
Revisão do Tópico 210 – Administração dos Clientes de Rede

210.1 – Configurações de DHCP

O serviço DHCP

Processo: dhcpd
Portas: UDP 67 e 68

Configuração

Arquivo de Configuração Principal: /etc/dhcp/dhcpd.conf

Principais Configurações:

- default-lease-time = Temo de verificação se o IP alocado ainda está em uso.
- max-lease-time = Tempo máximo de concessão do IP. Após esse tempo o IP será liberado, caso a máquina ainda esteja ativa, o IP será realocado para a mesma máquina.
- log-facility = Define o nome da facility que poderá ser utilizada como referência no syslog.
- option domain-name = Define o domínio a ser informado.
- option domain-name-servers = Servidores DNS que podem ser utilizados pelo cliente
- subnet = Define a rede e o range de IPs que será concedido. Exemplo:

```
subnet 192.168.1.0 netmask 255.255.255.0 {
        range 192.168.1.100 192.168.1.200;
        option routers 192.168.1.1;    <=== Gateway a ser utilizado pelo cliente
}
```

- host = Usado para definir um IP específico a um hardware específico. Exemplo:

```
host exemplo {
        hardware ethernet 08:00:27:0d:73:cc;  <=== MAC Address
        fixed-address 192.168.1.50;  <=== IP Fixo
}
```

- deny unknown-clients = Só distribui IPs para Hosts conhecidos
- allow bootp = Habilita o servidor a responder a requisições bootp.
  - Exemplo de configuração para bootp

```
host exemplo {
        hardware ethernet 08:00:27:0d:73:cc;  <=== MAC Address
        fixed-address 192.168.1.50;  <=== IP Fixo
        filename "/vmlinux.exemplo";
        server-name "boot.dominio.com";
}
```

Arquivo com Registro de Atribuições: /var/lib/dhcp/dhcpd.leases

---

Logs

Os logs são normalmente gerados nos arquivos **/var/log/messages** ou **/var/log/syslog**.

No entanto, através da opção de configuração "**log-facility**" no dhcpd.conf, pode também ser configurado através do rsyslog para que outro arquivo seja utilizado.

Os logs também podem ser acessados pelo **journalctl**:
journalctl -e -u dhcpd

DHCP Relay

O DHCP relay é um processo que redireciona as requisições DHCP da rede local para um servidor DHCP central, normalmente em outra rede.

O processo responsável é o **dhcrelay**. Por exemplo:
dhcrelay -i eth0 servidor.empresa.com.br

IPv6 – radvd

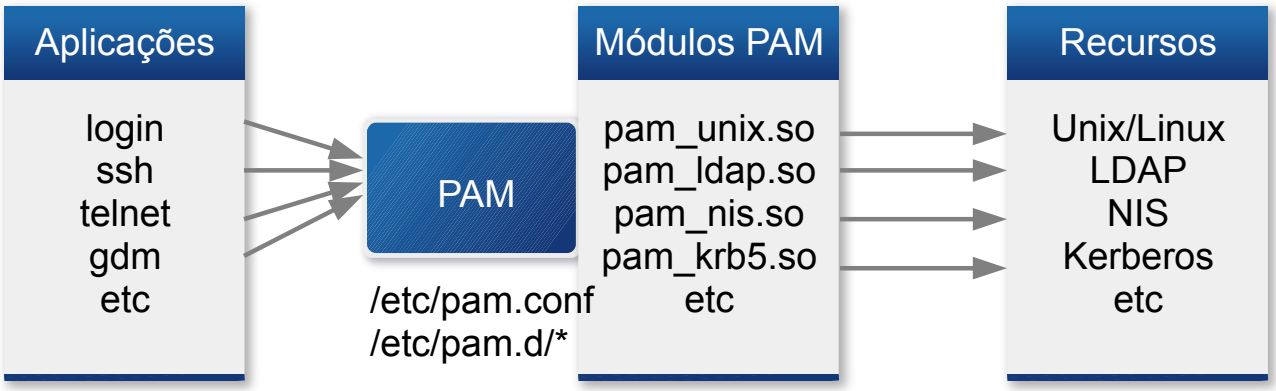
Em redes IPv6, o processo **radvd** é equivalente ao serviço DHCP, pois distribui aos clientes as informações da rede local e do gateway a ser utilizado,, serviço chamado de "router advertisement", possibilitando então a autoconfiguração da máquina. O processo é parte do protocolo NDP (Neighbor Discovery Protocol).

O arquivo de configuração é o **/etc/radvd.conf**.

210.2 – Autenticação via PAM

PAM = Pluggable Authentication Modules.

É uma interface para autenticação de usuários em diversas aplicações.



Configurações

As configurações ficam em arquivos específicos no diretório **/etc/pam.d/** ou no **/etc/pam.conf.** O mais comum é que cada serviço possua sua própria configuração no /etc/pam.d. Se houver duplicidade de configurações, a configuração do pam.conf é ignorada.

As configurações são basadas em 4 parâmetros:

- Tipo
- Controle
- Módulo
- Argumentos do Módulo (opcional)

Tipo:

- **auth** : Verifica a autenticidade do usuário. Normalmente por usuário e senha, mas também por chip, biometria e etc.
- **account** : Verifica se o usuário pode usar o serviço, se não há nenhum bloqueio de acesso.
- **password** : Definições referentes à atualização da autenticação.
- **session**: Algum procedimento que deve ser realizado após o login, antes do usuário receber o acesso.

Controle:

- **requisite** : Se o módulo falhar, todo o processo é interrompido.
- **required** : Se o módulo falhar, o acesso é negado, mas os demais módulos serão invocados.
- **sufficient** : Se o módulo tiver sucesso, a falha de outros módulos serão ignoradas. Uma falha não é fatal.
- **optional** : Sucesso ou falha não é relevante, a menos que seja o único.

Principais Módulos:

- **pam_unix.so** – Relacionado principalmente ao passwd/shadow
- **pam_limits.so** – Limitação de Recursos
- **pam_ldap.so** – Acessos via LDAP

- **pam_cracklib.so** – Checagem de senhas fracas
- **pam_listfile.so** – Uso de arquivos externos para controle
- **pam_sss.so** – Uso do SSS
- **pam_krb5.so** – Uso do Kerberos 5 para Autenticação
- **pam_userdb.so** – Uso de Datafiles .db
- **pam_nologin.so** – Uso do /etc/nologin
- **pam_time.so** – Recursos de controle por horário
- **pam_console.so** – Controle de acesso ao console por usuário

Exemplos:

/etc/pam.d/login
```
auth       requisite  pam_nologin.so
session    required   pam_limits.so
```

Para realizar a mesma configuração no /etc/pam.conf, é preciso incluir no primeiro campo o nome do serviço, por exemplo:
```
login   auth        requisite     pam_nologin.so
login   session     required      pam_limits.so
```

LDAP com PAM

Autenticação via LDAP é feito através do módulo **pam_ldap.so**

Exemplo de configuração do /etc/pam.d/login:

```
auth        sufficient    pam_ldap.so
auth        required      pam_unix.so   try_first_pass
account     sufficient    pam_ldap.so
account     required      pam_unix.so
```

SSSD (System Security Services Daemon)

Interface criada como melhoria ao PAM. O principal objetivo é ser uma interface para obter informações dos usuários a patir de diversas fontes, principalmente através do PAM e o do NSS e muito usado para comunicação com o LDAP e com serviços AD do Windows.

O processo é o sssd e o arquivo de configuração é o /etc/sssd.conf.

210.4 – Configurando um Servidor OpenLDAP

Definições e Conceitos

LDAP: Lightweighted Directory Access Protocol

- É um protocolo utilizado para armazenamento e acesso a uma base de dados no **modelo de árvore.**
- Muito utilizado para armazenar informações de usuários, funcionários, equipamentos e etc.
- Modelo favorece a performance na leitura de dados.
- Cada nó representa um conjunto de atributos e valores.
- Cada nó utiliza uma tipo de identificador, os mais utilizados são:
  - DC = Domain Component
  - OU = Organizational Unit
  - CN = Common Name
- O **DN** (Distinguished Name) é um identificador único de cada nó e é composto pela identificação do caminho até este nó, por exemplo:
  - dn: cn=Ricardo,ou=suporte,dc=empresa,dc=com

A cada nó podem ser atribuídos uma série de atributos e valores, esses atributos fazem parte de um objectClass e os objectClassess estão agrupados em Schemas:

- Schemas
  - ObjectClasses
    - Attributes

O Servidor LDAP

O OpenLDAP é a implementação de LDAP mais utilizada em ambientes Linux.

O processo é o **slapd**, que utiliza a porta TCP 389 por padrão e a porta 636 para LDAPS (LDAP Seguro).

As configurações são realizadas no diretório **/etc/ldap** ou **/etc/openldap.**

Por padrão, os bancos de dados são armazenados no diretório **/var/lib/ldap**.

Configurações

As configurações do OpenLDAP podem ser feitas através do arquivo /etc/ldap/slapd.conf ou através das definições do diretório /etc/ldap/slapd.d/

As principais opções do arquivo slapd.conf são:

- loglevel = Nível de log.
- backend = Modelo de armazenamento dos dados, por exemplo hdb, bdb, entre outos.
- database = Define o início da definição de um banco de dados e deve ser seguido pelo tipo de backend (hdb,bdb,etc)
- suffix = Endereço base do banco de dados. Por exemplo: dc=empresa,dc=com

- rootdn = Definição do administrador do BD
- rootpw = Senha do administrador do BD
- directory = Diretório que armazenará os dados

LDIF - LDAP Data Interchange Format

Formato de arquivo utilizado para importar, exportar e modificar dados de bancos LDAP.

As alterações são ser realizadas através das seguintes operações, também chamados de **changetype**:

- modify = Modifica os atributos de um DN
  - add = Adiciona um atributo
  - delete = Remove um atributo
  - replace = Altera o valor de um atributo
- add = Adiciona um novo DN
- delete = Remove um DN existente
- modrdn = Altera a descrição de um DN

Exemplo:
```
# cat altera-eduardo.ldif
dn: cn=Eduardo,ou=funcionarios,ou=testes,dc=dominioexemplo,dc=com,dc=br
changetype: modify
replace: mail
mail: silva.eduardo@dominioexemplo.com.br
```

Principais Comandos

- slapcat – Exibe todos os registros do LDAP ou de bases específicas. Pode ser usado para exportar dados de um banco em um arquivo no formato LDIF.
- slappasswd – Utilizado para gerar uma senha criptografada para ser utilizada em arquivos de configuração do sistema.
- slapindex – Utilizado para reindexar os registros de uma base LDAP
- slapadd – Adiciona registros diretamente à base LDAP. Para ser utilizado o serviço precisa estar parado.
- slaptest – Verifica a sintaxe das configurações do servidor LDAP.

210.3 – Uso do Cliente LDAP

Para o acesso e alteração de dados de uma base LDAP, são utilizados comandos que enviam as requisições através do protocolo LDAP pela rede ou localmente.

Os principais comandos e alguns exemplos de uso são:

- ldapsearch - Realizar consultas.
  - # ldapsearch -x -h localhost -b "dc=dominioexemplo,dc=com" cn=Eduardo
  - # ldapsearch -x -h localhost -b "dc=dominioexemplo,dc=com" '(&(cn=Carlos)(!(sn=Almeida)))'
  - # ldapsearch -x -h localhost -b "dc=dominioexemplo,dc=com" sn=A*
- ldapadd – Adicionar registros.
  - # ldapadd -x -W -D "cn=admin,dc=dominioexemplo,dc=com" -f novo-funcionario.ldif
- ldapdelete – Remover registros.
  - # ldapdelete -h localhost -D "cn=admin,dc=dominioexemplo,dc=com" -W "cn=Eduardo,ou=funcionarios,ou=testes,dc=dominioexemplo,dc=com"
  - # ldpelete -h localhost -D "cn=admin,dc=dominioexemplo,dc=com" -W -f arquivo.ldif
- ldapmodify – Alterar registros e seus atributos
  - # ldapmodify -x -D "cn=admin,dc=dominioexemplo,dc=com" -f arquivo.ldif
- ldappasswd – Alterar o atributo de senha de um registro de usuário
  - # ldappasswd -x -h localhost -D "cn=admin,dc=dominioexemplo,dc=com" -S -W uid=ricardo,ou=funcionarios,ou=suporte,dc=dominioexemplo,dc=com