Sessão 9: LDAP

1) Instalação do servidor OpenLDAP

Esta configuração será realizada na máquina virtual *Server_Linux*.

Instale e configure um servidor LDAP na máquina *Server_Linux* (192.168.0.10). Você deverá instalar os seguintes pacotes: `slapd, ldap-utils, migrationtools, attr, libpam-ldap, libnss-ldap, nscd`.

Tabela 1. Configuração libpam-ldap e libnss-ldap

Parâmetro	**Valor**
URI do servidor LDAP	`ldap://127.0.0.1`
Nome da base de pesquisa (*search base*)	`dc=empresa,dc=com,dc=br`
Versão do LDAP	3
Conta LDAP para o root	`cn=admin,dc=empresa,dc=com,dc=br`
Password da conta root do LDAP	`rnpesr`
Permitir que a conta administrativa do LDAP se comporte como o usuário root local	Sim
A base de dados LDAP requer autenticação	Não
Conta administrativa do LDAP	`cn=admin,dc=empresa,dc=com,dc=br`
Senha para a conta administrativa no LDAP	`rnpesr`

Após a instalação e configuração inicial, execute o comando `# dpkg-reconfigure slapd`.

Tabela 2. Configuração do slapd

Parâmetro	**Valor**
Omitir configuração LDAP	Não
Nome DNS	empresa.com.br
Nome da Organização	Empresa
Backend	MDB
Remover base atual em caso de `purge`	Não
Mover base de dados antiga	Sim
Permitir LDAPv2	Não

Finalmente, edite o arquivo `/etc/ldap/ldap.conf` e edite os parâmetros `BASE` e `URI` de acordo com o configurado nesta atividade. Reinicie o servidor LDAP e verifique se está operacional — faça uma consulta-teste usando o comando `ldapsearch`.

2) Usando o *migrationtools*

Esta configuração será realizada na máquina virtual *Server_Linux*.

O *migrationtools* é um conjunto de *scripts* que permite importar as contas locais de um sistema Linux para um diretório LDAP, que já foi instalado na máquina *Server_Linux* (192.168.0.10) durante a atividade 1.

1. Edite o arquivo `/etc/migrationtools/migrate_common.ph`, substituindo as variáveis `$DEFAULT_MAIL_DOMAIN` e `$DEFAULT_BASE` pelos valores configurados na atividade anterior.
2. Entre no diretório `/usr/share/migrationtools` e execute os *scripts* `migrate_base.pl`, `migrate_passwd.pl` e `migrate_group.pl` para exportar as bases (respectivamente) geral, de usuários/senhas e de grupos. Atente-se para a sintaxe de uso de cada *script*.
3. Remova os registros `dc=com,dc=br` e `dc=empresa,dc=com,dc=br` do topo do arquivo gerado pelo *script* `migrate_base.pl`, que já foram incluídos no diretório LDAP na primeira atividade.
4. Adicione os arquivos `.ldif` gerados anteriormente à base LDAP usando o comando `ldapadd`. Consulte sua página de manual para descobrir as opções apropriadas a passar para o comando. Lembre-se, apenas, que o diretório LDAP está utilizando autenticação simples, não SASL, e que é necessário informar um DN administrativo e senha para inserção de dados.
5. Use o comando `ldapsearch` juntamente com um filtro de pesquisa apropriado para listar todos os grupos que foram adicionados ao diretório LDAP pelos arquivos `.ldif` incluídos no passo anterior.

3) Configuração do cliente Linux para uso do LDAP

Esta configuração será realizada na máquina virtual *Client_Linux*.

Para que as clientes Linux possam se autenticar na base de dados do LDAP, é necessário configurar o PAM (*Pluggable Authentication Modules*) e NSS (*Name Service Switch*) para consultarem logins junto ao servidor LDAP.

Configure a máquina *Client_Linux* (192.168.0.20) para se autenticar na base LDAP que está instalada na máquina *Server_Linux* (192.168.0.10). Você deverá instalar os seguintes pacotes: `ldap-utils, libpam-ldap, libnss-ldap, nscd`.

Tabela 3. Configuração libpam-ldap e libnss-ldap no **Client_Linux**

Parâmetro	**Valor**
URI do servidor LDAP	`ldap://192.168.0.10`
Nome da base de pesquisa (*search base*)	`dc=empresa,dc=com,dc=br`
Versão do LDAP	3
Conta LDAP para o root	`cn=admin,dc=empresa,dc=com,dc=br`
Password da conta root do LDAP	`rnpesr`
Permitir que a conta administrativa do LDAP se comporte como o usuário root local	Sim

Parâmetro	Valor
A base de dados LDAP requer autenticação	Não
Conta administrativa do LDAP	`cn=admin,dc=empresa,dc=com,dc=br`
Senha para a conta administrativa no LDAP	`rnpesr`

Não se esqueça de editar os arquivos `/etc/ldap/ldap.conf` e `/etc/nsswitch.conf` para habilitar consulta às bases do LDAP durante procedimentos de login.

Se desejar que diretórios *home* sejam criados automaticamente para usuários LDAP inexistentes na máquina local, insira a linha a seguir ao final do arquivo `/etc/pam.d/common-session`:

```
session optional pam_mkhomedir.so skel=/etc/skel/ umask=022
```

Finalmente, para reiniciar a *cache* de usuários e grupos do LDAP, execute `# systemctl restart nscd`. Se houver algum registro de erro nos arquivos de log quanto à inexistência do arquivo `/etc/netgroup`, crie-o manualmente.

4) Configurança do servidor Linux para uso do LDAP

Esta configuração será realizada na máquina virtual *Server_Linux*.

Agora que a máquina *Client_Linux* (192.168.0.20) está configurada para se autenticar na base LDAP remota localizada na máquina *Server_Linux* (192.168.0.10), faça com que o próprio servidor *Server_Linux* autentique-se usando sua base LDAP local.

5) Criação e remoção de usuários e grupos LDAP

Esta configuração será realizada na máquina virtual *Server_Linux*.

Agora que a máquina *Client_Linux* está conectada ao servidor LDAP, adicione um novo usuário e grupo associado, ambos com o mesmo nome, e faça login com o usuário. Para realizar essa tarefa, crie arquivos LDIF manualmente e adicione-os via `ldapadd`. Não esqueça de definir a senha através do comando `ldappasswd`.

Observação: Para evitar confusões entre a base de usuários do LDAP e a base local dos clientes, é recomendável adotar um *buffer* numérico entre os usuários locais e os usuários do diretório. Faça com que o UID e GID dos novos usuários/grupos comece a partir de 5000.

6) Criação e deleção automática de usuários LDAP

Esta configuração será realizada na máquina virtual *Server_Linux*.

O esquema de criação de usuários manualmente acima funcionou, como visto. Não é, no entanto, muito conveniente do ponto de vista de manutenção do sistema proceder dessa forma. Seria mais interessante, se possível, automatizar essa tarefa para facilitar sua execução no dia-a-dia.

Crie um *script* que faça a adição e deleção automática de usuários na base LDAP. Atente-se para o fato de que os UIDs e GIDs desses usuários não devem se confundir com o dos sistemas locais. Use o valor mínimo de 5000 para ambos.