



Implementando o serviço NTP na sua rede local

CAIS - Centro de Atendimento a Incidentes de Segurança
agosto de 2000

Este documento descreve os procedimentos de como implementar o serviço NTP na sua rede local.

© Copyright. Os direitos autorais deste manual são reservados ao CAIS Centro de Atendimento a Incidentes de Segurança. A reprodução total ou parcial deste documento pode ser feita desde que mantida e citada a autoria do mesmo.

Sumário

1.	Apresentação	3
2.	Implementando o Servidor NTP (Sistemas Unix)	5
2.1.	Compilação e Instalação	5
2.2.	Configuração	6
2.2.1.	Opções de Configuração	9
3.	Implementando o Cliente NTP	18
3.1.	Instalação e Configuração em sistemas Unix	18
3.2.	Instalação e Configuração em sistemas Windows	18
4.	Implementando o serviço NTP em Roteadores	21
4.1.	Configuração do Serviço NTP em Roteadores Cisco	21
5.	Anexos	26

1. Apresentação

A RNP –Rede Nacional de Pesquisa– disponibilizou recentemente um novo serviço: o Serviço NTP –*Network Time Protocol*– Stratum 1. Mas, o que é este serviço e qual a importância do mesmo?

Os servidores NTP permitem aos seus clientes a sincronização dos relógios de seus computadores e outros equipamentos de rede a partir de uma referência padrão de tempo aceita mundialmente, conhecida como UTC (*Universal Time Coordinated*).

A extensão do alcance da Internet torna a sincronização do tempo crucial para a troca de informações entre milhares de computadores que operam na base 24x7, ou seja, 24 horas por dia, sete dias por semana. Os benefícios da utilização do NTP atingem tanto usuários quanto administradores de rede.

Pelo lado dos usuários, a sincronização dos relógios de computadores pode ser vital em certas operações. Tomando como exemplo a entrega da declaração de Imposto de Renda, podemos supor que seja o último dia para entrega, o relógio da máquina que hospeda o *website* da Receita Federal esteja adiantado um minuto e o prazo se encerre às 20h. Nesse caso, bastante plausível, qualquer declaração entregue após 19h59min será rejeitada, causando prejuízos ao contribuinte. Atrasos de até um ou dois minutos são bastante frequentes quando não se usa um esquema de NTP.

Do ponto de vista da administração de redes, a utilização do NTP é muito vantajosa, pois possibilita a sincronização automática de todos os equipamentos conectados em rede. Ou seja, o administrador não precisa ir de máquina em máquina acertando o relógio local.

Além disso, a questão da segurança é reforçada com a adoção da sincronização dos relógios dos equipamentos em rede pois a investigação de eventos de ataques em computadores depende da verificação de logs em diversos equipamentos. A inconsistência dos horários registrados inviabiliza esse trabalho.

O NTP implementa um modelo de sincronização hierárquico distribuído. No topo encontram-se os servidores de tempo stratum 1, computadores conectados diretamente a dispositivos conhecidos como "relógios de referência" (ou servidores stratum 0), de altíssima precisão. Tipicamente, estes dispositivos podem ser relógios atômicos, receptores GPS (Global Positioning Systems) ou receptores de rádio. Qualquer servidor NTP que tenha como referência de tempo um servidor stratum 1 passa a ser um stratum 2, qualquer servidor NTP que tenha como referência de tempo um servidor stratum 2 passa a ser um stratum 3, e assim por diante.

O servidor NTP stratum 1 da RNP, disponibilizado em ntp1.rnp.br, utiliza a tecnologia GPS, que obtém o tempo diretamente de um grupo de satélites. Atualmente, o acesso ao servidor não tem restrição, mas a RNP pretende organizar em alguns meses uma hierarquia de stratum 2 a partir dos seus PoPs, de redes estaduais e de outras redes autorizadas e viabilizar, com isso, a criação de servidores stratum 3 nas redes clientes para uso do público em geral. Esta hierarquia distribui a carga de processamento, o que resulta em um serviço mais estável e confiável para o usuário final.

Neste contexto e com o intuito de difundir e promover a implementação de servidores NTP nas redes locais, o CAIS elaborou o presente manual a fim de auxiliar administradores e usuários nesta tarefa.

2. Implementando o Servidor NTP (Sistemas Unix)

2.1. Compilação e instalação

1. Fazer o download da última versão do NTP a partir de: www.ntp.org

última versão atualmente: 4.0.99k

2. Descompactar o arquivo `ntp-<versão_atual>.tar.gz`
3. A compilação e instalação do servidor NTP é trivial, normalmente basta seguir os passos indicados no arquivo `install` contido na distribuição. Estes se resumem basicamente à execução dos seguintes comandos:

```
./configure
make
make check
make install (como usuário root)
```

4. A menos que seja indicado explicitamente outro diretório, dentre outros, os seguintes binários serão instalados no diretório default `/usr/local/bin`:

ntpd	Processo daemon.
ntpdate	Utilitário que permite configurar o horário e data locais usando como referência um servidor NTP remoto. Similar ao conhecido comando <code>rdate</code> .
ntpq e ntpdc	Programas de monitoramento e controle. Permitem realizar consultas a servidores NTP sobre o estado do mesmo e, eventualmente, requerer mudanças de tal estado.
ntptrace	Determina de onde um determinado servidor NTP obtém a referência de tempo e traça o caminho seguido até o servidor master (comumente, servidor NTP stratum 1).

Todos eles são criados com permissão 755 (isto é, `rwxr-x-r-x`), tendo como dono o usuário root. Maiores detalhes sobre o uso destes binários podem ser encontrados nos documentos:

ntpd - Network Time Protocol (NTP) daemon

http://www.eecis.udel.edu/~ntp/ntp_spool/html/ntpd.htm

ntpq - standard NTP query program

http://www.eecis.udel.edu/~ntp/ntp_spool/html/ntpq.htm

ntpdc - special NTP query program

http://www.eecis.udel.edu/~ntp/ntp_spool/html/ntpdc.htm

ntpdate - set the date and time via NTP

http://www.eecis.udel.edu/~ntp/ntp_spool/html/ntpdate.htm

ntptrace - trace a chain of NTP servers back to the primary source

http://www.eecis.udel.edu/~ntp/ntp_spool/html/ntptrace.htm

2.2. Configuração

A configuração do servidor NTP inclui os seguintes passos:

1. Criação do arquivo de configuração. Por default, este arquivo é o `/etc/ntp.conf`. Diretrizes de como construir este arquivo podem ser encontradas no item 2.2.1: Opções de Configuração.

Um modelo do arquivo de configuração pode ser consultado no **Anexo 02** deste documento.

2. Criação do arquivo de chaves, caso sejam implementadas as opções de autenticação. A diretiva `keys` no arquivo de configuração indicará a localização e nome deste arquivo. Por default, este arquivo é o arquivo `/etc/ntp.keys`. Diretrizes de como estruturar este arquivo podem ser encontrados no item 2.2.1: Opções de Configuração.
3. Criação do arquivo `drift` com conteúdo vazio. A diretiva `drift` no arquivo de configuração indicará a localização e nome deste arquivo. Por default, este arquivo é o `/etc/ntp.drift`. O comando `touch` pode auxiliar nesta operação:

```
# touch /etc/ntp.drift
```

4. Inicialização do daemon `ntpd`. O daemon pode ser inicializado usando o seguinte comando:

```
# /usr/local/bin/ntpd
```

Caso o arquivo de configuração seja outro diferente ao default, o caminho deste deverá ser explicitamente especificado usando o parâmetro `-c`:

```
# /usr/local/bin/ntpd -c <arquivo_config>
```

5. Existindo entre os respectivos relógios dos servidores local e remoto, um offset (diferença) maior do que 1000 seg (aprox. 20 minutos), o daemon não configurará o relógio local, gerará automaticamente uma mensagem de log e se auto-desativará.
6. Para verificar se o daemon `ntpd` foi corretamente inicializado podem ser usados os utilitários `ntpq` e `ntpdc`, executando qualquer um dos seguintes comandos:

```
# ntpq -p <ip_servidor_NTP_local>
# ntpdc <ip_servidor_NTP_local>
```

a) Uma inicialização sem sucesso será reportada no arquivo de logs por uma mensagem do tipo:

```
ntpq: read: Connection refused
```

Neste caso, será preciso ajustar previamente o relógio local com algum servidor NTP remoto, usando para tal algum mecanismo de ajuste conhecido, tal como o `ntpdate`, `rdate` ou mesmo manualmente, através do comando `date`. Usando o utilitário `ntpdate` bastará executar:

```
# ntpdate < ip_servidor_NTP_remoto >
```

b) Uma inicialização com sucesso será indicada por uma saída do tipo:

```
[root@maq2.cais.rnp.br]$ ntpq -p ntp.cais.rnp.br
remote  refid  st t when poll reach  delay  offset  jitter
=====
*server2.pop-df. .GPS.  1 u  34  64  75  26.471  16.068  0.844
-rackety.udel.ed .GPS1.  1 u  15  64  77  466.799 -134.49  25.549
+tick.gpsclocck.c .GPS.  1 u  15  64  77  532.347 -131.15  20.847
+listas.ansp.br  avantesma.agest  2 u  54  64  77  10.965  -74.994  0.679
```

Lembre-se que quando o daemon do servidor local inicializa, leva em torno de 5 minutos para sincronizar adequadamente com o servidor remoto. Uma diferença de tempo menor que 128 ms é requerida para sincronização, seja paciente.

7. Para inicializar o serviço NTP automaticamente durante o processo de boot, bastará realizar o seguinte:

Em plataformas Solaris:

a) Copiar o arquivo de inicialização do serviço NTP, para o diretório `/etc/init.d` (UID=root, GID=other, permissão=700). Este arquivo pode ser encontrado no **Anexo 03** deste documento.

b) No diretório `/etc/rc2.d` (nível 2), criar um link simbólico para o arquivo

```
/etc/init.d/ntp:
# ln -s /etc/init.d/ntp /etc/rc2.d/S74ntp
```

Em plataformas Linux (Red Hat):

a) Copiar o arquivo de inicialização do serviço **NTP** para o diretório `/etc/rc.d/init.d` (UID=root, GID=root, permissão=700). Este arquivo pode ser encontrado no **Anexo 04** deste documento.

b) No diretório `/etc/rc.d/rc2.d` (nível 2), criar um link simbólico para o arquivo `/etc/rc.d/init.d/ntp`:

```
# ln -s /etc/rc.d/init.d/ntp /etc/rc.d/rc2.d/S74ntp
```

Em plataformas FreeBSD:

a) Editar o arquivo `/etc/rc.local` (UID=root,GID=wheel, permissão=644)

b) Acrescentar as seguintes linhas:

```
# Arquivo de inicialização do servidor NTP
# O arquivo de configuração default é o /etc/ntp.conf
#
echo 'starting NTP server...'/usr/local/bin/ntpd
```

8. Devido à velocidade da conexão e tempo de respostas, o serviço NTP utiliza pacotes UDP, chegando eles pela porta 123. Assim, no caso de existir um filtro IP entre o seu servidor NTP e as máquinas que irão acessá-lo, deverão ser permitidas as conexões direcionadas à porta 123/udp do servidor NTP.

Em particular, se este filtro de pacotes for implementado usando um roteador Cisco, será suficiente a criação de uma lista de acesso (ACL) do tipo:

```
access-list 101 permit udp any host <ip_servidor_NTP_local> eq 123
```

Ela deverá ser associada à interface por onde chegam os pacotes UDP com destino à porta 123.

9. A seguinte URL pode ser visitada a fim de checar o perfeito funcionamento do seu servidor NTP:

<http://www.gpsclock.com/check.html>

Recomendações finais:

- Criar o alias `ntp.seu_dominio.br` para o host que abriga o seu servidor NTP local.
- Se você estiver implementando um servidor NTP stratum 2:

- Divulgar informações (abrangência, política de acesso, etc) sobre o seu servidor NTP, na lista internacional (<http://www.eecis.udel.edu/~mills/ntp/clock2.htm>) mantida por Dave Mills (mills@udel.edu).
- Divulgar informações (abrangência, política de acesso, etc.) sobre o seu servidor NTP, na lista nacional (<http://www.rnp.br/cais/ntp/stratum2.htm>) mantida pelo CAIS/RNP (cais@cais.rnp.br)

O **Modelo de Divulgação** pode ser consultado no **Anexo 05** deste documento.

- Idealmente, este servidor deverá estar disponível 24 horas/ 7dias, para tal é recomendável a criação de um endereço de contato para atender eventuais problemas técnicos que o servidor, ou o acesso a ele, apresente. Preferencialmente, deverá ser criado o alias `ntp-admin@seu_dominio.br` com este objetivo.

2.2.1. Opções de Configuração

Caso se tenha familiaridade com a estruturação de um arquivo de configuração, esta seção pode ser Este documento não tem a pretensão de abordar todas as opções de configuração em detalhes, mas apenas dar uma pincelada naquelas consideradas relevantes e as que contemplam aspectos de segurança. Maiores detalhes sobre como estruturar um arquivo de configuração do serviço NTP poderão ser encontrados nos documentos:

Notes on Configuring NTP and Setting up a NTP Subnet

http://www.eecis.udel.edu/~ntp/ntp_spool/html/notes.htm

Configuration of xntp

<http://www.eecis.udel.edu/~ntp/ntpfaq/NTP-s-config.htm>

2.2.1.1. Opções de associação

Modos de Associação

Existem quatro modos nos quais os servidores NTP podem se associar. Estes modos indicam o comportamento que o servidor NTP remoto espera do servidor NTP local. A seguir:

Modo cliente/servidor

Neste modo o servidor local, que atuará como **cliente**, poderá sincronizar-se com o servidor remoto, que atuará como **servidor**. O comando utilizado no arquivo de configuração que indica este tipo de associação é `server`.

Modo simétrico

O servidor local sincroniza com o servidor remoto e vice-versa, se preciso for. Neste modo, ambos os servidores concordam em que, caso a referência de tempo de algum deles falhe, o outro atuará como backup. O comando utilizado no arquivo de configuração que indica este tipo de associação é `peer`.

Modos multicast e broadcast

O servidor local envia periodicamente mensagens de broadcasting para o endereço de um grupo de servidores específicos, que comumente é o endereço (ou um dos endereços) de broadcasting da rede local ou o endereço multicast designado ao serviço NTP pelo IANA (224.0.1.1).

Quando usar cada tipo de associação?

De um modo geral, quando precisão e confiabilidade são requeridos, os servidores operam no modo cliente/servidor ou simetricamente. Em contrapartida, quando estes requerimentos não são fundamentais, podem ser usados os modos multicast e broadcast.

Em particular, no que diz respeito à hierarquia NTP a ser implantada no backbone RNP, precisão e confiabilidade são aspectos bastante desejáveis, levando em consideração o tipo de aplicações atuais e as que estarão futuramente sendo implementadas no novo backbone RNP2. Assim, este procedimento não incluirá maiores detalhes a respeito dos modos broadcast e multicast.

Servidores NTP, de modo geral, são comumente configurados para operar no modo cliente/servidor, de forma que ele possa sincronizar com outro servidor remotamente. No entanto, quando se quer implementar redundância, ou seja, configurações que envolvam um número de servidores de tempo redundantes interconectados via diversos caminhos de rede, o modo simétrico é o mais apropriado.

Os servidores NTP que operam no último nível, isto é, que provem sincronização apenas a clientes NTP ou que não provem sincronização a outros servidores locais, devem ser configurados no modo cliente/servidor.

Como escolher os servidores NTP com os quais sincronizar?

No processo de escolha dos servidores com os quais sincronizar, deverão ser considerados aspectos como: menor nível de stratum, precisão e proximidade física (para evitar delays altos e geração de tráfego desnecessário). Da mesma forma, deverão ser evitados pontos comuns de falha e a criação de loops. Para tal, recomenda-se o seguinte:

- Selecione, no mínimo, três servidores NTP como referência de tempo com os quais sincronizar. Um número menor é aceitável mas degrada a robustez.
- Considere sincronizar como "peer" com servidores fora da sua hierarquia NTP, de modo a prover redundância.

- Considere sincronizar como "server" com servidores na sua própria hierarquia NTP, de modo a diminuir a instabilidade dentro da própria hierarquia.
- Evite sincronizar o servidor local com outro servidor do mesmo stratum usando associação "peer", a menos que ambos pertençam a hierarquias NTP totalmente independentes, isto minimiza a ocorrência de pontos comuns de falha.
- Evite configurar associações "peer" com servidores de stratum maior que o seu servidor local.

Finalmente, lembre-se que ao considerar um servidor NTP para sincronização, é muito importante que isto seja notificado ao administrador indicado como contato. Servidores NTP não devem ser usados sem permissão prévia.

Comandos de configuração

A sintaxe dos comandos `server` e `peer` é como se segue:

```
server <host> [key <chave> | autokey | publickey <arq_chaves>] [burst]
           [version <versão>] [prefer] [minpoll <valor_min>]
           [maxpoll <valor_max>]
```

```
peer  <host> [key <chave> | autokey | publickey <arq_chaves>] [burst]
           [version <versão>] [prefer] [minpoll <valor_min>]
           [maxpoll <valor_max>]
```

Observações

- host pode ser tanto um nome DNS como um endereço IP. No entanto, devido ao fato de que endereços IP podem mudar com certa facilidade, recomenda-se que se opte por colocar o nome canônico do servidor de tempo.
- Das opções que os comandos acima podem utilizar, existem algumas que se destacam e serão detalhadas em seguida (nos outros casos serão utilizados os valores default):
 - O subcomando `prefer` marca o servidor NTP como sendo o preferido, isto é, em uma relação de igualdade, este servidor será escolhido para sincronização entre uma série de hosts operando corretamente. Embora este subcomando possa ser usado em qualquer associação, seja `peer` ou `server`, é comumente usada em configurações de servidores NTP stratum 1. Desta forma, o servidor NTP stratum 1 escolherá para sincronização, preferencialmente, o relógio de referência ao qual o servidor está conectado.
 - O subcomando `key`, se presente, especifica a chave a ser utilizada no processo de comunicação com o servidor NTP remoto. Este subcomando é usado em conjunto com as opções de autenticação descritas no item C.
 - Os subcomandos `autokey` e `publickey` são utilizados em conjunto com as opções de autenticação, especificamente no esquema de chaves públicas.

Referências adicionais

Configuration Options

http://www.eecis.udel.edu/~ntp/ntp_spool/html/confopt.htm

Association Management

http://www.eecis.udel.edu/~ntp/ntp_spool/html/assoc.htm

Mitigation Rules and the prefer Keyword

http://www.eecis.udel.edu/~ntp/ntp_spool/html/prefer.htm

2.2.1.2.

Opções de controle de acesso

O daemon NTPd implementa uma lista de restrição baseada na dupla endereço IP e máscara. Esta lista é ordenada, em primeira instância, por endereço IP e, em segunda instância, por máscara, obedecendo à seguinte regra básica: o último casamento (match) encontrado definirá as flags de restrição que serão associadas aos pacotes NTP que chegam ao servidor.

O comando básico que implementa o controle de acesso é o comando `restrict`, cuja sintaxe é como se segue:

```
restrict <endereço_IP> mask <máscara> [flag]
```

Algumas observações:

- O endereço IP pode indicar tanto o endereço de um host como o endereço de uma rede.
- A máscara default é 255.255.255.255 que presume que o endereço IP corresponda a um único host.
- A declaração `default` indica o endereço 0.0.0.0 com máscara 0.0.0.0.
- A flag sempre indica restrição de acesso, isto é, a ausência de qualquer flag indicará que não há nenhuma restrição de acesso para o endereço IP especificado.
- As flags de restrição de acesso podem ser de vários tipos, as principais são:
 - **ignore:** Pacotes NTP provenientes de hosts cujos endereços IP casem com a entrada `restrict`, serão ignorados.
 - **noquery:** Pacotes NTP provenientes de hosts cujos endereços IP casem com a entrada `restrict`, que façam algum tipo de consulta ou atentem alguma modificação na configuração do servidor local, serão bloqueados. Em contrapartida, pacotes NTP que requeiram sincronização de tempo, serão permitidos.
 - **nomodify:** Pacotes NTP provenientes de hosts cujos endereços IP casem com a entrada `restrict`, que atentem alguma modificação no servidor NTP local, serão negados.

- **notrust:** Pacotes NTP provenientes de hosts cujos endereços IP casem com a entrada `restrict` serão negados por serem considerados provenientes de uma referência de tempo não confiável.

A seguinte tabela resume a ação provocada por cada uma das flags descritas acima, de acordo à finalidade dos pacotes NTP que chegam:

flag	Sincronização de tempo com o servidor local	Modificação da configuração	Consulta ao o servidor NTP local
ignore	Bloqueado	Bloqueado	Bloqueado
noquery	Permitido	Bloqueado	Bloqueado
nomodify	Permitido	Bloqueado	Permitido

A facilidade de controle de acesso não pretende, nem deve, ser considerada como alternativa à facilidade de autenticação.

Recomenda-se fortemente que principalmente os servidores primários (stratum 1) implementem opções de controle de acesso e autenticação de modo a se protegerem contra intrusos hostis que visam desestabilizar o serviço NTP.

Referências adicionais

Access Control Options

http://www.eecis.udel.edu/~ntp/ntp_spool/html/accopt.htm

2.2.1.3. Opções de autenticação

Esta facilidade permite a um servidor NTP local:

- verificar se o servidor NTP remoto com o qual pretende sincronizar (seja como "peer" ou como "server"), é de fato quem diz ser;
- ser administrado por um servidor NTP remoto através dos utilitários `ntpq` e `ntpdc`. Por exemplo, é possível incluir ou revogar um servidor NTP qualquer que o servidor NTP local use para se sincronizar, sem precisar para tal efetuar login no servidor local e reinicializar o daemon `ntpd`. Por default, esta facilidade está desativada, ou seja, não é qualquer servidor que pode administrar remotamente um servidor NTP, apenas aqueles capazes de se "identificarem" como sendo servidores autorizados.

Dentre as razões que podem justificar o uso de autenticação, podemos citar estas:

- é uma forma de garantir que sejam usadas referências de tempo confiáveis;
- é uma forma de evitar que um atacante distribua (broadcast) tempo errado;
- é uma forma de evitar que um atacante se "disfarçe" como outro servidor e reconfigure remotamente o servidor NTP local.

Como o protocolo NTP implementa a autenticação?

O processo de autenticação no serviço NTP é através de chaves. Ao configurar uma associação (peer, server, broadcast, etc), uma chave de autenticação pode ser especificada, a qual será usada durante a troca de dados entre as máquinas que abrigam os servidores NTP envolvidos na associação em questão.

Quando uma associação acontece no modo autenticado, cada pacote NTP transmitido é acrescentado de um identificador de chave <id_chave> e de uma sequência criptográfica (checksum) gerada a partir desse novo pacote (que inclui o id_chave). Esta sequência é basicamente uma assinatura digital criada usando os algoritmos DES ou MD5. O servidor NTP que recebe o pacote NTP (de posse do arquivo de chaves) realiza o mesmo cálculo do checksum e compara os resultados. Existindo a concordância entre ambos os valores de checksum, a autenticação será realizada com sucesso.

De um modo geral, é preciso que a chave de autenticação seja conhecida previamente pelas partes envolvidas. As chaves e outras informações relacionadas são especificadas no arquivo de chaves, cuja estrutura é tratada com mais detalhes na seção seguinte. Quando o daemon `ntpd` é inicializado, ele lê este arquivo e instala as chaves no cache. A distribuição das chaves pode ser feita utilizando dois mecanismos: o de criptografia de chaves privadas ou o de criptografia de chaves públicas. A versão 3 do protocolo NTP suporta apenas o esquema de chaves privadas, já a versão 4 suporta ambos esquemas.

Por considerar-se que o esquema de criptografia através de chaves públicas ainda encontra-se em um estado de desenvolvimento, o presente documento abordará apenas o esquema de chaves privadas.

Como criar o arquivo de chaves?

No esquema de chaves privadas é utilizado um único arquivo de chaves, que por default é o arquivo `/etc/ntp.keys`. Este arquivo basicamente está formado por entradas que tem a seguinte sintaxe:

```
<id_chave> <tipo_chave> <chave>
```

Onde:

- `id_chave` : Indica o identificador da chave (número inteiro no range 1-65535);
- `tipo_chave`: Indica o formato da chave, que pode ser de quatro tipos:
 - S** - chave em formato DES (número hexadecimal de exatamente 16 dígitos);
 - N** - chave DES em formato NTP (número hexadecimal de exatamente 16 dígitos)
 - A** - chave DES em formato DES (string 1-8 de caracteres ASCII);
 - M** - chave MD5 em formato MD5 (string de 1-31 caracteres ASCII)
- `chave` : Entenda-se como a senha propriamente dita.

Um exemplo deste arquivo pode ser visto no arquivo anexo: `ntp.keys`

Sendo que as senhas associadas às chaves usadas pelos utilitários `ntpq` e `ntpd` são fornecidas manualmente, recomenda-se que elas tenham formato ASCII, isto é, tipo M ou A. Dentre as duas alternativas, opte pelo uso das chaves do tipo M, pois DES é um algoritmo de criptografia com restrições de exportação fora dos EUA.

O arquivo de chaves deverá ter como dono o usuário `root` e permissões de acesso igual a 600.

Comandos de autenticação

Os comandos básicos que permitem implementar autenticação são: `keys`, `trustedkey`, `requestkey`, `controlkey`. O comando `keys` especifica o caminho do arquivo de chaves, enquanto que o comando `trustedkey` especifica as chaves consideradas "confiáveis" (chaves não comprometidas). Os comandos `requestkey` e `controlkey` especificam as chaves que serão utilizadas como senhas pelos utilitários `ntpq` e `ntpd`, respectivamente, e que permitirão configurar remotamente o servidor NTP.

A sintaxe dos comandos acima mencionados é como se segue:

```
keys <arquivo_chaves>
trustedkey <id_chave1> <id_chave2> <id_chave3> ...<id_chave_ntpq>
                                                <id_chave_ntpd>
requestkey <id_chave_ntpq>
controlkey <id_chave_ntpd>
```

Repare que os identificadores das chaves usadas pelos utilitários `ntpq` e `ntpd` devem ser incluídas na lista de chaves "confiáveis".

Referências adicionais

Authentication Options

http://www.eecis.udel.edu/~ntp/ntp_spool/html/authopt.htm

Autonomous Authentication

<http://www.eecis.udel.edu/~mills/autokey.htm>

ntp_genkeys - generate public and private keys

http://www.eecis.udel.edu/~ntp/ntp_spool/html/genkeys.htm

2.2.1.4.

Opções de logging

É possível habilitar o registro de logs do servidor NTP através de dois comandos: `logconfig` e `logfile`.

O comando `logconfig` controla a quantidade e o tipo de informação que será registrada pelo sistema de logs usando o mecanismo de `syslog`. Alternativamente, estas mesmas informações podem ser armazenadas em um arquivo de logs específico. Neste último caso é utilizado o comando `logfile`. Na ausência da diretiva `logfile`, assume-se que será utilizado o mecanismo de `syslog`.

As mensagens de logs podem ser divididas em quatro classes:

clock	Informações relacionadas ao relógio
peer	Informações relacionadas aos servidores peer
sys	Informações relacionadas ao sistema
sync	Informações relacionadas ao processo de sincronização

Dentro destas classes, quatro tipos de mensagens podem ser controladas:

events	Mensagens que controlam o registro de eventos do tipo: facilidade de alcance, sincronização, condições de alarme, etc
statistics	Mensagens que controlam dados estatísticos
status	Mensagens que descrevem o status da sincronização
info	Mensagens que controlam informação de configuração

A sintaxe dos comandos `logconfig` e `logfile` é respectivamente:

```
logconfig < chave_de_configuração >  
logfile < outro_arquivo_de_logs >
```

As chaves de configuração são formadas concatenando a classe de mensagem e o tipo de evento, e elas podem ser precedidas pelos símbolos: +, - e =, que adicionam, removem e configuram uma mensagem, respectivamente. O prefixo `all` pode ser usado no lugar de uma classe de mensagem.

As combinações dependerão do objetivo que se tenha, por exemplo:

- Ao ser ativado o serviço NTP, recomenda-se que se configure o servidor para mostrar informações mais detalhadas das registradas por default, isto é, algo do tipo:

```
logconfig =syncevents +peerevents +sysevents +allclock
```

Que fará com que os eventos relacionados ao processo de sincronização, aos servidores `peers` e ao sistema sejam logados.

- Uma configuração mínima poderia ser como segue:

```
logconfig =syncall +clockall
```

Que implicará no registro de quaisquer mensagens relacionadas ao processo de sincronização e ao relógio.

- Na dúvida, habilite totalmente o sistema de logs através da seguinte cláusula:

```
logconfig =all
```

O CAIS recomenda que seja esta a opção escolhida.

Referências adicionais

Miscellaneous Options

http://www.eecis.udel.edu/~ntp/ntp_spool/html/miscopt.htm

2.2.1.5. Opções diversas

driftfile

Um dos primeiros passos que o daemon `ntpd` realiza quando inicializado, é computar o erro de frequência do relógio no computador onde ele está rodando. Normalmente, pode levar um dia ou mais para o daemon estimar um valor adequado (e ele precisa de uma boa estimativa para sincronizar com o servidor NTP). Uma vez que este valor é computado, ele mudará de maneira pouco significativa durante o transcurso da operação.

O comando `driftfile` indicará ao daemon o nome do arquivo que armazena o valor estimado corrente do erro da frequência. Caso a conexão de rede esteja temporariamente indisponível, ou mesmo se o daemon tiver que ser reinicializado, o protocolo NTP poderá usar este valor como valor inicial, de modo que seja evitada a perda de tempo no dia em recalculá-lo. Assim, a inclusão deste comando é primordial.

O nome e caminho default deste arquivo é `/etc/ntp.drift`. Lembre-se da necessidade de criá-lo previamente usando, para tal, o conhecido comando `touch`, tendo como valor inicial 0.

```
# touch /etc/ntp.drift (UID=root, permissões=600)
```

Referências adicionais

Miscellaneous Options

http://www.eecis.udel.edu/~ntp/ntp_spool/html/miscopt.htm

3. Implementando o Cliente NTP

3.1. Instalação e Configuração em sistemas UNIX

1. Verificar que o horário, data e timezone da máquina estejam apropriadamente configurados.
2. Copiar os binários `ntpd` e `ntpdate`, gerados durante o processo de compilação do servidor NTP, para o diretório `/usr/local/bin` da máquina que atuará como cliente NTP. O dono (UID=root) e as permissões de acesso (755) deverão ser mantidos.

3. Executar o comando:

```
# ntpdate <ip_servidor_NTP_local>
```

Lembre-se que leva em torno de 5 minutos para que o cliente NTP sincronize adequadamente com o servidor remoto, seja paciente.

4. Incluir no `crontab` do usuário root a seguinte linha:

```
0 * * * * /usr/local/bin/ntpdate <ip_servidor_NTP_local> /dev/null
```

Isto fará com que o cliente NTP, a cada hora, sincronize remotamente com o servidor NTP local e as mensagens geradas por esta operação sejam desprezadas.

Em particular, se a máquina cliente NTP também atua como LOGHOST, recomenda-se que o tempo entre uma sincronização e outra seja menor, talvez a cada 30 minutos. Nesse caso, a linha a ser incluída deverá ser:

```
0,30 * * * * /usr/local/bin/ntpdate <IP_servidor_NTP_local> /dev/null
```

3.2. Instalação do cliente NTP em sistemas Windows

Que cliente NTP usar?

O CAIS fez um levantamento das ferramentas freeware que atuam como clientes NTP/SNTP, dentre elas:

NTPdate (binário que acompanha a distribuição oficial do NTP4)

<http://www.eecis.udel.edu/~ntp>

AnalogX Atomic TimeSync

<http://www.analogx.com/contents/download/network/ats.htm>

Dimension 4

<http://www.thinkman.com/dimension4>

WorldTime

Após elas terem sido testadas e avaliadas, o CAIS considerou a ferramenta Dimension 4 como sendo a de configuração mais intuitiva e completa, bem como de tamanho razoável para ser instalada nas máquinas clientes. Assim sendo, o seguinte procedimento considera o uso desta ferramenta:

1. Fazer o download da ferramenta a partir do seguinte site:

<http://www.thinkman.com/dimension4>

2. Proceder com a instalação da mesma.
3. Após a instalação, será preciso realizar alguns ajustes na configuração, para tal:

a) Execute o programa `dimension4`.

O programa irá inicializar e ficará minimizado na barra inferior próximo ao relógio do Windows.

b) Posicionando o mouse em cima do ícone minimizado, clique o botão direito do mouse e escolha a opção **Open**. Imediatamente, uma janela de título **Dimension 4** será mostrada na tela.

c) A configuração em si envolve os seguintes passos:

- Remover todas as opções de servidores NTP listados, alguns deles não disponibilizam mais o serviço NTP e outros não podem ser livremente acessados.
- Adicionar na lista o seu servidor NTP local, para tal basta:
 - Clicar no botão **Add**
 - Preencher o campo **Server** com o IP/nome do servidor NTP local, de preferência use o IP
 - Preencher o campo **Location** com alguma informação que permita identificar o servidor, por exemplo: "Servidor NTP Local"
 - Escolher o SNTP como protocolo a ser usado
 - Clicar no botão **OK** para efetivar a inclusão do servidor NTP
- Clicar no botão **Advanced**. Uma janela de título **Dimension 4 Advanced Settings** será mostrada.

- Na caixa de diálogo **Message Boxes** desabilitar as opções **Display Errors** e **Display Synchronization**
- Clicar no botão **OK**

- Na caixa de diálogo **How Often**, configurar de modo que a cada 30 minutos seja feita a sincronização.

- Por último, clicar no botão **OK** e minimizar o programa. A configuração default já considera a execução automática do programa após a reinicialização da máquina.

4. Implementando o serviço NTP em Roteadores

4.1. Configuração do serviço NTP em roteadores Cisco

Um modelo com os comandos que devem ser incluídos no arquivo de configuração pode ser consultado no **Anexo 06** deste documento.

O seu roteador Cisco pode ser configurado para que o relógio do sistema esteja sincronizado via NTP ou até mesmo para que ele sirva como base de tempo a outros computadores/equipamentos de rede. Para tal, bastará seguir o procedimento abaixo descrito. Embora este tenha sido baseado no IOS versão 12.0 T(5), de um modo geral, pode ser considerado como procedimento padrão para outras versões.

1. Antes de proceder com a configuração do roteador para sincronizar usando o protocolo NTP, é preciso verificar que alguns parâmetros locais relacionados ao tempo e data do sistema tenham sido adequadamente configurados. Estes parâmetros dizem respeito ao timezone, horário de verão e relógio local.

a) Para configurar manualmente o timezone, utilize o comando `clock timezone`, no modo de configuração global, cuja sintaxe é como segue:

```
clock timezone < zona > < horas > [< minutos >]
Ex. clock timezone GMT-3 -3
```

b) Caso o seu roteador esteja localizado em uma área afetada pelo horário de verão, é possível usar qualquer uma das alternativas oferecidas pelo comando `clock summer-time`, executado no modo de configuração global:

```
clock summer-time < zona > recurring [< semana > < DD > < MM > < AA >
    hh:mm < semana > < DD > < MM > < AA > hh:mm [offset]]
clock summer-time < zona > date < DD > < MM > < AA > hh:mm < DD > < MM >
    < AA > hh:mm [offset]
```

No Brasil, não existindo um padrão para aplicação do horário de verão, deverá ser usada a segunda opção, na qual são colocados o início e fim do período do horário de verão.

```
Ex. clock summer-time GMT-2 date Oct 3 1999 0:00 Feb 27 2000 0:00
```

c) De igual forma, é importante que o relógio do sistema seja previamente configurado. O comando `clock set`, executado no modo EXEC, pode auxiliar nesta tarefa.

2. A configuração do roteador inclui:

a) Configuração das opções de associação

Como se viu no item 2.2.1: Opções de Configuração, existem 4 modos de associação entre servidores NTP. De modo particular, para implementar associações nos modos cliente/servidor (server) e simétrico (peer), bastará serem usados os comandos `ntp server` e `ntp peer`, respectivamente. A sintaxe destes comandos é como segue:

```
ntp server < endereço_IP > [version < versão >] [key < id_chave >]
[source < interface >] [prefer]
ntp peer < endereço_IP > [version < versão >] [key < id_chave >]
[source < interface >] [prefer]
```

Supondo que você queira sincronizar o seu roteador com o servidor primário da RNP (`ntp1.rnp.br`), no modo server, deverá ser incluída a seguinte diretiva:

```
ntp server ntp1.rnp.br
```

b) Configuração das opções de autenticação

Para configurar seu roteador de modo que seja feita a autenticação com outros servidores através de chaves, é preciso incluir as seguintes diretivas, no modo de configuração global:

ntp authenticate	Habilita a autenticação
ntp authentication-key <id_chave> <tipo_chave> <chave>	Define as chaves para autenticação
ntp trusted-key <id_chave>	Especifica as chaves confiáveis

Lembre-se que os IOS atuais suportam apenas chaves de tipo MD5 e o valor da chave está no intervalo < 1-65535 >. Assim, supondo que seu roteador sincronize com servidores de IP `aaa.aaa.aaa.aaa` e `bbb.bbb.bbb.bbb`, que os identificadores das chaves destes servidores sejam respectivamente 5 e 6, e, que os valores associados sejam 1000 e 1001, você deverá incluir as seguintes linhas na configuração:

```
ntp server aaa.aaa.aaa.aaa key 5
ntp server bbb.bbb.bbb.bbb key 6
ntp authenticate
ntp authentication-key 5 md5 1000
ntp authentication-key 6 md5 1001
ntp trusted-key 14
```

Nos sistemas Unix, estes valores são comumente definidos no arquivo `/etc/ntp.keys`.

c) Configuração das opções de controle de acesso

É possível implementar o controle de acesso em dois níveis:

- criando um grupo de acesso (AG - Access Group) e associando-o a uma lista de acesso (AL - Access List);
- desativando o serviço NTP em uma determinada interface.

No primeiro caso bastará usar o seguinte comando no modo de configuração global:

```
ntp access-group [query-only | serve-only | serve | peer] <lista_de_acesso>
```

As opções do grupo de acesso são como se segue (listadas por ordem de restrição, da menor à maior):

peer	Permite a servidores remotos, previamente autorizados, fazerem consultas e sincronizarem com o servidor NTP local. Assim também, se preciso for, é permitido que o servidor NTP remoto use o servidor
serve	NTP local como base de tempo. Permite a servidores remotos, previamente autorizados, fazerem consultas e sincronizarem com o servidor NTP local. No entanto, não é permitido que o servidor NTP remoto use o servidor NTP local como base de tempo
serve-only	Permite a servidores remotos, previamente autorizados, usarem o servidor NTP local como base de referência
query-only	Permite a servidores remotos, previamente autorizados, fazerem apenas consultas ao servidor NTP local

No segundo caso, o comando a ser usado será:

```
ntp disable
```

d) Configuração da interface de saída de pacotes NTP

A seguinte diretiva, usada no modo de configuração global, permitirá especificar a interface pela qual os pacotes NTP serão enviados:

```
ntp source <interface>
```

e) Configuração do calendário

Em sistemas que tenham calendários, é possível configurar o roteador de forma tal que este seja sincronizado periodicamente via NTP. Para tal, bastará incluir a seguinte diretiva no arquivo de configuração:

```
ntp update-calendar
```

f) Configuração do sistema como servidor NTP autoritativo

Caso a intenção seja, além de sincronizar o relógio do seu roteador via NTP, que **este** o roteador sirva também de base de tempo a outros computadores, deverá ser incluída a seguinte diretiva:

```
ntp master [stratum]
```

A opção `stratum` apenas será necessária caso o sistema não utilize nenhuma referência de tempo externa para sincronização.

A título de ilustração é incluído um modelo de configuração do serviço NTP em roteadores Cisco, veja o **Anexo 06**.

3. Para monitorar o relógio, o calendário (quando existir) e alguns serviços NTP, podem ser utilizados os seguintes comandos:

show calendar	Mostra o tempo corrente do calendário
show clock [detail]	Mostra o tempo corrente do relógio do sistema
show ntp associations [detail]	Mostra o status das associações NTP
show ntp status [detail]	Mostra o status do serviço NTP

A título de ilustração, são mostradas a seguir as saídas respectivas dos comandos acima, executados no roteador `cisco-cais.cais.rnp.br`:

```
cisco-cais#show clock
20:34:13.487 GMT-3 Tue Jul 11 2000
```

```
cisco-cais#show clock detail
20:35:04.318 GMT-3 Tue Jul 11 2000
Time source is NTP
Summer time starts 00:00:00 GMT-3 Sun Oct 3 1999
Summer time ends 00:00:00 GMT-2 Sun Feb 27 2000
```

```
cisco-cais#show ntp status
Clock is synchronized, stratum 3, reference is 200.144.121.33
nominal freq is 250.0000 Hz, actual freq is 249.9968 Hz, precision is 2**19
reference time is BD289F9C.8A8F5A49 (20:22:04.541 GMT-3 Tue Jul 11 2000)
clock offset is -8.3184 msec, root delay is 452.48 msec
root dispersion is 468.83 msec, peer dispersion is 376.28 msec
```

```
cisco-cais#show ntp associations
address          ref clock      st  when  poll reach  delay  offset  disp
*~200.144.121.33 128.4.1.1     2   36   64  177    4.1   -6.36  127.2
* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured
```

Referências

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_c/fcprt3/fcgenral.htm

5. ANEXOS

Anexo 01 Terminologia NTP

dispersão (clock dispersion/jitter)

Em um processo repetitivo de leitura do tempo de um relógio, as diferenças podem variar aleatoriamente. A diferença entre estas diferenças é chamada de jitter.

drift (clock drift)

Medida (em hertz por segundo) que determina que tão rápido varia o skew de um relógio.

estabilidade (clock stability)

Determina que tão bem um relógio pode manter uma frequência constante.

exatidão (clock accuracy)

Determina que tão perto um relógio encontra-se de uma referência de tempo padrão como a UTC.

GMT - Greenwich Mean Time

Referência padrão de tempo, predecessora do padrão UTC. Obtém o tempo a partir de eventos astronômicos, tal como o dia solar.

GPS - Global Positioning System

Constelação de 24 satélites orbitando a Terra que, através da transmissão de sinais, permite determinar o tempo corrente com altíssimo grau de precisão.

NTP - Network Time Protocol

Protocolo Internet usado para sincronizar os relógios de computadores (e alguns equipamentos de rede) com a referência de tempo padrão UTC.

offset (clock offset)

diferença de tempo entre dois relógios, comumente expressado em milissegundos.

pacote NTP (NTP packet)

Mensagem enviada pela rede em conformidade ao formato do protocolo NTP.

precisão (clock precision)

Menor incremento de tempo possível que pode ser lido por um programa.

relógio de referência (reference clock)

Dispositivo que provê tempo corrente com altíssima precisão. Tipicamente, estes dispositivos podem ser relógios atômicos, receptores GPS ou receptores de rádio.

resolução (clock resolution)

Menor incremento de tempo possível que um relógio permite.

roundtrip delay

Tempo que leva um host para enviar um pacote NTP a outro host e receber em resposta um outro pacote NTP.

servidor primário (primary server)

Outro nome dado a um servidor NTP stratum 1.

servidor secundário (secondary server)

Outro nome dado a um servidor NTP stratum 2.

skew (clock skew)

diferença (em hertz) entre a frequência real de um relógio e a frequência que deveria ter para atingir o tempo perfeito.

stratum

Nível da hierarquia NTP. NTP classifica os servidores em níveis (estratos), indicando desta forma qual a distância deste servidor a um relógio de referência. O nível 1 indica um servidor diretamente conectado a um relógio de referência, enquanto que o maior nível (stratum 16) costuma indicar que o relógio encontra-se inoperante ou inacessível. De modo geral, um servidor de stratum "n" encontra-se a (n-1) hops do stratum 1 da hierarquia NTP à qual pertence.

UTC - Universal Time Coordinated

Referência padrão de tempo aceita mundialmente. Obtém o tempo a partir da ressonância magnética do átomo de césio.

Anexo 02

Modelo de Arquivo de Configuração dos Servidores NTP da Hierarquia NTP

```
# @Copyright - Centro de Atendimento a Incidentes de Segurança (CAIS)
# Modelo de Arquivo de Configuração dos Servidores NTP da Hierarquia NTP
# Host      : ntp.pop-xx.rnp.br (IP_servidor_local)
# Stratum  : 2
# Arquivo  : /etc/ntp.conf (versão 4)
#
# Última atualização: 20/07/2000
#
# ----- OPÇÕES DE ASSOCIAÇÃO -----
server ntp1.rnp.br           # Stratum 1 da RNP
server ntp.outro.servidor.ntpS1 # Stratum 1 no Brasil
server ntp.outro.servidor.ntpS1 # Stratum 1 no exterior
peer  ntp.pop-zz.rnp.br      # Stratum 2 na hierarquia NTP da RNP
peer  ntp.outro.servidor.ntpS2 # Stratum 2 em outra hierarquia NTP
#
# ----- OPÇÕES DE AUTENTICAÇÃO -----
#
# Se você for implementar autenticação para permitir a configuração remota do
# seu servidor NTP, será preciso criar o arquivo de chaves ntp.keys. e definir
# as chaves associadas através das diretivas requestkey (ntpq) e controlkey
# (ntpd)
# NÃO USE OS VALORES DEFAULTS abaixo (65535), defina os seus próprios.
#
# keys /etc/ntp.keys
# trustedkey 65535
# requestkey 65535
# controlkey 65535
#
# ----- OPÇÕES DE CONTROLE DE ACESSO -----
# Descomente a linha 'restrict default', de acordo com a política de
# acesso que você irá adotar:
#
# a) Política de acesso "DENY DEFAULT", isto é, a menos que se indique o
# contrário não é permitido nenhum tipo de acesso (ignore =
# noquery+notime+nomodify)
# Assim também, por default, não considero confiável ("notrust") nenhum
# servidor NTP, mesmo este podendo acessar o servidor local.
#
# restrict default ignore notrust
#
# Neste caso será preciso permitir explicitamente o acesso às máquinas
# conectadas à rede local e a outros servidores (stratum 3) que atuem com
# clientes NTP.
#
# restrict IP_rede_local mask 255.255.255.0 nomodify
# restrict IP_cliente1_ntp nomodify
```

```

# restrict IP_cliente2_ntp nomodify
# restrict IP_cliente3_ntp nomodify
#   ... e assim por diante.
#
# -----
# b) Política de acesso "PERMIT DEFAULT", isto é, a menos que se indique o
#   contrário é permitido a qualquer servidor NTP sincronizar com o servidor
#   local (time) e fazer consultas remotas ("query"). No entanto, por default,
#   não considero confiável ("trust") nenhum servidor NTP, mesmo este podendo
#   acessar o servidor local.
#
# restrict default nomodify notrust
#
# -----
# As seguintes linhas deverão ser incluídas para ambas as políticas de acesso.
#
# - Não permitir aos servidores NTP com os quais o servidor local for
#   sincronizar,
#   fazerem modificacoes na configuração
#
restrict IP_ntp1.rnp.br          nomodify      # Stratum 1 da RNP
restrict IP_ntp.outro.servidor.ntpS1 nomodify  # Stratum 1 no Brasil
restrict IP_ntp.outro.servidor.ntpS1 nomodify  # Stratum 1 no exterior
restrict IP_ntp.pop-zz.rnp.br    nomodify    # Stratum 2 na hierarquia
NTP da RNP
restrict IP_ntp.outro.servidor.ntpS2 nomodify  # Stratum 2 em outra
hierarquia
#
# - Não deverá existir restrição nenhuma para a máquina local, a partir dela
#   será feita
#   inclusive a configuração.
restrict IP_servidor_NTP_local          # ntp.pop-xx.rnp.br
restrict 127.0.0.1## ----- OPÇÕES DE MONITORAMENTO-----
statistics loopstats
statsdir /var/log/ntp/
filegen peerstats file peers type day link enable
filegen loopstats file loops type day link enable
#
# ----- OPÇÕES DE LOGGING -----
logconfig all
logfile /var/log/ntp/ntp.log
#
# ----- OPÇÕES DIVERSAS -----
driftfile /etc/ntp.drift

```

Anexo 03

Arquivo de inicialização do servidor NTP (Solaris)

```
# Arquivo de inicializacao do servidor NTP (Solaris)
# O arquivo de configuracao e' o /etc/ntp.conf (default)
#
#!/bin/sh
killproc() {      # kill named processes
    pid=`usr/bin/ps -e |
        /usr/bin/grep ntpd |
        /usr/bin/sed -e 's/^ *//' -e 's/ .*//'\`
    [ "$pid" != "" ] && kill $pid
}
case "$1" in
'start')
    ps -e | grep ntpd > /dev/null 2>&1
    if [ $? -eq 0 ]
    then
        echo "ntp daemon already running. ntp start aborted"
        exit 0
    fi
    if [ -f /etc/ntp.conf -a -x /usr/local/bin/ntpd ]
    then
        /usr/local/bin/ntpd -c /etc/ntp.conf
    fi
    ;;
'stop')
    killproc ntpd
    ;;
*)
    echo "Usage: /etc/init.d/ntp { start | stop }"
    ;;
esac
```

Anexo 04

Arquivo de inicialização do servidor NTP (Red Hat Linux)

```
# Arquivo de inicializacao do servidor ntpd (RedHat Linux)
# O arquivo de configuracao e' o /etc/ntp.conf (default)
#
#!/bin/sh
#
# ntpd          This shell script takes care of starting and stopping
#               ntpd
#
# chkconfig: - 55 10
# description: ntpd is the NTPv3 daemon.

# Source function library.
. /etc/rc.d/init.d/functions

# Source networking configuration.
. /etc/sysconfig/network

# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0

[ -x /usr/local/bin/ntpd -a -f /etc/ntp.conf ] || exit 0

RETVAL=0

# See how we were called.
case "$1" in
  start)
    # Adjust time to make life easy for ntpd
    if [ -f /etc/ntp/step-tickers ]; then
      echo -n "Syncing time for ntpd. "
      /usr/local/bin/ntpdate -s -b -p 8 -u `cat /etc/ntp/step-
tickers`
    fi
    # Start daemons.
    echo -n "Starting ntpd: "
    daemon /usr/local/bin/ntpd
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && touch /var/lock/subsys/ntpd
    ;;
  stop)
    # Stop daemons.
    echo -n "Shutting down ntpd: "
    killproc ntpd
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/ntpd
```

```
;;
status)
    status ntpd
    RETVAL=$?
    ;;
restart|reload)
    $0 stop
    $0 start
    RETVAL=$?
    ;;
*)
    echo "Usage: ntpd {start|stop|restart|status}"
    exit 1
esac

exit $RETVAL
```

Anexo 05

Modelo para divulgação de informações sobre o seu servidor NTP stratum 2

```
# Modelo para divulgação de informações sobre o seu servidor NTP stratum 2
# Corresponde ao servidor NTP do CAIS/RNP (stratum 2)
#
ntp.cais.rnp.br (200.144.121.33)
Location: Brazilian Research Network/Rede Nacional de Pesquisa (RNP)
Synchronization: NTP V4 Secondary (stratum 2), SunSparc10/Solaris
Service Area: Brazil
Access Policy: Open access to stratum 2 and stratum 3 NTP servers.
                Please, send a mail to notify.
Contact: ntp-admin@cais.rnp.br
```

Anexo 06

Modelo de Arquivo de Configuração de Chaves

```
# @Copyright - Centro de Atendimento a Incidentes de Segurança (CAIS)
# Modelo de Arquivo de Configuração de Chaves
# Arquivo :/etc/ntp.keys
#
# Última atualização: 20/07/2000
#
#
# <id_chave> <tipo_chave> <chave>
#
1          N          461ECD6AE29233E0
#Chave DES em formato NTP (hexadecimal)
#
2          M          QvYotMRIrop8KPPv
#Chave MD5 em formato MD5 (ASCII 32 char)
#
8          A          c0nfred
#Chave DES em formato DES (ASCII 8 char)
#
9          M          c0nfredit0
#Chave MD5 em formato MD5 (ASCII 32 char)
#Esta chave será usada com os utilitários ntpq e ntpdc
```

Anexo 07

Modelo para configuração do serviço NTP em um roteador Cisco

```
! @Copyright - Centro de Atendimento a Incidentes de Segurança (CAIS)
! Modelo para configuração do serviço NTP em um roteador Cisco
!
! Última atualização: 20/07/2000
!
! ----- Configuração do horário e timezone local -----
clock timezone GMT-3 -3
!
! Se a região onde o roteador encontra-se é afetada pelo horário de verão, a
! seguinte linha deverá ser descomentada e modificada de acordo ao período que
! compreende o horário de verão.
!
! clock summer-time GMT-2 date Oct 3 1999 0:00 Feb 27 2000 0:00
!
! ----- Configuração do Serviço NTP -----
!
! A título de ilustração, considere o modelo seguinte:
!
!      ___      Eth1      ___      Eth0      ___
!      {___}-----|_____|-----|___|-----
!      Internet      Roteador      Rede Local
!
! Escolha a opção a) ou b), de acordo à função do seu roteador. Em seguida,
! descomente e substitua as informações contidas nas linhas abaixo com os seus
! dados:
!
! a) Configurando seu roteador como cliente NTP apenas
!     1. Aponte para o servidor NTP local.
!         ntp server ntp.cais.rnp.br
!     2. Desabilite o serviço ntp na interface externa
!         interface Eth1
!             ntp disable
!     3. Indique a interface por onde chegam os pacotes NTP
!         ntp source Eth0
!
! b) Configurando seu roteador como servidor NTP local (stratum 2)
!     1. Liste os servidores com os quais sincronizar, recomenda-se
!         no mínimo 3:
!         ntp server IP.ntp1.rnp.br          ! Stratum 1 da RNP
!         ntp server IP.servidor.ntp.S1     ! Stratum 1 no Brasil
!         ntp server IP.servidor.ntp.S1     ! Stratum 1 no exterior
!         ntp peer  IP.servidor.ntp.S2     ! stratum 2 na hierarquia NTP
!     2. Indique a(s) interface(s) por onde chegam os pacotes NTP
!         ntp source Eth0
!         ntp source Eth1
!     3. Configure as opções de autenticação, se achar necessário.
!         Substitua <id_chaveN> e <chaveN> por valores escolhidos.
!         ntp authenticate
```

```
!         ntp authentication-key <id_chave1> md5 <chave1>
!         ntp authentication-key <id_chave2> md5 <chave2>
!         ntp trusted-key <id_chave1> <id_chave2> <id_chave_ntpq>
!         <id_chave_ntpdc>
! 4. Configure as opções de controle de acesso, se achar necessário.
! 5. Configure o calendário, caso o seu roteador o tenha.
!         ntp update-calendar
! 6. Configure seu roteador como servidor NTP autoritativo
!         ntp master
```