Hardening de Servidores Web Apache

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

- Introdução
- Configurações gerais
- Multi-Processes Modules
- Logs
- Ocultando informações do sistema
- Ativando/Desativando sites de usuários do sistema
- Configurando diretório restrito
- Outras Configurações de Segurança
  - Módulos de segurança

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Introdução

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Introdução

- Servidor livre mais utilizado
- Compatível com o protocolo HTTP versão 1.1
- Funcionalidades são mantidas através de uma estrutura de módulos

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Introdução

- Versão 1.3
  - multiprocessos
- Versão 2.0 em diante
  - threads
- Hardening?

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Configurações Gerais

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Configurações Gerais

- Como testar as modificações?
  # apache2ctl configtest

- Reiniciar servidor ("*restart* " ou "*stop* " / "*start* " não recomendados para servidor em produção)
  # apache2ctl graceful

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Configurações Gerais

- Permissões dos diretórios

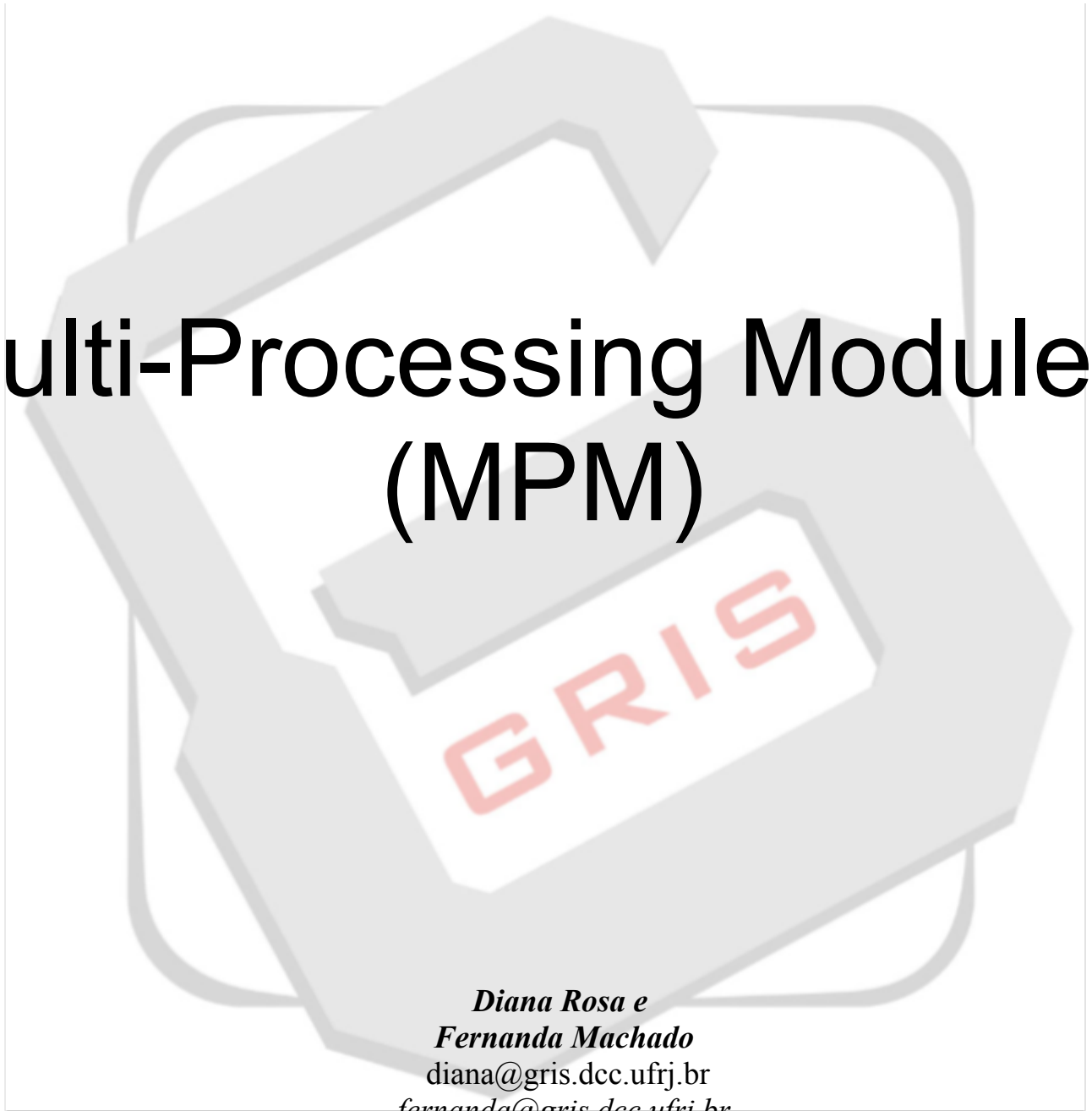
```
# chown 0 . bin conf logs cgi-bin htdocs
# chgrp 0 . bin conf logs cgi-bin htdocs
# chmod 755 . bin conf logs cgi-bin htdocs
# chown 0 bin/apache2 *
# chgrp 0 bin/apache2
# chmod 511 bin/apache2
# chown 0 sbin/apache2ctl
# chgrp 0 sbin/apache2ctl
# chmod 511 sbin/apache2ctl
```

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Configurações Gerais

- Diretivas
- **Timeout**
  Timeout 300
- **KeepAlive**
  KeepAlive On
- **MaxKeepAliveRequests**
  MaxKeepAliveRequests 100
- **KeepAliveTimeout**
  KeepAliveTimeout 15

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br



Multi-Processing Modules (MPM)

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Multi-Processing Modules

- MPM Prefork
  processos
- MPM Worker
  threads

$ ./configure --prefix=/usr/local/apache2 –with-mpm=<TIPO_MPM>

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

MPM Prefork

- *StartServers* : número de processos para iniciar. O valor deve estar entre 5 e 10.
- *MinSpareServers* : número mínimo de processos ociosos em dado momento. O valor deve estar entre 5 e 10.
- *MaxSpareServers* : número máximo de processos ociosos em dado momento. Recomenda-se 10 ou menos.

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

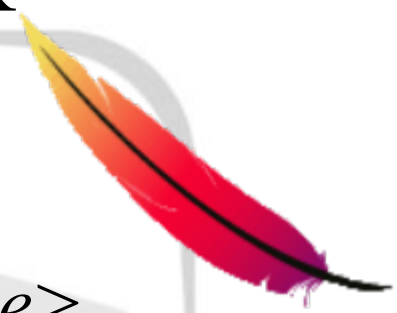
MPM Prefork

- *MaxClients* : número máximo de processos que podem ser ativados. O valor deve ser igual ou menor que o da diretiva *ServerLimit* (cuja configuração recomendada é 256).

- *MaxRequestsPerChild* : número máximo de conexões que um processo servidor pode atender.

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

MPM Prefork



- *<IfModule mpm_prefork_module>*
- *StartServers 5*
- *MinSpareServers 5*
- *MaxSpareServers 10*
- *MaxClients 150*
- *MaxRequestsPerChild 150*
- *</IfModule>*

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

MPM Worker

- StartServers: número inicial de processos para iniciar.
- MaxClients: número máximo de conexões simultâneas de cliente.
- MinSpareThreads: número mínimo de threads em dado momento.

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

MPM Worker

- *MaxSpareThreads: número máximo de threads em dado momento.*
- *ThreadsPerChild: número constante de threads em cada processo.*
- *MaxRequestsPerChild: número máximo de conexões ao servidor de processo.*

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

MPM Worker

- *<IfModule mpm_worker_module>*
- *StartServers 5*
- *MaxClients 150*
- *MinSpareThreads 25*
- *MaxSpareThreads 75*
- *ThreadsPerChild 25*
- *MaxRequestsPerChild 150*
- *</IfModule>*

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

LOG

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

LogLevel

- /var/log/apache2/error.log

Exemplo: LogLevel warn

- debug: nível de depuração de mensagem
- info: informativo
- notice: normal mas condição importante
- warn: condições de aviso
- error: condições de erro
- crit: condições críticas
- alert: a ação deve ser empregada imediatamente
- emerg: sistema em emergência, inutilizável

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

LogFormat

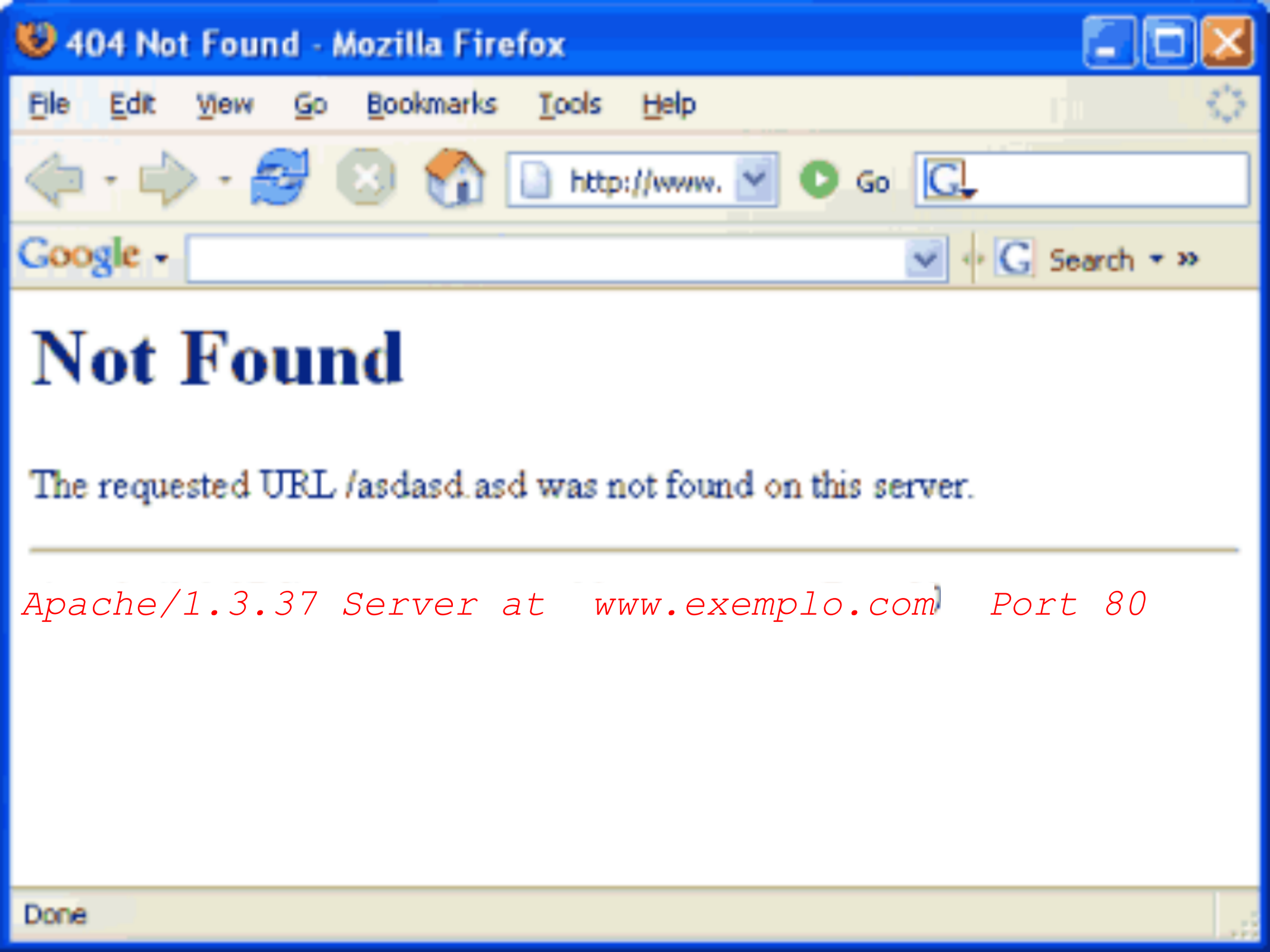
- LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined

Isto significa, na ordem: hostname ou endereço IP do cliente, o usuário remoto via identd, o usuário remoto via autenticação HTTP, o período em que a solicitação foi servida, o texto da solicitação, o código do status, e o tamanho em bytes do conteúdo servido.

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Ocultando informações do sistema

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br


404 Not Found - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.
Go
Google
Search
Not Found
The requested URL /asdasd.asd was not found on this server.
Apache/1.3.37 Server at www.exemplo.com Port 80
Done

Redirecionando página de erro

Configurando essas directivas, as páginas de erro default que mostram a assinatura do servidor serão trocadas por páginas personalizadas criadas junto às demais.

ErrorDocument 400 400.html
ErrorDocument 403 403.html
ErrorDocument 404 404.html
ErrorDocument 500 500.html

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

ServerTokens

- Prod: exibe apenas o nome do produto. (ex: "Apache")
- Major: exibe o valor da versão principal (ex: "Apache/2")
- Minor: exibe a versão com "duas casas" (ex: "Apache/2.0")
- Min: exibe a versão completa (ex: "Apache/2.0.41")
- OS: inclui versão completa e sistema operacional (ex: "Apache/2.0.41 (Unix)")
- Full: inclui também versão de módulos carregados (ex: "Apache/2.0.41 (Unix) mod_ssl/2.0.49 OpenSSL/0.9.7d DAV/2")

- `ServerTokens Prod`

Diana Rosa
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

ServerSignature

- On: exibirá todas as informações sobre o Apache
- Off : não exibirá nenhuma informação
- Email: pode-se colocar o link para seu endereço de correio eletrônico

```
ServerSignature Off
```

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

ServerSignature

- **FingerPrint**

$ nc 202.41.76.251 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Sun, 15 Jun 2003 17:10: 49 GMT
Server: Apache/1.3.23
Last-Modified: Thu, 27 Feb 2003 03: 48: 19 GMT
ETag: 32417-c4-3e5d8a83
Accept-Ranges: bytes
Content-Length: 196
Connection: close
Content-Type: text/HTML

$ nc iis.example.com 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Content-Location: http://iis.example.com/x.htm
Date: Fri, 01 Jan 1999 20:13: 52 GMT
Content-Type: text/HTML
Accept-Ranges: bytes
Last-Modified: Fri, 01 Jan 1999 20:13: 52 GMT
ETag: W/e0d362a4c335be1: ae
Content-Length: 133

Diana Rosalia
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

ServerSignature

- **`FingerPrint`**

403 HTTP/1.1
Forbidden Date: Mon, 16 Jun 2003 02:41: 27 GMT
Server: Unknown-Webserver/1.0
Connection: close
Content-Type: text/HTML;
charset=iso-8859-1

httprint

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Escondendo uso de PHP

- *Escondendo o PHP como outra linguagem*

AddType application/x-httpd-php .asp .py .pl

- *Ocultando usando extensões desconhecidas*

AddType application/x-httpd-php .bop .foo .133t

- *Escondendo o PHP usando extensão HTML*

AddType application/x-httpd-php .htm .html

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Ativando/Desativando sites de usuários do sistema

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Ativando/Desativando sites de usuários do sistema

- Para permitir que os usuários do sistema possam adicionar conteúdo Web em seus diretórios “public_html”, acessado da Web como “http://www.site.com/~usuario/”:
  - *UserDir enabled*
  - *UserDir disabled root*

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Configurando diretório restrito

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Configurando diretório restrito

```
<Directory "/var/www/pagina">
Options Indexes FollowSymLinks Includes
AllowOverride AuthConfig
AuthName "Acesso ao meu Diretório Restrito"
AuthType Basic
AuthUserFile /etc/apache/htpasswd
require valid-user
Order allow,deny
Allow from all
</Directory>
```

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Configurando diretório restrito

- Para criar o arquivo de senhas e/ou adicionar senha para um determinado usuário, digite o comando abaixo:

htpasswd -c /etc/apache/httpd_passwd usuário

- Para acrescentar mais usuários digite:

htpasswd /etc/apache/httpd_passwd usuário

- Neste passo, será necessário digitar a senha e em seguida confirmá-la.

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Evitando listagem de arquivos

A diretiva “indexes” permite que visitantes naveguem pelos arquivos no servidor. Se não for absolutamente necessário, remova esta diretiva de dentro das opções de configuração de seu diretório. Dessa forma, você evita expor os arquivos de seu servidor desnecessariamente.

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Outras Configurações de Segurança

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Outras configurações de segurança

- *User e Group*
  - *Mude o grupo e usuário donos do servidor:*
    - *User nobody*
    - *Group nobody*
  - *Listen*
    - *Listen 192.168.1.1:80*
    - *Listen 192.168.7.1:81*

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Ativando CGI em diretório específico

<Directory /home//public_ html / cgi -bin>*
Options + ExecCGI
AddHandler cgi-script. cgi .pl.sh. py
DirectoryIndex index.pl index. cgi index.sh index. py
</Directory>

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Desativando CGI em diretório específico

#ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
#<Directory "/usr/lib/cgi-bin">
 # AllowOverride None
Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
Order allow,deny
Allow from all
#</Directory>

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Desative e remova diretórios padrão (/icons, /manual)

```
# Alias /icons/ "/etc/apache2/icons/"
# <Directory "/etc/apache2/icons">
# Options Indexes MultiViews
# AllowOverride None
# Order allow,deny
# Allow from all
# </Directory>
```

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Desative indexação de diretórios e links simbólicos

<Directory /etc/apache2/htdocs">
Options Indexes FollowSymLinks
Order allow,deny
Allow from all
</Directory>

<Directory /etc/apache2/htdocs">
Options None
Order allow,deny
Allow from all
</Directory>

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Limitando GET e POST

<Directory /opt/apache2/htdocs">
<LimitExcept GET POST>
deny from all
</LimitExcept>
Options -FollowSymLinks -Includes -Indexes -MultiViews
AllowOverride None
Order allow,deny
Allow from all
</Directory>

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Bloqueando acesso à documentação do sistema

```
# Alias /doc/ "/usr/share/doc/"
# <Directory "/usr/share/doc/">
# Options Indexes MultiViews FollowSymLinks
# AllowOverride None
# Order deny,allow
# Deny from all
# Allow from 127.0.0.0/255.0.0.0 ::1/128
#</Directory>
```

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Redirecionamento para HTTPS

- *<Directory "/paginaexemplo/">*
  AllowOverride AuthConfig
  </Directory>

  <Location /paginaexemplo>
  RewriteEngine on
  RewriteCond %{HTTPS} !^on$ [NC]
  RewriteRule . https://%{HTTP_HOST}%{REQUEST_URI} [L]
  </Location>

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Módulos de Segurança

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Adicionando Módulos

Para adicionar um módulo ao Apache:

- **Em sistemas Debian/Ubuntu:**

```
# aptitude install <nome_do_modulo>
# a2enmod <nome_do_modulo>
```

- **Em Red Hat/CentOS/Fedora:**

```
# yum install mod_$nome_do_modulo
```

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Adicionando Módulos

Instalando o source:

- Baixe
- Descompacte
- Confira as opções do arquivo Makefile
- Execute ./configure
- Make
- Make install.

- **Adicione as linhas abaixo ao apache2.conf ou equivalente.**
  - AddModule < nome _modulo>.c
  - LoadModule < nome _modulo> modules/< nome _modulo>.so

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Desativando Módulos

Para desativar um módulo no Apache

a2dismod <nome_do_modulo>

- mod_usertrack
- mod_status
- mod_proxy
- mod_isapi
- mod_info
- mod_include
- mod_ imap
- mod_example
- mod_dav
- mod_cern_meta
- mod_autoinde
- mod_userdir
- mod_auth_anon
- mod_ asis

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

MOD_SSL

Instalando o OpenSSL:

```
# wget http://www.openssl.org/source/openssl-0.9.8g.tar.gz
#./config --prefix=/usr/local --openssldir=/usr/local/openssl
# make
# make test
# make install
```

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

MOD_SSL

Gerando as chaves:

mkdir /etc/apache2/conf/ssl.crt
mkdir /etc/apache2/conf/ssl.key
mkdir /tmp/apache
cd /tmp/apache/
opensslreq -new -x509 -keyout server.key -out server.crt -days 365
mv / tmp / apache /server. crt /etc/ apache 2/ conf / ssl. crt /server. crt

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

MOD_SSL

Em apache2.conf, adicione:

SSLEngine on
SSLCertificateFile /etc/apache2/conf/ssl.crt/server.crt
SSLCertificateKeyFile /etc/apache2/conf/ssl.key/server.key

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

MOD_BWSHARE

< IfModule mod_ bwshare.c>
<Location / bwshare -info>
SetHandler bwshare -info
</Location>
<Location / bwshare -trace>
SetHandler bwshare -trace
</Location>
<Directory />
1debt_max 25
1cred_rate 0.095
2debt_max 3000000
2cred_rate 2500
</Directory>
</ IfModule >

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

MOD_SECURITY

< IfModule mod_security.c>
SecFilterEngine On
SecAuditEngine RelevantOnly
SecFilterCheckURLEncoding On
SecFilterCheckUnicodeEncoding On
SecFilterForceByteRange 1 255
SecFilterCheckCookieFormat On
SecAuditLog logs/audit_log
SecFilterDebugLog /var/\u8230./ modsecurity _debug.log

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

MOD_SECURITY

```
SecFilterSelective "HTTP_CONTENT_TYPE" multipart /form-data
SecFilter xp _ enumdsn
SecFilter xp _ filelist
SecFilter xp _ availablemedia
SecFilter xp _ cmdshell
SecFilter xp _ regread
SecFilter xp _ regwrite
SecFilter xp _ regdeletekey
SecFilterSelective " ARG _recipient" "!@ de. ey.com$
SecServerSignature Microsoft- IIS /5.0\u8243?
</ IfModule >
```

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br

Dúvidas?

Diana Rosa e
Fernanda Machado
diana@gris.dcc.ufrj.br
fernanda@gris.dcc.ufrj.br