Administração de Sistemas: Trabalho sobre LDAP

André Rodrigues up201505639 CC
Eduardo Morgado up201706894 MIERSI
Jorge Sousa up201603421 MIERSI

dezembro, 2019

1 Configurar OpenLDAP:

1.1 Hierarquia LDAP

1.1.1 Configuração da base de dados

A configuração do sistema LDAP é realizada indirectamente através de ficheiros LDIF, presentes no directório ***cn=config*** do *Standalone LDAP Daemon*(slapd).

Durante o processo de configuração é necessário definir uma *password* mestre (necessária para alterar configurações base do LDAP), de seguida, procede-se à configuração das permissões de acesso aos logs do LDAP, bem como, a definição do sufixo da *Directory Information Tree*(DIT) garantindo que todos os objectos criados possuam o mesmo sufixo base[1].

De seguida, é gerado um gestor/*manager* com **dn: cn=Manager,dc=grupod,dc=ads,dc=dcc** e é-lhe associada uma *password* mestre e um conjunto de permissões permitindo-lhe alterar instâncias na base de dados, este possuí todas as permissões inerentes às de leitura bem como as de escrita. São também fornecidas permissões de leitura[2] possibilitando a leitura da hierarquia a qualquer utilizador. Após terem sido realizadas estas configurações é possível gerar componentes que irão constituir a hierarquia desta organização.

1.1.2 Atributos

Cada componente utilizada requer atributos tais como *userPasswords, homeDirectories, loginShell, uidNumber, gidNumber e sshPublicKey*, no entanto, tais atributos são desconhecidos ao LDAP, sendo necessário fornecer-lhe **esquemas/*schemes*** correspondendo a esses atributos. Dessa forma, através de esquemas como **cosine.ldif**, **inetorgperson.ldif** e **nis.ldif**, é possível adicionar objectos que representam a organização, o papel do gestor e as *organizational units* onde estão alocados os utilizadores, respectivamente.
Nota: Utilizadores presentes em ambiente Linux podem ser migrados para LDAP atrés das ***migrationtools*** ou manualmente, pela geração de um ficheiro LDIF e consequentemente executando um comando *ldapadd*.

1.2 Autenticação para Workstation e Windows

Uma vez que pretende-se estabelecer uma conexão segura[3] entre o servidor LDAP e o *desktop/workstation* é necessário providenciar a comunicação por TLS, dessa forma, para comunicar com o OpenLDAP através do protocolo TLS deixa de ser utilizada a porta 389 e passa a ser utilizada exclusivamente a porta **636**, sendo também necessário gerar um certificado[4] para representar a chave pública da organização. Quando um cliente verifica a validade do certificado fornecido pelo servidor, o protocolo TLS gera uma resposta ao servidor, dando inicio à troca de informação de forma encriptada. Para o LDAP poder aceitar certificados TLS é necessário modificar a sua configuração adicionando `TLS_REQCERT allow` ao ficheiro.

[1] Entre esses objectos irão estar incluídos os utilizadores,grupos e unidades organizacionais implementadas no trabalho. O DIT é uma árvore de directórios com informações **únicas** dessa forma para se poder identificar unicamente um objecto é necessário fornecer o caminho/posicionamento correto para esse objecto a partir da raiz(enunciando o comando **dn**), sendo assim cada objecto tem um dn, caminho único. Ao definir o sufixo base da DIT estaremos a definir a *root* para qualquer operação consequente.

[2] Nestas permissões estão incluídas permissões de procura e autenticação, dessa forma, utilizadores podem executar *bind* para autenticação ou correr comandos ***ldapsearch***

[3] Por segura, pretende-se que ninguém externo a estes dois sistemas tenha acesso aos dado na rede

[4] A geração do certificado será feita no servidor(sendo o certificado *self-signed*), dessa forma, quando um cliente realiza um pedido TLS, o *desktop* irá necessitar da identificação do servidor, nesse instante o servidor fornece uma cópia da chave pública, o certificado ao cliente.

Após estas etapas, é possivel utilizar uma ligação segura com o OpenLDAP, sendo então possível, configurar a autenticação no *desktop* (até agora a autenticação e os dados de autenticação são locais ao *desktop*).

Para realizar a autenticação através do OpenLDAP é utilizado o recurso *System Security Services Deamon*(SSSD) e é alterado o modo *authconfig* para o modo ***authselect***[5] procedendo-se depois à configuração do SSSD para aceder ao OpenLDAP para a autenticação.
Nota: É ainda adicionado um serviço, ***oddjob-mkhomedir***[6] enunciado imediatamente após a autenticação de um utilizador. É adicionada também a opção de modificar a palavra passe dos utilizadores remotos directamente no *desktop* através do comando `passwd`.

Para realizar a autenticação de um utilizador LDAP no Windows, é necessário recorrer ao software **pGina**, que fornece um serviço similar ao SSSD, sendo necessário no pGina especificar o método de autenticação para ser através do LDAP, fornecendo tabém o IP do LDAP e a estrutura representativa da nossa hierarquia (o sufixo base, e atributos essenciais), para que lhe seja possível navegar o DIT de forma a procurar utilizadores.

1.3 Montar directórios do utilizador autenticado no Desktop

Os directórios podem ser montados manualmente para cada utilizador, através do comando mount, fornecendo a versão do NFS, IP da máquina que contém os directórios, o caminho para esses directórios (para a versão 4 do NFS apenas é necessário fornecer `/` e o directório local que servirá como destino dos remotos. Uma vez que, para montar manualmente, requer permissões *superuser*, permissões indisponíveis para alguns utilizadores deverá ser utilizado o sistema ***automount*** ou **autofs**[7], este sistema gera um ficheiro **/etc/auto.master** onde será especificado o directório onde o utilizador deve realizar o pedido de *mount* assim como a localização do ficheiro que contém os directórios a serem montados, os protocolos a serem utilizados, entre outras informações.

1.4 Ligação SSH ao LDAP

Da mesma forma que é possível aceder ao *desktop* por ssh através de um utilizador local[8], pretende-se permitir o acesso por ssh de utilizadores LDAP sem ser necessário guardar a chave pública na máquina que realiza o acesso, para isso, é guardado, para cada utilizador LDAP que deseje conectar-se ao LDAP por ssh, um atributo `sshPublicKey` que irá conter a chave pública desse cliente, possibilitando a sua autenticação por ssh.

O LDAP não possuí nenhum atributo `sshPublicKey` de raiz, como tal é necessário adicionar um novo esquema ao LDAP através de um ficheiro ldif. Esse esquema adiciona um novo objecto `ldapPublicKey` com o atributo `sshPublicKey`. Após adicionar o esquema, é necessário gerar as chaves de acesso, em cada sessão remota no *desktop* irá ser gerado um par chave pública/privada e a chave pública será, para o utilizador em questão, adicionada à entrada do utilizador LDAP através de um ficheiro ldif e o sistema LDAP será reiniciado.

Após serem geradas e adicionadas todas as chaves ao LDAP, o ficheiro `ldap.conf` no clinte(*desktop*) deve já estar a apontar para o servidor LDAP correcto (com ligação por TLS) e deve ser gerado um *script bash* para correr uma `ldapsearch` para o utilizador em questão e obter a sua chave pública, esse *script* deve ser adicionado ao `ssh_config` da máquina cliente numa entrada `AuthorizedKeysCommand <script>` reiniciando depois o sistema `sshd` da máquina.

Após terem sido completados todos estes passos, um utilizador remoto pode ser autenticado no *desktop* por ssh sem ser necessário armazenar a sua chave pública na máquina que realiza essa conexão, sendo a chave guardada no LDAP.

[5] Desta forma, o próprio sistema realiza de forma automática todas as alterações necessárias para colocar o SSSD como o **provedor de autenticação**, para realizar automáticamente o *nsswitch* e o PAM.

[6] Este serviço cria, caso ainda não exista, o *homeDirectory* de utilizadores que sejam, ou utilizadores locais à maquina(no ficheiro *passwd*), ou utilizadores pertencentes ao OpenLDAP.

[7] Serviço que permite montar *file system* automaticamente. Uma das suas vantagens é o facto do **directório remoto não ter que ser montado manualmente**, quando um utilizador acede ao directório ele é **automaticamente montado** e caso o utilizador se ausente desse directório o autofs realiza o *unmount* automaticamente.

[8] Sendo necessário guardar a chave pública na máquina que realiza o acesso externo.

2 Open Media Vault (OMV):

O OMV será utilizado como a máquina de armazenamento para o sistema de ficheiros dos utilizadores LDAP, devendo ser configurada para comunicar com o LDAP. Esta máquina contém nove discos no total, quatro discos de 2GB, quatro de 1GB e um de 11GB que contém o OS.

2.1 Sitema RAID/LV

A máquina apresenta 8 discos disponíveis, com quadras de capacidades diferentes, sendo assim, uma vez que, um sistema RAID é **limitado pelos discos de menor capacidade**, irão ser criados **dois** sistemas RAID. Um sistema **RAID 10**[9] com quatro discos de 2GB que servirá para criar um LV, para isso são atribuídos *loop devices* aos discos e depois é executado o comando ***mdadm***.

Após a criação desse RAID 10 irá ser gerado um *Physical Volume* desse sistema e por conseguinte um *Volume Group* que irá dar origem a um *Logical Volume*(LV) sendo depois formatado com um sistema de ficheiros **ext4**. Esse LV irá ser montado através a interface web do OMV[10].

2.2 Interface Web OMV e autenticação por LDAP

O OMV possui uma interface web que pode ser acedida através de um *browser*, fornecendo o endereço IP da máquina, através de uma conta *admin* é possível configurar a comunicação e estruturação dos dados do LDAP, nomeadamente, a criação dos sistemas LVM que servirão como armazenamento para as *homedirs* de utilizadores.

Para podermos comunicar com o servidor LDAP é necessário instalar um *plugin* na interface web designado por LDAP, após o qual, irá ficar disponível uma opção denominada por ***Directory Service*** a partir da qual é possivel configurar a ligação LDAP, fornecendo o IP do servidor, a sua porta (neste caso irá ser a porta **636**, uma vez que, desejamos que as comunicações sejam seguras, utilizem TLS) e as opções de LDAP, tais como, o sufixo da DIT, o caminho na árvore a partir do qual serão feitas pesquisas e os sufixos de utilizadores e grupos, irá ser também ativado o serviço PAM.

Para configurar o sistema TLS no OMV, é necessário gerar um certificado *self-signed* e activar o serviço SSL/TLS nas definições gerais da interface, bem como no *Directory Service* adicionando `TLS_REQCERT allow` nas opções extra para clientes. Após estas configurações, é possível realizar a autenticação no OMV através do LDAP.

2.2.1 Exportar directórios OMV por NFS

Foi escolhido o NFS, sendo um método de autenticação clássico de *trusted-host* onde o *autentica* utilizadores e passa os seus identificadores para a unidade de armazenamento, foi escolhido devido à facilidade de implementação em sistemas Linux (o Windows não utiliza directórios remotos, sendo assim o NFS é o método mais simples, no entanto, se fosse necessário, seria recomendado o samba). Primeiramente os sistemas RAID e LV são formatados num *file system* ext4.

Na interface *web* nas opções NFS é criada uma nova *share* com nome **radi-sh** fornecendo os IPs dos clientes que podem montar os directórios, neste caso será o IP da *workstation*, são também fornecidos privilégios *read/write*, são ainda fornecidas opções extra de `root_squash` e `no_subtree_check`. Após estes passos, o sistema NFS pode ser montado na *workstation*.
Nota: Uma vez que, os utilizadores remotos serão mapeados nos utilizadores do OMV utilizando os seus **uid** e **gid**, será necessário atribuir a titularidade de cada *home* aos seus respectivos uids e gids do LDAP, dessa forma, quando um utilizador LDAP se autenticar no *desktop* e o seu atributo **homeDirectory** coincidir com o directório definido no `auto.master`, o autofs irá contactar o OMV para fornecer os directórios aos quais esse utilizador é titular, como o utilizador não existe localmente no OMV é necessário contactar o LDAP para obter os uids desse mesmo de forma a identificar os seus directórios.

[9] Este sistema foi escolhido devido a grande quantidade de espaço, 8GB, que, uma vez que, o RAID 10 consome metade da memória apresentando, no entanto, menor redundância quando comparado com um sistema RAID 5 (sendo especialmente importante, uma vez que, estaremos a trabalhar com *homes* de utilizadores), acaba por se tornar em 4GB úteis. Uma das vantagens do RAID 10 quando comparado ao 5 é o facto deste duplicar e distribuir os dados por vários discos permitindo escritas de leituras em simultâneo.

[10] Por convenção, o OMV monta sistemas dentro da pasta **srv** e automaticamente acrescenta as suas configurações ao /etc/fstab.