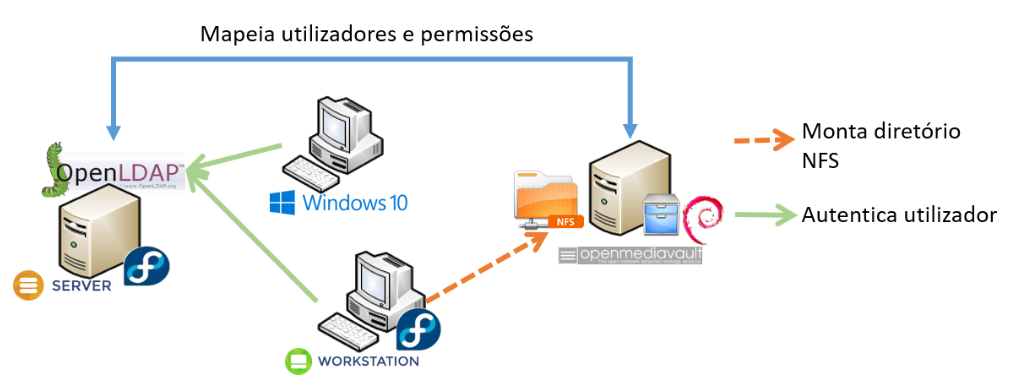
Trabalho sobre LDAP

Tiago Coelho <up201604170> Vasco Soares <up201604364> Nuno Nunes <201606441>

**1 Introdução**

O objetivo deste trabalho prático consiste na definição e implementação de um sistema de informação de diretório baseado em LDAP/NFS para autenticação e exportação de diretórios, de acordo com a imagem seguinte:

Para tal se verificar, é necessário cumprir todo um conjunto de configurações as quais iremos aprofundar nos tópicos que se seguem.

**2 LDAP**

É através do OpenLDAP, uma implementação *open source* do LDAP, que o servidor (10.0.0.1) vai conseguir autenticar os utilizadores nas máquinas Desktop e Win10 (10.0.0.2 e 10.0.0.3 respetivamente), assim como saber quais os diretórios a montar do utilizador autenticado.

Utilizando uma configuração de exemplo como base, foram configuradas as passwords de root e Manager, alterado olcSuffic para dc=admins,dc=ads,dc=dcc, assim como o DN do gestor para ficar de acordo com o novo sufixo.

A nível de permissões associadas aos logs, configuramos o acesso de leitura aos próprios logs de um utilizador autenticado, acesso de escrita ao Manager e nenhuma permissão para os restantes.

No entanto, as permissões de acesso á BD foram configuradas como: permissão de escrita para o Manager, e de leitura para os restantes.

Foram também alteradas as permissões de acesso e mudança de password da seguinte forma: Permissões de escrita para o Manager, permissões de autenticação para anonymous, permissões de escrita para o próprio utilizador e nenhuma permissão para os restantes.

A base de dados possui 3 utilizadores, 3 grupos e 2 unidades organizacionais. Os utilizadores são identificados pelos uids user1, user2, user3, sendo que cada um pertence apenas a um posixGroup com um cn igual ao seu próprio uid (ex: uid=user1 é membro do grupo cn=user1,...).

As unidades organizacionais criadas são identificadas por ou=Administrativos e ou=Developers, sendo que o utilizador user1 e o seu respetivo grupo pertencem aos Administrativos enquanto os user2 e user3 e os seus grupos pertencem aos Developers.

Por fim, de modo a garantir a segurança no acesso, foi necessário o uso de TLS para a cifragem de ligações. Foi criado um certificado self-signed e o LDAP foi configurado no servidor de modo a utilizar esse certificado e no Desktop e Win10 de modo a confiar nesse certificado.

**3 Arquitetura Utilizada**

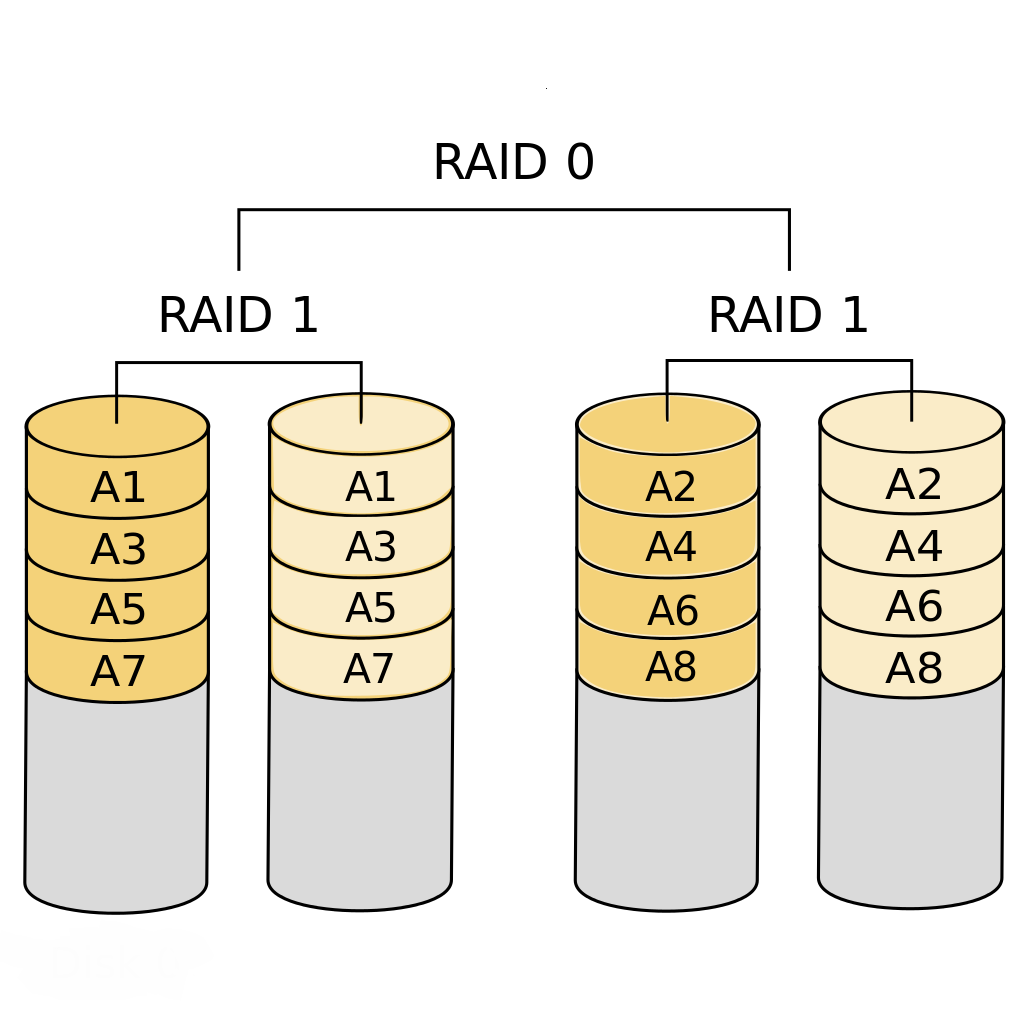
**3.1 RAID**

Neste trabalho decidimos utilizar um dispositivo RAID 10, ou RAID 1+0, pois este tipo de configuração combina duas características que identificamos como importantes: O mirroring e striping dos discos.

O RAID 10 funciona como um RAID 0 de dois dispositivos RAID 1, onde a informação é escrita de forma alternada entre cada um dos RAIDs 1 e dentro dos RAIDs 1 ela duplicada pelos 2 discos. Desde que um disco em cada par espelhado esteja operacional, os dados podem ser recuperados. Se dois discos no mesmo par espelhado falharem, todos os dados serão perdidos.

O RAID 10 fornece redundância de dados e melhora o desempenho, é uma boa opção para aplicações com uso intensivo de I/O e organizações que exigem pouco ou nenhum tempo de inatividade.

O dispositivo RAID foi criado no omv (10.0.0.4) com 4 discos: /dev/sdb, /dev/sbc, dev/sdd, dev/sde, cada um com 1GB de capacidade e foi-lhe atribuído o nome rd10.



/dev/sdb

/dev/sdc

/dev/sdd

/dev/sde

rd10 - RAID 1 + 0

**3.2 NFS**

O NFS foi configurado da seguinte forma:

- O dipositivo rd10 foi formatado com um sistema de ficheiros ext4 e posteriormente montado.

- Foi criada uma nova partilha, de nome radi-sh, utilizando o sistema de ficheiros assente no RAID com permissões de acesso de escrita e leitura a utilizadores e apenas das máquinas da rede 10.0.0.0/24.

- No Desktop, esta nova partilha foi adicionada ao /etc/fstab e montada no diretório /net/home

De seguida, para possibilitar a exportação das homes dos utilizadores autenticados por LDAP, foram criadas os seus diretórios home nessa partilha do omv e alterado a ownership e permissões de acesso dos diretórios em questão, de modo a mapearam corretamente com os uid e gid do LDAP (ex: criado o diretório /export/radi-sh/user1, alterado a sua ownership para 1003:1003, uid e gid do user1. Diretório acessível no Desktop no caminho /net/home/user1).

**4 Autenticação**

De modo a permitir o login de utilizadores LDAP nas máquinas Win10 e Desktop, o método de autenticação foi alterado na máquina linux, mudando a autenticação para o modo authselect, colocando o SSSD como o provedor de autenticação e configurando o mesmo para autenticar por LDAP utilizando TLS, e na máquina windows, fazendo uso do pGina, adicionando o módulo do LDAP para autenticação por TLS e garantindo a sua correta configuração.