Manual Linux

SERVIÇOS DE REDE

Configurando o servidor NIS

Significado do NIS

NIS é Network Information Service (serviço de informação de rede). Mantém informações administrativas da rede na forma de domínios, possibilitando aos usuários terem acesso à suas contas em qualquer máquina da rede. Para que seus arquivos sejam centralizados de forma que sejam acessados de qualquer lugar, utiliza-se o NFS, que exporta os arquivos do servidor para qualquer máquina onde exista um usuário que tenha o direito a estes arquivos.

Função do NIS

No GNU/Linux, como em qualquer outro sistema operacional, existe a possibilidade de realizar logon (autenticação) remoto. Para isso o NIS servidor tem a função de informar aos clientes NIS da rede os usuários disponíveis no servidor para serem logados remotamente. Assim, quando um cliente NIS envia uma solicitação para um servidor NIS, ele verifica se o usuário e a senha estão corretos, caso não estejam, ele rejeita a autenticação, caso estejam corretos ele devolve para aquele terminal todas os programas, arquivos e configurações daquele usuário como se ele tivesse na sua máquina real.

Configurando o servidor NIS

A configuração do NIS no servidor consiste de onze simples passos.

1° passo:

Baixar o pacote nis e o portmap utilizando o comando:

apt-get install portmap

Depois:

apt-get install nis

Geralmente no Ubuntu Desktop 9.04 o portmap já vem instalado.

2° passo:

Após baixado o pacote NIS ele será executado e apresentará a seguinte mensagem:

"Você precisa agora escolher o nome de domínio NIS para seu sistema.
Se você quer que esta máquina seja apenas um cliente, informe o nome
de domínio NIS de sua rede."

Ele pode sugerir um nome. Você deve excluir e deixar em branco, depois basta pressionar "enter".

3° passo:

Vamos editar o arquivo /etc/hosts utilizando o vi colocando o seguinte conteúdo no final do arquivo:

192.168.10.101 server.rede.br server

Obs.: Como sempre, utilizando o IP do seu servidor, não o do exemplo. Huahauha...

Feito isso salve o arquivo.

4° passo:

Vamos editar o arquivo /etc/defaultdomain utilizando o vi colocando o seguinte conteúdo no final do arquivo:

rede.br

Feito isso salve o arquivo.

5° passo:

Vamos editar o arquivo /etc/ypserv.securenets utilizando o vi, colocando o seguinte conteúdo no final do arquivo:

255.255.255.0 192.168.10.0

Obs.: Como sempre, utilizando a sua faixa de IP e máscara de rede.

Feito isso salve o arquivo.

6° passo:

Vamos editar o arquivo /etc/default/nis utilizando o vi. Altere os seguintes campos do arquivo:

NISSERVER=false

Para:

NISSERVER=master

Estaremos dizendo que essa máquina, de fato, será o servidor quando alteramos este campo. Altere o campo:

NISCLIENT=true

Para:

NISCLIENT=false

Estaremos dizendo que essa máquina não é um cliente quando alteramos este campo.

Obs.: Dentro do arquivo existem mais campos, mas não mexa neles.

Feito isso salve o arquivo.

7° passo:

Estando tudo configurado e os arquivos bem editados, precisamos parar e iniciar o serviço. Para isso, dentro do diretório /etc/init.d/, digite:

./nis stop

E depois que ele parar o serviço digite:

./nis start

8° passo:

Agora que o serviço foi iniciado precisamos criar os mapas e validar as configurações do servidor. Para tal, entre no diretório /usr/lib/yp e digite o seguinte comando:

./ypinit -m

Feito isso ele irá perguntar qual máquina rodará o servidor, basta digitar o nome da máquina servidor, no meu caso lab1-pc01 e apertar "Control + D".

9° passo:

Precisamos editar o arquivo /etc/ypserv.conf, onde adicionaremos no final do mesmo as seguintes informações:

dns: no
files: 30
slp: no
xfr_check_port: yes

Feito isso salve o arquivo.

10° passo:

Edite o arquivo /etc/yp.conf adicionando a seguinte linha ao final do arquivo:

ypserver 192.168.10.101

Obs.: Este IP é do meu servidor, você deve colocar o IP do seu servidor.

Feito isso salve o arquivo.

11° passo:

Edite o arquivo /var/yp/Makefile alterando os campos:

MERGE_PASSWD=true
MERGE_GROUP=true

Para:

MERGE_PASSWD=false
MERGE_GROUP=false

Feito isso salve o arquivo.

Assim que todas essas configurações estiverem realizadas você pode começar a criar os usuários.

Após cada usuário criado basta ir no diretório /var/yp e executar o comando make, isso garantirá sua base de dados de usuários atualizada para que todos os terminais clientes possam logar no servidor utilizando seu usuário.

Dica: É sempre bom, depois de muitas configurações, desligar e ligar novamente o computador, mesmo que o sistema nos permita reiniciar ou parar manualmente os serviços.

Configurando o cliente NIS

A configuração do NIS no cliente consiste de cinco simples passos:

1° passo:

Baixar o pacote nis e o portmap utilizando o comando:

apt-get install portmap

Depois:

apt-get install nis

Geralmente no Ubuntu Desktop 9.04 o portmap já vem instalado.

2° passo:

Após baixado o pacote nis, ele será executado e apresentará a seguinte mensagem:

"Você precisa agora escolher o nome de domínio NIS para seu sistema.
Se você quer que esta máquina seja apenas um cliente, informe o nome
de domínio NIS de sua rede."

Ele pode sugerir um nome, você deve excluir e deixar em branco, depois basta pressionar "enter".

3° passo:

Vamos editar o arquivo /etc/defaultdomain utilizando o vi colocando o seguinte conteúdo no final do arquivo:

rede.br

Feito isso salve o arquivo.

4° passo:

Agora precisamos editar o arquivo /etc/yp.conf acrescentando a seguinte linha:

ypserver 192.168.10.101

Feito isso salve o arquivo.

5° passo:

Depois de tudo configurado, só falta adicionarmos um "+" aos seguintes arquivos: passwd, group, shadow e gshadow, que são encontrados no diretório /etc/.

Para isso basta, estando no diretório /etc, executar os seguintes comandos:

```
# echo + >> /etc/passwd
# echo + >> /etc/group
# echo + >> /etc/shadow
# echo + >> /etc/gshadow
```

Onde o echo manda imprimir o "+" e os dois maiores ">>" dizem que o "+", do echo, ao invés de ser impresso na tela, deve ser impresso no final do arquivo.

Feito essas configurações reinicie o computador.

Conclusão

Se caso todos esses passos tiverem sido seguidos atentamente e você, estando certo de que seu sistema não tem nenhum erro, bem como sua configuração de rede estiver certinha, isso lhe garantirá um servidor de arquivos e de autenticação de usuário seguro e clientes aptos a acessá-lo.

Espero que este artigo tenha sido de ajuda. E para todo bom aluno e pesquisador existe sempre o Google para aprendermos mais e tirar dúvidas quando as coisas persistem em dar errado... rsrs

O que é o DHCP?

A configuracao automatica e dinamica de computadores ligados a uma rede TCP/IP, no que tange aos inumeros parametros de rede, ja' e' possivel utilizando-se o Dynamic Host Configuration Protocol (DHCP) ([RFC2131]). O DHCP, que e' hoje um protocolo recomendado, em vias de ser padronizado pelo Internet Activities Board (IAB), facilita, e ate' mesmo viabiliza, a gerencia de grandes redes IPs, assim como a vida dos usuarios itinerantes com seus computadores portateis.

Para o perfeito funcionamento de um computador ligado a uma rede Internet, nao apenas precisa-se configurar o seu endereco IP, mas tambem uma serie de outros parametros de rede. Um cliente DHCP busca encontrar um ou mais servidores DHCP que possam fornecer os parametros desejados, para que sua maquina possa ser automaticamente configurada.

Embora nao seja o unico parametro indispensavel, o endereco IP e', sem duvida, o mais importante deles, assim como o mais peculiar, posto que um determinado endereco nao deve ser utilizado por mais de um cliente ao mesmo tempo. O DCHP possibilita a implementacao uma politica de alocacao dinamica de enderecos IPs, que possibilita a reutilizacao de enderecos disponiveis ao longo do tempo.

^

Como Funciona?

Um servidor DHCP, respondendo a uma solicitacao de parametros de um cliente, oferece uma opcao, dentre as que tiver disponivel, para o solicitante, informando-lhe o tempo de arrendamento (leasing) dos parametros oferecidos.

Em resposta aos oferecimentos dos diversos servidores, o cliente podera' optar por aceitar, ou nao, uma das proposta, indicando o fato ao servidor da proposta eleita, ou optando por fazer nova requisicao.

Recebendo o aceite do cliente, o servidor reserva o endereco IP (se ainda estiver disponivel) e indica o fato ao cliente, que, a partir de entao, podera' fazer a correta e almejada configuracao do seu computador.

É facultado ao cliente, solicitar um re-arrendamento dos parame- tros obtidos ao servidor. Tal solicitacao devera' ser feita quando atingido a metade do tempo de arrendamento combinado, minorando assim a possibilidade de ocorrencia de problemas com eventuais descompassos entre os relogios dos dois equipamentos.

Espera-se tambem que o cliente informe ao servidor quando nao for mais utilizar os recursos alocados - por exemplo, quando estiver sendo desligado. Porem, esta atitude cordial do cliente, se nao ocorrer, nao fara' com que o endereco seja indefinidamente inutilizado, posto que, ao final do tempo de arrendamento, o servidor assumira' que tal endereco podera' ser re-alocado sem problemas.

É possivel que o servidor DHCP nao esteja no mesmo enlace do cliente e que entre eles haja algum roteador que nao faca o roteamento dos pacotes DHCP. Deve-se lembrar que o cliente DHCP, por nao saber inicialmente quem e' o servidor DHCP, utiliza o broadcast para procura-lo, e que o mesmo pode ser feito pelo servidor ate' que o cliente tenha um endereco IP fixo. No caso entao de, entre o servidor e o cliente, haver um roteador que nao encaminhe devidamente pacotes DHCP, ha' a necessidade de um elemento intermediario: o relay DHCP. O relay DHCP e' uma maquina capaz de receber pacotes dos clientes DHCP de sua rede, por exemplo, e encaminhar essas solicitacoes a um ou mais servidores em outras redes.

Configurando o servidor DHCP

Para que o servidor passe a fornecer a configuração de rede aos clientes, instale o pacote "dhcp3-server" usando o apt-get, como em:

$ sudo apt-get install dhcp3-server

Em seguida, edite o arquivo "**/etc/dhcp3/dhcpd.conf**", deixando-o com o seguinte conteúdo:

```
ddns-update-style none;
default-lease-time 600;
max-lease-time 7200;
authoritative;
subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.101 192.168.1.201;
option routers 192.168.1.1;
option domain-name-servers 208.67.222.222,208.67.220.220;
option netbios-name-servers 192.168.1.254;
option broadcast-address 192.168.1.255;
}
```

A opção "**range**" determina a faixa de endereços IP que será usada pelo servidor. Se você utiliza a faixa de endereços 192.168.1.1 até 192.168.1.254, por exemplo, pode reservar os endereços de 192.168.1.1 a 192.168.1.100 para estações configuradas com IP fixo e usar os demais para o DHCP, ou então reservar uma faixa específica para ele, de 192.168.1.101 a 192.168.1.201, por exemplo. O importante é usar faixas separadas para o DHCP e os micros configurados com IP fixo.

Na "**option routers**" vai o endereço do default gateway da rede, ou seja, o endereço do servidor que está compartilhando a conexão. Não é necessário que o mesmo micro que está compartilhando a conexão rode também o servidor DHCP. Pode ser, por exemplo, que na sua rede o gateway seja o próprio modem ADSL que está compartilhando a conexão e o DHCP seja um dos PCs.

A opção "**option domain-name-servers**" contém os servidores DNS que serão usados pelas estações. Ao usar dois ou mais endereços, eles devem ser separados por vírgula, sem espaços.

A opção "**option netbios-name-servers**" faz com que os clientes sejam orientados a utilizarem o endereço IP do servidor na rede local como servidor WINS, agilizando a navegação na rede. Naturalmente, o "192.168.1.254" deve ser substituído pelo endereço correto, caso diferente.

Depois de salvar o arquivo, não esqueça de reiniciar o serviço para que a configuração entre em vigor:

$ sudo /etc/init.d/dhcp3-server restart

Configurando o servidor DNS

Agora vamos partir para a primeira parte de configuração do **DNS**. Esta primeira parte engloba:

- Instalanção do Bind;
- Configuração do cache de DNS;
- Configuração do log (logging) do Bind;
- Instalação e configuração do BindGraph.

Instalação do Bind

A instalação do **Bind** no **Ubuntu** é extremamente simples, pois os pacotes estão no *repositório* principal e assim não necessita de nenhuma configuração ou adição de repositórios no *sources.list* do **APT**.

Para instalar basta digitar o comando:

```
# apt-get install bind9 dnsutils bind9-doc
```

Sobre os pacotes:

- **Bind9** – é o pacote contendo o servidor para o protocolo **DNS**. Para mais informações acesse: http://www.bind9.net/ não é o site oficial, porém possui grande fonte de informação;
- **DNSUtils** – pacote contendo três softwares fundamentais para testes e correção de problemas. São eles: dig, nslookup e nsupdate. Para mais informações, após a instalação digite *# man dig* ou *# man nslookup*;
- **Bind9-Doc** – contém basicamente a documentação do **Bind**.

Configuração do cache de DNS

Eu particularmente considero essa a tarefa mais simples de todo o processo, pois quase não requer esforço ou raciocínio. Porém, vale ressaltar que o conceito é mais importante que a configuração em si. Um **cache de DNS**, ou *dns caching*, é responsável por manter um histórico das consultas ao servidor de DNS do provedor. Por exemplo, um dos usuários acessou o domínio www.logicadigital.com.br, então é feita a comunicação com o servidor de DNS do provedor (caso você não saiba o porquê desse procedimento, então acesse os links sugeridos no primeiro post), se outro usuário acessar o mesmo site e a rede local não possuir um cache de DNS, então novamente será feita a consulta ao DNS do provedor. Com o **cache de DNS** configurado, as consultas são armazenadas em um *"histórico"*, agilizando o tempo de busca e retorno da informação. Claro que esta explicação é superficial, existem pontos como a configuração *TTL* do domínio que vai determinar o tempo que uma consulta DNS ficará no "*histórico*", ou melhor cache. Vale a pena acessar o link What is DNS caching?.

Chega de conversa e vamos configurar o cache de DNS. Para isso vamos editar o arquivo *named.conf.options*:

```
# vi /etc/bind/named.conf.options
```

Você verá três linhas comentadas e são justamente estas que precisam ser modificadas. Antes de partirmos pra modificação, vale lembrar que é necessário que você tenha em mãos os IPs dos servidores de DNS do seu provedor.

Altere o arquivo e deixe-o como abaixo:

```
forwarders {
<IP-DO-SERVIDOR-DNS-PRIMÁRIO>;
<IP-DO-SERVIDOR-DNS-SECUNDÁRIO>;
};
```

Salve o arquivo com *:wq!* e vamos configurar o arquivo *resolv.conf* para que até o próprio servidor de DNS utilize o cache de DNS.

```
# vi /etc/resolv.conf
```

Modifique o arquivo e deixe-o como o abaixo. Atenção: A primeira linha, relativa a *search* é opcional para esta configuração, porém será utilizada quando configurarmos a integração com o **Active Directory**.

```
search <NOME-DO-DOMINIO>
nameserver <IP-DO-SEU-SERVIDOR>
```

Salve o arquivo *resolv.conf* e reinicialize o **Bind** e sua configuração de rede:

```
# /etc/init.d/bind9 restart
# /etc/init.d/networking restart
```

Configuração de Log (logging clause)

A configuração de log é fundamental para acompanharmos as ocorrências de utilização do servidor de DNS e também será utilizado para montagem dos gráficos da ferramenta BindGraph que instalaremos na sequência. Em versões anteriores a configuração de log era feita no arquivo *named.conf*, porém no Ubuntu 8.10 esta configuração foi deslocada para o arquivo *named.conf.local* (nada impede que você faça a configuração no *named.conf*). Caso não seja configurada nenhuma opção de log, então você ainda poderá pesquisar informações nos arquivos */var/log/messages* e */var/log/syslog*. Vamos editar o arquivo */etc/bind/named.conf.local* e inserir as informações de log.

```
# vi /etc/bind/named.conf.local
```

E insira as linhas abaixo:

```
logging {
channel "BindGraphQuery" {
file "/var/log/bindQuery.log";
print-time yes;
severity debug 3;
};
category queries { BindGraphQuery; };
};
```

Explicando cada uma das linhas:

- **logging** – clausula responsável pela configuração de log;
- **channel** – nome do canal de configuração de log. Você poderá ter vários canais;
- **file** – caminho e nome do arquivo onde será armazenado o log;
- **print-time** – é clausula fundamental para que o **BindGraph** funcione, pois esta ferramenta mostra os gráficos de utilização do servidor baseando em datas e horários de utilização;
- **severity** – controla o nível de log. Como coloquei *debug 3*, então todos os níveis iguais ou superiores a três serão gravados. Quanto maior o nível, maior o detalhamento;
- **category** – a categoria é para onde deverá ser enviado os logs, no caso defini **queries** para que as consultas sejam enviadas ao arquivo de log. Existem outros tipos de categoria. Veja mais em: BIND 9 Configuration Reference.

Bom, após configurado o *logging*, então precisaremos salvar o arquivo de configuração, criar o arquivo de log e definir o proprietário do arquivo de log.

Criando o arquivo de log e definindo o usuário *bind* como proprietário:

```
# touch /var/log/bindQuery.log
# chown bind /var/log/bindQuery.log
```

Vamos agora novamente reinicializar o **Bind**.

```
# /etc/init.d/bind9 restart
```

Se você acha que está tudo ok com seu log, ledo engano. Visualize o arquivo **/var/log/syslog** e veja a mensagem que não foi possível gravar o log por falta de permissão de acesso ao arquivo. A mensagem será parecida com esta:

```
logging channel 'BindGraphQuery' file '/var/log/bindQuery.log':
permission denied
```

Hm… este problema me deu um bom trabalho pra achar a solução, apesar de estar o tempo todo a minha frente. Na documentação oficial do Ubuntu tem uma seção de solução de problemas que trata justamente disso. Link para a documentação oficial.

Para solucionar vamos ter que alterar configurações do **AppArmor** que é um módulo de segurança, desenvolvido pela *Novell*, que tem como função determinar, através de perfis, quais arquivos e permissões uma aplicação pode acessar ou utilizar.

Edite o arquivo *usr.sbin.named*:

```
# vi /etc/apparmor.d/usr.sbin.named
```

Adicione na ultima linha, antes do fechamento da chave (**}**) o caminho do arquivo acompanhado da permissão concedido ao *bind*:

```
/var/log/bindQuery.log w,
```

Feito isso, salve o arquivo e vamos recarregar o perfil do *bind* no **AppArmor**:

```
# cat /etc/apparmor.d/usr.sbin.named | sudo apparmor_parser -r
```

A mensagem de retorno deverá ser como esta:

```
Replacement succeeded for "/usr/sbin/named".
```

Vamos agora novamente reinicializar o **Bind**.

```
# /etc/init.d/bind9 restart
```

Para testar se as configurações de log estão funcionando vamos realizar duas consultas:

```
# dig uol.com.br
# nslookup mail.google.com
```

Agora visualize o conteúdo do arquivo bindQuery.log:

```
# cat /var/log/bindQuery.log
```

Se as duas consultas estiverem lá, então seu log está funcionando corretamente e podemos passar para o passo de instalação e configuração do **BindGraph**.

Instalação e configuração do BindGraph

O **BindGraph** é uma ferramenta que lê o arquivo de log e gera **gráficos** relativos à consultas dos variados tipos de registro no servidor de DNS. Importante: Ao instalar o BindGraph, automaticamente será instalado o **Apache 2** e mais uma série de ferramentas de suporte ao Apache 2, totalizando mais de 10 mb em download. Esta instalação poderá causar *perda de performance*

dependendo da configuração de hardware do seu servidor. Outro problema é que aumentamos a superfície de monitoramento e controle da segurança. Neste exemplo instalei o BindGraph no próprio servidor de DNS, mas o ideal é instalar o BindGraph em outro servidor que já tenha o Apache instalado com uma função mais abrangente e disponibilizar o log via **NFS**. Veja mais sobre NFS em "What is NFS?"

Então vamos fazer a instalação, para isso execute o comando:

```
# apt-get install bindgraph
```

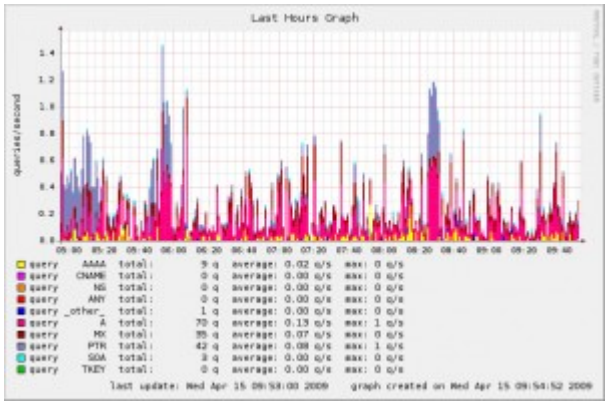
Agora basta editar o arquivo de configuração do BindGraph, mudando a configuração do arquivo de log para o arquivo criado no passo anterior, ou seja, */var/log/bindQuery.log*:

```
# vi /etc/default/bindgraph
```

Configure corretamente a linha **DNS_LOG** para **/var/log/bindQuery.log**.
Após esta configuração basta parar e reiniciar o serviço BindGraph:

```
# /etc/init.d/bindgraph stop
# /etc/init.d/bindgraph start
```

Agora em seu navegador acesse o endereço: **http://<IP-DO-SEU-SERVIDOR>/cgi-bin/bindgraph.pl** Você deverá visualizar um gráfico como este abaixo:



BindGraph - Gráfico de exemplo

Pronto. Esta etapa de configuração chegou ao fim.