



Assignment 2: Authentication, Authorization and Accounting

Segurança de Sistemas de Informação

João Figueiredo 1230194
João Tiago Araújo 1200584
Diogo Magalhães 1201100

Novembro 2023

Contents

1	Organização do Trabalho	2
1.1	Escolha das Opções do Trabalho pelos membros	2
2	Opção 1 - FreeRadius	3
2.1	Introdução	3
2.2	Configuração respetiva à P12	3
2.2.1	Criação de utilizadores e Grupos	6
2.3	Comando <code>radtest</code> para Autenticação RADIUS	7
2.3.1	Autenticação dos utilizadores	8
2.4	Configuração do FreeRadius de acordo com o assignment-2	9
2.4.1	Adição de Novos utilizadores e Grupos	9
2.4.2	Atribuição de Usuários a Grupos	9
2.4.3	Manutenção das Especificações Originais	12
2.5	Informações Adicionais sobre RADIUS	12
2.6	Conclusão	13
3	Opção 2 - Federated Radius	14
3.1	Introdução	14
3.2	Adicione os utilizadores Isaac e Moses ao Active Directory e os utilizadores Sara e Abraham ao FreeRadius	14
3.3	Permitir que todos os utilizadores façam o Login na máquina Linux	15
4	Opção 3 - LDAP	20
4.1	Introdução	20
4.2	Configuração OpenLDAP	20
4.3	Evidências	23
4.4	Conclusão	24

Chapter 1

Organização do Trabalho

1.1 Escolha das Opções do Trabalho pelos membros

Aluno	Opção do Trabalho
João Figueiredo 1230194	Opção 1 - FreeRadius
João Araújo 1200584	Opção 2 - Federated Radius
Diogo Magalhães 1201100	Opção 3 - LDAP

Table 1.1: Escolha das opções do trabalho pelos alunos.

Chapter 2

Opção 1 - FreeRadius

O Free Radius é uma implementação de código aberto do protocolo RADIUS. Ele fornece um servidor que pode ser usado para centralizar a gestão de autenticação, autorização e contabilidade (AAA) em uma rede.

O FreeRADIUS é altamente personalizável e extensível, tornando-o adequado para uma ampla variedade de cenários de autenticação. Suporta vários métodos de autenticação, incluindo PAP, CHAP, EAP, etc. O FreeRADIUS pode ser integrado a várias bases de dados e serviços de diretório para autenticação e autorização de utilizadores. É frequentemente usado em redes corporativas, fornecedores de serviços de Internet (ISPs) e outros ambientes onde sejam necessários serviços AAA centralizados.

2.1 Introdução

Neste relatório, descreverei a implementação do FreeRadius e a configuração realizada para atender a requisitos específicos. A implementação envolve a criação de utilizadores, grupos e a configuração do FreeRadius para autenticação diferenciada.

2.2 Configuração respetiva à Pl2

Começou-se por identificar a forma mais fácil e adequada de podermos introduzir utilizadores no sistema e associarmos aos mesmo, várias características, como grupo, se o aceitamos ou não.

Para realizar a instalação do FreeRadius no sistema operacional Ubuntu, o seguinte comando foi utilizado:

```
sudo apt-get install freeradius freeradius-mysql
```

Este comando instala o FreeRadius e o módulo MySQL, fornecendo suporte para a integração do FreeRadius com um banco de dados MySQL. Certifique-se

de que todas as dependências necessárias sejam satisfeitas durante o processo de instalação.

Através de extensa pesquisa, descobriu-se que o freeradius oferece suporte a várias base de dados. Eis uma lista de todas os tipos que são permitidos:

- sqlite
- postgresql
- oracle
- ndb
- mysql
- mssql
- mongo

Foi optado, o uso de mysql visto que a sua configuração é relativamente fácil. O freeradius, já fornece o schema da base de dados. Eis uma explicação das várias tabelas:

- **Tabela radacct:** Armazena informações sobre as contas do RADIUS, incluindo detalhes sobre a sessão, autenticação e uso de dados.
- **Tabela radcheck:** Contém informações de verificação (como senha) para autenticação dos usuários.
- **Tabela radgroupcheck:** Mantém informações específicas de grupos para verificar atributos de usuários.
- **Tabela radgroupreply:** Armazena informações de grupos, mas para respostas.
- **Tabela radreply:** Contém informações para respostas de autenticação para usuários específicos.
- **Tabela radusergroup:** Mantém informações sobre a associação de usuários a grupos.
- **Tabela radpostauth:** Armazena informações pós-autenticação, como detalhes de resposta e data de autenticação.
- **Tabela nas:** Contém informações sobre os servidores NAS (Network Access Server) que se comunicam com o FreeRadius.

Para, efetivamente, configurar o mysql no freeradius, o ficheiro, `/etc/freeradius/3.0/mods-available/sql.txt` foi editado de forma a permitir a interligação do freeradius ao mysql. Para além da associação tb estão presentes os dados de ligação.

```

sql {
    #
    # The dialect of SQL being used.
    #
    # Allowed dialects are:
    #
    #     mssql
    #     mysql
    #     oracle
    #     postgresql
    #     sqlite
    #     mongo
    #
    dialect = "mysql"

    #
    # The driver module used to execute the queries. Since we
    # don't know which SQL drivers are being used, the default is
    # "rlm_sql_null", which just logs the queries to disk via the
    # "logfile" directive, below.
    #
    # In order to talk to a real database, delete the next line,
    # and uncomment the one after it.
    #
    # If the dialect is "mssql", then the driver should be set to
    # one of the following values, depending on your system:
    #
    #     rlm_sql_db2
    #     rlm_sql_firebird
    #     rlm_sql_freetds
    #     rlm_sql_iodbc
    #     rlm_sql_unixodbc
    #
    # driver = "rlm_sql_null"
    driver = "rlm_sql_${dialect}"
}

```

Figure 2.1: SQL - Mysql

```

# Connection info:
#
server = "localhost"
port = 3306
login = "radius"
password = "radpass"

```

Figure 2.2: Informação de ligação Mysql

2.2.1 Criação de utilizadores e Grupos

Para atender aos requisitos, foram criados os seguintes utilizadores: Bob, Alice, John, Madeleine e Jake. Destes, o Bob e a Alice são utilizadores padrão, Madeleine é uma "accountant" e Jake é o administrador de IT. Eis a presença destes utilizadores na base de dados com os seus dados definidos

```
mysql> select * from radcheck;
```

id	username	attribute	op	value
1	Bob	Cleartext-Password	:=	password_bob
2	Alice	Cleartext-Password	:=	password_alice
3	John	Cleartext-Password	:=	password_john
4	Madeleine	Cleartext-Password	:=	password_madeleine
5	Jake	Cleartext-Password	:=	password_jake

Figure 2.3: Utilizadores da PL2

```
mysql> select * from radgroupcheck;
```

id	groupname	attribute	op	value
1	standard_users	Auth-Type	:=	Accept
2	accountant	Auth-Type	:=	Reject
3	IT_guy	Auth-Type	:=	Accept

Figure 2.4: Grupos da PL2

id	username	groupname	priority
1	Bob	standard_users	1
2	Alice	standard_users	1
3	Madeleine	accountant	1
4	Jake	IT_guy	1
5	Isaac	PU	1
6	Moses	PU	1
7	Sara	NPU	1
8	Abraham	NPU	1
9	John	standard_users	1

Figure 2.5: Utilizadores e grupos associados

2.3 Comando `radtest` para Autenticação RADIUS

A autenticação dos utilizadores é feita através do comando `radtest`. Aqui está uma breve explicação:

Exemplo de Utilização

```
radtest <username> <password> <radius-server>[:<port>] <radius-secret> <nas-port>
```

- `<username>`: Nome do usuário que está sendo autenticado.
- `<password>`: Senha associada ao usuário.
- `<radius-server>`: Endereço IP do servidor RADIUS.
- `<port>`: (Opcional) Porto do servidor RADIUS (normalmente 1812).
- `<radius-secret>`: Senha compartilhada entre o cliente e o servidor RADIUS.
- `<nas-port>`: Número da porta do dispositivo de acesso à rede.
- `<nas-port-id>`: (Opcional) Identificador da porta NAS.
- `<nas-ip>`: (Opcional) Endereço IP do NAS.
- `<nas-ipv6>`: (Opcional) Endereço IPv6 do NAS.

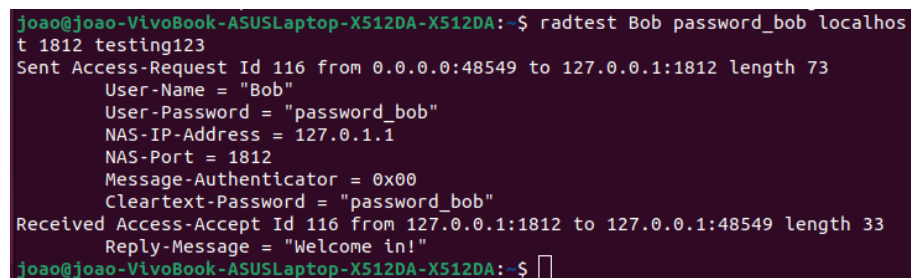
Exemplo Prático

```
radtest Alice password_alice 127.0.0.1 0 testing123
```

Neste exemplo, estamos testando a autenticação para o usuário Alice com a senha 'password_alice', usando um servidor RADIUS em 127.0.0.1, porta padrão 1812 e a senha compartilhada 'testing123'.

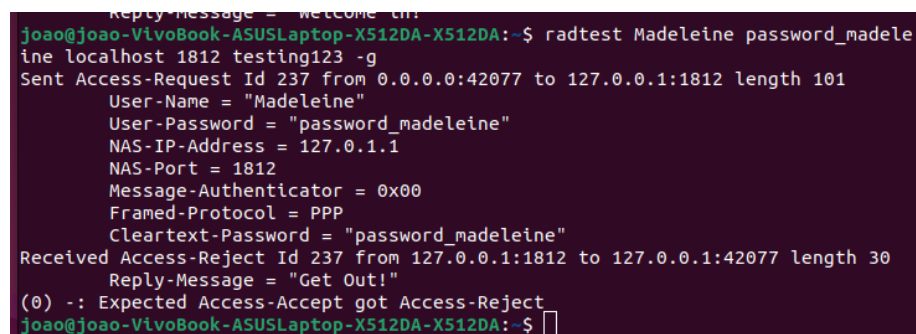
2.3.1 Autenticação dos utilizadores

Tal como mencionado no ex1 do guião respetivo à Pl2, o Bob e a Alice são utilizadores normais, a Madeleine é uma contabilista e o Jake é o administrador de IT. Posteriormente o radius foi configurado de forma a permitir a autenticação de todos os grupos exceto os administradores e os utilizadores normais. A autenticação dos utilizadores é feito através do comando radtest.



```
joao@joao-VivoBook-ASUSLaptop-X512DA-X512DA:~$ radtest Bob password_bob localhost 1812 testing123
Sent Access-Request Id 116 from 0.0.0.0:48549 to 127.0.0.1:1812 length 73
  User-Name = "Bob"
  User-Password = "password_bob"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 1812
  Message-Authenticator = 0x00
  Cleartext-Password = "password_bob"
Received Access-Accept Id 116 from 127.0.0.1:1812 to 127.0.0.1:48549 length 33
  Reply-Message = "Welcome in!"
joao@joao-VivoBook-ASUSLaptop-X512DA-X512DA:~$
```

Figure 2.6: RadTest do Bob



```
joao@joao-VivoBook-ASUSLaptop-X512DA-X512DA:~$ radtest Madeleine password_madeleine localhost 1812 testing123 -g
Sent Access-Request Id 237 from 0.0.0.0:42077 to 127.0.0.1:1812 length 101
  User-Name = "Madeleine"
  User-Password = "password_madeleine"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 1812
  Message-Authenticator = 0x00
  Framed-Protocol = PPP
  Cleartext-Password = "password_madeleine"
Received Access-Reject Id 237 from 127.0.0.1:1812 to 127.0.0.1:42077 length 30
  Reply-Message = "Get Out!"
(0) -: Expected Access-Accept got Access-Reject
joao@joao-VivoBook-ASUSLaptop-X512DA-X512DA:~$
```

Figure 2.7: Radtest da Madeleine

```

joao@joao-VivoBook-ASUSLaptop-X512DA-X512DA:~$ radtest Jake password_jake localh
ost 1812 testing123 -g
Sent Access-Request Id 36 from 0.0.0.0:38302 to 127.0.0.1:1812 length 80
    User-Name = "Jake"
    User-Password = "password_jake"
    NAS-IP-Address = 127.0.1.1
    NAS-Port = 1812
    Message-Authenticator = 0x00
    Framed-Protocol = PPP
    Cleartext-Password = "password_jake"
Received Access-Accept Id 36 from 127.0.0.1:1812 to 127.0.0.1:38302 length 45
    Framed-Protocol = PPP
    Framed-Compression = Van-Jacobson-TCP-IP
    Reply-Message = "Welcome in!"
joao@joao-VivoBook-ASUSLaptop-X512DA-X512DA:~$

```

Figure 2.8: RadTest do Jake

2.4 Configuração do FreeRadius de acordo com o assignment-2

2.4.1 Adição de Novos utilizadores e Grupos

Os utilizadores Isaac, Moses, Sara e Abraham foram adicionados à base de dados. Foram criados os grupos PU e NPU para diferenciar os privilégios dos utilizadores.

2.4.2 Atribuição de Usuários a Grupos

Isaac e Moses foram atribuídos ao grupo PU, enquanto Sara e Abraham foram associados ao grupo NPU. Isso garante que utilizadores no grupo PU tenham privilégios administrativos, enquanto os do grupo NPU possuam apenas permissões não administrativas.

```
mysql> select * from radcheck;
```

id	username	attribute	op	value
1	Bob	Cleartext-Password	:=	password_bob
2	Alice	Cleartext-Password	:=	password_alice
3	John	Cleartext-Password	:=	password_john
4	Madeleine	Cleartext-Password	:=	password_madeleine
5	Jake	Cleartext-Password	:=	password_jake
6	Isaac	Cleartext-Password	:=	password_isaac
7	Moses	Cleartext-Password	:=	password_moses
8	Sara	Cleartext-Password	:=	password_sara
9	Abraham	Cleartext-Password	:=	password_abraham

Figure 2.9: Novos Utilizadores

```
mysql> select * from radgroupcheck;
```

id	groupname	attribute	op	value
1	standard_users	Auth-Type	:=	Accept
2	accountant	Auth-Type	:=	Reject
3	IT_guy	Auth-Type	:=	Accept
6	PU	Group-Name	:=	Administrator
7	NPU	Group-Name	:=	Non-Administrator

Figure 2.10: Novos Grupos

```
mysql> select * from radusergroup;
```

id	username	groupname	priority
1	Bob	standard_users	1
2	Alice	standard_users	1
3	Madeleine	accountant	1
4	Jake	IT_guy	1
5	Isaac	PU	1
6	Moses	PU	1
7	Sara	NPU	1
8	Abraham	NPU	1
9	John	standard_users	1

Figure 2.11: Mapeamento de Utilizadores com os grupos

```
mysql> select * from radgroupreply;
```

id	groupname	attribute	op	value
1	standard_users	Reply-Message	:=	Welcome in!
2	accountant	Reply-Message	:=	Get Out!
3	IT_guy	Reply-Message	:=	Welcome in!
4	PU	Reply-Message	:=	Welcome, you have privileges of an Administrator!
5	NPU	Reply-Message	:=	Welcome, you have privileges of an Non-Administrator

Figure 2.12: Mensagem de reply de acordo com o grupo do utilizador

```

Reply-Message = Welcome, lin
joao@joao-VivoBook-ASUSLaptop-X512DA-X512DA:~$ radtest Sara password_sara localh
ost 1812 testing123 -g
Sent Access-Request Id 147 from 0.0.0.0:45233 to 127.0.0.1:1812 length 80
  User-Name = "Sara"
  User-Password = "password_sara"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 1812
  Message-Authenticator = 0x00
  Framed-Protocol = PPP
  Cleartext-Password = "password_sara"
Received Access-Accept Id 147 from 127.0.0.1:1812 to 127.0.0.1:45233 length 86
  Framed-Protocol = PPP
  Framed-Compression = Van-Jacobson-TCP-IP
  Reply-Message = "Welcome, you have privileges of an Non-Administrator"
joao@joao-VivoBook-ASUSLaptop-X512DA-X512DA:~$

```

Figure 2.13: Radtest da Sara

```

Reply-Message = Welcome, you have privileges of an Non-Administrator
joao@joao-VivoBook-ASUSLaptop-X512DA-X512DA:~$ radtest Isaac password_isaac loca
lhost 1812 testing123 -g
Sent Access-Request Id 55 from 0.0.0.0:34322 to 127.0.0.1:1812 length 81
  User-Name = "Isaac"
  User-Password = "password_isaac"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 1812
  Message-Authenticator = 0x00
  Framed-Protocol = PPP
  Cleartext-Password = "password_isaac"
Received Access-Accept Id 55 from 127.0.0.1:1812 to 127.0.0.1:34322 length 83
  Framed-Protocol = PPP
  Framed-Compression = Van-Jacobson-TCP-IP
  Reply-Message = "Welcome, you have privileges of an Administrator!"
joao@joao-VivoBook-ASUSLaptop-X512DA-X512DA:~$

```

Figure 2.14: Radtest do Isaac

2.4.3 Manutenção das Especificações Originais

Os utilizadores criados inicialmente (Bob, Alice, John e Madeleine) foram mantidos sem alteração em suas especificações, garantindo consistência no ambiente.

2.5 Informações Adicionais sobre RADIUS

Nesta seção, forneceremos informações adicionais sobre o RADIUS que podem ser relevantes para o entendimento geral do sistema.

RADIUS (Remote Authentication Dial-In User Service)

O RADIUS é um protocolo padrão para autenticação, autorização e contabilidade (AAA) em redes. Aqui estão algumas informações adicionais:

- **AAA Paradigma:** O RADIUS segue o paradigma AAA, que envolve Autenticação, Autorização e Contabilidade. Ele é amplamente utilizado em ambientes de rede para controlar o acesso de usuários.
- **Portas Padrão:** As portas padrão usadas pelo RADIUS são 1812 para autenticação e 1813 para contabilidade. Essas portas podem variar dependendo da configuração do servidor.
- **Segurança:** O RADIUS usa uma abordagem de compartilhamento de segredo para garantir a segurança nas comunicações entre o cliente RADIUS e o servidor RADIUS. Isso ajuda a evitar acesso não autorizado.
- **Contabilidade:** Além da autenticação, o RADIUS fornece recursos de contabilidade para registrar informações sobre o uso da rede pelos usuários. Isso inclui detalhes como tempo de sessão, dados transferidos e muito mais.
- **Extensibilidade:** O RADIUS é projetado para ser extensível, permitindo a adição de novos atributos para atender a requisitos específicos do ambiente.
- **Compatibilidade com Diversos Protocolos:** Embora tenha sido inicialmente desenvolvido para autenticação de discagem, o RADIUS é agora usado em uma variedade de cenários, incluindo redes sem fio, VPNs e redes corporativas.

Estas são apenas algumas informações adicionais para fornecer um contexto mais amplo sobre o RADIUS. Dependendo das necessidades do seu projeto, você pode incluir informações mais específicas ou personalizadas.

2.6 Conclusão

A implementação bem-sucedida do FreeRadius, juntamente com a configuração cuidadosa de utilizadores e grupos, foi de encontro com os requisitos estabelecidos. A diferenciação de privilégios entre grupos e a restrição de autenticação contribuem para a segurança e eficiência do sistema.

Chapter 3

Opção 2 - Federated Radius

3.1 Introdução

Federated Radius refere-se ao conceito de interconexão de vários servidores Radius numa arquitetura federada. Isto permite o compartilhamento de informações de autenticação e autorização entre diferentes domínios ou realms.

Numa configuração de Federated Radius, cada organização ou domínio participante opera seu próprio servidor Radius. Os servidores Radius são configurados para confiar uns nos outros, permitindo que utilizadores de um domínio autenticuem e acessem recursos em outro domínio sem precisar criar e gerir contas de utilizadores duplicadas. O Federated Radius é frequentemente usado em cenários em que as organizações desejam fornecer acesso contínuo e seguro a recursos para utilizadores de diferentes domínios ou quando há necessidade de colaboração entre diversas entidades.

Active Directory (AD) é um serviço de diretório desenvolvido pela Microsoft para redes de domínio Windows. É um componente crucial do sistema operativo Windows Server e desempenha um papel central na gestão e organização de recursos em uma rede. O Active Directory fornece uma maneira centralizada e padronizada de gerir e autenticar recursos de rede, facilitando aos administradores o controlo de acesso e das permissões de utilizadores e dispositivos.

3.2 Adicione os utilizadores Isaac e Moses ao Active Directory e os utilizadores Sara e Abraham ao FreeRadius

Para demonstrar a existência do Active Directory foi efetuado o comando "Get-ADDomainController -Discover" na PowerShell do Windows Server criado e configurado na PL3, no resultado é apresentado domínio criado como demonstra a figura 3.1.

```
PS C:\Users\Administrator> Get-ADDomainController -Discover

Domain       : projeto.segsi
Forest       : projeto.segsi
HostName     : {WIN-SEGSI.projeto.segsi}
IPv4Address  : 192.168.0.4
IPv6Address  :
Name         : WIN-SEGSI
Site         : Default-First-Site-Name
```

Figure 3.1: AD Domain

De seguida foram adicionados ao Active Directory os utilizadores Isaac e Moses através do comando "New-ADUser" com os parâmetros do nome, nome de logon e password como mostra nas duas seguintes figuras.

```
Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PS C:\Users\Administrator> New-ADUser -Name "Isaac" -SamAccountName "isaac" -AccountPassword(Read-Host -AsSecureString "Password") -Enabled $true
Password: *****
```

Figure 3.2: Adicionar Isaac ao AD

```
PS C:\Users\Administrator> New-ADUser -Name "Moses" -SamAccountName "moses" -AccountPassword(Read-Host -AsSecureString "Password") -Enabled $true
```

Figure 3.3: Adicionar Moses ao AD

De modo a verificar a existência dos utilizadores anteriormente criados foi executado o comando "Get-ADUser" com o nome à frente. (Figura 3.4 e 3.5)

Para adicionar os utilizadores "Sara" e "Abraham" ao Free Radius configurado na PL2, é efetuado o comando "sudo mysql -u root -p radius" de forma a aceder à base de dados "radius" que contém os utilizadores do Free Radius.

De seguida foram efetuadas as queries SQL de "INSERT" na tabela "rad-check" para introduzir os utilizadores na base de dados.

3.3 Permitir que todos os utilizadores façam o Login na máquina Linux

Com o comando "radtest" é possível testar a autenticação com o RADIUS, para isso é executado o comando com o utilizador, password, a PORT 1812


```
Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PS C:\Users\Administrator> Get-ADUser isaac

DistinguishedName : CN=Isaac,CN=Users,DC=vdom,DC=local
Enabled           : False
GivenName        :
Name             : Isaac
ObjectClass      : user
ObjectGUID       : 659a2257-65fa-492b-99db-ffa1eda48b4c
SamAccountName   : isaac
SID              : S-1-5-21-2452056864-3241267430-1040679499-1103
Surname          :
UserPrincipalName :
```

Figure 3.4: Ver o utilizador Isaac no AD

```
Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PS C:\Users\Administrator> Get-ADUser isaac

DistinguishedName : CN=Isaac,CN=Users,DC=vdom,DC=local
Enabled           : False
GivenName        :
Name             : Isaac
ObjectClass      : user
ObjectGUID       : 659a2257-65fa-492b-99db-ffa1eda48b4c
SamAccountName   : isaac
SID              : S-1-5-21-2452056864-3241267430-1040679499-1103
Surname          :
UserPrincipalName :
```

Figure 3.5: Ver o utilizador Moses no AD

(Port de autenticação) e o secret para os dois utilizadores anteriormente criados no RADIUS (Sara e Abraham) como é possível observar na Figura 3.9.

Com o comando "realm", da package realmd é possível entrar no domínio e criar a configuração sssd. (Fig 3.10). Após isso é feito o "join" ao domínio "projeto.segsi" criado no Windows Server. (Fig 3.11)

Por fim para verificar na máquina Linux os utilizadores criados no Active Directory, executa-se o comando "getent passwd" e o nome com o domínio AD. (Fig 3.11 e Fig 3.12)

Para verificar os grupos dos utilizadores de AD é efetuado o comando "groups" seguido do nome e domínio AD. (Fig 3.14 e 3.15)

Por fim são executados os comandos "id" no Linux com o nome e domínio AD e onde é possível observar os id's do utilizador e grupos.

```
root@UbuntuDesktop:~# sudo mysql -u root -p radius
```

Figure 3.6: MySQL Radius

```

root@UbuntuDesktop:~# sudo mysql -u root -p radius
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 449
Server version: 10.6.12-MariaDB-0ubuntu0.22.04.1 Ubuntu 22.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [radius]> INSERT INTO radcheck (username, attribute, op, value) VALUES ('Sara', 'Cleartext-Password', '=', 'Sara123!');

```

Figure 3.7: Adicionar Sara ao Free Radius

```

MariaDB [radius]> INSERT INTO radcheck (username, attribute, op, value) VALUES ('Abraham', 'Cleartext-Password', '=', 'Abraham123!');

```

Figure 3.8: Adicionar Abraham ao Free Radius

```

root@UbuntuDesktop:/home/ubuntuadmin# radtest Sara Sara123! localhost 1812 testing123
Sent Access-Request Id 3 from 0.0.0.0:48007 to 127.0.0.1:1812 length 74
  User-Name = "Sara"
  User-Password = "Sara123!"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 1812
  Message-Authenticator = 0x00
  Cleartext-Password = "Sara123!"
Received Access-Accept Id 3 from 127.0.0.1:1812 to 127.0.0.1:48007 length 20
root@UbuntuDesktop:/home/ubuntuadmin# radtest Abraham Abraham123! localhost 1812 testing123
Sent Access-Request Id 76 from 0.0.0.0:43474 to 127.0.0.1:1812 length 77
  User-Name = "Abraham"
  User-Password = "Abraham123!"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 1812
  Message-Authenticator = 0x00
  Cleartext-Password = "Abraham123!"
Received Access-Accept Id 76 from 127.0.0.1:1812 to 127.0.0.1:43474 length 20
root@UbuntuDesktop:/home/ubuntuadmin#

```

Figure 3.9: Radtest

```

root@UbuntuDesktop:/home/ubuntuadmin# realm -v discover projeto.segsi
* Resolving: _ldap._tcp.projeto.segsi
* Performing LDAP DSE lookup on: 192.168.0.4
* Successfully discovered: projeto.segsi
projeto.segsi
  type: kerberos
  realm-name: PROJETO.SEGSI
  domain-name: projeto.segsi
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
  login-formats: %U@projeto.segsi
  login-policy: allow-realm-logins

```

Figure 3.10: Realm Discovery

```

root@UbuntuDesktop:/home/ubuntuadmin# realm -v join projeto.segsi
* Resolving: _ldap._tcp.projeto.segsi
* Performing LDAP DSE lookup on: 192.168.0.4
* Successfully discovered: projeto.segsi
realm: Already joined to this domain

```

Figure 3.11: Realm Join

```

root@UbuntuDesktop:/home/ubuntuadmin# getent passwd moses@projeto.segsi
moses@projeto.segsi:*:1558801109:1558800513:Moses:/home/moses@projeto.segsi:/bin/bash

```

Figure 3.12: Utilizador Moses

```

root@UbuntuDesktop:/home/ubuntuadmin# getent passwd isaac@projeto.segsi
isaac@projeto.segsi:*:1558801106:1558800513:Isaac:/home/isaac@projeto.segsi:/bin/bash

```

Figure 3.13: Utilizador Isaac

```

root@UbuntuDesktop:/home/ubuntuadmin# groups moses@projeto.segsi
moses@projeto.segsi : domain users@projeto.segsi

```

Figure 3.14: Grupos Moses

```
root@UbuntuDesktop:/home/ubuntuadmin# groups isaac@projeto.segsi
isaac@projeto.segsi : domain users@projeto.segsi
```

Figure 3.15: Grupos Isaac

```
root@UbuntuDesktop:/home/ubuntuadmin# id isaac@projeto.segsi
uid=1558801106(isaac@projeto.segsi) gid=1558800513(domain users@projeto.segsi) groups=1558800513(domain users@projeto.segsi)
root@UbuntuDesktop:/home/ubuntuadmin# id moises@projeto.segsi
uid=1558801109(moses@projeto.segsi) gid=1558800513(domain users@projeto.segsi) groups=1558800513(domain users@projeto.segsi)
```

Figure 3.16: Id's

```
1 # /etc/nsswitch.conf
2 #
3 # Example configuration of GNU Name Service Switch functionality.
4 # If you have the 'glibc-doc-reference' and 'info' packages installed, try:
5 # 'info libc "Name Service Switch"' for information about this file.
6
7 passwd:          files systemd sss
8 group:           files systemd sss
```

Figure 3.17: nsswitch.conf

Chapter 4

Opção 3 - LDAP

LDAP é um protocolo utilizado para aceder e gerir serviços de informação de diretórios. Um serviço de diretório é uma base de dados centralizada que armazena e organiza informações sobre utilizadores, recursos e outros objetos dentro de uma rede. O LDAP é projetado como um protocolo leve para aceder a serviços de diretórios através de uma rede TCP/IP. **OpenLDAP** é uma implementação de código aberto do LDAP. O OpenLDAP fornece uma alternativa gratuita e de código aberto para organizações e indivíduos que procuram implementar serviços de diretórios baseados em LDAP.

4.1 Introdução

Nas próximas secções deste documento, será descrito a implementação do OpenLDAP e a configuração do servidor e cliente. A implementação consiste na criação dos utilizadores e grupos que foram propostos no trabalho.

4.2 Configuração OpenLDAP

A configuração do servidor e cliente do OpenLDAP foi realizada com o uso de Virtual Machines em Linux com as seguintes informações:

Servidor

- **Endereço de IP:** 192.168.1.108
- **Hostname:** server
- **Domain:** g07.segsi.mei.isep.ipp.pt
- **FQDN:** server.g07.segsi.mei.isep.ipp.pt

Cliente

- **Endereço de IP:** 192.168.1.10

```

127.0.0.1      localhost
127.0.1.1      server.g07.segsi.mei.isep.ipp.pt server

192.168.1.108  server.g07.segsi.mei.isep.ipp.pt  server

# The following lines are desirable for IPv6 capable hosts
::1          ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

```

Figure 4.1: Hosts do servidor

```

127.0.0.1      localhost
127.0.1.1      client.g07.segsi.mei.isep.ipp.pt
192.168.1.107  client.g07.segsi.mei.isep.ipp.pt client
192.168.1.108  server.g07.segsi.mei.isep.ipp.pt

# The following lines are desirable for IPv6 capable hosts
::1          ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

```

Figure 4.2: Hosts do cliente

- **Hostname:** client
- **Domain:** g07.segsi.mei.isep.ipp.pt
- **FQDN:** client.g07.segsi.mei.isep.ipp.pt

A criação de utilizadores e grupos foi realizada com o auxílio do LDAP Account Manager(LAM). O LAM é uma interface web para gerir entradas (como utilizadores, grupos, configurações DHCP, etc.) armazenadas num diretório LDAP. Assim, foram criados os grupos Privileged Users (PU) e Non-Privileged-Users (NPU), com os utilizadores Isaac and Moses no grupo PU e os utilizadores Sara e Abraham no grupo NPU.

Primeiramente, são criados os dois main OUs People e Grupos como pode ser visto na seguinte figura.

De seguida, foram criados os OUs dos grupos pretendidos no ou=People. Já no ou=Groups foram criados os grupos PU e NPU.

LAM Login

User name: admin

Password:

Language: English (Great Britain)

Login

LDAP server: ldap://localhost:389

Server profile: lam

Figure 4.3: enu de Login do LAM

```
dn: ou=People,dc=g07,dc=segsi,dc=mei,dc=isep,dc=ipp,dc=pt
objectClass: organizationalUnit
ou: People
structuralObjectClass: organizationalUnit
entryUUID: e34a83e8-20fc-103e-88b2-e15b691ca047
creatorsName: cn=admin,dc=g07,dc=segsi,dc=mei,dc=isep,dc=ipp,dc=pt
createTimestamp: 20231126231134Z
entryCSN: 20231126231134.821912Z#000000#000#000000
modifiersName: cn=admin,dc=g07,dc=segsi,dc=mei,dc=isep,dc=ipp,dc=pt
modifyTimestamp: 20231126231134Z

dn: ou=Groups,dc=g07,dc=segsi,dc=mei,dc=isep,dc=ipp,dc=pt
objectClass: organizationalUnit
ou: Groups
structuralObjectClass: organizationalUnit
entryUUID: e34c7ff4-20fc-103e-88b3-e15b691ca047
creatorsName: cn=admin,dc=g07,dc=segsi,dc=mei,dc=isep,dc=ipp,dc=pt
createTimestamp: 20231126231134Z
entryCSN: 20231126231134.834953Z#000000#000#000000
modifiersName: cn=admin,dc=g07,dc=segsi,dc=mei,dc=isep,dc=ipp,dc=pt
modifyTimestamp: 20231126231134Z
```

Figure 4.4: Criação de OUs

OU editor

New OU created successfully.

New organisational unit

Parent DN: People > g07 > segsi > mei > isep > ipp > pt

Name: NPU

Ok

Figure 4.5: Criação de OU dos grupos







Actions	Group name	GID number	Group members	Group description
Sort sequence ▼▲				
<input type="checkbox"/> Filter ?				
<input type="checkbox"/>   	NPU	10001		Group NPU
<input type="checkbox"/>   	PU	10000		Group PU

Figure 4.6: Grupos

Após a criação dos grupos foi realizada a criação dos utilizadores nos grupos pretendidos.

Resultando assim na seguinte árvore de utilizadores e grupos.

4.3 Evidências

Confirmação da criação dos utilizadores e dos grupos utilizando o comando sudo slapcat.

Para confirmar que ambas as Virtual Machines estão a comunicar foi realizado um ping do client para o servidor.

Isaac

Suffix: PU > People > g07 > segsi > mei > isep > ipp > pt

RDN identifier: cn

Personal

Unix

Shadow

User name: isaac

Common name: isaac

UID number: 10000

Gecos:

Primary group: PU

Create group with same name

Additional groups: Edit groups

Home directory: /home/isaac

Login shell: /bin/bash

Figure 4.7: Criação do Isaac

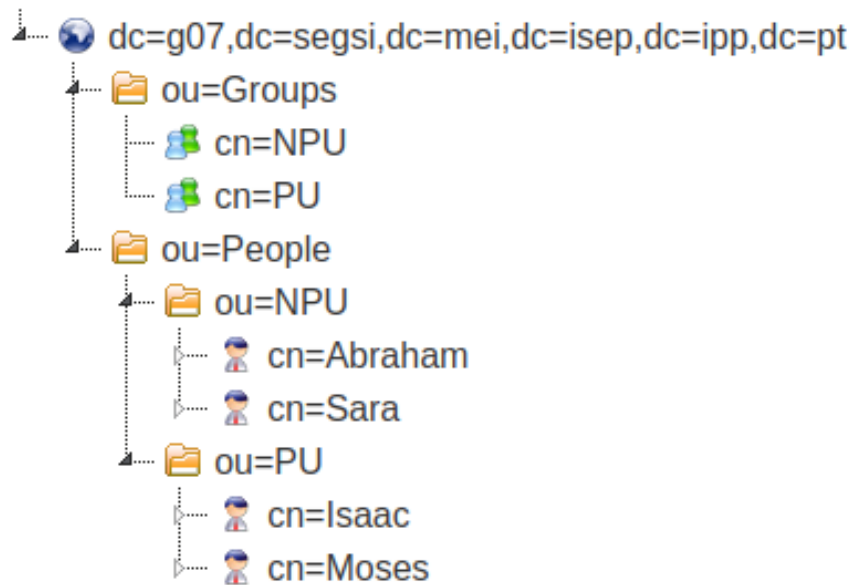


Figure 4.8: Tree View dos grupos e utilizadores

Foi realizado um `ldapsearch` no ambiente do cliente para o servidor para confirmar que o cliente consegue realizar uma query.

Outra forma de validar a conexão foi através de um `sudo login` no ambiente do servidor com os dados utilizador Isaac.

4.4 Conclusão

A conclusão destaca a bem-sucedida implementação do OpenLDAP, evidenciando a criação de utilizadores e grupos, a validação da comunicação entre servidor e cliente, e a capacidade de realizar queries LDAP. Esses passos fundamentais são essenciais para estabelecer e verificar a funcionalidade de um diretório LDAP em um ambiente de rede.

```

dn: cn=NPU,ou=Groups,dc=g07,dc=segsi,dc=mei,dc=isep,dc=ipp,dc=pt
objectClass: posixGroup
description: Group NPU
gidNumber: 10001
structuralObjectClass: posixGroup
entryUUID: 768ede14-20fe-103e-88b8-e15b691ca047
creatorsName: cn=admin,dc=g07,dc=segsi,dc=mei,dc=isep,dc=ipp,dc=pt
createTimestamp: 20231126232251Z
cn: NPU
entryCSN: 20231126232500.005594Z#000000#000#000000
modifiersName: cn=admin,dc=g07,dc=segsi,dc=mei,dc=isep,dc=ipp,dc=pt
modifyTimestamp: 20231126232500Z

dn: cn=Isaac,ou=PU,ou=People,dc=g07,dc=segsi,dc=mei,dc=isep,dc=ipp,dc=pt
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
loginShell: /bin/bash
homeDirectory: /home/isaac
uid: isaac
cn: Isaac
uidNumber: 10000
gidNumber: 10000
userPassword:: e1NTSEF90UhxSFI0RW52a3ZKME9meGp1VXE0TEgwWmLSUnJqRnI=
sn: Isaac
structuralObjectClass: inetOrgPerson
entryUUID: 7a3211c0-20ff-103e-88b9-e15b691ca047
creatorsName: cn=admin,dc=g07,dc=segsi,dc=mei,dc=isep,dc=ipp,dc=pt
createTimestamp: 20231126233006Z
entryCSN: 20231126233006.991161Z#000000#000#000000
modifiersName: cn=admin,dc=g07,dc=segsi,dc=mei,dc=isep,dc=ipp,dc=pt
modifyTimestamp: 20231126233006Z

```

Figure 4.9: Peça do Output do sudo slapcat

```

client@client:~$ ping server.g07.segsi.mei.isep.ipp.pt
PING server.g07.segsi.mei.isep.ipp.pt (192.168.1.109) 56(84) bytes of data:
64 bytes from server.g07.segsi.mei.isep.ipp.pt (192.168.1.109): icmp_seq=1 ttl=64 time=3.51 ms
64 bytes from server.g07.segsi.mei.isep.ipp.pt (192.168.1.109): icmp_seq=2 ttl=64 time=1.56 ms
64 bytes from server.g07.segsi.mei.isep.ipp.pt (192.168.1.109): icmp_seq=3 ttl=64 time=1.24 ms
64 bytes from server.g07.segsi.mei.isep.ipp.pt (192.168.1.109): icmp_seq=4 ttl=64 time=1.26 ms
^C
--- server.g07.segsi.mei.isep.ipp.pt ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3018ms
rtt min/avg/max/mdev = 1.242/1.890/3.505/0.940 ms

```

Figure 4.10: Ping Client - Servidor

```

client@client:~$ ldapsearch -x -H ldap://192.168.1.109 -b "dc=g07,dc=segsi,dc=mei,dc=isep,dc=ipp,dc=pt"
# extended LDIF
#
# LDAPv3
# base <dc=g07,dc=segsi,dc=mei,dc=isep,dc=ipp,dc=pt> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# g07.segsi.mei.isep.ipp.pt
dn: dc=g07,dc=segsi,dc=mei,dc=isep,dc=ipp,dc=pt
objectClass: top
objectClass: dcObject
objectClass: organization
o: g07.segsi.mei.isep.ipp.pt
dc: g07

# People, g07.segsi.mei.isep.ipp.pt
dn: ou=People,dc=g07,dc=segsi,dc=mei,dc=isep,dc=ipp,dc=pt
objectClass: organizationalUnit
ou: People

# Groups, g07.segsi.mei.isep.ipp.pt
dn: ou=Groups,dc=g07,dc=segsi,dc=mei,dc=isep,dc=ipp,dc=pt
objectClass: organizationalUnit
ou: Groups

# PU, People, g07.segsi.mei.isep.ipp.pt
dn: ou=PU,ou=People,dc=g07,dc=segsi,dc=mei,dc=isep,dc=ipp,dc=pt
objectClass: organizationalUnit
ou: PU

```

Figure 4.11: Query Cliente

```

client@client:~$ sudo login
client login: Isaac
Password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-37-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: dom nov 26 02:46:25 WET 2023 on pts/1

```

Figure 4.12: Login Isaac