 25 12:18:42 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016184.428784 wlan.N[4354] AppleBCMWLANCore::startRoamScan(): 3581 Delaying RoamScan; because Join Mgr Busy 0 isWaitingforIP 1
Mar 25 12:18:42 Rui-Ribeiros-iPhone eapolclient[798] <Notice>: en0 EAP-TTLS: successfully authenticated
Mar 25 12:18:42 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016184.882218 wlan.N[4355] AppleBCMWLANCore::setCIPHER_KEY(): [eapolclient]: type = CIPHER_MSK, index = 0, flags = 0x0, key length = 0, key rsc length = 0
Mar 25 12:18:42 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016184.969541 wlan.N[4356] AppleBCMWLANCore::setCIPHER_KEY(): [eapolclient]: type = CIPHER_MSK, index = 0, flags = 0x0, key length = 64, key rsc length = 0
Mar 25 12:18:42 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016185.122369 wlan.N[4357] AppleBCMWLANJoinManager::handleSupplicantEvent(): status = 6 WLC_SUP_KEYED, reason = 0 Other reason, flags = 0x0, authtype = 0, addr = ec:76:5f:41:c0:fa
Mar 25 12:18:42 Rui-Ribeiros-iPhone configd[42] <Notice>: network changed: DNS* Proxy
Mar 25 12:18:42 Rui-Ribeiros-iPhone configd[42] <Notice>: Captive: [CNInfoNetworkActive:1698] en0: SSID 'eduroam' making interface primary (cache indicates network not captive)
Mar 25 12:18:42 Rui-Ribeiros-iPhone configd[42] <Notice>: Captive: CNPluginHandler en0: Evaluating
Mar 25 12:18:42 Rui-Ribeiros-iPhone Preferences[793] <Warning>: -[APNetworksController isVisible]: _visible(1), _formSheetVisibile(0)
Mar 25 12:18:42 Rui-Ribeiros-iPhone configd[42] <Notice>: Captive: en0: Not probing 'eduroam' (cache indicates not captive)
Mar 25 12:18:42 Rui-Ribeiros-iPhone configd[42] <Notice>: network changed: v4(en0!:172.17.18.245) DNS+ Proxy+
Mar 25 12:18:42 Rui-Ribeiros-iPhone configd[42] <Notice>: Captive: CNPluginHandler en0: Authenticated
Mar 25 12:18:42 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016185.172764 wlan.N[4358] AppleBCMWLANCore::handleIPv4AddressNotificationGated(): Local IPv4 address 172.17.18.245
Mar 25 12:18:42 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016185.174152 wlan.A[4359] AppleBCMWLANNetManager::receivedIPv4Address(): Received address 172.17.18.245, entering powersave mode 2
Mar 25 12:18:42 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016185.174161 wlan.N[4360] AppleBCMWLANCore::startRoamScan(): 3590 SKPPING RoamScan; MultiAPEnv:1 isdualBand:1 isOn5G:1
Mar 25 12:19:15 Rui-Ribeiros-iPhone mstreamd[796] <Notice>: (Note) mstreamd: Not monitoring for external power.
Mar 25 12:19:15 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016194.380294 wlan.A[4361] AppleBCMWLANNetManager::checkRealTimeTraffic(): now 16194.380280208 num entries 4
Mar 25 12:19:15 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016194.380322 wlan.A[4362] AppleBCMWLANCore::dumpWmeCounters(): per TIDs tx counters: 44501 23155 0 0 0 0 9972 0, per TIDs rx counters: 85124 0 0 0 0 0 0 0
Mar 25 12:19:15 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016194.380340 wlan.A[4363] AppleBCMWLANCore::dumpWmeCounters(): AWDL: Tx 5 0 0 0 0 0 0 0, Rx: 0 0 0 0 0 0 0 0
Mar 25 12:19:15 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016209.437419 wlan.A[4364] AppleBCMWLANNetManager::updateLinkQualityMetrics(): Report LQM to User Land 100, fAverageRSSI -70
Mar 25 12:19:15 Rui-Ribeiros-iPhone kernel[0] <Debug>: 016214.443931 wlan.A[4365] AppleBCMWLANNetManager::updateLinkQualityMetrics(): Report LQM to User Land 50, fAverageRSSI -71

Logs de certificado de cliente errado

Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>:
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.050740]: EAP: Inner Association of eduroam succeeded (0)
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.051758]: EAP: eapState=2
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.051915]: EAP: Status=0 SupplicationStatus=Inactive
Jul 2 15:57:30 Rui-Ribeiros-iPhone kernel[0] <Debug>: 002934.419132 wlan.N[318] AppleBCMWLANCore::startRoamScan(): 3581 Delaying RoamScan; because Join Mgr Busy 0 isWaitingforIP 1
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.513436]: EAP: eapState=2
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.513639]: EAP: Status=0 SupplicationStatus=Connecting
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.553111]: EAP: eapState=2
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.553275]: EAP: Status=0 SupplicationStatus=Acquired
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.562640]: EAP: eapState=2
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.563015]: EAP: Status=0 SupplicationStatus=Authenticating
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.563983]: EAP: eapState=2
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.564125]: EAP: Status=0 SupplicationStatus=Authenticating
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.565530]: EAP: eapState=2
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.565685]: EAP: Status=0 SupplicationStatus=Authenticating
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.593739]: EAP: eapState=2
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.593901]: EAP: Status=0 SupplicationStatus=Authenticating
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.605046]: EAP: eapState=2
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.605205]: EAP: Status=0 SupplicationStatus=Authenticating
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.633857]: EAP: eapState=2
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.634018]: EAP: Status=0 SupplicationStatus=Authenticating
Jul 2 15:57:30 Rui-Ribeiros-iPhone eapolclient[252] <Notice>: [eapttls_plugin.c:968] eapttls_verify_server(): server certificate not trusted status 1001 -9807
Jul 2 15:57:30 Rui-Ribeiros-iPhone eapolclient[252] <Notice>: en0 EAP-TTLS: authentication failed with status 1001
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.656340]: EAP: eapState=2
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.656501]: EAP: Status=1001 SupplicationStatus=Held
Jul 2 15:57:30 Rui-Ribeiros-iPhone wifid[40] <Notice>: WiFi:[426005850.728303]: WiFiDeviceEAPCancel: EAPOLControlStop

OS/X

Gestão de perfis/profiles

Pode-se gerir profiles a partir da linha de comando, ou de scripts. Para gerir os perfis a partir do Terminar pode-se usar o comando profiles.

Para instalar um ficheiro de configuração profile no utilizador corrente:

```
$profiles -I -F /testfile.mobileconfig
```

Para remover um profile:

```
$profiles -R -F /profiles/testfile2.mobileconfig
```

Para mostrar os profiles instalados:

```
$profiles -L
ruiribeiro[1] attribute: profileIdentifier: org.1x-config.eduroam.pt.iscte_-_instituto_universitrio_de_lisboa.
eduroam.en_GB
There are 1 user configuration profiles installed for 'ruiribeiro'
$ profiles -Lv
profiles: verbose mode ON
profiles: using user name = ruiribeiro
ruiribeiro[1] attribute: name: eduroam
ruiribeiro[1] attribute: configurationDescription: Network configuration profile 'EDUROAM' of 'ISCTE -
Instituto Universitário de Lisboa' - provided by eduroam
ruiribeiro[1] attribute: installationDate: 2015-01-21 19:59:51 +0000
ruiribeiro[1] attribute: organization: ISCTE - Instituto Universitário de Lisboa
ruiribeiro[1] attribute: profileIdentifier: org.1x-config.eduroam.pt.iscte_-_instituto_universitrio_de_lisboa.
eduroam.en_GB
ruiribeiro[1] attribute: profileUUID: bb42c3a2-0b23-7617-3029-baf645117695
ruiribeiro[1] attribute: profileType: Configuration
ruiribeiro[1] attribute: removalDisallowed: FALSE
ruiribeiro[1] attribute: version: 1
ruiribeiro[1] attribute: containsComputerItems: FALSE
ruiribeiro[1] attribute: internaldata: TRUE
ruiribeiro[1] payload count = 4
ruiribeiro[1]            payload[1] name                        = SSID eduroam
ruiribeiro[1]            payload[1] description                 = eduroam configuration for network name eduroam
ruiribeiro[1]            payload[1] type                        = com.apple.wifi.managed
ruiribeiro[1]            payload[1] organization                = eduroam.1x-config.org
ruiribeiro[1]            payload[1] identifier                  = org.1x-config.eduroam.pt.iscte_-
_instituto_universitrio_de_lisboa.eduroam.en_GB.wifi.0
ruiribeiro[1]            payload[1] uuid                        = adcdb520-839d-e24d-e790-cfd125f6f272
ruiribeiro[1]            payload[2] name                        = Identity Provider's CA
ruiribeiro[1]            payload[2] description                 = Your Identity Providers Certification Authority
ruiribeiro[1]            payload[2] type                        = com.apple.security.root
ruiribeiro[1]            payload[2] organization                = eduroam.1x-config.org
ruiribeiro[1]            payload[2] identifier                  = org.1x-config.eduroam.pt.iscte_-
_instituto_universitrio_de_lisboa.eduroam.credential.2
ruiribeiro[1]            payload[2] uuid                        = f0192be5-3eb2-24ee-fb02-1b3b119fcd18
ruiribeiro[1]            payload[3] name                        = Identity Provider's CA
ruiribeiro[1]            payload[3] description                 = Your Identity Providers Certification Authority
ruiribeiro[1]            payload[3] type                        = com.apple.security.root
ruiribeiro[1]            payload[3] organization                = eduroam.1x-config.org
ruiribeiro[1]            payload[3] identifier                  = org.1x-config.eduroam.pt.iscte_-
_instituto_universitrio_de_lisboa.eduroam.credential.0
ruiribeiro[1]            payload[3] uuid                        = cd826d78-442b-2467-fa68-8edbc6a55415
ruiribeiro[1]            payload[4] name                        = Identity Provider's CA
ruiribeiro[1]            payload[4] description                 = Your Identity Providers Certification Authority
ruiribeiro[1]            payload[4] type                        = com.apple.security.root
ruiribeiro[1]            payload[4] organization                = eduroam.1x-config.org
ruiribeiro[1]            payload[4] identifier                  = org.1x-config.eduroam.pt.iscte_-
_instituto_universitrio_de_lisboa.eduroam.credential.1
ruiribeiro[1]            payload[4] uuid                        = 7c0d46b5-a96e-89e7-5966-7b481c0cb180
There are 1 user configuration profiles installed for 'ruiribeiro'
pass
```

Reportar bugs de FreeRadius

O autor detectou já vários bug no FreeRadius e uns dos mais sérios foi introduzido formalmente no sistema de bugtracking do FreeRadius. O bug em questão foi um crash do freeradius, que se conseguiu determinar que era um problema de roaming de accounting correndo o servidor em modo debug com freeradius -X.

```
Listening on command file /var/run/freeradius/freeradius.sock
Listening on auth address 127.0.0.1 port 18120 as server inner-tunnel
Listening on auth address * port 1812 as server default
Listening on acct address * port 1813 as server default
Listening on status address 127.0.0.1 port 18121 as server status
Opening new proxy socket 'proxy address * port 0'
Listening on proxy address * port 59771
Ready to process requests
(0) Received Access-Request Id 193 from 193.136.192.43:48455 to 193.136.188.36:1812 length 213
(0) Dropping packet without response because of error:
Waking up in 0.3 seconds.
```

```
(0) Cleaning up request packet ID 193 with timestamp +0
Ready to process requests
(1) Received Access-Request Id 4 from 95.94.70.135:38746 to 193.136.188.36:1812 length 20
(1) # Executing section authorize from file /etc/freeradius/sites-enabled/default
(1) authorize {
(1) if ( User-name == "radius-teste@iscte.pt" ) {
ERROR: (1) Failed retrieving values required to evaluate condition
(1) else {
(1) auth_log: EXPAND /var/log/freeradius/radacct/%{%{Packet-Src-IP-Address}:-%{Packet-Src-IPv6-Address}}/auth-detail-%Y%m%d
(1) auth_log: --> /var/log/freeradius/radacct/95.94.70.135/auth-detail-20150102
(1) auth_log: /var/log/freeradius/radacct/%{%{Packet-Src-IP-Address}:-%{Packet-Src-IPv6-Address}}/auth-detail-%Y%m%d expands to /var/log
/freeradius/radacct/95.94.70.135/auth-detail-20150102
(1) auth_log: EXPAND %t
(1) auth_log: --> Fri Jan 2 22:27:51 2015
(1) [auth_log] = ok
(1) if (!(User-Name =~ /^([^@]*)@(.+)$/)) {
ERROR: (1) Failed retrieving values required to evaluate condition
(1) else {
(1) update request {
(1) EXPAND %{1}
(1) -->
(1) Stripped-User-Name := ""
(1) EXPAND %{2}
(1) -->
(1) Realm := ""
(1) } # update request = noop
(1) if ( (Realm == "iscte.pt")) {
(1) if ( (Realm == "iscte.pt") ) -> FALSE
(1) else {
(1) update control {
(1) Proxy-To-Realm := 'TO_EDUROAM'
(1) } # update control = noop
(1) } # else = noop
(1) } # else = noop
(1) } # else = ok
(1) eap: No EAP-Message, not doing EAP
(1) [eap] = noop
(1) policy local_blacklist {
(1) if (!(Calling-Station-Id)) {
(1) if (!(Calling-Station-Id)) -> TRUE
(1) if (!(Calling-Station-Id)) {
(1) update reply {
(1) Reply-Message := 'No Calling-Station-Id'
(1) } # update reply = noop
(1) [reject] = reject
(1) } # if (!(Calling-Station-Id)) = reject
(1) } # policy local_blacklist = reject
(1) } # authorize = reject
(1) Using Post-Auth-Type Reject
(1) # Executing group from file /etc/freeradius/sites-enabled/default
(1) Post-Auth-Type REJECT {
(1) f_ticks: EXPAND f_ticks.%{%{reply:Packet-Type}:-format}
(1) f_ticks: --> f_ticks.Access-Reject
(1) f_ticks: EXPAND /var/log/freeradius/awesant/Stats-Awesant-Auth.log
(1) f_ticks: --> /var/log/freeradius/awesant/Stats-Awesant-Auth.log
(1) f_ticks: EXPAND AUTH-ID=%I#TIME=%l#REALM=%{Realm}#CSI=%{Calling-Station-Id}/%{Called-Station-Id}#USER=%{md5:%{User-Name}}
#NASIP=%{NAS-IP-Address}#RESULT=FAIL
(1) f_ticks: --> AUTH-ID=4#TIME=1420237671#REALM=#CSI=/#USER=#NASIP=#RESULT=FAIL
(1) [f_ticks] = ok
(1) sql: EXPAND .query
(1) sql: --> .query
(1) sql: Using query template 'query'
rlm_sql (sql): Reserved connection (4)
(1) sql: EXPAND %{User-Name}
(1) sql: -->
(1) sql: SQL-User-Name set to ''
(1) sql: EXPAND INSERT INTO radpostauth (username, pass, reply, authdate) VALUES ( '%{SQL-User-Name}', '%{%{User-Password}:-%{Chap-
Password}}', '%{reply:Packet-Type}', '%S')
(1) sql: --> INSERT INTO radpostauth (username, pass, reply, authdate) VALUES ( '', '', 'Access-Reject', '2015-01-02 22:27:51')
rlm_sql (sql): Executing query: 'INSERT INTO radpostauth (username, pass, reply, authdate) VALUES ( '', '', 'Access-Reject', '2015-01-02 22:27:51')'
rlm_sql (sql): Released connection (4)
rlm_sql (sql): 0 of 5 connections in use. Need more spares
rlm_sql (sql): Opening additional connection (5)
rlm_sql_mysql: Starting connect to MySQL server
(1) [sql] = ok
(1) attr_filter.access_reject: EXPAND %{User-Name}
(1) attr_filter.access_reject: -->
(1) [attr_filter.access_reject] = noop
(1) } # Post-Auth-Type REJECT = ok
```

(1) Delaying response for 1.000000 seconds
Waking up in 0.3 seconds.
(2) Received Accounting-Request Id 65 from 95.94.70.135:38746 to 193.136.188.36:1813 length 26
(2) Acct-Status-Type = Start
(2) # Executing section preacct from file /etc/freeradius/sites-enabled/default
(2) preacct {
(2) update request {
(2) EXPAND %{expr: %l - %{%{Acct-Session-Time}:-0} - %{%{Acct-Delay-Time}:-0}}
(2) --> 1420237671
(2) FreeRADIUS-Acct-Session-Start-Time = "Jan 2 2015 22:27:51 WET"
(2) } # update request = noop
(2) if (!Event-TimeStamp) {
(2) if (!Event-TimeStamp) -> TRUE
(2) if (!Event-TimeStamp) {
(2) update request {
(2) EXPAND %l
(2) --> 1420237671
(2) Event-Timestamp := "Jan 2 2015 22:27:51 WET"
(2) } # update request = noop
(2) } # if (!Event-TimeStamp) = noop
(2) policy acct_unique {
(2) if ("%{string:Class}" =~ /ai:([0-9a-f]{32})/i) {
(2) EXPAND %{string:Class}
(2) -->
(2) if ("%{string:Class}" =~ /ai:([0-9a-f]{32})/i) -> FALSE
(2) else {
(2) update request {
(2) EXPAND %{md5:%{User-Name},%{Acct-Session-ID},%{%{NAS-IPv6-Address}:-%{NAS-IP-Address}},%{NAS-Identifier},%{NAS-Port-ID},%{NAS-Port}}
(2) --> 8daa390830619c3758c0f67ab6e59c22
(2) &Acct-Unique-Session-Id := "8daa390830619c3758c0f67ab6e59c22"
(2) } # update request = noop
(2) } # else = noop
(2) } # policy acct_unique = noop
(2) [suffix] = noop
(2) } # preacct = noop
(2) # Executing section accounting from file /etc/freeradius/sites-enabled/default
(2) accounting {
(2) detail: EXPAND /var/log/freeradius/radacct/%{%{Packet-Src-IP-Address}:-%{Packet-Src-IPv6-Address}}/detail-%Y%m%d
(2) detail: --> /var/log/freeradius/radacct/95.94.70.135/detail-20150102
(2) detail: /var/log/freeradius/radacct/%{%{Packet-Src-IP-Address}:-%{Packet-Src-IPv6-Address}}/detail-%Y%m%d expands to /var/log/freeradius/radacct/95.94.70.135/detail-20150102
(2) detail: EXPAND %t
(2) detail: --> Fri Jan 2 22:27:51 2015
(2) [detail] = ok
(2) sql: EXPAND %{tolower:type.%{Acct-Status-Type}.query}
(2) sql: --> type.start.query
(2) sql: Using query template 'query'
rlm_sql (sql): Reserved connection (5)
(2) sql: EXPAND %{User-Name}
(2) sql: -->
(2) sql: SQL-User-Name set to ''
(2) sql: EXPAND INSERT INTO radacct (acctsessionid, acctuniqueid, username, realm, nasipaddress, nasportid, nasporttype, acctstarttime, acctupdatetime, acctstoptime, acctsessiontime, acctauthentic, connectinfo_start, connectinfo_stop, acctinputoctets, acctoutputoctets, calledstationid, callingstationid, acctterminatecause, servicetype, framedprotocol, framedipaddress) VALUES ('%{Acct-Session-Id}', '%{Acct-Unique-Session-Id}', '%{SQL-User-Name}', '%{Realm}', '%{NAS-IP-Address}', '%{NAS-Port}', '%{NAS-Port-Type}', FROM_UNIXTIME(%{integer:Event-Timestamp}), FROM_UNIXTIME(%{integer:Event-Timestamp}), NULL, '0', '%{Acct-Authentic}', '%{Connect-Info}', '', '0', '0', '%{Called-Station-Id}', '%{Calling-Station-Id}', '', '%{Service-Type}', '%{Framed-Protocol}', '%{Framed-IP-Address}')
(2) sql: --> INSERT INTO radacct (acctsessionid, acctuniqueid, username, realm, nasipaddress, nasportid, nasporttype, acctstarttime, acctupdatetime, acctstoptime, acctsessiontime, acctauthentic, connectinfo_start, connectinfo_stop, acctinputoctets, acctoutputoctets, calledstationid, callingstationid, acctterminatecause, servicetype, framedprotocol, framedipaddress) VALUES ('', '8daa390830619c3758c0f67ab6e59c22', '', '', '', '', FROM_UNIXTIME (1420237671), FROM_UNIXTIME(1420237671), NULL, '0', '', '', '', '0', '0', '', '', '', '', '')
rlm_sql (sql): Executing query: 'INSERT INTO radacct (acctsessionid, acctuniqueid, username, realm, nasipaddress, nasportid, nasporttype, acctstarttime, acctupdatetime, acctstoptime, acctsessiontime, acctauthentic, connectinfo_start, connectinfo_stop, acctinputoctets, acctoutputoctets, calledstationid, callingstationid, acctterminatecause, servicetype, framedprotocol, framedipaddress) VALUES ('', '8daa390830619c3758c0f67ab6e59c22', '', '', '', '', FROM_UNIXTIME(1420237671), FROM_UNIXTIME(1420237671), NULL, '0', '', '', '', '0', '0', '', '', '', '', '', '')'
rlm_sql (sql): Released connection (5)
(2) [sql] = ok
(2) Accounting-Request: EXPAND Accounting-Request.%{%{Acct-Status-Type}:-unknown}
(2) Accounting-Request: --> Accounting-Request.Start
(2) Accounting-Request: EXPAND /var/log/freeradius/awesant/Stats-Awesant-Acct.log
(2) Accounting-Request: --> /var/log/freeradius/awesant/Stats-Awesant-Acct.log
(2) Accounting-Request: EXPAND ACCT-ID=%{Acct-Session-Id}#TIME=%l#TYPE=Start#CSI=%{Calling-Station-Id}/%{Called-Station-Id}#NASIP=%{NAS-IP-Address}#USER=%{md5:%{User-Name}}#REALM=%{Realm}
(2) Accounting-Request: --> ACCT-ID=#TIME=1420237671#TYPE=Start#CSI=/#NASIP=#USER=#REALM=
(2) [Accounting-Request] = ok
(2) if (noop) {
(2) if (noop) -> FALSE

```
(2) attr_filter.accounting_response: EXPAND %{User-Name}
(2) attr_filter.accounting_response: -->
(2) [attr_filter.accounting_response] = noop
(2) } # accounting = ok
(2) Sent Accounting-Response Id 65 from 193.136.188.36:1813 to 95.94.70.135:38746 length 20
(2) Finished request
Waking up in 0.2 seconds.
(3) Received Accounting-Request Id 67 from 95.94.70.135:38746 to 193.136.188.36:1813 length 26
(3) Acct-Status-Type = Interim-Update
(3) # Executing section preacct from file /etc/freeradius/sites-enabled/default
(3) preacct {
(3) update request {
(3) EXPAND %{expr: %l - %{%{Acct-Session-Time}:-0} - %{%{Acct-Delay-Time}:-0}}
(3) --> 1420237671
(3) FreeRADIUS-Acct-Session-Start-Time = "Jan 2 2015 22:27:51 WET"
(3) } # update request = noop
(3) if (!Event-TimeStamp) {
(3) if (!Event-TimeStamp) -> TRUE
(3) if (!Event-TimeStamp) {
(3) update request {
(3) EXPAND %l
(3) --> 1420237671
(3) Event-Timestamp := "Jan 2 2015 22:27:51 WET"
(3) } # update request = noop
(3) } # if (!Event-TimeStamp) = noop
(3) policy acct_unique {
(3) if ("%{string:Class}" =~ /ai:([0-9a-f]{32})/i) {
(3) EXPAND %{string:Class}
(3) -->
(3) if ("%{string:Class}" =~ /ai:([0-9a-f]{32})/i) -> FALSE
(3) else {
(3) update request {
(3) EXPAND %{md5:%{User-Name},%{Acct-Session-ID},%{%{NAS-IPv6-Address}:-%{NAS-IP-Address}},%{NAS-Identifier},%{NAS-Port-ID},%{NAS-
Port}}
(3) --> 8daa390830619c3758c0f67ab6e59c22
(3) &Acct-Unique-Session-Id := "8daa390830619c3758c0f67ab6e59c22"
(3) } # update request = noop
(3) } # else = noop
(3) } # policy acct_unique = noop
(3) [suffix] = noop
(3) } # preacct = noop
(3) # Executing section accounting from file /etc/freeradius/sites-enabled/default
(3) accounting {
(3) detail: EXPAND /var/log/freeradius/radacct/%{%{Packet-Src-IP-Address}:-%{Packet-Src-IPv6-Address}}/detail-%Y%m%d
(3) detail: --> /var/log/freeradius/radacct/95.94.70.135/detail-20150102
(3) detail: /var/log/freeradius/radacct/%{%{Packet-Src-IP-Address}:-%{Packet-Src-IPv6-Address}}/detail-%Y%m%d expands to /var/log/freeradius
/radacct/95.94.70.135/detail-20150102
(3) detail: EXPAND %t
(3) detail: --> Fri Jan 2 22:27:51 2015
(3) [detail] = ok
(3) sql: EXPAND %{tolower:type.%{Acct-Status-Type}.query}
(3) sql: --> type.interim-update.query
(3) sql: Using query template 'query'
rlm_sql (sql): Reserved connection (5)
(3) sql: EXPAND %{User-Name}
(3) sql: -->
(3) sql: SQL-User-Name set to ''
(3) sql: EXPAND UPDATE radacct SET acctupdatetime = (@acctupdatetime_old:=acctupdatetime), acctupdatetime = FROM_UNIXTIME(%{integer:
Event-Timestamp}), acctinterval = %{integer:Event-Timestamp} - UNIX_TIMESTAMP(@acctupdatetime_old), framedipaddress = '%{Framed-IP-
Address}', acctsessiontime = '%{Acct-Session-Time}', acctinputoctets = '%{%{Acct-Input-Gigawords}:-0}' << 32 | '%{%{Acct-Input-Octets}:-0}',
acctoutputoctets = '%{%{Acct-Output-Gigawords}:-0}' << 32 | '%{%{Acct-Output-Octets}:-0}' WHERE acctsessionid = '%{Acct-Session-Id}' AND
username = '%{SQL-User-Name}' AND nasipaddress = '%{NAS-IP-Address}'
(3) sql: --> UPDATE radacct SET acctupdatetime = (@acctupdatetime_old:=acctupdatetime), acctupdatetime = FROM_UNIXTIME(1420237671),
acctinterval = 1420237671 - UNIX_TIMESTAMP(@acctupdatetime_old), framedipaddress = '', acctsessiontime = '', acctinputoctets = '0' << 32 | '0',
acctoutputoctets = '0' << 32 | '0' WHERE acctsessionid = '' AND username = '' AND nasipaddress = ''
rlm_sql (sql): Executing query: 'UPDATE radacct SET acctupdatetime = (@acctupdatetime_old:=acctupdatetime), acctupdatetime = FROM_UNIXTIME
(1420237671), acctinterval = 1420237671 - UNIX_TIMESTAMP(@acctupdatetime_old), framedipaddress = '', acctsessiontime = '', acctinputoctets = '0'
<< 32 | '0', acctoutputoctets = '0' << 32 | '0' WHERE acctsessionid = '' AND username = '' AND nasipaddress = ''
rlm_sql_mysql: Rows matched: 18 Changed: 18 Warnings: 18
rlm_sql (sql): Released connection (5)
(3) [sql] = ok
(3) Accounting-Request: EXPAND Accounting-Request.%{%{Acct-Status-Type}:-unknown}
(3) Accounting-Request: --> Accounting-Request.Interim-Update
No such configuration item .Accounting-Request.Interim-Update
(3) Accounting-Request: No such entry ''.Accounting-Request.Interim-Update''
(3) [Accounting-Request] = noop
(3) if (noop) {
(3) if (noop) -> TRUE
(3) if (noop) {
```

```
(3) [ok] = ok
(3) } # if (noop) = ok
(3) attr_filter.accounting_response: EXPAND %{User-Name}
(3) attr_filter.accounting_response: -->
(3) [attr_filter.accounting_response] = noop
(3) } # accounting = ok
(3) Sent Accounting-Response Id 67 from 193.136.188.36:1813 to 95.94.70.135:38746 length 20
(3) Finished request
Waking up in 0.2 seconds.
(4) Received Accounting-Request Id 70 from 95.94.70.135:38746 to 193.136.188.36:1813 length 60
(4) User-Name = 'rffro@isla.pt'
(4) Calling-Station-Id = '11:11:11:11:11:11'
(4) Acct-Status-Type = Stop
(4) # Executing section preacct from file /etc/freeradius/sites-enabled/default
(4) preacct {
(4) update request {
(4) EXPAND %{expr: %l - %{%{Acct-Session-Time}:-0} - %{%{Acct-Delay-Time}:-0}}
(4) --> 1420237671
(4) FreeRADIUS-Acct-Session-Start-Time = "Jan 2 2015 22:27:51 WET"
(4) } # update request = noop
(4) if (!Event-TimeStamp) {
(4) if (!Event-TimeStamp) -> TRUE
(4) if (!Event-TimeStamp) {
(4) update request {
(4) EXPAND %l
(4) --> 1420237671
(4) Event-Timestamp := "Jan 2 2015 22:27:51 WET"
(4) } # update request = noop
(4) } # if (!Event-TimeStamp) = noop
(4) policy acct_unique {
(4) if ("%{string:Class}" =~ /ai:([0-9a-f]{32})/i) {
(4) EXPAND %{string:Class}
(4) -->
(4) if ("%{string:Class}" =~ /ai:([0-9a-f]{32})/i) -> FALSE
(4) else {
(4) update request {
(4) EXPAND %{md5:%{User-Name},%{Acct-Session-ID},%{%{NAS-IPv6-Address}:-%{NAS-IP-Address}},%{NAS-Identifier},%{NAS-Port-ID},%{NAS-
Port}}
(4) --> 06dc868691ae159ec1f9a619002b6638
(4) &Acct-Unique-Session-Id := "06dc868691ae159ec1f9a619002b6638"
(4) } # update request = noop
(4) } # else = noop
(4) } # policy acct_unique = noop
(4) suffix: Checking for suffix after "@"
(4) suffix: Looking up realm "isla.pt" for User-Name = "rffro@isla.pt"
Segmentation fault (core dumped)
```

Em consequência abriu-se um bilhete "freeradius 3.0.6 crashing on roaming accounting stop message #868 https://github.com/FreeRADIUS/freeradius-server/issues/868

As instruções oficiais estão em https://github.com/FreeRADIUS/freeradius-server/blob/master/doc/bugs e aqui pretendemos desenvolver, ampliar e clarificar os passos a efectuar.

wget ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-3.0.6.tar.bz2

debian/rules -> mudar disable-developer para enable-developer
e CFLAGS += -O0 -ggd

apt-get install libcurl4-openssl-dev
fakeroot dpkg-buildpackage -b -uc
apt-get install libcap-dev libgdbm-dev libiodbc2-dev libjson-c-dev
fakeroot dpkg-buildpackage -b -uc
apt-get install libkrb5-dev libldap2-dev libpam0g-dev libpcap-dev libperl-dev libmysqlclient-dev libpq-dev libreadline-dev libsasl2-dev libsqlite3-dev libtalloc-dev libyubikey-dev
fakeroot dpkg-buildpackage -b -uc
cd ..

dpkg -i freeradius-config_3.0.6+git_amd64.deb freeradius_3.0.6+git_amd64.deb freeradius-common_3.0.6+git_all.deb freeradius-ldap_3.0.6+git_amd64.deb freeradius-mysql_3.0.6+git_amd64.deb freeradius-utils_3.0.6+git_amd64.deb libfreeradius3_3.0.6+git_amd64.deb

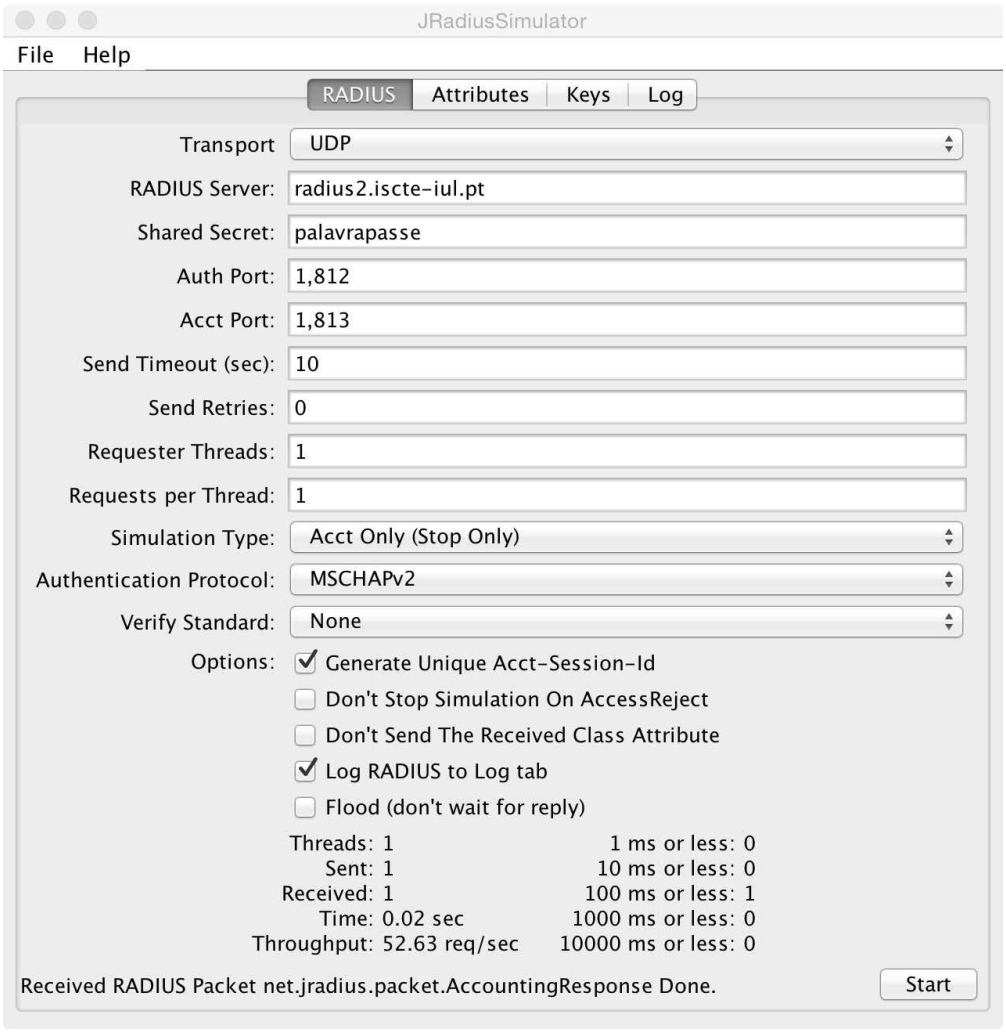
Em /etc/freeradius/radius.conf mudar temporariamente allow_core_dumps para yes.

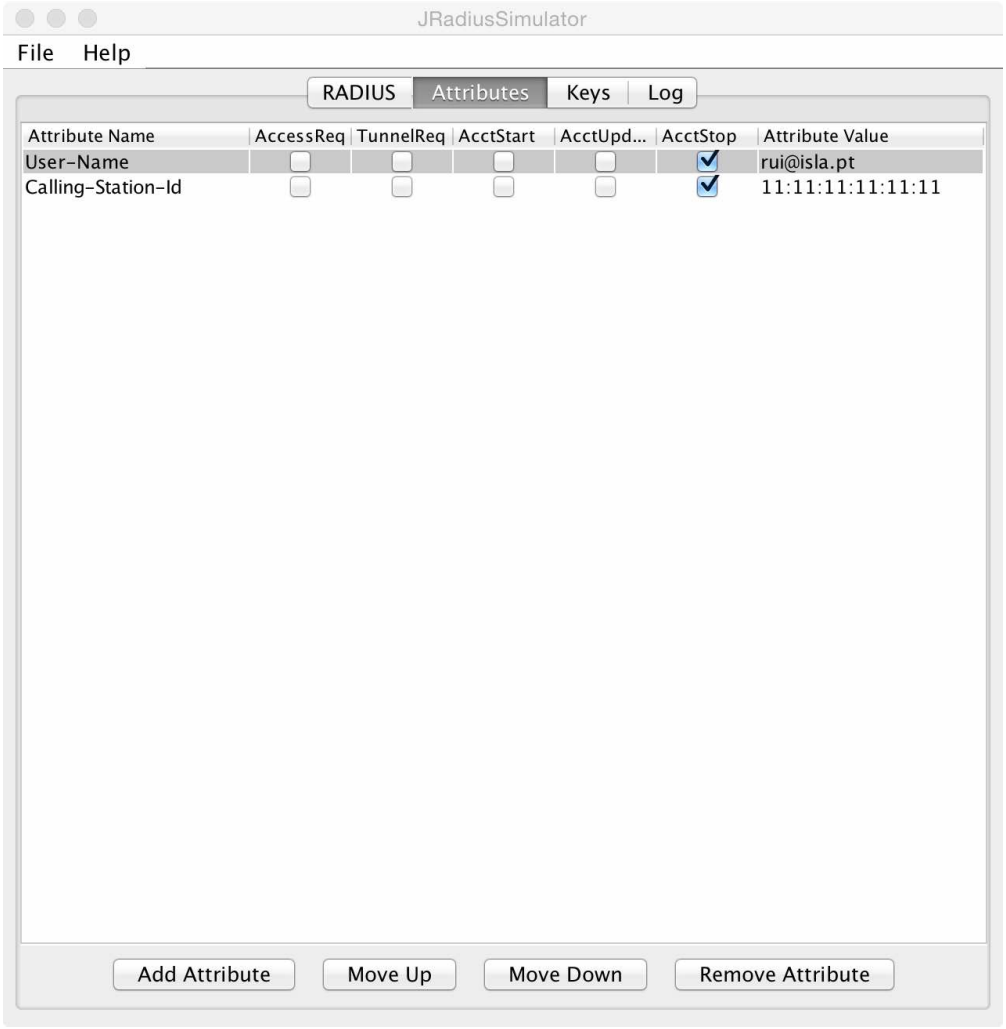
radius.conf

allow_core_dumps = yes

ulimit -c unlimited

Em seguida foi preciso detectar porque crashava o servidor. Como estamos a fazer o setup de um servidor de teste temos de "fabricar" o pedido, e para tal, usamos o JRadius Simulator. Depois de vários testes com mensagens de accounting, conseguimos perceber que o crash era em mensagens de stop de accounting. Construímos portanto um cenário de pedido que crashava o daemon freeradius 100% das vezes. A mensagem de accounting foi construida de acordo com os ecrans seguintes, com um utilizador ficcional de roaming:





Em seguida, mudamos para um directório onde o utilizador freerad tenha direitos de escrita, por exemplo /tmp. Colocamos o daemon a correr com freeradius -X, e seleccionamos o botão start no JRadius Simulator para crashar o servidor. Ficamos portanto com um ficheiro core no directório local.

Para o analisar, corremos o comando gdb.

```
#gdb /usr/sbin/freeradius core
GNU gdb (Debian 7.7.1+dfsg-5) 7.7.1
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from /usr/sbin/freeradius...(no debugging symbols found)...done.
[New LWP 12852]
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Core was generated by `freeradius -X'.
Program terminated with signal SIGSEGV, Segmentation fault.
#0 0x00007ff34e9335fa in regex_exec ()
from /usr/lib/freeradius/libfreeradius-radius.so
```

```
(gdb) info threads
Id Target Id Frame
* 1 Thread 0x7ff34ef91740 (LWP 12852) 0x00007ff34e9335fa in regex_exec ()
from /usr/lib/freeradius/libfreeradius-radius.so
(gdb)
(gdb) thread apply all bt full
Thread 1 (Thread 0x7ff34ef91740 (LWP 12852)):
#0 0x00007ff34e9335fa in regex_exec ()
from /usr/lib/freeradius/libfreeradius-radius.so
No symbol table info available.
#1 0x0000000000445da1 in realm_find ()
No symbol table info available.
#2 0x00007ff34548bfce in ?? () from /usr/lib/freeradius/rlm_realm.so
No symbol table info available.
#3 0x00007ff34548c6dc in ?? () from /usr/lib/freeradius/rlm_realm.so
No symbol table info available.
#4 0x0000000000424dde in ?? ()
No symbol table info available.
#5 0x00000000004253f8 in ?? ()
No symbol table info available.
#6 0x0000000000424f9f in ?? ()
No symbol table info available.
#7 0x0000000000425c6d in ?? ()
No symbol table info available.
#8 0x0000000000426833 in modcall ()
No symbol table info available.
#9 0x00000000004225b2 in indexed_modcall ()
No symbol table info available.
#10 0x000000000042468c in module_preacct ()
No symbol table info available.
#11 0x000000000040db7d in rad_accounting ()
No symbol table info available.
#12 0x0000000000438e45 in ?? ()
No symbol table info available.
#13 0x0000000000437da2 in ?? ()
No symbol table info available.
#14 0x000000000043965c in request_receive ()
No symbol table info available.
---Type <return> to continue, or q <return> to quit---
#15 0x000000000041666b in ?? ()
No symbol table info available.
#16 0x000000000043fafb in ?? ()
No symbol table info available.
#17 0x00007ff34e93b717 in fr_event_loop ()
from /usr/lib/freeradius/libfreeradius-radius.so
No symbol table info available.
#18 0x0000000000441543 in radius_event_process ()
No symbol table info available.
#19 0x000000000042c674 in main ()
No symbol table info available.
```

E por fim colocou-se no ticket o resultado do comando valgrind --tool=memcheck --leak-check=full freeradius -Xm

Outra forma de ter mais informações de debug é compilar activando DEBUG_STATE_MACHINE em src/main/process.c. Ainda não experimentamos.

Obter certificados eduPKI

Para solicitar certificados da CA eduPKI para serviços EDUROAM é necessário coordenar-se com a sua NREN local, sendo no caso da RCTS a FCCN /FCT. Ver também a pagina seguinte para os passos necessários para o registo. https://www.eduroam.org/index.php?p=europe&s=edupki

O que a sua NREN vai fazer, além dos passos burocráticos, é visitar o endereço https://www.edupki.org/edupki-ca/get-certificates/ e fazer download do applet Java para registo em https://pki.edupki.org/edupki-ca/cert-req-gen/eduroam-cert-req-gen.jnlp . Em seguida correr o mesmo (tem-se de ter Java instalado na estação de trabalho), preencher e seleccionar "Generate key pair and certificate request".



Administração de sistemas sys V versus Systemd

No Debian 8, foi criada uma transição forçada para systemd.

Antes de fazer o upgrade de Debian 7 para Debian 8, é possível proibir com políticas do Debian a instalação do systemd, i.e. fazer pinning do pacote.

Para tal, criar o ficheiro:

/etc/apt/preferences.d/01systemd

```
Package: systemd
Pin: origin ""
Pin-Priority: -1
```

Ao instalar de raiz, pensamos que o mais prático será usar preseeding para desinstalar o systemd e instalar o sysvinit. Adicionar a seguinte linha no preseed

```
preseed/late_command="in-target apt-get install -y sysvinit-core"
```

ou fazer TAB no menu de boot e acrescentar essa linha.

Caso opte por usar o systemd, esta é uma tabela prática de conversão de comandos.

https://fedoraproject.org/wiki/SysVinit_to_Systemd_Cheatsheet

Criação de conta github com script ansible

https://github.com/ruyrybeyro/ansible-freeradius

https://github.com/ruyrybeyro/ansible-freeradius.git

```
backups01-vlx:/etc/ansible/playbooks/ruy.freeradius$ git init
Initialized empty Git repository in /etc/ansible/playbooks/ruy.freeradius/.git/
backups01-vlx:/etc/ansible/playbooks/ruy.freeradius$ git config --global user.name "Rui Ribeiro"
backups01-vlx:/etc/ansible/playbooks/ruy.freeradius$ git config --global user.email ruyrybeyro@gmail.com
backups01-vlx:/etc/ansible/playbooks/ruy.freeradius$ git add .
backups01-vlx:/etc/ansible/playbooks/ruy.freeradius$ git commit -m "FR 3 - first commit"
[master (root-commit) e8065a0] FR 3 - first commit
 36 files changed, 3234 insertions(+)
 create mode 100644 LICENSE
 create mode 100644 README.md
 create mode 100644 group_vars/all
 create mode 100644 main.yml
 create mode 100644 meta/main.yml
 create mode 100644 roles/eapol/tasks/main.yml
 create mode 100644 roles/freeradius/files/mods-available/f_ticks
 create mode 100644 roles/freeradius/files/mods-config/attr_filter/post-proxy
 create mode 100644 roles/freeradius/files/mods-config/attr_filter/pre-proxy
 create mode 100644 roles/freeradius/files/policy.d/local_blacklist
 create mode 100644 roles/freeradius/files/sites-available/control-socket
 create mode 100644 roles/freeradius/handlers/main.yml
 create mode 100644 roles/freeradius/tasks/main.yml
 create mode 100644 roles/freeradius/templates/certs/ca.cnf
 create mode 100644 roles/freeradius/templates/certs/client.cnf
 create mode 100644 roles/freeradius/templates/certs/server.cnf
 create mode 100644 roles/freeradius/templates/clients.conf
 create mode 100644 roles/freeradius/templates/mods-available/eap
 create mode 100644 roles/freeradius/templates/mods-available/ldap
 create mode 100644 roles/freeradius/templates/mods-available/mschap
 create mode 100644 roles/freeradius/templates/proxy.conf
 create mode 100644 roles/freeradius/templates/sites-available/default
 create mode 100644 roles/freeradius/templates/sites-available/inner-tunnel
 create mode 100644 roles/freeradius/templates/sites-available/tls
 create mode 100644 roles/kerberos/tasks/main.yml
 create mode 100644 roles/kerberos/templates/krb5.conf
 create mode 100644 roles/mysql/files/banned_schema.sql
 create mode 100644 roles/mysql/files/my.cnf
 create mode 100644 roles/mysql/handlers/main.yml
 create mode 100644 roles/mysql/tasks/main.yml
 create mode 100644 roles/ntp/tasks/main.yml
 create mode 100644 roles/prepare/tasks/main.yml
 create mode 100644 roles/samba/handlers/main.yml
 create mode 100644 roles/samba/tasks/main.yml
 create mode 100644 roles/samba/templates/setup.sh
 create mode 100644 roles/samba/templates/smb.conf
backups01-vlx:/etc/ansible/playbooks/ruy.freeradius$ git remote add origin https://github.com/ruyrybeyro
/ansible-freeradius.git
backups01-vlx:/etc/ansible/playbooks/ruy.freeradius$ git push -u origin master
Username for 'https://github.com': ruyrybeyro
Password for 'https://ruyrybeyro@github.com':
Counting objects: 71, done.
Delta compression using up to 2 threads.
Compressing objects: 100% (51/51), done.
Writing objects: 100% (71/71), 35.65 KiB | 0 bytes/s, done.
Total 71 (delta 2), reused 0 (delta 0)
To https://github.com/ruyrybeyro/ansible-freeradius.git
 * [new branch]      master -> master
Branch master set up to track remote branch master from origin.
```

Script básico de ansible para instalação do software em Debian

Playbook para instalar FreeRadius 3 em Debian testado em Ansible 1.8.

meta/main.yml

```
---
galaxy_info:
  author: Rui Ribeiro
  description: FreeRadius 3 setup for PT EDUROAM
  company: ISCTE-IUL
  license: BSD
  min_ansible_version: 1.2

  platforms:
  - name: Debian
    versions:
    - jessie
  categories:
  - networking
  - system
dependencies: []
```

group_vars/all

```
---
freeradius_role_version: '2015012602'

freeradius_version: 3.0.7
eapol_version: 2.3

realm: iscte.pt
federation_password: xxxxxxxxx
fst_parent_fed: 193.136.192.43
snd_parent_fed: 193.136.192.44
local_wireless_secret: yyyyyyyy

ad_server: 192.168.1.1
domain: ISCTE.LOCAL
domain_l: iscte.local
workgroup: ISCTE
user_to_add_machine: administrator
hostname_dc: DC01


base_dn: CN=Users,DC=iscte,DC=local
filter: (sAMAccountName=%{Stripped-User-Name})
membership_filter: (sAMAccountName=%{Stripped-User-Name})
membership_attribute: memberOf
domain_user: CN=Radius_Bind,CN=Users,DC=iscte,DC=local
domain_user_pass: zzzzzzzz


VLAN_roaming: 100
VLAN_employees: 101
VLAN_students: 102


private_key: kkkkkkkk
countryName: PT
stateOrProvinceName: Lisboa
localityName: Lisboa
emailAddress: rui.ribeiro@iscte.pt
organizationName: ISCTE-IUL
```

main.yml

```
---
- hosts: debtestes
  gather_facts: true
  sudo: yes
  roles:
    - prepare
    - ntp
    - kerberos
    - samba
    - freeradius
    - mysql
    - eapol
```

roles/prepare/tasks/main.yml

```
---
- name: updates a server
  apt: update_cache=yes
- name: install pre-requisites
  apt: pkg={{ item }} state=installed
  with_items:
     - python-mysqldb
     - libperl4-corelibs-perl
     - chkconfig
     - liblog-handler-perl
     - libjson-perl
     - libparams-validate-perl
     - libio-string-perl
     - libclass-accessor-perl
     - openssl
     - krb5-user
     - libnl-3-200
     - libssl-dev
     - apt-src
     - make
     - libssl-dev
     - quilt
     - libtool
     - libltdl3-dev
     - libpam0g-dev
     - libmysqlclient-dev
     - libgdbm-dev
     - libldap2-dev
     - libsasl2-dev
     - libiodbc2-dev
     - libkrb5-dev
     - libperl-dev
     - libperl-dev
     - python-dev
     - libsnmp-dev
     - libpq-dev
     - debhelper
     - fakeroot
     - ssl-cert
     - build-essential
     - libcurl4-openssl-dev
     - libjson0-dev
     - libreadline-dev
     - libsqlite3-dev
     - libtalloc-dev
     - libyubikey-dev
     - libcap-dev
     - libpcap-dev
```

roles/ntp/tasks/main.yml

```
---
- name: Install NTP
  apt: package=ntp state=present
- name: Make sure NTP is started up
  service: name=ntp state=started enabled=yes
```

roles/kerberos/tasks/main.yml

```
---
- name: Install kerberos
  apt: package=krb5-user state=present
- name: install kerberos config
  template: src=krb5.conf dest=/etc
```

roles/kerberos/templates/krb5.conf

```
[libdefaults]
        default_realm = {{ domain }}
        clockskew = 300
        dns_lookup_realm = false
        dns_lookup_kdc = false
        dns_fallback = false
[realms]
{{ domain }} = {
kdc = {{ ad_server }}
default_domain = {{ domain_l }}
admin_server = {{ ad_server }}
}
[domain_realm]
.{{ domain_l }} = {{ domain }}
{{ domain_l }} = {{ domain }}
```

roles/samba/tasks/main.yml

```
---
- name: Install samba
  apt: package=samba state=present
- name: Install winbind
  apt: package=winbind state=present
- name: install config file
  template: src=smb.conf dest=/etc/samba
- service: name=samba state=restarted
- template: src=setup.sh dest=/usr/local/bin
```

roles/samba/templates/smb.conf

```
[global]
        netbios name = {{ inventory_hostname }}
        workgroup = {{ workgroup }}
        realm = {{ domain }}
        server string = %h server
        interfaces = lo
        bind interfaces only = Yes
        wins support = no
        security = ADS
        encrypt passwords = true
        passdb backend = tdbsam
        obey pam restrictions = Yes
        pam password change = Yes
        passwd program = /usr/bin/passwd %u
        passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n
*password\supdated\ssuccessfully* .
        syslog = 0
        log file = /var/log/samba/log.%m
        max log size = 1000
        load printers = No
        printcap name = /dev/null
        disable spoolss = Yes
        os level = 0
        local master = No
        domain master = No
        dns proxy = No
        panic action = /usr/share/samba/panic-action %d
        winbind enum users = Yes
        winbind enum groups = Yes
        winbind use default domain = Yes
        idmap config * : range = 10000-20000
        idmap config * : backend = tdb
        printing = bsd
```

roles/samba/templates/setup.sh

```
#!/bin/bash
sudo net rpc join -U {{user_to_add_machine}} -S {{hostname_dc}} -I {{ad_server}}
sudo sudo net ads join -U administrator
service winbind restart
```

roles/freeradius/main.yml

```
---
- name: gets tarball freeradius
  get_url: url="ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-{{freeradius_version}}.tar.gz" dest="
/usr/local/src/"
  register: new_archive
- name: untar freeradius source
  unarchive: src="/usr/local/src/freeradius-server-{{freeradius_version}}.tar.gz" dest="/usr/local/src/" copy=no
- template: src=certs/{{ item }} dest=/usr/local/src/freeradius-server-{{freeradius_version}}/raddb/certs
  with_items:
     - server.cnf
     - ca.cnf
     - client.cnf
- name: copy freeradius templates
  template: src={{ item }} dest=/usr/local/src/freeradius-server-{{freeradius_version}}/raddb/{{ item }}
  with_items:
     - mods-available/eap
     - mods-available/ldap
     - mods-available/mschap
- name: compile freeradius
  command: creates=/usr/local/src/freeradius_{{freeradius_version}}+git_amd64.deb chdir=/usr/local/src
```

```
/freeradius-server-{{freeradius_version}} fakeroot dpkg-buildpackage -b -uc
- name: create group for radmin
  group: name=radius state=present
- name: install debs
  shell: dpkg -i freeradius-config_{{freeradius_version}}*.deb freeradius-common_{{freeradius_version}}*.deb
libfreeradius3_{{freeradius_version}}*.deb freeradius_{{freeradius_version}}*.deb freeradius-utils_
{{freeradius_version}}*.deb
  args:
    chdir: /usr/local/src/
- name: install debs ldap
  shell: dpkg -i freeradius-ldap_{{freeradius_version}}*.deb
  args:
    chdir: /usr/local/src/
- name: install debs mysql
  shell: dpkg -i freeradius-mysql_{{freeradius_version}}*.deb
  args:
    chdir: /usr/local/src/
- name: add FreeRadius user to group winbindd_priv
  user: name=freerad groups=freerad,winbindd_priv
- name: change /var/lib/samba/winbindd_privileged group ownership to winbindd_priv
  file: path=/var/lib/samba/winbindd_privileged group=winbindd_priv
- name: restart winbind
  service: name=winbind state=restarted
- name: copy freeradius files
  copy: src={{ item }} dest=/etc/freeradius/{{ item }}
  with_items:
     - mods-available/f_ticks
     - mods-config/attr_filter/post-proxy
     - mods-config/attr_filter/pre-proxy
     - sites-available/control-socket
     - policy.d/local_blacklist
- name: copy freeradius templates
  template: src={{ item }} dest=/etc/freeradius/{{ item }}
  with_items:
     - mods-available/eap
     - mods-available/ldap
     - sites-available/default
     - sites-available/inner-tunnel
     - sites-available/tls
- name: create radacct directory with freerad.freerad owner and 600
  file: path=/var/log/freeradius/radacct owner=freerad group=freerad state=directory mode=600
- name: create symlinks to virtual servers
  file: src=/etc/freeradius/sites-available/{{ item }} dest=/etc/freeradius/sites-enabled/{{ item }} state=link
  with_items:
     - status
     - control-socket
- name: delete symlinks to modules not used
  file: path=/etc/freeradius/mods-enabled/{{ item }} state=absent
  with_items:
     - chap
     - dhcp
     - digest
     - echo
     - exec
     - expiration
     - dynamic_clients
     - logintime
     - pap
     - passwd
     - radutmp
     - replicate
     - soh
     - sradutmp
     - unix
- name: create symlinks in /etc/freeradius/mods-enabled/
  file: src=/etc/freeradius/mods-available/{{ item }} dest=/etc/freeradius/mods-enabled/{{ item }} state=link
  with_items:
     - f_ticks
     - ldap
     - sql
- name: create proxy.conf and clients.conf
```

```
  template: src={{ item }} dest=/etc/freeradius/
  with_items:
     - clients.conf
     - proxy.conf
```

roles/freeradius/handlers/main.yml

```
---
-   name: restart freeradius
    service:  name=freeradius state=restarted enabled=yes
```

Para files e templates do freeradius, consulte o github

roles/mysql/tasks/main.yml

```
---
- name: Install MySQL
  apt: package=mysql-server state=present
- name: copy mysql config
  copy: src=my.cnf dest=/etc/mysql/my.cnf
- copy: src=banned_schema.sql dest=/tmp
- mysql_db: name=radius state=present
- shell: mysql -u root < /etc/freeradius/mods-config/sql/main/mysql/setup.sql
- shell: mysql -u root radius < /etc/freeradius/mods-config/sql/main/mysql/schema.sql
- shell: mysql -u root radius < /tmp/banned_schema.sql
- service: name=mysql state=restarted enabled=yes
```

Para files, consulte o gitbub.

roles/eapol/tasks/main.yml

```
---
- name: create symlink to compile eapol_test in Debian 8
  file: src=/lib/x86_64-linux-gnu/libnl-3.so.200 dest=/lib/x86_64-linux-gnu/libnl.so state=link
- name: gets tarball eapol
  get_url: url="http://hostap.epitest.fi/releases/wpa_supplicant-{{eapol_version}}.tar.gz" dest="/usr/local/src
/"
  register: new_archive
- name: untar eapol
  unarchive: src="/usr/local/src/wpa_supplicant-{{eapol_version}}.tar.gz" dest="/usr/local/src/" copy=no
  when: new_archive|changed
- name: copy eapol config
  command: cp /usr/local/src/wpa_supplicant-{{eapol_version}}/wpa_supplicant/defconfig /usr/local/src
/wpa_supplicant-{{eapol_version}}/wpa_supplicant/.config
- name: compile eapol
  command: creates=/usr/local/bin/eapol_test chdir=/usr/local/src/wpa_supplicant-{{eapol_version}}
/wpa_supplicant make eapol_test
- name: install eapol
  command: cp /usr/local/src/wpa_supplicant-{{eapol_version}}/wpa_supplicant/eapol_test /usr/local/bin
```

Correndo o playbook.

```
$ ansible-playbook main.yml


PLAY [debtestes] ***************************************************************
```

GATHERING FACTS ***

ok: [debtestes]

TASK: [prepare | updates a server] **

ok: [debtestes]

TASK: [prepare | install pre-requisites] **************************************

changed: [debtestes] => (item=python-mysqldb,libperl4-corelibs-perl,chkconfig,liblog-handler-perl,libjson-perl,libparams-validate-perl,libio-string-perl,libclass-accessor-perl,openssl,krb5-user,libnl-3-200,libssl-dev,apt-src,make,libssl-dev,quilt,libtool,libltdl3-dev,libpam0g-dev,libmysqlclient-dev,libgdbm-dev,libldap2-dev,libsasl2-dev,libiodbc2-dev,libkrb5-dev,libperl-dev,libperl-dev,python-dev,libsnmp-dev,libpq-dev,debhelper,fakeroot,ssl-cert,build-essential,libcurl4-openssl-dev,libjson0-dev,libreadline-dev,libsqlite3-dev,libtalloc-dev,libyubikey-dev,libcap-dev,libpcap-dev)

TASK: [ntp | Install NTP] ***

changed: [debtestes]

TASK: [ntp | Make sure NTP is started up] *************************************

ok: [debtestes]

TASK: [kerberos | Install kerberos] ***

ok: [debtestes]

TASK: [kerberos | install kerberos config] ************************************

changed: [debtestes]

TASK: [samba | Install samba] ***

changed: [debtestes]

TASK: [samba | Install winbind] ***

changed: [debtestes]

TASK: [samba | install config file] ***

changed: [debtestes]

TASK: [samba | service name=samba state=restarted] ****************************

changed: [debtestes]

TASK: [samba | template src=setup.sh dest=/usr/local/bin] *********************

changed: [debtestes]

TASK: [freeradius | gets tarball freeradius] **********************************

changed: [debtestes]

TASK: [freeradius | untar freeradius source] ***********************************

changed: [debtestes]

TASK: [freeradius | template src=certs/{{ item }} dest=/usr/local/src/freeradius-server-{{freeradius_version}}/raddb/certs] ***

changed: [debtestes] => (item=server.cnf)

changed: [debtestes] => (item=ca.cnf)

changed: [debtestes] => (item=client.cnf)

TASK: [freeradius | copy freeradius templates] *********************************

changed: [debtestes] => (item=mods-available/eap)

changed: [debtestes] => (item=mods-available/ldap)

changed: [debtestes] => (item=mods-available/mschap)

TASK: [freeradius | compile freeradius] **

changed: [debtestes]

TASK: [freeradius | create group for radmin] ***********************************

ok: [debtestes]

TASK: [freeradius | install debs] **

changed: [debtestes]

TASK: [freeradius | install debs ldap] ***

changed: [debtestes]

TASK: [freeradius | install debs mysql] **

changed: [debtestes]

TASK: [freeradius | add FreeRadius user to group winbindd_priv] ***************

changed: [debtestes]

TASK: [freeradius | change /var/lib/samba/winbindd_privileged group ownership to winbindd_priv] ***

changed: [debtestes]

TASK: [freeradius | restart winbind] ***

changed: [debtestes]

TASK: [freeradius | copy freeradius files] *************************************

changed: [debtestes] => (item=mods-available/f_ticks)

changed: [debtestes] => (item=mods-config/attr_filter/post-proxy)

changed: [debtestes] => (item=mods-config/attr_filter/pre-proxy)

changed: [debtestes] => (item=sites-available/control-socket)

changed: [debtestes] => (item=policy.d/local_blacklist)

TASK: [freeradius | copy freeradius templates] *********************************

ok: [debtestes] => (item=mods-available/eap)

ok: [debtestes] => (item=mods-available/ldap)

changed: [debtestes] => (item=sites-available/default)

changed: [debtestes] => (item=sites-available/inner-tunnel)

changed: [debtestes] => (item=sites-available/tls)

TASK: [freeradius | create radacct directory with freerad.freerad owner and 600] ***

ok: [debtestes]

TASK: [freeradius | create symlinks to virtual servers] ***********************

changed: [debtestes] => (item=status)

changed: [debtestes] => (item=control-socket)

TASK: [freeradius | delete symlinks to modules not used] ***********************

changed: [debtestes] => (item=chap)

changed: [debtestes] => (item=dhcp)

changed: [debtestes] => (item=digest)

changed: [debtestes] => (item=echo)

changed: [debtestes] => (item=exec)

changed: [debtestes] => (item=expiration)

changed: [debtestes] => (item=dynamic_clients)

changed: [debtestes] => (item=logintime)

changed: [debtestes] => (item=pap)

changed: [debtestes] => (item=passwd)

changed: [debtestes] => (item=radutmp)

changed: [debtestes] => (item=replicate)

changed: [debtestes] => (item=soh)

changed: [debtestes] => (item=sradutmp)

changed: [debtestes] => (item=unix)

TASK: [freeradius | create symlinks in /etc/freeradius/mods-enabled/] *********

changed: [debtestes] => (item=f_ticks)

changed: [debtestes] => (item=ldap)

changed: [debtestes] => (item=sql)

TASK: [freeradius | create proxy.conf and clients.conf] ***********************

changed: [debtestes] => (item=clients.conf)

changed: [debtestes] => (item=proxy.conf)

TASK: [mysql | Install MySQL] **

changed: [debtestes]

TASK: [mysql | copy mysql config] **

changed: [debtestes]

TASK: [mysql | copy src=banned_schema.sql dest=/tmp] **************************

ok: [debtestes]

TASK: [mysql | mysql_db name=radius state=present] ****************************

changed: [debtestes]

TASK: [mysql | shell mysql -u root < /etc/freeradius/mods-config/sql/main/mysql/setup.sql] ***

changed: [debtestes]

TASK: [mysql | shell mysql -u root radius < /etc/freeradius/mods-config/sql/main/mysql/schema.sql] ***

changed: [debtestes]

TASK: [mysql | shell mysql -u root radius < /tmp/banned_schema.sql] ***********

changed: [debtestes]

TASK: [mysql | service name=mysql state=restarted enabled=yes] ****************

changed: [debtestes]

TASK: [eapol | create symlink to compile eapol_test in Debian 8] **************

ok: [debtestes]

TASK: [eapol | gets tarball eapol] ***

changed: [debtestes]

TASK: [eapol | untar eapol] **

changed: [debtestes]

TASK: [eapol | copy eapol config] **

changed: [debtestes]

```
TASK: [eapol | compile eapol] ***************************************************
changed: [debtestes]

TASK: [eapol | install eapol] ***************************************************
changed: [debtestes]

PLAY RECAP ********************************************************************
debtestes                  : ok=45   changed=37   unreachable=0    failed=0
```

```
backups01-vlx:/etc/ansible/playbooks/ruy.freeradius# ls -laR
.:
total 11
drwxr-xr-x 6 rui rui 1024 Jan 26 16:42 .
drwxr-xr-x 7 rui rui 1024 Jan 29 10:03 ..
drwxr-xr-x 8 rui rui 1024 Jan 29 10:09 .git
drwxr-xr-x 2 rui rui 1024 Jan 26 16:23 group_vars
-rw-rw-r-- 1 rui rui 1082 Jul  7  2014 LICENSE
-rw-rw-r-- 1 rui rui  157 Jan 25 19:17 main.yml
drwxr-xr-x 2 rui rui 1024 Jan 24 14:25 meta
-rw-r--r-- 1 rui rui 1775 Jan 26 16:34 README.md
drwxr-xr-x 9 rui rui 1024 Jan 25 19:16 roles

./group_vars:
total 3
drwxr-xr-x 2 rui rui 1024 Jan 26 16:23 .
drwxr-xr-x 6 rui rui 1024 Jan 26 16:42 ..
-rw-r--r-- 1 rui rui  831 Jan 26 16:23 all

./meta:
total 3
drwxr-xr-x 2 rui rui 1024 Jan 24 14:25 .
drwxr-xr-x 6 rui rui 1024 Jan 26 16:42 ..
-rw-r--r-- 1 rui rui  269 Jan 24 14:25 main.yml

./roles:
total 9
drwxr-xr-x 9 rui rui 1024 Jan 25 19:16 .
drwxr-xr-x 6 rui rui 1024 Jan 26 16:42 ..
drwxr-xr-x 3 rui rui 1024 Jan 23 23:53 eapol
```

drwxr-xr-x 6 rui rui 1024 Jan 24 13:06 **freeradius**

drwxr-xr-x 4 rui rui 1024 Jan 24 00:37 **kerberos**

drwxr-xr-x 5 rui rui 1024 Jan 24 12:30 **mysql**

drwxr-xr-x 3 rui rui 1024 Jan 24 00:07 **ntp**

drwxr-xr-x 3 rui rui 1024 Jan 24 00:04 **prepare**

drwxr-xr-x 5 rui rui 1024 Jan 24 12:50 **samba**

./roles/eapol:

total 3

drwxr-xr-x 3 rui rui 1024 Jan 23 23:53 **.**

drwxr-xr-x 9 rui rui 1024 Jan 25 19:16 **..**

drwxr-xr-x 2 rui rui 1024 Jan 25 19:55 **tasks**

./roles/eapol/tasks:

total 3

drwxr-xr-x 2 rui rui 1024 Jan 25 19:55 **.**

drwxr-xr-x 3 rui rui 1024 Jan 23 23:53 **..**

-rw-r--r-- 1 rui rui 940 Jan 25 19:55 main.yml

./roles/freeradius:

total 6

drwxr-xr-x 6 rui rui 1024 Jan 24 13:06 **.**

drwxr-xr-x 9 rui rui 1024 Jan 25 19:16 **..**

drwxr-xr-x 6 rui rui 1024 Jan 24 10:51 **files**

drwxr-xr-x 2 rui rui 1024 Jan 26 14:58 **handlers**

drwxr-xr-x 2 rui rui 1024 Jan 26 15:52 **tasks**

drwxr-xr-x 5 rui rui 1024 Jan 29 10:06 **templates**

./roles/freeradius/files:

total 6

drwxr-xr-x 6 rui rui 1024 Jan 24 10:51 **.**

drwxr-xr-x 6 rui rui 1024 Jan 24 13:06 **..**

drwxr-xr-x 2 rui rui 1024 Jan 24 07:53 **mods-available**

drwxr-xr-x 3 rui rui 1024 Jan 23 14:33 **mods-config**

drwxr-xr-x 2 rui rui 1024 Jan 23 14:21 **policy.d**

drwxr-xr-x 2 rui rui 1024 Jan 24 10:51 **sites-available**

./roles/freeradius/files/mods-available:

total 6

drwxr-xr-x 2 rui rui 1024 Jan 24 07:53 **.**

drwxr-xr-x 6 rui rui 1024 Jan 24 10:51 **..**

-rw-r--r-- 1 rui rui 3340 Jan 24 07:40 f_ticks

./roles/freeradius/files/mods-config:

total 3

drwxr-xr-x 3 rui rui 1024 Jan 23 14:33 **.**

drwxr-xr-x 6 rui rui 1024 Jan 24 10:51 **..**

drwxr-xr-x 2 rui rui 1024 Jan 26 09:41 **attr_filter**

./roles/freeradius/files/mods-config/attr_filter:

total 4

drwxr-xr-x 2 rui rui 1024 Jan 26 09:41 **.**

drwxr-xr-x 3 rui rui 1024 Jan 23 14:33 **..**

-rw-r--r-- 1 rui rui 798 Jan 26 09:40 post-proxy

-rw-r--r-- 1 rui rui 410 Jan 26 09:41 pre-proxy

./roles/freeradius/files/policy.d:

total 4

drwxr-xr-x 2 rui rui 1024 Jan 23 14:21 **.**

drwxr-xr-x 6 rui rui 1024 Jan 24 10:51 **..**

-rw-r--r-- 1 rui rui 1171 Jan 23 14:21 local_blacklist

./roles/freeradius/files/sites-available:

total 4

drwxr-xr-x 2 rui rui 1024 Jan 24 10:51 **.**

drwxr-xr-x 6 rui rui 1024 Jan 24 10:51 **..**

-rw-r--r-- 1 rui rui 2003 Jan 24 10:51 control-socket

./roles/freeradius/handlers:

total 3

drwxr-xr-x 2 rui rui 1024 Jan 26 14:58 **.**

drwxr-xr-x 6 rui rui 1024 Jan 24 13:06 **..**

-rw-r--r-- 1 rui rui   91 Jan 24 13:07 main.yml

./roles/freeradius/tasks:

total 6

drwxr-xr-x 2 rui rui 1024 Jan 26 15:52 **.**

drwxr-xr-x 6 rui rui 1024 Jan 24 13:06 **..**

-rw-r--r-- 1 rui rui 3472 Jan 26 15:52 main.yml

./roles/freeradius/templates:

total 8

drwxr-xr-x 5 rui rui 1024 Jan 29 10:06 **.**

drwxr-xr-x 6 rui rui 1024 Jan 24 13:06 **..**

drwxr-xr-x 2 rui rui 1024 Jan 25 19:29 **certs**

-rw-r--r-- 1 rui rui 887 Jan 29 10:06 clients.conf

drwxr-xr-x 2 rui rui 1024 Jan 26 13:39 **mods-available**

-rw-r--r-- 1 rui rui 1228 Jan 26 15:59 proxy.conf

drwxr-xr-x 2 rui rui 1024 Jan 29 10:07 **sites-available**

./roles/freeradius/templates/certs:

total 8

drwxr-xr-x 2 rui rui 1024 Jan 25 19:29 **.**

drwxr-xr-x 5 rui rui 1024 Jan 29 10:06 **..**

-rw-r--r-- 1 rui rui 1467 Jan 25 19:22 ca.cnf

-rw-r--r-- 1 rui rui 1160 Jan 25 19:29 client.cnf

-rw-r--r-- 1 rui rui 1176 Jan 25 19:11 server.cnf

./roles/freeradius/templates/mods-available:

total 44

drwxr-xr-x 2 rui rui 1024 Jan 26 13:39 **.**

drwxr-xr-x 5 rui rui 1024 Jan 29 10:06 **..**

-rw-r--r-- 1 rui rui 23373 Jan 25 12:49 eap

-rw-r--r-- 1 rui rui 13938 Jan 24 12:12 ldap

-rw-r--r-- 1 rui rui 2890 Jan 26 13:39 mschap

./roles/freeradius/templates/sites-available:

total 28

drwxr-xr-x 2 rui rui 1024 Jan 29 10:07 **.**

drwxr-xr-x 5 rui rui 1024 Jan 29 10:06 **..**

-rw-r--r-- 1 rui rui 5631 Jan 24 12:13 default

-rw-r--r-- 1 rui rui 2569 Jan 24 12:14 inner-tunnel

-rw-r--r-- 1 rui rui 15604 Jan 29 10:07 tls

./roles/kerberos:

total 4

drwxr-xr-x 4 rui rui 1024 Jan 24 00:37 **.**

drwxr-xr-x 9 rui rui 1024 Jan 25 19:16 **..**

drwxr-xr-x 2 rui rui 1024 Jan 24 07:24 **tasks**

drwxr-xr-x 2 rui rui 1024 Jan 24 09:39 **templates**

./roles/kerberos/tasks:

total 3

drwxr-xr-x 2 rui rui 1024 Jan 24 07:24 **.**

drwxr-xr-x 4 rui rui 1024 Jan 24 00:37 **..**

-rw-r--r-- 1 rui rui 136 Jan 24 07:24 main.yml

./roles/kerberos/templates:

total 3

drwxr-xr-x 2 rui rui 1024 Jan 24 09:39 **.**

drwxr-xr-x 4 rui rui 1024 Jan 24 00:37 **..**

-rw-r--r-- 1 rui rui 359 Jan 24 09:39 krb5.conf

./roles/mysql:

total 5

drwxr-xr-x 5 rui rui 1024 Jan 24 12:30 **.**

drwxr-xr-x 9 rui rui 1024 Jan 25 19:16 **..**

drwxr-xr-x 2 rui rui 1024 Jan 28 15:48 **files**

drwxr-xr-x 2 rui rui 1024 Jan 26 09:48 **handlers**

drwxr-xr-x 2 rui rui 1024 Jan 28 15:50 **tasks**

./roles/mysql/files:

total 6

drwxr-xr-x 2 rui rui 1024 Jan 28 15:48 **.**

drwxr-xr-x 5 rui rui 1024 Jan 24 12:30 **..**

-rw-r--r-- 1 rui rui 158 Jan 26 16:13 banned_schema.sql

-rw-r--r-- 1 rui rui 2400 Jan 24 12:48 my.cnf

./roles/mysql/handlers:

total 3

drwxr-xr-x 2 rui rui 1024 Jan 26 09:48 **.**

drwxr-xr-x 5 rui rui 1024 Jan 24 12:30 **..**

-rw-r--r-- 1 rui rui   81 Jan 24 12:25 main.yml

./roles/mysql/tasks:

total 3

drwxr-xr-x 2 rui rui 1024 Jan 28 15:50 **.**

drwxr-xr-x 5 rui rui 1024 Jan 24 12:30 **..**

-rw-r--r-- 1 rui rui 483 Jan 28 15:50 main.yml

./roles/ntp:

total 3

drwxr-xr-x 3 rui rui 1024 Jan 24 00:07 **.**

drwxr-xr-x 9 rui rui 1024 Jan 25 19:16 **..**

drwxr-xr-x 2 rui rui 1024 Jan 24 00:23 **tasks**

./roles/ntp/tasks:

total 3

drwxr-xr-x 2 rui rui 1024 Jan 24 00:23 **.**

drwxr-xr-x 3 rui rui 1024 Jan 24 00:07 **..**

-rw-r--r-- 1 rui rui 141 Jan 24 00:23 main.yml

./roles/prepare:

total 3

drwxr-xr-x 3 rui rui 1024 Jan 24 00:04 **.**

drwxr-xr-x 9 rui rui 1024 Jan 25 19:16 **..**

drwxr-xr-x 2 rui rui 1024 Jan 25 20:57 **tasks**

./roles/prepare/tasks:

total 3

drwxr-xr-x 2 rui rui 1024 Jan 25 20:57 **.**

drwxr-xr-x 3 rui rui 1024 Jan 24 00:04 **..**

-rw-r--r-- 1 rui rui 985 Jan 25 20:57 main.yml

./roles/samba:

total 5

drwxr-xr-x 5 rui rui 1024 Jan 24 12:50 **.**

drwxr-xr-x 9 rui rui 1024 Jan 25 19:16 **..**

drwxr-xr-x 2 rui rui 1024 Jan 24 12:52 **handlers**

drwxr-xr-x 2 rui rui 1024 Jan 26 14:44 **tasks**

drwxr-xr-x 2 rui rui 1024 Jan 26 15:23 **templates**

./roles/samba/handlers:

total 3

drwxr-xr-x 2 rui rui 1024 Jan 24 12:52 **.**

drwxr-xr-x 5 rui rui 1024 Jan 24 12:50 **..**

-rw-r--r-- 1 rui rui   82 Jan 24 12:51 main.yml

./roles/samba/tasks:

total 3

```
drwxr-xr-x 2 rui rui 1024 Jan 26 14:44 .

drwxr-xr-x 5 rui rui 1024 Jan 24 12:50 ..

-rw-r--r-- 1 rui rui  274 Jan 26 14:44 main.yml


./roles/samba/templates:

total 5

drwxr-xr-x 2 rui rui 1024 Jan 26 15:23 .

drwxr-xr-x 5 rui rui 1024 Jan 24 12:50 ..

-rw-r--r-- 1 rui rui  157 Jan 26 15:23 setup.sh

-rw-r--r-- 1 rui rui 1116 Jan 24 10:02 smb.conf

backups01-vlx:/etc/ansible/playbooks/ruy.freeradius#
```

Monitorar FreeRadius com dtrace

https://github.com/dtrace4linux/linux

Usando Logstash

https://github.com/FreeRADIUS/freeradius-server/tree/v3.0.x/doc/schemas/logstash

A partir 3.0.8

Debugging em Meru

```
meruc(15)# station-log 78:7e:61:ae:c7:f3
Added station 78:7e:61:ae:c7:f3 at position 0
Interactive Per-Station Event Logging Shell (enter "help" for help)
By default logging is Disabled (enter "enable" to Enable logging)
station-log> enable
Logging enabled
station-log>

problemas...

2015-May-28 11:21:35.226522 | 78:7e:61:ae:c7:f2 | Band Steering          | Steering initiated to 5Ghz under steering policy = A, staType = ABGN
2015-May-28 11:21:35.879622 | 78:7e:61:ae:c7:f2 | Station Assign        | <AID=53> assigned to <AP_ID=33><ESSID=EDUROAM_1020><BSSID=00:
0c:e6:6a:34:9a><reason=Station probed>
2015-May-28 11:21:35.879680 | 78:7e:61:ae:c7:f2 | Station Assign        | Reassigning from <AP_ID=33>(rssi=-85) to <AP_ID=113>(rssi=-58)
<ESSID=EDUROAM_1020><BSSID=00:0c:e6:6a:34:9a>
2015-May-28 11:21:35.879736 | 78:7e:61:ae:c7:f2 | Station Assign        | <AID=53> Assign Removed From
<AP_ID=33><ESSID=EDUROAM_1020><BSSID=00:0c:e6:6a:34:9a><reason=Probe RSSI handoff>
2015-May-28 11:21:35.881613 | 78:7e:61:ae:c7:f2 | Station Assign        | <AID=53> assigned to <AP_ID=113><ESSID=EDUROAM_1020><BSSID=00:
0c:e6:6a:34:9a><reason=Probe RSSI handoff>
2015-May-28 11:21:56.260462 | 78:7e:61:ae:c7:f2 | Band Steering          | Band steering disabled due to BandSteeringTimeout(5) expiry staType =
ABGN policy = A
2015-May-28 11:21:56.260537 | 78:7e:61:ae:c7:f2 | Station Assign        | <AID=100> assigned to
<AP_ID=113><ESSID=EDUROAM_1020><BSSID=00:0c:e6:6a:6e:bf><reason=Station probed>

normal....(manual)
```

```
station-log> enable
Logging enabled
2015-May-28 11:38:37.113660 | 78:7e:61:ae:c7:f2 | 802.11 State | state change <old=Associated><new=Associated><AP=00:0c:e6:12:0a:
a9><BSSID=00:0c:e6:6a:34:9a>
2015-May-28 11:38:37.677938 | 78:7e:61:ae:c7:f2 | 1X Authentication | <auth method=WPA2_EAP>:<pkt type=EAPOL_START> recvd
<ESSID=eduroam> <BSSID=00:0c:e6:6a:34:9a>
2015-May-28 11:38:37.678125 | 78:7e:61:ae:c7:f2 | 1X Authentication | <EAP code=request> <EAP ID=1> <EAP type=Identity> sent
2015-May-28 11:38:37.684899 | 78:7e:61:ae:c7:f2 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=response><EAP ID=1>
2015-May-28 11:38:37.684985 | 78:7e:61:ae:c7:f2 | 1X Authentication | Radius <msg code=access_request><msg ID=174> sent <ip=193.136.188.36>:
<port=1812>
2015-May-28 11:38:37.685894 | 78:7e:61:ae:c7:f2 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=request><EAP ID=2> <info=relay eap-
request from Radius> sent
2015-May-28 11:38:37.699006 | 78:7e:61:ae:c7:f2 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=response><EAP ID=2>
2015-May-28 11:38:37.699095 | 78:7e:61:ae:c7:f2 | 1X Authentication | Radius <msg code=access_request><msg ID=175> sent <ip=193.136.188.36>:
<port=1812>
2015-May-28 11:38:37.702563 | 78:7e:61:ae:c7:f2 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=request><EAP ID=3> <info=relay eap-
request from Radius> sent
2015-May-28 11:38:37.808424 | 78:7e:61:ae:c7:f2 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=response><EAP ID=3>
2015-May-28 11:38:37.808515 | 78:7e:61:ae:c7:f2 | 1X Authentication | Radius <msg code=access_request><msg ID=176> sent <ip=193.136.188.36>:
<port=1812>
2015-May-28 11:38:37.809577 | 78:7e:61:ae:c7:f2 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=request><EAP ID=4> <info=relay eap-
request from Radius> sent
2015-May-28 11:38:37.872551 | 78:7e:61:ae:c7:f2 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=response><EAP ID=4>
2015-May-28 11:38:37.872649 | 78:7e:61:ae:c7:f2 | 1X Authentication | Radius <msg code=access_request><msg ID=177> sent <ip=193.136.188.36>:
<port=1812>
2015-May-28 11:38:37.874248 | 78:7e:61:ae:c7:f2 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=request><EAP ID=5> <info=relay eap-
request from Radius> sent
2015-May-28 11:38:37.943898 | 78:7e:61:ae:c7:f2 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=response><EAP ID=5>
2015-May-28 11:38:37.943992 | 78:7e:61:ae:c7:f2 | 1X Authentication | Radius <msg code=access_request><msg ID=178> sent <ip=193.136.188.36>:
<port=1812>
2015-May-28 11:38:37.944837 | 78:7e:61:ae:c7:f2 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=request><EAP ID=6> <info=relay eap-
request from Radius> sent
2015-May-28 11:38:37.952072 | 78:7e:61:ae:c7:f2 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=response><EAP ID=6>
2015-May-28 11:38:37.952152 | 78:7e:61:ae:c7:f2 | 1X Authentication | Radius <msg code=access_request><msg ID=179> sent <ip=193.136.188.36>:
<port=1812>
2015-May-28 11:38:37.952857 | 78:7e:61:ae:c7:f2 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=request><EAP ID=7> <info=relay eap-
request from Radius> sent
2015-May-28 11:38:38.071666 | 78:7e:61:ae:c7:f2 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=response><EAP ID=7>
2015-May-28 11:38:38.071758 | 78:7e:61:ae:c7:f2 | 1X Authentication | Radius <msg code=access_request><msg ID=181> sent <ip=193.136.188.36>:
<port=1812>
2015-May-28 11:38:38.095303 | 78:7e:61:ae:c7:f2 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=request><EAP ID=8> <info=relay eap-
request from Radius> sent
2015-May-28 11:38:38.130462 | 78:7e:61:ae:c7:f2 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=response><EAP ID=8>
2015-May-28 11:38:38.130550 | 78:7e:61:ae:c7:f2 | 1X Authentication | Radius <msg code=access_request><msg ID=182> sent <ip=193.136.188.36>:
<port=1812>
2015-May-28 11:38:38.138752 | 78:7e:61:ae:c7:f2 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=request><EAP ID=9> <info=relay eap-
request from Radius> sent
2015-May-28 11:38:38.149445 | 78:7e:61:ae:c7:f2 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=response><EAP ID=9>
2015-May-28 11:38:38.149526 | 78:7e:61:ae:c7:f2 | 1X Authentication | Radius <msg code=access_request><msg ID=183> sent <ip=193.136.188.36>:
<port=1812>
2015-May-28 11:38:38.151915 | 78:7e:61:ae:c7:f2 | 1X Authentication | Radius ACCESS-ACCEPT received : Session Timeout: None, VLAN Tag : 211,
Filter id : , CUI : None
2015-May-28 11:38:38.152024 | 78:7e:61:ae:c7:f2 | 1X Authentication | <pkt type=EAP_PACKET> <EAP code=success><EAP ID=9> <info=relay eap-
request from Radius> sent
2015-May-28 11:38:38.153357 | 78:7e:61:ae:c7:f2 | 1X Authentication | M1 <msg type=EAPOL_KEY> PTK sent
2015-May-28 11:38:38.160512 | 78:7e:61:ae:c7:f2 | 1X Authentication | M2 <pkt type=EAPOL_KEY> MIC Verified
2015-May-28 11:38:38.160771 | 78:7e:61:ae:c7:f2 | 1X Authentication | M3 <msg type=EAPOL_KEY> WPA2 PTK Negotiation sent
2015-May-28 11:38:38.165620 | 78:7e:61:ae:c7:f2 | 1X Authentication | M4 <pkt type=EAPOL_KEY> <key type=Unicast Key> Key Pairwise
2015-May-28 11:38:38.175907 | 78:7e:61:ae:c7:f2 | DHCP | <msg_type=REQUEST><server_ip=255.255.255.255><server_mac=ff:ff:ff:ff:ff:
ff><client_ip=0.0.0.0>
2015-May-28 11:38:38.177498 | 78:7e:61:ae:c7:f2 | DHCP | <msg_type=ACK><server_ip=10.10.20.4><gateway_ip=172.17.16.1><offered_ip=172.
17.18.104>
```

Links úteis

https://wiki.terena.org/display/H2eduroam/freeradius3-flr (RadSec em FR 3)

https://confluence.fccn.pt/display/eduroam/RadSec

https://community.ja.net/groups/eduroam/document/nws-40-freeradius-demystified

Migração de freeradius 2.x para 3.x - https://github.com/FreeRADIUS/freeradius-server/blob/v3.0.x/raddb/README.rst

https://github.com/nmav/radiusclient-dtls

FreeRADIUS Beginner´s Guide, Dirk van der Walt - http://www.amazon.com/FreeRADIUS-Beginners-Guide-Dirk-Walt/dp/1849514089

http://aureliengeron.free.fr/livrewifi/

http://en.wikipedia.org/wiki/Eduroam

http://en.wikipedia.org/wiki/FreeRADIUS

http://en.wikipedia.org/wiki/MS-CHAP

http://freeradius.1045715.n5.nabble.com/definitive-info-on-authenticating-to-AD-via-NTLMv2-td5719249.html

http://en.wikipedia.org/wiki/NT_LAN_Manager

http://en.wikipedia.org/wiki/Kerberos_(protocol)

http://en.wikipedia.org/wiki/Active_Directory

http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

http://en.wikipedia.org/wiki/RADIUS

http://en.wikipedia.org/wiki/RadSec

http://www.wiligear.com/wiki/index.php/Standard_RADIUS_Attributes

http://tools.ietf.org/html/rfc6929

http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

http://en.wikipedia.org/wiki/Protected_Extensible_Authentication_Protocol

http://en.wikipedia.org/wiki/EAP-TTLS#EAP-TTLS

http://en.wikipedia.org/wiki/IEEE_802.11

http://en.wikipedia.org/wiki/IEEE_802.1X

http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

https://confluence.terena.org/display/H2eduroam/%27How+to....%27+%28deploy%2C+promote+and+support%29+eduroam

http://www.scribd.com/doc/125531184/Eduroam-Acesso-sem-Fio-Seguro-para-Comunidade-Academica-Federada

https://wiki.terena.org/display/H2eduroam/EAP+Server+Certificate+considerations