

Como instalar e configurar o eGroupWare

Versão 0.4

Este documento é publicado sob uma licença :

Creative Commons Attribution-ShareAlike

Extensões e comentários a este documento são bem-vindos.

Favor contatar o autor.

Autor: Reiner Jung

Copyright: Reiner Jung

Contato: r.jung@creativix.net

Projeto: eGroupWare

Data de publicação: 18-Jun-04

Índice

Índice	3
1 Checklist para a instalação do eGroupWare.....	6
2 Como fazer uma instalação rápida	7
3 Migre sua instalação de phpGroupWare para eGroupWare	12
4 Atualizar o eGroupWare.....	13
4.1 Como atualizar o eGroupWare	13
4.2 Você precisa mover suas configurações para a nova versão do header.inc.php.....	13
5 Os passos necessários para a instalar o eGroupWare	14
5.1 Baixando os pacotes de instalação	14
5.2 Porque os pacotes com assinatura GPG e o md5sum são necessários?.....	14
5.2.1 Instale a chave GPG para tar.gz.gpg, tar.bz2.gpg e zip.gpg.....	14
5.2.2 Verifique a chave GPG.....	14
5.2.3 Instale a chave GPG para os pacotes rpm.....	16
5.3 Como eu posso validar os pacotes?	16
5.4 Instale os pacotes em seu servidor	17
5.4.1 Recompile os pacotes para outros caminhos RPM	18
5.4.2 Instalando um pacote não assinado em seu servidor.....	18
5.4.3 Instalando um pacote gpg assinado em seu servidor	18
5.4.4 Instalando do CVS	19
6 Garantindo a segurança básica do seu servidor	20
6.1 A plataforma do servidor	20
6.1.1 Verifique as portas abertas e serviços rodando em seu servidor	20
6.1.1.1 Portas necessárias para rodar o servidor eGroupWare	20
6.1.1.2 O portscanner	21
6.1.1.3 A saída do portscanner	21
6.1.1.4 Desabilitando serviços/servidores desnecessários	21
6.1.2 Desinstalando softwares desnecessários em seu servidor	22
6.1.3 Busca local a procura de sinais de um rootkit	22
6.1.3.1 Amostra do chkrootkit.....	23
6.1.3.2 Instalando o chkrootkit rpm.....	23
6.1.3.3 Instalando o chkrootkit.tar.gz	24
6.1.4 Administrando a segurança do servidor	24
6.1.4.1 Conectando com seu servidor em uma sessão segura.....	25
6.1.4.2 Trabalhando com pares de chave SSH.....	25
6.1.4.2.1 Crie um par de chaves SSH (Secure shell key par)	26
6.1.4.2.2 Copie sua chave publica para o servidor	26
6.1.4.2.3 A ferramenta ssh-add.....	26
6.1.4.2.4 Garantindo a segurança do seu cliente SSH	26
6.1.4.2.5 Garantindo a segurança do seu SSHD	27













6.1.5	Instale um software para monitorar os logs no seu servidor	27
6.1.6	Ambiente de detecção de intrusão	28
6.1.6.1	Instalando o AIDE.....	28
6.1.6.2	O arquivo de configuração do AIDE – aide.conf	28
6.1.6.3	Crie um arquivo cronjob para rodar o AIDE automaticamente	30
6.1.6.4	Amostra do relatório do AIDE	32
6.1.6.5	Crie uma nova base de dados após as mudanças	33
6.1.7	Daemon security	33
6.1.8	Firewall.....	33
6.2	Segurança da aplicação web	33
6.2.1	Instalando o ModSecurity.....	34
6.2.2	Configuração Básica	34
6.2.3	Teste do ModSecurity	35
6.2.4	Amostra do log do ModSecurity.....	36
6.3	Otimização e segurança do servidor web Apache	37
6.3.1	Módulos recomendados para rodar.....	37
6.3.2	Outras opções de configuração do Apache	37
6.4	Turck MMCache	38
6.4.1	Requisitos	38
6.4.1.1	Pre-requisitos para o RedHat 3.....	38
6.4.2	Compatibilidade.....	39
6.4.3	Instalação Rápida	39
6.4.4	Interface web	41
6.5	Garantindo a segurança da instalação do PHP.....	42
6.6	Criando um certificado para o seu servidor web	43
6.6.1	Associando-se ao CA Cert	44
6.6.2	Criando o pedido de assinatura do seu certificado	44
6.6.2.1	Alterando o arquivo openssl.cnf	44
6.6.2.2	Criando a chave de segurança do seu servidor e o pedido de assinatura	45
6.6.2.3	Enviando o pedido de para o seu CA.....	46
6.6.2.4	Instalando o certificado do servidor.....	46
6.7	O servidor Web.....	47
6.8	O servidor SQL	47
7	Configurando o eGroupWare (setup).....	48
7.1	Crie seu banco de dados.....	48
7.2	Como iniciar a configuração?	49
7.3	Verificando a instalação do eGroupWare.....	49
7.4	Crie seu “header.inc.php”	50
7.5	Setup / Config Admin	51
7.5.1	Passo 1 – Gerenciamento simplificado da Aplicação	51
7.5.2	Passo2 – Configuração	52
7.5.2.1	Crie as pastas de arquivos	52
7.5.2.2	Editando a configuração atual.....	53

7.5.3	Passo 3: Configure as contas dos seus usuários	55
7.5.4	Passo 4: Gerenciamento de Idiomas	56
7.5.5	Passo 5: Gerenciamento da Aplicação	56
8	Inicie uma sessão no eGroupWare (login)	56
9	Solução de problemas (troubleshooting)	57
9.1	Esqueceu a senha do administrador.....	57
9.2	Administrador ou outro usuário está bloqueado.....	57
9.3	Erro de banco de dados: lock(Array, write) failed.....	57
9.4	Verificando as permissões de arquivo.....	57
9.5	Não conseguiu passar da página de verificação da instalação (Check install page)	58
9.6	Não conseguiu passar da página de verificação da instalação (Check install page)	58
9.7	(WINDOWS) fudforum/3814*****9): Permissão Negada	58
9.8	Sitemgr:mkdir(./sitemgr-link): Permissão negada (Permission denied).....	59
10	Software Map	60
11	Próximos passos e Registro de alterações	63
11.1	Próximos passos para este documento.....	63
11.2	Registro de alterações deste documento.....	63
12	Voluntários no desenvolvimento deste documento.....	65
13	Licenças de uso	66

1 Checklist para a instalação do eGroupWare

Esta lista apresenta um resumo do que você precisa para rodar o eGroupWare.

Você não necessita de um compilador para sua instalação. O eGroupWare é composto apenas por PHP, html, e arquivos de imagens..

O que você precisa para rodar o eGroupWare	Software de exemplo	Verifique os requisitos			
Você precisa de um sistema operacional, como um dos seguintes	Linux, Unix, *BSD MAC WIN NT / 2000 / XP		<input type="checkbox"/>		<input type="checkbox"/>
O eGroupWare requer um servidor web. Ao lado alguns exemplos.	IIS Roxen Apache 1.3 or 2.0		<input type="checkbox"/>		<input type="checkbox"/>
O eGroupWare requer um banco de dados. Ao lado alguns exemplos	MYSQL MS-SQL PostgreSQL		<input type="checkbox"/>		<input type="checkbox"/>
Se você quer mandar e-mails através do eGroupWare então você precisa de um servidor SMTP	Postfix Sendmail Exim ...		<input type="checkbox"/>		<input type="checkbox"/>
Se você quer usar o eGroupWare como um cliente de e-mail você vai precisar de um servidor POP ou IMAP	Cyrus Courier Dovecot		<input type="checkbox"/>		<input type="checkbox"/>
O eGroupWare exige PHP	PHP > 4.1 recomendado PHP > 4.2		<input type="checkbox"/>		<input type="checkbox"/>

2 Como fazer uma instalação rápida

Esta sessão “Como Fazer” apresenta uma pequena introdução sobre os passos necessários para configurar o eGroupWare. Uma instalação típica pode ser feita em menos de 10 minutos. Quando você precisar de descrições mais detalhadas sobre a instalação e segurança leia as demais páginas deste “Guia de Instalação e Configuração”.

- 1) Baixe os pacotes do eGroupWare da área de download no [sourceforge](http://sourceforge.net).
Atualmente estão disponíveis pacotes nos formatos .zip, .tar.gz, .bz2 e .rpm.
- 2) **(LINUX)** Instale os pacotes no diretório raiz do seu servidor web ou em qualquer outro diretório que você desejar usar. O pacote RPM automaticamente instalará no diretório /var/www/html

```
(root@server tmp)# rpm -ivh eGroupWare-x.x.xx.xxx-x.rpm
```

Para instalar um outro pacote do eGroupWare, mude para o diretório raiz do servidor web e descompacte o pacote.

```
(root@server tmp)# cd /var/www
```

```
(root@server www)# tar xzvf eGroupWare-x.x.xx.xxx-x.tar.gz
```



(WINDOWS) Utilizando um programa que descompacte arquivos zip como o [Winzip](http://www.winzip.com) descompacte o arquivo em alguma pasta que esteja sob seu servidor web. Em outras palavras a pasta que você escolheu deve estar acessável pela internet.

Tenha certeza que a estrutura de diretórios pré-existente seja mantida quando o arquivo zip for extraído e então sua instalação parecerá algo do tipo:


D:\websites\yourwebsite\eGroupware\ (todos os arquivos extraídos do eGroupware zip).



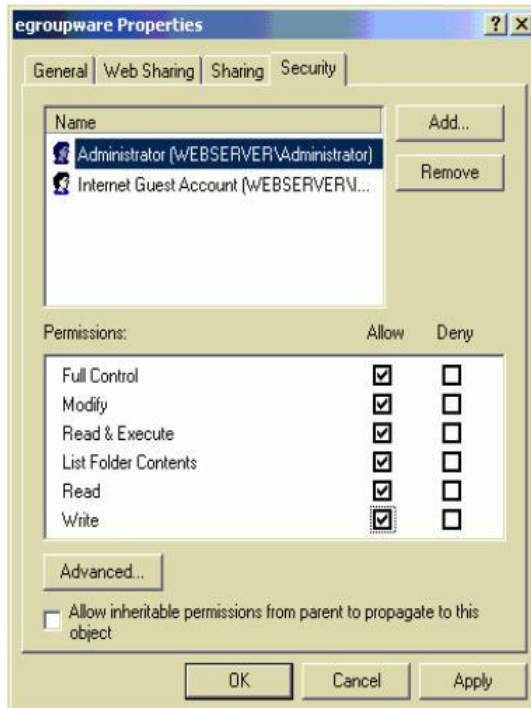
- 3) **(LINUX)** Mude as permissões dos arquivos da sua instalação do eGroupWare
- O usuário administrador deve ter permissão para ler e escrever.

- O usuário do servidor web deve ter permissão apenas para leitura.

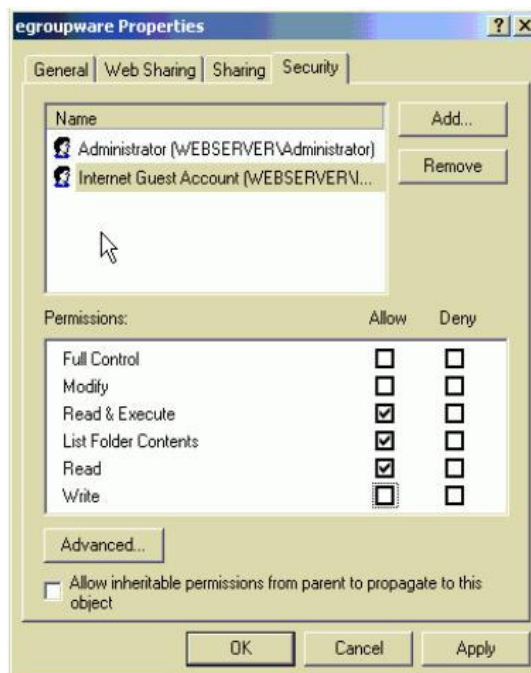
Exceto na pasta fudforum, na qual o usuário do servidor web tem que ter permissão de escrita.

 **(WINDOWS)** Agora você deve ajustar as “permissões” apropriadas para os arquivos do eGroupware.

O usuário administrador deve ter pelo menos permissão de leitura e escrita



O usuário do servidor web precisa ter permissão de leitura.



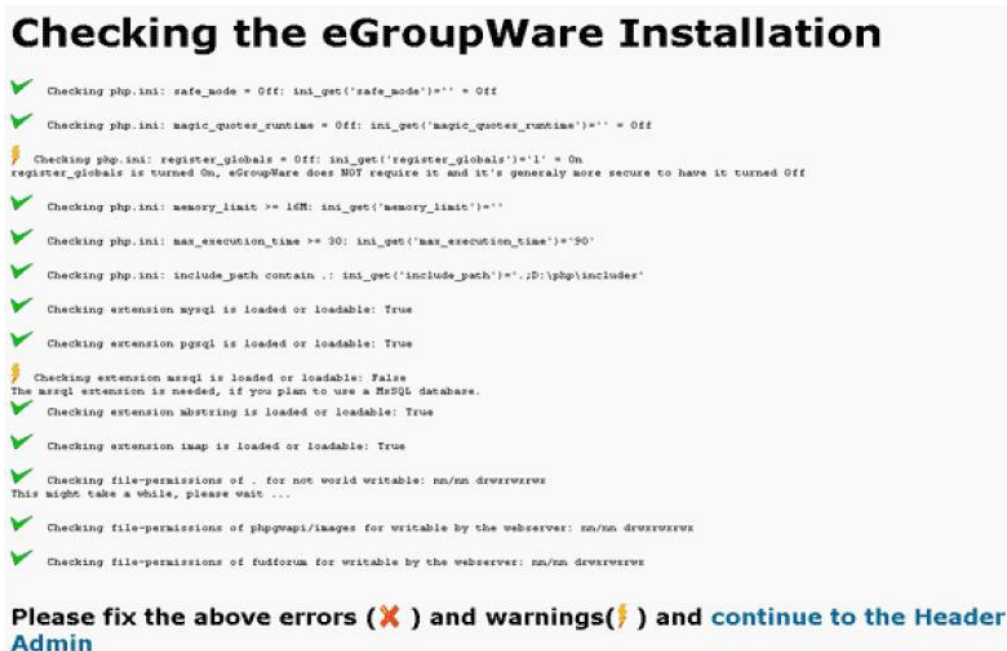
Apenas para a pasta FUDFORUM o usuário web precisa de permissão de leitura e escrita

- 4) servidor web e de banco de dados está iniciado? Por favor verifique isso.
- 5) Aponte o seu navegador para a URL <http://yourserver/egroupware/setup>
- 6) O script de verificação da instalação iniciará automaticamente
 - Aguarde até o final da execução do script
 - Faça a correção dos erros que eventualmente sejam mostrados.
 - Quando não houver mais erros apontados, role a tela para baixo e clique em "Retornar as configurações"



(WINDOWS) Você pode ter algumas coisas que não foram resolvidas por completo. Por exemplo a configuração do **register_globals = on** no seu arquivo PHP.ini (Geralmente na pasta C:\WINNT). Alguns scripts exigem que o register_globals esteja em on, e outros exigem que esteja em off. Caso você ajuste para off – alguns de seus sites podem não funcionar. A maneira certa de descobrir é configurá-lo da forma recomendada pelo eGroupware (off) e verificar os outros sites. Se eles não funcionarem, configure de volta para register_globals=on. Por favor preste atenção: o eGroupware não exige que esteja configurado para off!

E também as extensões do banco de dados MySQL (Microsoft) não serão carregadas se você esta usando MySQL!



Com estes conflitos resolvidos - agora você pode clicar em "continue to the Header Admin"

- 7) A configuração para a inicialização do "header admin"
 - Preencha todos os campos



(WINDOWS) Server Root – Este é o diretório raiz da sua instalação do eGroupware, ex:

D:\websites\yourwebsite\egroupware

Include Root – faça o mesmo, ex: D:\websites\yourwebsites\egroupware\

(Note que: este não é o endereço .com.br, é o caminho para o diretório atual da sua instalação do egroupware)

- Baixe o arquivo header.inc.php e salve ele no diretório raiz da instalação do eGroupware (exemplo: var/www/html/egroupware) e dê permissão de leitura para o servidor web.
- Clique continuar.



(WINDOWS) Escolha a opção "Download" do arquivo header.inc.php que você acabou de criar e salve-o no diretório raiz da sua instalação do eGroupWare (se você tiver acesso ao servidor), ou faça um upload via FTP para esse diretório. Ex: D:\websites\your website\eGroupware



Não esqueça a senha. Ela será encriptada e não poderá ser lida depois.

8) Inicie uma nova sessão no Setup/Config Admin (login to Setup/Config admin)

9) Crie seu banco de dados / tabelas

- Preencha o formulário com a identificação de usuário e senha do administrador do banco, para que seu banco seja criado automaticamente.
- Continue a criação do banco.
- Re-verifique a instalação
- Continue a criação das tabelas



(WINDOWS) Isto deverá ser bem simples se você souber o nome e a senha para seu servidor MySQL.

Preencha a informação e crie as tabelas ("Create Database").

No momento em que você clicar "Re-check My Installation" - você verá que nenhuma aplicação está instalada ("have no application installed") e a opção para instalar as aplicações ("install the core tables and the admin and preferences application.") Siga em frente e instale as tabelas

* Se você receber erros vá para a seção de correção de erros (troubleshooting).

10) Edite a configuração atual

- Crie um diretório fora do diretório raiz do servidor web e dê ao usuário do servidor web permissão de leitura, escrita e execução para este diretório. Por exemplo, se a raiz do seu servidor web está em /var/www/html crie uma pasta: /var/www/arquivos



(WINDOWS) Isto significa criar um diretório/pasta que não está sob a instalação em D:\websites\yourwebsite\eGroupware. Por exemplo se a instalação do eGroupWare tem por diretório raiz D:\websites\yourwebsite\eGroupware, você precisa criar o diretório em algo do tipo D:\websites\yourwebsite\arquivos\ . Uma vez criado o diretório assegure-se que o usuário web tenha permissão de leitura, escrita e execução nesse diretório/pasta.

11) Crie o usuário administrador (admin user)

- Não use esse usuário para os serviços diários. Este deve ser usado apenas para fazer backup e para a configuração inicial.

12) Faça a escolha dos idiomas

- Instale os idiomas que você deseja usar

13) Faça a escolha das aplicações

- Desinstale as aplicações que você não deseja usar.

14) Inicie uma nova sessão no eGroupWare (login)

- Aponte seu browser para <http://yourservername/egroupware>

3 Migre sua instalação de phpGroupWare para eGroupWare

Baixe os pacotes necessários da nossa página.
Instale os pacotes no seu diretório do servidor web.
Copie o arquivo "header.inc.php" da sua pasta phpGroupWare para a pasta eGroupWare e altere as seguintes linhas no arquivo "header.inc.php":

onde está:

```
define('PHPGW_SERVER_ROOT','/var/www/html/phpgroupware');  
define('PHPGW_INCLUDE_ROOT','/var/www/html/phpgroupware');
```

altere para:

```
define('PHPGW_SERVER_ROOT','/var/www/html/egroupware');  
define('PHPGW_INCLUDE_ROOT','/var/www/html/egroupware');
```

Aposte seu navegador para o endereço

<https://www.domain.com/egroupware/setup>

Inicie uma nova sessão (login) em **Setup / Config Admin Login**

Clique em "Editar configurações atuais"

altere o conteúdo do terceiro campo (Enter the location ...) para : /egroupware.

Isso é tudo. Divirta-se!

4 Atualizar o eGroupWare

4.1 Como atualizar o eGroupWare

- 1) Baixe os pacotes necessários da nossa página [sourceforge](http://sourceforge.net).
- 2) Instale os pacotes no seu servidor:

Para pacotes rpm, faça o seguinte:

```
(root@server tmp)# rpm -Uvh eGroupWare*
```

Para pacotes tar.gz vá para o diretório root do seu servidor web (acima da sua instalação do eGroupWare)

```
(root@server tmp)# cd /var/www/html  
(root@server html)# tar xzvf eGroupWare-x.xx.xxx-x.tar.gz
```

Para pacotes tar.bz2 vá para o diretório root do seu servidor web (acima da sua instalação do eGroupWare)

```
(root@server tmp)# cd /var/www/htm  
(root@server html)# tar xjvf eGroupWare-x.xx.xxx-x.tar.bz2
```

Também é possível atualizar através do CVS. Mas atualize apenas das versões estáveis do CVS e não daquelas em desenvolvimento

```
(root@server tmp)# cd /var/www/html/egroupware  
(root@server egroupware)# cvs update -Pd
```

- 3) Inicie uma nova sessão (login) em Setup / Config Admin Login
- 4) Se for necessário o eGroupWare avisará para que você atualize seu banco de dados.
- 5) Verifique as atualizações necessárias no passo 4, "Advanced Application Management"

4.2 Você precisa mover suas configurações para a nova versão do header.inc.php

- 1) Após instalar você verá a seguinte mensagem
Você precisa mover suas configurações para a nova versão do header.inc.php
- 2) Vá para <http://yourserver/egroupware/setup>
 - Desça a tela até "Checking the eGroupware Installation" (Verificando a Instalação do eGroupware)
 - confirme com "continue to the Header Admin"
- 3) Inicie uma nova sessão (login) com seu usuário e sua senha
- 4) Quando necessário, altere as configurações
- 5) Salve o arquivo.

5 Os passos necessários para a instalar o eGroupWare

5.1 Baixando os pacotes de instalação

Você pode baixar os pacotes de instalação no site:

http://sourceforge.net/project/showfiles.php?group_id=78745

Na área de download do sourceforge estão disponíveis os seguintes pacotes:

**.tar.gz*

**.tar.bz2*

**.zip*

Por razões de segurança, esses pacotes também estão disponíveis assinados com uma chave gpg

**.tar.gz.gpg*

**.tar.gz.gpg*

**.zip.gpg*

Estes pacotes rpm funcionam no RedHat e na maioria das distribuições baseadas em rpm.

*eGroupWare*noarch.rpm*

O pacote eGroupWare-all-apps*.noarch.rpm contém todos os pacotes disponíveis.

Os outros disponibilizam todas as aplicações em pacotes separados.

5.2 Porque os pacotes com assinatura GPG e o md5sum são necessários?

As vezes os hackers atacam os servidores de desenvolvimento para alterar os pacotes e incluir neles trojans ou sniffers, etc. Os pacotes assinados garantem a integridade dos pacotes baixados..

5.2.1 Instale a chave GPG para tar.gz.gpg, tar.bz2.gpg e zip.gpg

Instale a chave gpg junto com o respectivo pacote tar.gz.gpg, tar.bz2.gpg, zip.gpg, md5sum-eGroupWare version.txt.asc e os rpm's assinados.

Usando Linux você pode usar os seguintes comandos para importar a chave e validar os pacotes

tar.gz.gpg, tar.bz2.gpg, zip.gpg e md5sum*.asc.

```
[root@server root]# gpg --keyserver blackhole.pca.dfn.de --recv-keys 0xD9B2A6F2
```

5.2.2 Verifique a chave GPG

Se você deseja validar os pacotes, é preciso antes validar a chave. Se não fizer isso, você receberá uma mensagem de erro avisando que a chave não é confiável a todo momento.

Liste as chaves disponíveis no seu "key ring". Você deverá visualizar a chave que foi importada

```
[root@server root]# gpg --list-keys
gpg: Warning: using insecure memory!
gpg: please see http://www.gnupg.org/faq.html for more information
/root/.gnupg/pubring.gpg
-----
pub 1024D/D9B2A6F2 2002-12-22 Reiner Jung <r.jung@creativix.net>
sub 1024g/D08D986C 2002-12-22
```

Agora modifique a chave com o código **D9B2A6F2**

```
[root@server root]# gpg --edit-key D9B2A6F2
gpg (GnuPG) 1.0.7; Copyright (C) 2002 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.
gpg: Warning: using insecure memory!
gpg: please see http://www.gnupg.org/faq.html for more information
gpg: checking the trustdb
gpg: no ultimately trusted keys found

pub 1024D/D9B2A6F2 created: 2002-12-22 expires: never    trust: -/-
sub 1024g/D08D986C created: 2002-12-22 expires: never
(1). Reiner Jung <r.jung@creativix.net>
```

Se você desejar, pode verificar a impressão digital da chave, mas não é obrigatório. A impressão digital da chave é: BBFF 354E CA1F 051E 932D 70D5 0CC3 882C D9B2 A6F2

```
Command> fpr
pub 1024D/D9B2A6F2 2002-12-22 Reiner Jung <r.jung@creativix.net>
Fingerprint: BBFF 354E CA1F 051E 932D 70D5 0CC3 882C D9B2 A6F2
```

Agora você pode assinar a chave

```
Command> trust
pub 1024D/D9B2A6F2 created: 2002-12-22 expires: never    trust: f/-
sub 1024g/D08D986C created: 2002-12-22 expires: never
(1). Reiner Jung <r.jung@creativix.net>
```

Please decide how far you trust this user to correctly
verify other users' keys (by looking at passports,
checking fingerprints from different sources...)?

1 = Don't know

2 = I do NOT trust

3 = I trust marginally
4 = I trust fully
5 = I trust ultimately
i = please show me more information
m = back to the main menu

Your decision? 5
Do you really want to set this key to ultimate trust? yes

pub 1024D/D9B2A6F2 created: 2002-12-22 expires: never trust: u/-
sub 1024g/D08D986C created: 2002-12-22 expires: never
(1). Reiner Jung <r.jung@creativix.net>
Please note that the shown key validity is not necessary correct
unless you restart the program.

Agora você pode verificar a chave pelo prompt com "check" ou saindo da sessão.

5.2.3 Instale a chave GPG para os pacotes rpm

Para importar a chave necessária para a validação dos pacotes rpm, procure pela chave D9B2A6F2 no servidor de chaves: <http://www.dfn-pca.de/eng/pgpkserv/>

Clique no link D9B2A6F2 em uma nova janela e copie tudo, incluindo as seguintes linhas

----BEGIN PGP PUBLIC KEY BLOCK----
-----END PGP PUBLIC KEY BLOCK-----

e salve o texto copiado em um arquivo chamado:

EGROUPWARE-GPG-KEY

Como último passo, importe a chave para seu rpm keyring:

```
[user@server tmp]$ rpm --import EGROUPWARE-GPG-KEY
```

5.3 Como eu posso validar os pacotes?

Se você deseja conferir o **md5sum** de um pacote, execute os seguintes passos:

Para isso, na linha de comando do seu ambiente Linux informe o seguinte:

Baixe o arquivo **md5sum-eGroupWare-version.txt.asc** da página da Sourceforge e verifique sua validade.

```
[user@server tmp]$ gpg --verify md5sum-eGroupWare-version.txt.asc
```

Encontre o md5sum do pacote


```
[user@server tmp]$ md5sum eGroupWare-x.x.xx.xxx-x.tar.gz
41bee8f27d7a04fb1c3db80105a78d03 eGroupWare-x.x.xx.xxx-x.tar.gz
```

Abra o arquivo do md5sum para ver o md5sum original (acima foi apenas um exemplo)

```
user@server tmp]$ less md5sum-eGroupWare-x.x.xx.xxx-x.txt.asc
```

```
-----BEGIN PGP SIGNED MESSAGE-----
```

```
Hash: SHA1
```

```
md5sum from file eGroupWare-x.x.xx.xxx.tar.gz is:
```

```
41bee8f27d7a04fb1c3db80105a78d03
```

```
- -----
```

```
md5sum from file eGroupWare-x.x.xx.xxx.tar.bz2 is:
```

```
3c561e82996349d596540f476b9624f2
```

```
- -----
```

```
md5sum from file eGroupWare-x.x.xx.xxx.zip is:
```

```
c3bb1f67ca143236e8603c6995e82db0
```

```
-----BEGIN PGP SIGNATURE-----
```

```
Version: GnuPG v1.2.1 (GNU/Linux)
```

```
iD8DBQE/WM2wDMOILNmypvIRAm5GAJ0e6IlneU0quVQxWOP/pF+QGpwCgptbH
```

```
O02LpinLNqnr6epxt9vB9sw=
```

```
=OBcn
```

```
-----END PGP SIGNATURE-----
```

Aqui podemos observar que a chave no arquivo md5sum e o teste checksum da linha de comando são iguais, e que o pacote não foi alterado após a compilação.

Para verificar a “checksum” dos pacotes tar.gz.gpg, tar.gz.gpg ou zip.gpg siga estes passos:

Na linha de comando do seu sistema Linux digite o seguinte:

```
[user@server tmp]$ gpg --verify eGroupWare-x.x.xx.xxx-x.tar.gz.gpg
```

Para verificar a “checksum” dos pacotes RPM, siga estes passos:

Na linha de comando do seu sistema Linux digite o seguinte:

```
[user@server tmp]$ rpm --checksig eGroupWare-all-apps-x.x.xx.xxx-x.noarch.rpm
```

5.4 Instale os pacotes em seu servidor

5.4.1 Recompilar os pacotes para outros caminhos RPM

Você pode recompilar os pacotes para o SuSE Linux. Baixe o arquivo *.src.rpm e digite

```
[user@server tmp]$ rpmbuild --rebuild eGroupWare-x.xx.xxx-x.src.rpm
```

Isso irá criar para você um pacote com caminho de instalação em "srv/www/htdocs".

O pacote será localizado para instalação em /usr/src/packages/RPMS/noarch

5.4.2 Instalando um pacote não assinado em seu servidor

Para instalar um pacote não assinado e não RPM faça:

Mude para o diretório raiz do seu servidor web (ou qualquer outro lugar que você deseja instalar os pacotes)

```
[user@server tmp]$ cd /var/www/html
```

Extraia os pacotes para dentro desta pasta. Se o seu pacote está no diretório /tmp, você pode instalá-lo com

```
[user@server tmp]$ tar xzvf /tmp/eGroupWare-x.xx.xxx-x.tar.gz .
```

```
[user@server tmp]$ tar xjvf /tmp/eGroupWare-x.xx.xxx-x.tar.bz2 .
```

```
[user@server tmp]$ unzip /tmp/eGroupWare-x.xx.xxx-x.zip .
```

5.4.3 Instalando um pacote gpg assinado em seu servidor

Para instalar um pacote GPG assinado e não RPM faça:

Separe o pacote da chave GPG

```
[user@server tmp]$ gpg -o eGroupWare-X.XX.XXX-X.tar.gz -decrypt  
eGroupWare-X.XX.XXX-X.tar.gz.gpg
```

Mude para o diretório raiz do seu servidor web (ou qualquer outro lugar que você deseja instalar os pacotes)

```
[user@server tmp]$ cd /var/www/html
```

Extraia os pacotes dentro desta pasta. Por exemplo, Se o seu pacote está no diretório /tmp, você pode instalá-lo com:

```
[user@server tmp]$ tar xzvf /tmp/eGroupWare-x.x.xxx-x.tar.gz .
```

```
[user@server tmp]$ tar xjvf /tmp/eGroupWare-x.xx.xxx-x.tar.bz2 .
```

```
[user@server tmp]$ unzip /tmp/eGroupWare-x.xx.xxx-x.zip
```

Para instalar um pacote RPM em seu servidor faça:

Verifique que o RPM é válido

```
[user@server tmp]$ rpm --checksig /tmp/eGroupWare-x.x.xxx-x.noarch.rpm
```

Instale o pacote

```
[user@server tmp]$ rpm -ivh /tmp/eGroupWare-all-apps-x.x.xxx-x.noarch.rpm
```



Se o diretório raiz do servidor web **não** for /var/www/html você pode instalar o RPM em outro diretório. Para fazer isso, use o seguinte comando

```
[user@server tmp]$ rpm -ivh --prefix /your_new_server/root /tmp/eGroupWare-all-apps-x.x.xxx-x.noarch.rpm
```

5.4.4 Instalando do CVS

Para instalar os pacotes do nosso repositório CVS, execute os seguintes passos:

Mude para o diretório raiz do seu servidor web (ou qualquer outro lugar que você deseja instalar os pacotes)

```
[root@server tmp]# cd /var/www/html
```

```
[root@server html]# cvs -d:pserver:anonymous@cvs.sourceforge.net:  
/cvsroot/egroupware login
```

```
[root@server html]# cvs -z3 -d:pserver:anonymous@cvs.sourceforge.net:  
/cvsroot/egroupware co egroupware
```

```
[root@server html]# cd egroupware
```

```
[root@server egroupware]# cvs co all
```


```
[root@server egroupware]# cvs update -Pd
```

6 Garantindo a segurança básica do seu servidor

6.1 A plataforma do servidor

Você possui diversas maneiras para garantir a segurança do seu servidor. A medida de segurança mais importante que você deve tomar é manter sua instalação sempre atualizada. Para acompanhar as atualizações você pode assinar a lista de e-mail egroupware-announcement@lists.sourceforge.net. Nesta lista são publicadas as novas liberações e também as atualizações de segurança do eGroupWare.

6.1.1 Verifique as portas abertas e serviços rodando em seu servidor

 Uma porta aberta, significa que seu servidor está oferecendo um serviço de acesso público. Esse serviço pode ser por exemplo um servidor de arquivos, um servidor DNS, servidor Telnet, Xserver ou outro serviço qualquer. É recomendável que seu servidor disponibilize apenas os serviços/portas que são necessários para rodar o eGroupware. Mais portas abertas aumentam a chance de se encontrar uma vulnerabilidade no servidor e eventuais ataques. Se você precisa de mais portas abertas, que não são necessárias ao eGroupWare, você deve garantir a segurança da sua instalação através de um Firewall ou TCP Wrappers. Se possível, permita somente serviços com **Secure Socket Layer** (SSL).

6.1.1.1 Portas necessárias para rodar o servidor eGroupWare

As portas necessárias são:

<i>Webserver Port:</i>	<i>HTTP/80</i>
<i>Webserver SSL Port:</i>	<i>HTTPS/443</i>
<i>Remote Administration, Secure Shell:</i>	<i>SSH/22</i>

É recomendável que o servidor de e-mail esteja em uma outra máquina. Caso isso não seja possível, mais portas são necessárias.

<i>Email Server MTA:</i>	<i>SMTP/25</i>
<i>Email Server MTA:</i>	<i>SMTPS/465</i>

Para pegar os e-mails do seu servidor com um cliente de e-mail, como o cliente eGroupWare, você vai precisar de uma dessas portas.

<i>IMAP server:</i>	<i>IMAP/143</i>
<i>IMAP server SSL:</i>	<i>IMAPS/993</i>
<i>POP-3:</i>	<i>POP-3/110</i>
<i>POP-3 over SSL:</i>	<i>POP-3/995</i>

Se você bloquear as portas com algum firewall lembre-se que você necessitará permitir determinado tráfego. Isso pode incluir NTP, procura de DNS, etc ...

Conclusão:

<i>Seu servidor precisa no mínimo as portas:</i>	<i>22, 80, 443</i>
<i>E no máximo as portas:</i>	<i>22, 25, 80, 110, 143, 443, 465, 993, 995</i>
<i>Recomendação mínima :</i>	<i>22, 443</i>
<i>Recomendação máxima:</i>	<i>22, 25, 443, 993, 995</i>

6.1.1.2 O portscanner

Existem diversas ferramentas para checar as portas abertas em sua instalação. Uma que está disponível em ambas as plataformas *NIX e Windows.

[Nmap](#)

Instale Nmap em seu computador e verifique as portas que estão abertas.

6.1.1.3 A saída do portscanner

Aqui está um exemplo de saída para uma varredura do Nmap em um servidor. O Nmap mostra as portas que estão disponíveis (abertas) no servidor.

```
[root@server root]# nmap -sV yourserver.com
Starting nmap 3.45 ( http://www.insecure.org/nmap/ ) at 2003-09-17 00:48 CEST
Interesting ports on xxx.xxx.xx.xxx:
(The 1651 ports scanned but not shown below are in state: closed)
PORT      STATE  SERVICE  VERSION
22/tcp    open   ssh      OpenSSH 3.1p1 (protocol 2.0)
80/tcp    open   http     Apache httpd 1.3.27 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.12
          OpenSSL/0.9.6b PHP/4.1.2 mod_perl/1.26)
137/tcp   filtered netbios-ns
138/tcp   filtered netbios-dgm
139/tcp   filtered netbios-ssn
443/tcp   open   ssl      OpenSSL
```

Nmap run completed -- 1 IP address (1 host up) scanned in 23.000 seconds

6.1.1.4 Desabilitando serviços/servidores desnecessários

Se você encontrar, rodando em seu servidor, serviços que são desnecessários, você pode pará-los. Assim, ao reiniciar o servidor, o serviço não deverá iniciar automaticamente.

Em uma instalação em RedHat você pode usar os seguintes comandos para desabilitar os serviços

```
[root@server home]# service name_from_the_service stop

[root@server home]# chkconfig --level 345 name_from_the_service off
```

Em uma instalação baseada em Debian use as seguintes ferramentas.

```
Server:~# /etc/init.d/ name_from_the_service stop
```

```
Server:~# rcconf
```

6.1.2 Desinstalando softwares desnecessários em seu servidor

Em sua instalação padrão, são alocados muitos aplicativos que não são necessários. Por razões de segurança, delete esses aplicativos do seu servidor. Programas não necessários como, por exemplo, clientes ftp, wget, gcc, arquivos header, arquivos fonte...

Para verificar quais os pacotes que estão instalados na distribuição Linux baseado em **rpm** faça:

```
[root@server home]# for i in `rpm -qa`; do rpm -qi $i >> rpm_packages; done
```

```
[root@server home]# less rpm_packages
```

Apague todos os pacotes que você não vai precisar

```
[root@server home]# rpm -e package
```

Para verificar quais os pacotes instalados na distribuição Linux **Debian**, existem muitas ferramentas. Uma delas é:

```
Server:~# aptitude
```

6.1.3 Busca local a procura de sinais de um rootkit

Chkrootkit é uma ferramenta de verificação local de sinais de tentativas de um rootkit. Chkrootkit foi testada em: Linux 2.0.x, 2.2.x, e 2.4.x, FreeBSD 2.2.x, 3.x, 4.x, e 5.x, OpenBSD 2.x e 3.x, NetBSD 1.5.2, Solaris 2.5.1, 2.6 e 8.0, HP-UX 11, True64 e BSDI. O Chkrootkit contém:

- chkrootkit: shell script que verifica arquivos binários do sistema em busca de alguma alteração de rootkit. Os seguintes testes são realizados:

```
aliens asp bindshell lkm rexedcs sniffer wted w55808 scalper slapper z2 amd  
basename biff chfn chsh cron date du dirname echo egrep env find fingerd gpm  
grep hdparm su ifconfig inetd inetdconf init identd killall ldsopreload login ls lsof mail  
mingetty netstat named passwd pidof pop2 pop3 ps pstree rpcinfo rlogind rshd  
slogin sendmail sshd syslogd tar tcpd tcpdump top telnetd timed traceroute vdir w  
write
```

- ifpromisc.c: verifica se a interface está em modo promíscuo.
- chklastlog.c: verifica as últimas exclusões de logs.
- chkwtm.c: verifica as exclusões de wtmp.
- check_wtmpx.c: verifica as últimas exclusões de wtmpx (apenas Solaris)
- chkproc.c: busca por sinais de LKM trojans.
- chkdirs.c: busca por sinais de LKM trojans.

- strings.c: substituição rápida e suja de strings

Você pode baixar o chkrootkit como um pacote compilado rpm ou como um pacote tar.gz

[chkrootkit.tar.gz](#)

[chkrootkit rpm](#)

6.1.3.1 Amostra do chkrootkit

```
Checking `timed'... not found
Checking `traceroute'... not infected
Checking `vdir'... not infected
Checking `w'... not infected
Checking `write'... not infected
Checking `aliens'... no suspect files
Searching for sniffer's logs, it may take a while... nothing found
Searching for HiDrookit's default dir... nothing found
Searching for t0rn's default files and dirs... nothing found
Searching for t0rn's v8 defaults... nothing found
Searching for Lion Worm default files and dirs... nothing found
Searching for RSHA's default files and dir... nothing found
Searching for RH-Sharpe's default files... nothing found
Searching for Ambient's rootkit (ark) default files and dirs... nothing found
```

6.1.3.2 Instalando o chkrootkit rpm

O chkrootkit deve rodar em todas as distribuições baseadas em rpm.

Faça o download através do endereço acima e instale-o

```
[root@server tmp]# rpm -ivh chkrootkit-x.xx-x.i386.rpm
```

Após a instalação você pode editar o arquivo chkrootkit_cronfile de acordo com as suas necessidades. Esse passo não é necessário, mas torna o seu relatório mais personalizado

```
[root@server tmp]# vi /etc/cron.daily/chkrootkit_cronfile
```

```
#!/bin/sh
```

```
cd /usr/bin ./chkrootkit 2> /dev/null | mail -s "chkrootkit output" root
```

Altere os seguintes valores:

<i>"chkrootkit output"</i>	<i>para</i>	<i>"chkrootkit myserver output"</i>
<i>root</i>	<i>para</i>	<i>your_email_adress@yourserver.com</i>

6.1.3.3 Instalando o chkrootkit.tar.gz

Descompacte e instale o chkrootkit

```
[root@server tmp]# cp chkrootkit.tar.gz /usr/local; rm chkrootkit.tar.gz
```

```
[root@server tmp]# cd /usr/local/
```

```
[root@server local]# tar xzvf chkrootkit.tar.gz
```

```
[root@server local]# mv chkrootkit-x.xx chkrootkit
```

```
[root@server local]# chown -R root.root chkrootkit
```

```
[root@server chkrootkit]# cd chkrootkit
```

```
[root@server chkrootkit]# make sense
```

Para fazer o chkrootkit emitir-lhe um relatório você tem duas possibilidades. Crie um arquivo chamado chkrootkit_cronfile ou adicione uma linha à do arquivo crontab.

Crie um arquivo `chkrootkit_cronfile`

```
[root@server cron.daily]# vi chkrootkit_cronfile
```

```
#!/bin/sh
```

```
cd /usr/local/chkrootkit ./chkrootkit 2> /dev/null | mail -s "chkrootkit myserver output" your_email_adress
```

Estender o arquivo crontab com a seguinte linha


```
0 1 * * * root (cd /usr/local/chkrootkit; ./chkrootkit 2>&1 | mail -s
```

```
"chkrootkit output" your_email_adress)
```

Agora, o chkrootkit irá enviar relatórios para o endereço acima.


6.1.4 Administrando a segurança do servidor

Se você quer administrar seu servidor com segurança, então use o protocolo SSH. Com esse protocolo, todas as conexões são criptografadas. Com protocolos como telnet e ftp, as contas de usuários e suas senhas são transmitidas sem criptografia (transmitidas em formato texto). A transferência de contas e senhas são fáceis de serem capturadas por um hacker. Com as senhas o hacker pode acessar sua conta.

 Se possível use apenas SSH2 e não SSH1. Também não use a conta de ROOT para iniciar a sessão no servidor remoto. Conecte-se com um usuário com permissões normais e use "su" ou "sudo" para executar tarefas de administração no servidor.

6.1.4.1 Conectando com seu servidor em uma sessão segura

Se o seu servidor suporta conexões via SSH, então é bem fácil administra-lo remotamente. Você apenas tem que conectar-se ao servidor através do seu cliente SSH.

 Quando você conectar-se pela primeira, receberá uma mensagem de aviso semelhante a abaixo. Você deve concordar com um YES (sim) apenas se tiver certeza que este é o servidor ao qual você deseja se conectar.

```
[user@client home]$ ssh yourserver
The authenticity of host 'yourserver (100.178.76.207)' can't be established.
RSA key fingerprint is 7e:8e:55:8b:49:57:5d:41:40:ab:93:64:18:af:60:ea.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'yourserver' (RSA) to the list of known hosts.
```

✍ Conecte-se ao servidor para administração remota


```
[user@client home]$ ssh yourserver
```

✍ Copie arquivos para seu servidor usando secure copy (scp) (cópia segura)

```
[user@client home]$ scp yourfile.txt yourserver:/home/
```

✍ Você também pode usar sftp usando um cliente de ftp seguro "secure ftp client"

```
[user@client home]$ sftp yourserver
```

 Em algumas instalações/distribuições, a função sftp está desabilitada por padrão (por exemplo no Debian). Se você quiser habilitá-la, adicione a seguinte linha ao arquivo **sshd_config** em seu servidor.

Na distribuição Debian:

```
subsystem sftp /usr/lib/sftp-server
```

Na distribuição RedHat:

```
subsystem sftp /usr/libexec/openssh/sftp-server
```

6.1.4.2 Trabalhando com pares de chave SSH

Trabalhar com pares de chave SSH tem suas vantagens. A primeira vantagem é que não é necessário digitar a senha toda vez que você conectar-se com o servidor, e a segunda é que dessa forma é mais seguro. Quando você usa pares de chave você pode permitir o uso da autenticação da senha do lado do servidor.



Para cada usuário que desejar se conectar no servidor você vai necessitar de um par de chave

6.1.4.2.1 Crie um par de chaves SSH (Secure shell key par)

Você deve criar o par da chave ssh do lado do cliente!

```
[user@client home]$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /user/.ssh/id_dsa.
Your public key has been saved in /user/.ssh/id_dsa.pub.
The key fingerprint is:
f0:00:f7:95:e9:73:37:11:aa:e8:06:3e:60:9e:0d:25 user@yourserver
```

6.1.4.2.2 Copie sua chave publica para o servidor

Você deve copiar sua nova chave publica (*.pub) do seu cliente local para o seu servidor.

```
[user@client home]$ scp .ssh/id_dsa.pub useratserver@yourserver:/home/yourservername/
```

Instale a chave pública no servidor.

```
[user@client home]$ ssh yourserver
[user@server home]$ cat id_dsa.pub >> .ssh/authorized_keys
[user@client home]$ chmod 600 .ssh/authorized_keys
```

Agora, ao você se conectar com o servidor, este exigirá a senha que você digitou quando criou o par de chaves SSH. Se você não desejar digitar a senha sempre que se conectar ao servidor, você pode usar a ferramenta `ssh-add`

6.1.4.2.3 A ferramenta ssh-add

Se você conecta-se ao seu servidor (ou outro servidor) com frequência, você pode usar a ferramenta `ssh-add` para armazenar a senha de sua chave ssh. Aqui, você digitará a senha uma vez e ela será armazenada

```
[user@client home]$ ssh-add
Enter passphrase for /home/youruser/.ssh/id.dsa:
Identify added: /home/youruser/.ssh/id.dsa (/home/youruser/.ssh/id.dsa)
```

6.1.4.2.4 Garantindo a segurança do seu cliente SSH

No arquivo de configuração do cliente SSH uma linha é importante. Por razões de segurança o valor no arquivo `ssh_config` deverá ser:

Protocol 2

Isto permite a seus clientes conexões somente com a versão 2 do protocolo de SSH

6.1.4.2.5 Garantindo a segurança do seu SSHD

Para seu SSH Daemon você pode usar os seguintes valores para torná-lo mais seguro:

Protocol 2

PermitRootLogin no

PubKeyAuthetifikation yes

PasswordAuthentication no

PermitEmptyPassword no

6.1.5 Instale um software para monitorar os logs no seu servidor

Analisar seus arquivos de log é uma obrigação de cada administrador. Quando você não monitora seus arquivos de log, você não tem a oportunidade de ver os problemas de segurança ou anomalias. Existem vários produtos no mercado para monitorar seus arquivos de log.

[logcheck](#)

[logwatch](#)

[logsurfer](#)

O produto recomendado é o logcheck. Logcheck funciona em plataformas Linux, BSD, Sun, HP-UX. É fácil de instalar e fazer relatórios claros. Para instalar logcheck digite o seguinte comando no diretório raiz do logcheck após ter descompactado (tar) o arquivo.

```
[root@server logcheck-1.1.1]# make linux
```

Para iniciar o logcheck automaticamente, uma linha deve ser adicionada ao arquivo crontab. No RedHat o arquivo se encontra em `/etc/crontab`. Abra o arquivo e adicione a seguinte linha

```
00 * * * * root /bin/sh /usr/local/etc/logcheck.sh
```

Edite o shell script do logcheck para adicionar o receptor dos relatórios de log. O receptor é o valor da variável `SYSADMIN` no script.

```
[root@egroupware logcheck-1.1.1]# vi /usr/local/etc/logcheck.sh
```

Para receber relatórios mais detalhados, usuários avançados podem também alterar as seguintes linhas:

```
logcheck.violations
logcheck.violations.ignore
logcheck.hacking
logcheck.ignore
```

6.1.6 Ambiente de detecção de intrusão

Instale um ambiente de detecção de intrusão para verificar a integridade dos arquivos do sistema e detectar mudanças no seu servidor.

[AIDE](#)

[Tripwire](#)

[Samhain](#)

Dos três acima, o AIDE é o mais fácil de configurar.

6.1.6.1 Instalando o AIDE

A maioria das distribuições já possui o AIDE incluído e você pode instalá-lo com qualquer ferramenta padrão como RPM ou apt-get. AIDE tem como dependência o pacote mhash, o qual você também deve instalar. Se nenhum desses pacotes estiver disponível na sua plataforma, você deve compilá-lo.

```
./configure  
make  
make install
```

6.1.6.2 O arquivo de configuração do Aide – aide.conf

Você deve configurar o arquivo aide.conf, de modo que todos os arquivos importantes do servidor sejam verificados e diminua o número de alarmes falsos.



Salve os arquivos /etc/aide.conf, /usr/sbin/aide e /var/lib/aide.db.gz em um local seguro, por exemplo em um disco somente leitura (como um CD-ROM). Alternativamente, mantenha a impressão digital MD5 ou assinatura GPG desses arquivos em um local seguro, assim você tem meios para verificar que ninguém modificou esses arquivos.

```
# Example configuration file for AIDE.  
@@define DBDIR /var/lib/aide  
  
# The location of the database to be read.  
database=file:/mnt/floppy/aide.db.gz  
  
# The location of the database to be written.  
database_out=file:@@{DBDIR}/aide.db.new.gz  
  
# Whether to gzip the output to database  
gzip_dbout=yes  
  
# Default.  
verbose=5
```

```
report_url=file:/var/log/aide.log
report_url=stdout
```

```
# These are the default rules.
```

```
#
#p:  permissions
#i:  inode:
#n:  number of links
#u:  user
#g:  group
#s:  size
#b:  block count
#m:  mtime
#a:  atime
#c:  ctime
#S:  check for growing size
#md5: md5 checksum
#sha1: sha1 checksum
#rmd160: rmd160 checksum
#tiger: tiger checksum
#haval: haval checksum
#gost: gost checksum
#crc32: crc32 checksum
#R:  p+i+n+u+g+s+m+c+md5
#L:  p+i+n+u+g
#E:  Empty group
#>:  Growing logfile p+u+g+i+n+S
```

```
# You can create custom rules like this.
```

```
NORMAL = R+b+sha1
```

```
DIR = p+i+n+u+g
```

```
# Next decide what directories/files you want in the database.
```

```
/boot  NORMAL
```

```
/bin   NORMAL
```

```
/sbin  NORMAL
```

```
/lib   NORMAL
```

```
/opt   NORMAL
```

```
/usr   NORMAL
```

```
/root  NORMAL
```

```
# Check only permissions, inode, user and group for /etc, but
```

```
# cover some important files closely.
/etc p+i+u+g
!/etc/mtab
/etc/exports NORMAL
/etc/fstab NORMAL
/etc/passwd NORMAL
/etc/group NORMAL
/etc/gshadow NORMAL
/etc/shadow NORMAL
```

Execute o "aide --init" para construir o banco de dados inicial.

```
[root@server root]# /mnt/floppy/aide --init
```

Copie o arquivo /var/lib/aide/aide.db.new.gz para um local seguro

```
(root@server root)# cp /var/lib/aide/aide.db.new.gz /mnt/floppy/var/lib/aide/aide.db.gz
```

Verifique o seu sistema atrás de inconsistências na base de dados do AIDE. Antes de executar a verificação manualmente, assegure-se que o binário do AIDE e o banco de dados não foi modificado sem o seu conhecimento.

```
(root@server root)# /mnt/floppy/aide --check
```

6.1.6.3 Crie um arquivo cronjob para rodar o Aide automaticamente

Este arquivo está incluído no pacote AIDE para Debian, então, se você instalou o AIDE de um *.deb você não precisa criar esse arquivo. O arquivo mostrado abaixo é um exemplo o qual foi modificado para distribuição RedHat / Fedora.

Se você quiser criar um arquivo cronjob para outra distribuição, provavelmente você terá que mudar o caminho.

```
#!/bin/sh

PATH="/bin:/usr/sbin:/usr/bin"
LOGFILE="/var/log/aide.log"
CONFFILE="/etc/aide.conf"
ERRORLOG="/var/log/error.log"

[ -f /usr/sbin/aide ] || exit 0

MAILTO="yourusername"
DATABASE=`grep "^database=file:/" $CONFFILE | head -1 | cut -d: -f2`
LINES="1000"
FQDN=`hostname -f`
DATE=`date +"at %X on %x"``
```

```
[ -z "$MAILTO" ] && MAILTO="root"
```

```
if [ ! -f $DATABASE ]; then
```

```
(
```

```
echo "Fatal error: The AIDE database does not exist!"
```

```
echo "This may mean you haven't created it, or it may mean that someone has removed  
it."
```

```
) | /bin/mail -s "Daily AIDE report for $FQDN" $MAILTO
```

```
exit 0
```

```
fi
```

```
aide --check >$LOGFILE 2>$ERRORLOG
```

```
(cat << EOF;
```

```
This is an automated report generated by the Advanced Intrusion Detection  
Environment on $FQDN ${DATE}.
```

```
EOF
```

```
if [ -s $LOGFILE ]; then
```

```
loglines=`wc -l $LOGFILE | awk '{ print $1 }'`
```

```
if [ ${loglines:=0} -gt $LINES ]; then
```

```
echo
```

```
echo "TRUNCATED (!) output of the daily AIDE run:"
```

```
echo "Output is $loglines lines, truncated to $LINES."
```

```
head -$LINES $LOGFILE
```

```
echo "The full output can be found in $LOGFILE."
```

```
else
```

```
echo "Output of the daily AIDE run:"
```

```
cat $LOGFILE
```

```
fi
```

```
else
```

```
echo "AIDE detected no changes."
```

```
fi
```

```
if [ -s $ERRORLOG ]; then
```

```
errorlines=`wc -l $ERRORLOG | awk '{ print $1 }'`
```

```
if [ ${errorlines:=0} -gt $LINES ]; then
```

```
echo "TRUNCATED (!) output of errors produced:"
```

```
echo "Error output is $errorlines lines, truncated to $LINES."
```

```
head -$LINES $ERRORLOG
```

```
echo "The full output can be found in $ERRORLOG."
```

```
else
```

```
echo "Errors produced:"
```


```
cat $ERRORLOG
```

```
fi
```

```

else
    echo "AIDE produced no errors."
fi
) | /bin/mail -s "Daily AIDE report for $FQDN" $MAILTO

```

 Não é recomendado que você execute o AIDE automaticamente sem executar freqüentemente uma verificação você mesmo. E, além disso, AIDE não implementa nenhuma senha ou proteção em seus próprios arquivos.

6.1.6.4 Amostra do relatório do AIDE

O relatório criado pelo AIDE te mostra todas as mudanças em seus arquivos de sistema. Compare os relatórios com as mudanças que você fez (ex.: instalação ou atualização ou alteração na configuração do servidor).

This is an automated report generated by the Advanced Intrusion Detection Environment on egroupware at 05:27:16 PM on 02/14/2004.

Output of the daily AIDE run:

AIDE found differences between database and filesystem!!

Start timestamp: 2004-02-14 17:27:16

Summary:

Total number of files=34691,added files=2,removed files=0,changed files=5

Added files:

added:/etc/cron.daily/aide

added:/var/log/error.log

Changed files:

changed:/etc/aide.conf

changed:/root

changed:/root/.viminfo

changed:/root/.bash_history

changed:/root/chkrootkit-0.43-1.i386.rpm

Detailed information about changes:

File: /etc/aide.conf

Inode : 89090 , 89173

Directory: /root

Mtime : 2004-02-14 16:35:58 , 2004-02-14 17:27:12

Ctime : 2004-02-14 16:35:58 , 2004-02-14 17:27:12

File: /root/.viminfo

Size : 6683 , 6513

Mtime : 2004-02-14 16:35:58 , 2004-02-14 17:27:12


```
Ctime : 2004-02-14 16:35:58 , 2004-02-14 17:27:12
Inode : 111362 , 111363
MD5 : UM0erzXMWPEdiCgKV/t91g== , l9E0UBQu7PKTCJIS3b2Fzw==
SHA1 : jNlzWrSY/Q4zk3Rd7dnpyth2a0Y= , R1wFnTg2scWSaRnn47zcZ+syS3E=
```

File: /root/.bash_history

```
Size : 14824 , 14872
Mtime : 2004-02-14 16:16:30 , 2004-02-14 16:48:32
Ctime : 2004-02-14 16:16:30 , 2004-02-14 16:48:32
MD5 : zIVCx+39n8XLd3/ip757vA== , nCs18yzJdwDD/BfsUssuhQ==
SHA1 : Al8brD3i+B6P2RMxpn6IaC+I5fE= , bWBEjLA0Hnt6XXTszzKi8gaTZQ=
```

File: /root/chkrootkit-0.43-1.i386.rpm

```
Permissions: -rw-r--r-- , -rw-r-----
Ctime : 2004-01-26 13:43:35 , 2004-02-14 16:51:06
```

AIDE produced no errors.

6.1.6.5 Crie uma nova base de dados após as mudanças

Depois que o relatório for verificado, você deve criar uma nova base de dados e salvar essa base em um local seguro. Execute sempre a atualização da base de dados depois de cada relatório que você verificar!.

```
[root@server root]# /mnt/floppy/aide --init
```

```
(root@server root)# cp /var/lib/aide/aide.db.new.gz /mnt/floppy/var/lib/aide/aide.db.gz
```

6.1.7 Daemon security

Rode os daemons necessários em ambiente chroot em *nix.

Use TCP Wrappers ou xinetd para garantir a segurança dos seus daemons

6.1.8 Firewall

Configure um Firewall em seu servidor para proteger seu sistema.

6.2 Segurança da aplicação web

Com um software de segurança você pode proteger suas aplicações web, como o eGroupware, contra injunções no SQL, execução de scripts laterais e outros ataques. Existem várias aplicações desse tipo no mercado para o servidor Apache e para o IIS. Duas com código-aberto são:

[ModSecurity](#) (para servidor Apache 1.3x e 2.x)

[IISShield](#) (Para Internet Information Server)

ModSecurity é um software de código aberto que atua na detecção e prevenção de intrusão para aplicações web. Funciona embutido no servidor web, atuando como um poderoso “guarda-chuva” - protegendo as aplicações de ataques.

O ModSecurity suporta Apache 1.3x e Apache 2.x.

6.2.1 Instalando o ModSecurity

Descompacte o código fonte do mod_security.

```
[root@server tmp]# tar xzvf mod_security-x.x.x.tar.gz
```

Mude para o diretório do mod_security

```
(root@server tmp)# cd mod_security-x.x.x/apache2
```

Você pode compilá-lo como se fosse um módulo Apache DSO (Dynamic Shared Object) ou estáticamente no servidor web. Se você compilar estáticamente, você deve também recompilar o Apache. Aqui descrevo apenas como usar o ModSecurity como um DSO

```
(root@server apache2)# apxs -cia mod_security.c
```

Usando RedHat, adicione a seguinte linha no arquivo httpd.conf sob a sessão onde os módulos são carregados.

```
(root@server mod_security-1.7.4)# vi /etc/httpd/conf/httpd.conf  
Include /etc/httpd/conf.d/mod_security.conf
```

Você deve reiniciar seu servidor web Apache para ativar o ModSecurity

```
[root@server mod_security-1.7.4]# apachectl stop  
[root@server mod_security-1.7.4]# apachectl start
```

6.2.2 Configuração Básica

O ModSecurity inclui algumas amostras de arquivos de configuração para ajudar você a configurá-lo. Você pode também converter as regras Snort e usá-las dentro do ModSecurity. Amostras das regras Snort podem ser encontradas no servidor do projeto ou você mesmo pode convertê-las.

```
<IfModule mod_security.c>
```

```
# Turn the filtering engine On or Off  
SecFilterEngine On
```

```
# Make sure that URL encoding is valid  
SecFilterCheckURLEncoding On
```

```
# The audit engine works independently and  
# can be turned On or Off on the per-server or  
# on the per-directory basis. "On" will log everything,  
# "DynamicOrRelevant" will log dynamic requests or violations,  
# and "RelevantOnly" will only log policy violations  
SecAuditEngine RelevantOnly
```

```
# The name of the audit log file
```

```

SecAuditLog logs/audit_log

SecFilterDebugLog logs/modsec_debug_log
SecFilterDebugLevel 0

# Should mod_security inspect POST payloads
SecFilterScanPOST On

# Action to take by default
SecFilterDefaultAction "deny,log,status:500"

# Prevent path traversal (..) attacks
SecFilter ".|.|./"

# Weaker XSS protection but allows common HTML tags
SecFilter "<[[:space:]]*script"

# Very crude filters to prevent SQL injection attacks
SecFilter "delete[[:space:]]+from"
SecFilter "insert[[:space:]]+into"
SecFilter "select.+from"

# Require HTTP_USER_AGENT and HTTP_HOST headers
SecFilterSelective "HTTP_USER_AGENT|HTTP_HOST" "^$"

</IfModule>

```



Tome cuidado! A configuração do ModSecurity depende dos outros módulos que você está usando. Você deve fazer um ajuste fino da sua configuração a medida em que for recebendo erros. Use apenas os filtros que são necessários ao seu servidor. Por exemplo, se você está rodando um servidor Linux, não é necessário testar ou usar as regras do Windows.

6.2.3 Teste do ModSecurity

Você pode executar um teste rápido das funcionalidades do ModSecurity. Mude para o diretório de testes no modsecurity e execute alguns dos testes de exemplo.

```

[root@server tests]# ./run-test.pl yourIpAdress 09-directory-traversal-in-parameters.test
11-xss-attack.test 13-sql-injection.test

```

```

Test "09 Directory traversal in parameters": Failed (status = 406)
Test "11 XSS attack": Failed (status = 406)
Test "13 SQL injection": Failed (status = 406)

```

6.2.4 Amostra do log do ModSecurity

Este é um exemplo de log dos testes realizados acima.

```
Request: xxx.xxx.xxx.xxx - - [[21/Feb/2004:20:40:29 +0100]] "GET
/cgi-bin/modsec-test.pl?p=../../tmp/file.txt HTTP/1.0" 406 352
Handler: cgi-script
-----
GET /cgi-bin/modsec-test.pl?p=../../tmp/file.txt HTTP/1.0
Host: xxx.xxx.xxx.xxx :80
User-Agent: mod_security regression test utility
Connection: Close
mod_security-message: Access denied with code 406. Pattern match "\.|\./"
at THE_REQUEST.
mod_security-action: 406

HTTP/1.0 406 Not Acceptable
Content-Length: 352
Connection: close
Content-Type: text/html; charset=iso-8859-1
=====

Request: xxx.xxx.xxx.xxx - - [[21/Feb/2004:20:40:29 +0100]] "GET
/cgi-bin/modsec-test.pl?p=<script>alert('Bang!')</script> HTTP/1.0" 406
352
Handler: cgi-script
-----
GET /cgi-bin/modsec-test.pl?p=<script>alert('Bang!')</script> HTTP/1.0
Host: xxx.xxx.xxx.xxx:80
User-Agent: mod_security regression test utility
Connection: Close
mod_security-message: Access denied with code 406. Pattern match "<(\n)*script" at THE_REQUEST.
mod_security-action: 406

HTTP/1.0 406 Not Acceptable
Content-Length: 352
Connection: close
Content-Type: text/html; charset=iso-8859-1
=====

Request: xxx.xxx.xxx.xxx - - [[21/Feb/2004:20:40:29 +0100]] "GET
/cgi-bin/modsec-test.pl?p=DELETE%20FRoM+users HTTP/1.0" 406 352
Handler: cgi-script
-----
GET /cgi-bin/modsec-test.pl?p=DELETE%20FRoM+users HTTP/1.0
```

```
Host: xxx.xxx.xxx.xxx
User-Agent: mod_security regression test utility
Connection: Close
mod_security-message: Access denied with code 406. Pattern match
"delete[:,space:]]+from" at THE_REQUEST.
mod_security-action: 406

HTTP/1.0 406 Not Acceptable
Content-Length: 352
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

6.3 Otimização e segurança do servidor web Apache

Para garantir a segurança do servidor web você deve desabilitar todos os módulos desnecessários. Deixe ativo apenas o que você precisa para rodar as aplicações web. Executar o Apache com menos módulos também melhora o desempenho.

6.3.1 Módulos recomendados para rodar

Nesta seção, apresentamos um pequeno resumo do que você precisa para rodar Apache para o eGroupware. Todos ou outros módulos podem e devem ser desabilitados.



Otimização do servidor web Apache não é para iniciantes! Quando você desabilita alguns módulos no arquivo httpd.conf é possível que algumas outras opções também devam ser comentadas. É fortemente recomendado que você desabilite um módulo, pare o Apache e inicie-o novamente. Examine as mensagens de erro.

```
mod_access.so
mod_auth.so
mod_include.so
mod_log_config.so
mod_expires.so
mod_deflate.so
mod_headers.so
mod_unique_id.so
mod_setenvif.so
mod_mime.so
mod_negotiation.so
mod_dir.so
mod_alias.so
```

6.3.2 Outras opções de configuração do Apache

Você pode esconder informações sobre seu servidor web Apache por razões de segurança. Existem diversas possibilidades para o Apache 1.3 e Apache2.x.

A variável **ServerTokens** em seu arquivo `httpd.conf` deve ter o valor **OS**, a variável **ExtendedStatus** o valor **OFF**. **ServerSignature** deve estar com o valor **OFF**, o diretório do manual `/var/www/manual` deve ter o **acesso negado a todos** (`deny from all`). Se você não precisar do **cgi-bin** desabilite-o. O **AddHandler** para o `type-map INCLUDES`, comente toda essa linha, adicionando um `#` no início da linha. Dentro de `/var/www/error/` mude de **Order deny, allow** para **Deny from all**. Os diretórios `/server-status` e `/server-info` nunca devem ser legíveis ao público por razões de segurança.

6.4 Turck MMCache

O Turck MMCache é um acelerador PHP de código aberto, otimizador, codificador e dinamizador do conteúdo da cache para PHP. Aumenta o desempenho dos scripts cacheando-os em modo compilado, de modo que o overhead da compilação é quase completamente eliminado. O Turck MMCache também usa algumas otimizações para acelerar a execução dos scripts PHP, e seu uso reduz a carga no servidor e aumenta a velocidade do seu código PHP em até 10 vezes.

Para maiores informações visite a [página de desenvolvimento](#).

6.4.1 Requisitos

É necessário o `phpize` para compilar o script de configuração. Verifique a disponibilidade do `phpize` através de busca ou procura. Na distribuição Fedora você deve instalar `php-devel` para compilar `mmcache`.



O RedHat 3 **não possui** o pacote `phpize`. Você deve recompilar o pacote do PHP e compilar dois pacotes de desenvolvimento.

6.4.1.1 Pre-requisitos para o RedHat 3

Para compilar o pacote de desenvolvimento PHP (PHP Devel Package) você precisa dos seguintes pacotes.

```
bzip2-devel curl-devel db4-devel expat-devel freetype-devel gd-devel gdbm-devel gmp-devel  
pspell-devel httpd-devel libjpeg-devel, libpng-devel pam-devel libstdc++-devel libxml2-devel  
ncurses-devel openssl-devel zlib-devel pcre-devel imap-devel
```

Os pacotes `pcre-devel` e `imap-devel` não são oferecidos para RedHat e você deve construí-los. Baixe o `srpm` para seu servidor, copie-os para `/usr/src/redhat/SRPMS`, e construa os pacotes `devel`.

```
[root@server SRPM]#rpmbuild --rebuild pcre-x.x-xx.src.rpm  
[root@server SRPM]#rpmbuild --rebuild imap-x.x-xx.src.rpm
```

Mude para o diretório RPM e instale os `devel` RPMs necessários no seu servidor

```
[root@server SRPM]#cd /usr/src/redhat/RPM/i386  
[root@server i386]#rpm -ivh pcre-devel-x.x-xx.i386 imap-devel-xxxxx-x.rpm
```

Instale o PHP `src` RPM em seu servidor e mude para o diretório `SPEC`

```
[root@server SRPM]#cd /usr/src/redhat/SPEC
```

Agora você deve editar o arquivo `php.spec` com o `VI` ou `VIM`

Após a linha 55 adicione as seguintes linhas e

```
%package devel  
Group: Development/Libraries  
Summary: Files needed for building PHP extensions.
```

%description devel

The php-devel package contains the files needed for building PHP extensions. If you need to compile your own PHP extensions, you will need to install this package.

Altere a seguinte linha. Onde está:

```
$RPM_BUILD_ROOT%{_bindir}/{phptar,pearize,php-config,phpextdist,phpize}
```

Para:

```
$RPM_BUILD_ROOT%{_bindir}/{phptar,pearize}
```

Remova estas linhas:

```
rm -rf $RPM_BUILD_ROOT%{_includedir} |  
$RPM_BUILD_ROOT%{_libdir}/php
```

Adicione este bloco após a primeira %seção de arquivos

```
%files devel  
%defattr(-,root,root)  
%{_bindir}/php-config  
%{_bindir}/phpize  
%{_bindir}/phpextdist  
%{_includedir}/php  
%{_libdir}/php
```

Salve o arquivo e compile o novo pacote


```
[root@server SPECS]# rpmbuild -bb php.spec
```

Instale **apenas** o pacote php-devel e seu servidor!

6.4.2 Compatibilidade

Essa versão do Turck MMCache foi testada com sucesso com o PHP 4.1.0-4.3.2 sob RedHat 7.0, 7.3 e 8.0; RedHat ES e AS; e Windows com Apache 1.3 e 2.0.

6.4.3 Instalação Rápida

```
 Compilando o Turck MMCache  
export PHP_PREFIX="/usr"  
$PHP_PREFIX/bin/phpize  
./configure --enable-mmcache=shared --with-php-config=  
$PHP_PREFIX/bin/php-config  
make
```

No comando "export" você deve especificar o prefix real onde o PHP está instalado. Pode ser "/usr/local/", ou alguma outra coisa.

✍ Instalando o Turck MMCache

```
make install
```

✍ Configurando o Turck MMCache

O Turck MMCache pode ser instalado como extensão Zend ou PHP. Você necessitará alterar seu arquivo php.ini (geralmente /etc/php.ini))

Para instalar como extensão Zend:

```
zend_extension="/usr/lib/php4/mmcache.so"
mmcache.shm_size="16"
mmcache.cache_dir="/tmp/mmcache"
mmcache.enable="1"
mmcache.optimizer="1"
mmcache.check_mtime="1"
mmcache.debug="0"
mmcache.filter=""
mmcache.shm_max="0"
mmcache_ttl="0"
mmcache.shm_prune_period="0"
mmcache.shm_only="0"
mmcache.compress="1"
```

Se você estiver usando uma compilação de PHP "thread-safe" deve usar "zend_extensions_ts" ao invés de "zend_extension".

Para instalar como extensão PHP:

```
extension="mmcache.so"
mmcache.shm_size="16"
mmcache.cache_dir="/tmp/mmcache"
mmcache.enable="1"
mmcache.optimizer="1"
mmcache.check_mtime="1"
mmcache.debug="0"
mmcache.filter=""
mmcache.shm_max="0"
mmcache_ttl="0"
mmcache.shm_prune_period="0"
mmcache.shm_only="0"
mmcache.compress="1"
mmcache.content
```

✍ Criando um diretório de cache

```
mkdir /tmp/mmcache
chmod 0777 /tmp/mmcache
```


6.4.4 Interface web

O Turck MMCache pode ser gerenciado através do script de interface web mmcache.php, assim, você tem que colocar este arquivo no seu no seu site web. Por razões de segurança é recomendado restringir o acesso a esse script ao seu IP local. A partir da versão 2.3.18 a interface de administrador pode ser protegida por uma senha. Para gerar essa senha execute o arquivo mmcache_password.php através de uma linha de comando e siga as instruções.



Crie a senha mmcache

```
[root@server turck-mmcache***]# php -q mmcache_password.php
Changing password for Turck MMCache Web Interface (mmcache.php)
Enter admin name: cacheadminname
New admin password: yourpassword
Retype new admin password: yourpassword
```

Adicione as seguintes linhas no arquivo php.ini e reinicie o HTTPD

```
mmcache.admin.name="cacheadminname"
mmcache.admin.password="$1$0ScD9gkb$nOEmFerNMvQ576hELrG0"
```

6.5 Garantindo a segurança da instalação do PHP

Proteja os diretórios do seu servidor web, alterando as permissões, de forma que estes estejam visíveis apenas para o usuário do webserver.

```

//////////
; Language Options ;
//////////
; open_basedir, if set, limits all file operations to the defined directory
; and below. This directive makes most sense if used in a per-directory
; or per-virtualhost web server configuration file.
open_basedir = /var/www/html:/var/www/files:/tmp:/usr/share/pear:/usr/bin/crontab

; Decides whether PHP may expose the fact that it is installed on the server
; (e.g. by adding its signature to the Web server header). It is no security
; threat in any way, but it makes it possible to determine whether you use PHP
; on your server or not.
expose_php = Off

//////////
; Resource Limits ;
//////////
max_execution_time = 30 ; Maximum execution time of each script, inseconds
memory_limit = 24M ; Maximum amount of memory a script may consume (8MB)

//////////
; Error handling and logging ;
//////////
; Print out errors (as a part of the output). For production web sites,
; you're strongly encouraged to turn this feature off, and use error logging
; instead (see below). Keeping display_errors enabled on a production web site
; may reveal security information to end users, such as file paths on your Web
; server, your database schema or other information.
display_errors = Off

; Even when display_errors is on, errors that occur during PHP's startup
; sequence are not displayed. It's strongly recommended to keep
; display_startup_errors off, except for when debugging.
display_startup_errors = Off

; Log errors into a log file (server-specific log, stderr, or error_log (below))
; As stated above, you're strongly advised to use error logging in place of
; error displaying on production web sites.

```

```
log_errors = On
```

```
; Store the last error/warning message in $php_errormsg (boolean).
```

```
track_errors = Off
```

```
; Log errors to syslog (Event Log on NT, not valid in Windows 95).
```


```
error_log = syslog
```

```
//////////
```

```
; Data Handling ;
```

```
//////////
```

```
register_globals = OFF
```

 É mais seguro configurar os caminhos para `session.save_path` e `upload_tmp_dir` em seu arquivo `php.ini` e incluí-los para serem abertos com restrições.

6.6 Criando um certificado para o seu servidor web

Para proteger sua privacidade na conexão com o eGroupWare você pode usar um certificado do servidor. Com um certificado, você conecta-se com seu servidor web através de uma conexão criptografada (https no lugar de http). Sem uma conexão segura (https), outras pessoas podem capturar sua senha ou outras informações.

Você tem algumas opções para criar um certificado para seu servidor web:

- 1.) Crie sua própria autoridade de certificação e assine o certificado do seu servidor

(Grau de Confiabilidade= baixa)

- 2.) Use uma autoridade de certificação não paga

<https://www.cacert.org>

(Grau de confiabilidade= Alta)

- 3.) Use uma autoridade de certificação paga

<http://www.thawte.com>

<https://www.verisign.com>

(Grau de confiabilidade= Alta)

 Se você deseja usar uma autoridade paga, vá direto para o item **5.3.2**

6.6.1 Associando-se ao CA Cert

O primeiro passo para receber um certificado digital para seu servidor é associar-se ao [cacert](https://www.cacert.org).

Abra seu navegador na seguinte URL: <https://www.cacert.org>

Clique no link: "Join CA Cert" ao lado esquerdo.

Prossiga com o registro


Preencha todas as informações necessárias para receber sua conta no CA Cert.

Depois de submeter sua senha você receberá mais instruções via e-mail.

6.6.2 Criando o pedido de assinatura do seu certificado

Você deve criar uma chave e um pedido de assinatura de um certificado em seu servidor.

6.6.2.1 Alterando o arquivo openssl.cnf

 Você só precisará alterar o arquivo openssl.cnf se quiser usar um certificado de uma autoridade não comercial (não paga). Em Debian Linux o arquivo se encontra em /usr/lib/ssl/ e no RedHat o caminho é /usr/share/ssl/

Verifique se seu arquivo openssl.cnf é semelhante aos seguintes trechos. As linhas importantes aqui são as que estão comentadas ou alteradas no valor do nome do Estado (stateOrProvinceName value).

```
[root@server ssl]# vi openssl.cnf
```

```
# For the CA policy
[ policy_match ]
countryName                = match
stateOrProvinceName        = optional
organizationName           = match
organizationalUnitName     = optional
commonName                 = supplied
emailAddress               = optional

[ req_distinguished_name ]
countryName                = Country Name (2 letter code)
countryName_default        = GB
countryName_min            = 2
countryName_max            = 2

stateOrProvinceName        = State or Province Name (full name)
#stateOrProvinceName_default = Berkshire
```

localityName = Locality Name (eg, city)

#localityName_default = Newbury

0.organizationName = Organization Name (eg, company)

#0.organizationName_default = My Company Ltd

organizationalUnitName = Organizational Unit Name (eg, section)

#organizationalUnitName_default =

6.6.2.2 Criando a chave de segurança do seu servidor e o pedido de assinatura

Para ter um certificado, você deve criar uma chave no seu servidor e uma requisição de assinatura.

1.) Crie uma chave para o servidor. No Debian, essa chave ficará na pasta `/etc/ssl/certs/` e no RedHat na pasta `/etc/httpd/conf/ssl.csr/`



Os comandos a seguir criam uma chave de segurança que é protegida por senha. Caso você não tenha acesso ao seu servidor via console, **NÃO** crie uma chave protegida por senha. Seu servidor ficará esperando por uma senha no boot e não iniciará enquanto a senha não for dada. Se você tiver acesso via console, use a chave protegida por senha. É mais seguro..

```
[root@server ssl]# /usr/bin/openssl genrsa -des3 1024 > /etc/httpd/conf/ssl.key/server.key
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
Enter PEM pass phrase:
```

Para criar uma chave **não protegida por senha**

```
[root@server ssl]# /usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
```

Mude as permissões de acesso à sua chave

```
[root@server ssl]# chmod go-rwx /etc/httpd/conf/ssl.key/server.key
```

2.) Agora você deve criar o pedido de assinatura do certificado. Lembre-se de mudar os caminhos específicos para as chaves no seu servidor

```
[root@server ssl]# /usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-out /etc/httpd/conf/ssl.csr/server.csr
Utilizando a configuração que está em /usr/share/ssl/openssl.cnf
```

Enter PEM pass phrase:

O sistema irá solicitar uma senha, a mesma que você digitou quando criou a chave. Se você a criou sem uma senha, esta não será necessária.

Você precisará responder algumas informações que serão incorporadas em sua requisição do certificado. O que você vai responder é chamado de Distinguished Name ou DN. São relativamente poucos campos e inclusive você pode deixar alguns em branco. Alguns campos possuem um valor padrão. Se você digitar "." (ponto), o campo será deixado em branco.

*Country Name (2 letter code) [GB]:***DE**

State or Province Name (full name) []:

Locality Name (eg, city) [Newbury]:

*Organization Name (eg, company) [My Company Ltd]:***egroupware.org**

Organizational Unit Name (eg, section) []:

*Common Name (your name or server's hostname) []:***egroupware.org**

*Email Address []:*yourname@yourdomain.org

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:

Você irá encontrar, nas suas pastas, um novo arquivo chamado server.csr. Este arquivo tem que ser enviado para a autoridade de certificação escolhida.

6.6.2.3 Enviando o pedido de para o seu CA

A requisição da assinatura do certificado tem de ser enviada para a autoridade de certificação. Aqui nós mandamos para CA Cert.

Abra o navegador no endereço: <https://www.cacert.org>

Vá até o link "Server Certificate" => "Login"

Adicione um novo domínio

Confirme o e-mail que te enviaram

Vá até o link "Certificates" => "Request"

Copie tudo do seu arquivo server.csr nos campos de texto

Concorde com o processo s

6.6.2.4 Instalando o certificado do servidor.

Após a submissão do .csr, você receberá um e-mail do CA com seu certificado assinado. Todo o corpo do e-mail tem que ser copiado em seu servidor em um arquivo chamado server.crt.

Após salvar o arquivo, o servidor web deve ser reiniciado.

6.7 O servidor Web

Garanta a segurança dos diretórios do seu servidor web, de forma que eles só estejam visíveis para o usuário do próprio servidor.

```
[root@server html]# chown -R root.webserveruser egroupware
[root@server html]# find egroupware -type d -exec chmod 550 {} \;
[root@server html]# find egroupware -type f -exec chmod 440 {} \;
```

Recomendamos fortemente a proteção do diretório do seu Apache. Adicione as seguintes linhas no arquivo httpd.conf.

```
<Directory /var/www/html/egroupware>
    <Files ~ ".inc|.php$ /|.tpl$">
        Order allow,deny
        Deny from all
    </Files>
</Directory>
```

6.8 O servidor SQL

MySQL

- ✍ Assegure-se de que seu banco de dados está rodando e que é também iniciado automaticamente quando o servidor é iniciado
- ✍ Se esta é a primeira vez que você configura seu banco de dados MySQL não se esqueça de estabelecer uma senha para ele. A senha padrão é um **"string" vazio**.

Para definir a senha do MySQL use o seguinte comando

```
[root@server html]# mysqladmin -u root password 'new-password'
```

- ✍ O servidor MySQL inclui um banco de teste. Este banco não é necessário ao ambiente de produção. Apague-o.

```
[root@server html]# mysql -u root -p
Enter Password:
mysql> drop database test;
Query OK, 0 rows affected (0,03 sec)
```

- ✍ Em bancos de dados MySQL, adicione o seguinte parâmetro para ter certeza que seu servidor MySQL só poderá ser acessado via localhost. Altere o arquivo /etc/my.cnf e adicione a seguinte linha:

```
[mysqld]
bind-address=127.0.0.1
```

7 Configurando o eGroupWare (setup)

7.1 Crie seu banco de dados



Nas versões mais novas do eGroupware, o setup pode criar o banco de dados automaticamente para você. Até o momento, isto funciona apenas nos bancos MySQL e PostgreSQL. No MSSQL, você deve criar seu banco manualmente. Se você quer que o eGroupware crie o banco de dados automaticamente (MySQL e PostgreSQL), vá para o tópico **5.3**

MySQL

✍ Crie seu banco de dados e um usuário para se conectar ao DB

Crie o banco

```
[root@server html]# mysqladmin -u yourmysqladmin -p create database
Enter password:
```

Crie o usuário e dê a ele os privilégios do banco

```
[root@server html]# mysql -u yourmysqladmin -p
Enter password:
mysql> grant all on egroupware.* to egroupwaredbuser@localhost
identified by "password"
```

PostgreSQL

✍ Confirme se a conexão com o banco é possível

Apartir da conta de root mude para a conta do postgres

```
[root@server html]# su - postgres
```

Edite o arquivo postgresql.conf

```
-bash-2.05b$ cd data
-bash-2.05b$ vi postgresql.conf
```

Seu arquivo deve se parecer com o exemplo abaixo

```
#Connection Parameter
tcpip_socket = true
#ssl = false
#max_connections = 32
port = 5432
```

Modifique o arquivo pg_hba.conf para que ele fique parecido com nosso exemplo

```
# TYPE DATABASE USER IP_ADDRESS MASK AUTH_TYPE AUTH_ARGUMENT
local egroupware trust
host egroupwaredbname all 127.0.0.1 255.255.255.255 md5
```



O valor Usuário (User) está disponível à partir do PostgreSQL 7.3.X

Reinicie o servidor PostgreSQL e teste sua conectividade

```
[root@server html]# /etc/init.d/postgresql restart
[root@server html]# su - postgres
bash-2.05b$ psql -h localhost template1
```

Feche a conexão do banco de dados

```
template1=# \q
```

✍ Configure seu banco de dados PostgreSQL

Crie um usuário que possua privilégios de acessar o banco de dados do eGroupware

```
bash-2.05b$ createuser yourdbusername -P
Answer the next questions with yes:
bash-2.0.5b$ Shall the new user be allowed to create databases?
(y/n) Y
bash-2.0.5b$ Shall the new user be allowed to create more new
users? (y/n) N
```

Crie o novo banco eGroupWare

```
bash-2.05b$ createdb -U yourdbusername yourdatabasename
```

7.2 Como iniciar a configuração?

Aponte seu navegador para a URL do seu servidor para abrir o menu de configuração.

<https://www.seuservidor.com.br/egroupware/setup>

Você será automaticamente redirecionado para a verificação da instalação do eGroupware, que é nosso próximo passo

7.3 Verificando a instalação do eGroupWare

Se nenhum arquivo header.inc.php já estiver criado, o eGroupWare executará uma checagem em alguns parâmetros de configuração em seu php.ini e no seu sistema de arquivos local. A checagem mostrará alguns erros e avisos.



Os erros são mostrados com uma cruz vermelha e **têm** de ser resolvidos por você!

Os avisos podem ser **ignorados**. Por exemplo, um aviso da verificação do safe_mode. Se você souber como configurar as restrições do safe_mode isto não será problema pra você, mas para novos usuários é melhor que essa função seja desabilitada.

Checking the eGroupWare Installation

```

Checking php.ini: safe_mode = Off: ini_get('safe_mode')='1' = On
safe_mode is turned on, which is generally a good thing as it makes your install more secure.
If safe_mode is turned on, eGW is not able to change certain settings on runtime, nor can we load any not yet loaded m
*** You have to do the changes manually in your php.ini (usually in /etc on linux) in order to get eGW fully working !!!
*** Do NOT update your database via setup, as the update might be interrupted by the max_execution_time, which leaves

✓ Checking php.ini: magic_quotes_runtime = Off: ini_get('magic_quotes_runtime')='' = Off

✓ Checking php.ini: register_globals = Off: ini_get('register_globals')='' = Off

✗ Checking php.ini: memory_limit >= 16M: ini_get('memory_limit')='8M'
memory_limit is set to less than 16M: some applications of eGroupWare need more than the recommend 8M, expect occasion
*** Please make the following change in your php.ini: memory_limit = 16M

✓ Checking php.ini: max_execution_time >= 30: ini_get('max_execution_time')='30'

✓ Checking php.ini: include_path contain .: ini_get('include_path')='.:usr/share/pear'

✓ Checking extension mysql is loaded or loadable: True


```

7.4 Crie seu “header.inc.php”

A maior parte da configuração para seu header.inc.php é auto-explicativa. Este menu está disponível em outros idiomas que não o inglês, mas provavelmente não está traduzido para seu idioma nativo.

Até o momento o eGW suporta os bancos: MySQL, PostgreSQL e MSSQL. O suporte a bancos Oracle não foi bem testado.

Com a caixa de seleção de domínio, você pode configurar mais de uma instalação do eGroupWare. Por exemplo, se você quer ter uma instalação de produção, na qual seus funcionários irão trabalhar, e uma como ambiente de treinamento.

 Se você quis configurar seu banco de dados manualmente, no passo 4.4., você já forneceu o nome do banco de dados, usuário, senha... Se você quiser que o programa de configuração do eGroupWare crie o banco de dados automaticamente, você deve dar os valores pela primeira vez aqui.

Os próximos campos descrevem qual o banco de dados que você deseja utilizar para o eGroupWare e o usuário para se conectar a este banco. Não use o usuário administrador do banco para conectar-se a ele. Crie um outro usuário!

DH Host	Se o seu banco de dados roda na mesma máquina que sua instalação do eGroupWare o DB host será localhost. Você também pode usar um servidor separado para rodar seu banco de dados.
DB Name	O nome do banco de dados que você deseja criar no seu servidor de BD.
DB User	O usuário que o eGroupWare usará para se conectar ao banco.
DB Password	A senha necessária para se conectar ao BD
DB Type	Selecione o tipo de banco que se quer utilizar

Faça o download do header.inc.php criado em sua máquina local.

Copie o arquivo header.inc.php para o diretório raiz do eGroupWare e altere os privilégios de acesso, de forma que apenas o servidor web tenha acesso para leitura

```
[user@server tmp]$ scp header.inc.php youregwserver:/tmp
[user@server tmp]$ ssh youregwserver
[user@youregwserver user]$ su -
Password:
[root@server root]# mv /tmp/header.inc.php /var/www/html/egroupware; chmod 400
/var/www/html/egroupware/header.in.php;
chown apache /var/www/html/egroupware/header.in.php
```

Continue o próximo passo no seu navegador

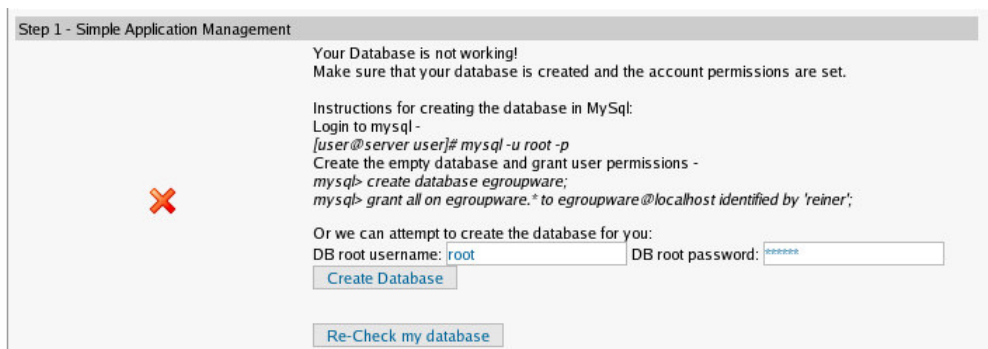
7.5 Setup / Config Admin

Após você ter terminado a criação do arquivo header.inc.php e continuado, você verá uma nova janela, que permite iniciar uma nova sessão (login). Inicie a nova sessão em **Setup/Config Admin Login** com a senha que você forneceu no último passo. (7.4)

7.5.1 Passo 1 – Gerenciamento simplificado da Aplicação

Aqui você tem duas possibilidades: Se quiser criar seu banco de dados automaticamente neste passo, então vá para “**create your database** (crie sua base de dados)” now. Se você criou o banco manualmente, então vá para “**create your tables** (crie suas tabelas)”.

Criar sua base de dados



Step 1 - Simple Application Management

Your Database is not working!
Make sure that your database is created and the account permissions are set.

Instructions for creating the database in MySQL:
Login to mysql -
[user@server user]# mysql -u root -p
Create the empty database and grant user permissions -
mysql> create database egroupware;
mysql> grant all on eggroupware.* to eggroupware@localhost identified by 'reiner';

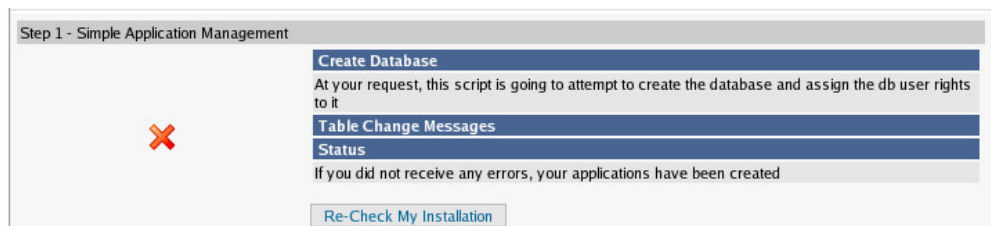
Or we can attempt to create the database for you:
DB root username: DB root password:

Preencha o formulário para criar um banco de dados automaticamente:

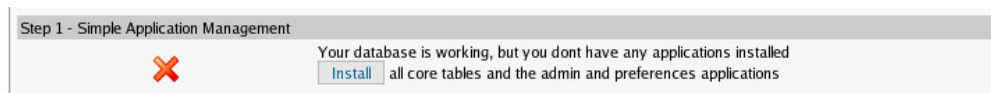
DB root username nome do usuário a ser usado para acessar o banco de dados

BD Password senha do DB root

E submeta através do botão “Create Database”

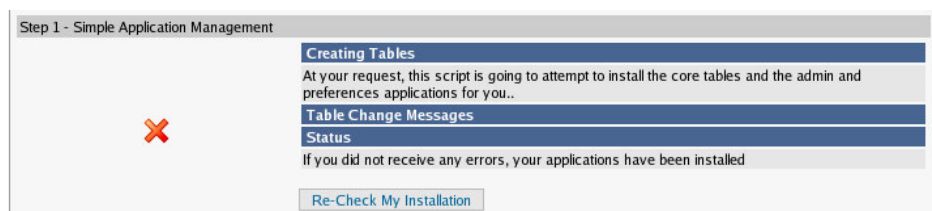


Re-Check Installation (Verifique novamente a instalação)



Criar suas tabelas.

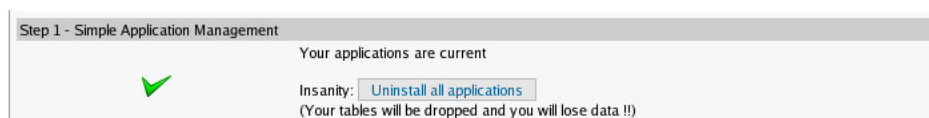
Se você **não** visualizar nenhum erro, você pode instalar as tabelas. Clique em "install" (instalar)



Criar suas tabelas.

Agora, observe o status. Se você não visualizar nenhum erro aqui, continue com

"Re-Check My Installation".



7.5.2 Passo2 – Configuração

A maioria das partes neste passo são auto-explicativas. Apenas algumas informações freqüentemente mal compreendidas serão fornecidas aqui.

7.5.2.1 Crie as pastas de arquivos

Você tem que criar o diretório de **arquivos** manualmente no prompt do shell. Nesse diretório, o eGroupWare armazenará os anexos do Infolog, Filemanager (gerenciador de arquivos) e outras aplicações.



Este diretório não deve pertencer ao diretório raiz do seu servidor web! Se você não sabe onde está o diretório raiz do seu servidor, observe o arquivo httpd.conf ou digite o seguinte comando no Linux:

```
[root@server www]$ cat /etc/httpd/conf/httpd.conf | grep ^DocumentRoot
DocumentRoot "/var/www/html"
```

Crie o diretório de arquivos e os subdiretórios necessários.

```
[root@server www]$ mkdir /var/www/files  
[root@server www]$ mkdir /var/www/files/users /var/www/files/groups
```

Você precisa assegurar que o usuário do servidor web tenha os privilégios de leitura e gravação nestes diretórios.

```
[root@server www]$ chown -R apache.apache /var/www/files  
[root@server www]$ chmod -R 0700 /var/www/files
```

7.5.2.2 Editando a configuração atual

Informações do Path

Entre com os valores necessários para as informações do Path (caminho)

- ✍ O diretório tmp é necessário para armazenar as sessões e outras informações da sua instalação do eGroupWare. Se você executa a instalação do eGroupWare em um ambiente raiz alterado ou com restrições open_basedir em seu php.ini, é exigida a alteração do valor do path.
- ✍ O path completo para os arquivos de usuários e de grupos deve ser externo ao diretório raiz do servidor web por razões de segurança. Não é possível ter esse diretório dentro da raiz do servidor web!
- ✍ Entre com a localização da URL do eGW. Se você deseja usar conexões HTTP e HTTPS, use /egroupware (se você deseja impor o uso de HTTPS, então use https://yourdomain/egroupware)
- ✍ Por favor não altere o critério de seleção do tipo de imagens do seu padrão (o qual pode ser diferente do exemplo mostrado abaixo). Isso pode quebrar o design do UI

Path information	
Enter the full path for temporary files. Examples: /tmp, C:\TEMP:	<input type="text" value="/tmp"/>
Enter the full path for users and group files. Examples: /files, E:\FILES: This has to be outside the webserver's document-root!!! or http://webdav.domain.com (WebDAV):	<input type="text" value="/var/www/files_directory"/>
Enter the location of eGroupWare's URL. Example: http://www.domain.com/egroupware or /egroupware No trailing slash:	<input type="text" value="/egroupware"/>
Image type selection order:	<input type="text" value="GIF->JPG->PNG"/>

Informações do Host

- Informe o nome do host do seu servidor. Pode ser um nome DNS válido ou um endereço IP sobre o qual a instalação será executada.
- Quando sua instalação do eGroupWare está localizada atrás de um Servidor Proxy (como o SQUID) e você deseja usar as aplicações headlines ou stocks, você deve configurar os valores deste proxy.

Host information	
Enter the hostname of the machine on which this server is running:	<input type="text" value="www.creativix.net"/>
Enter your default FTP server:	<input type="text"/>
Attempt to use correct mimetype for FTP instead of default 'application/octet-stream':	<input type="text" value="No"/>
Enter your HTTP proxy server:	<input type="text" value="proxy.company"/>
Enter your HTTP proxy server port:	<input type="text" value="3381"/>
Enter your HTTP proxy server username:	<input type="text" value="proxy_username"/>
Enter your HTTP proxy server password:	<input type="text" value="proxy_password"/>

Contas / Autenticação

- Existem diversos tipos de autenticação disponíveis: SQL, SQL/SSL, LDAP, Mail, NIS e PAM. Selecione qual tipo você deseja utilizar para autenticar seus usuários do eGW.
- Selecione o tipo de encriptação para as senhas dos usuários. A senha dos usuários será armazenada criptografada no banco de dados.
- Se você deseja usar uma árvore LDAP para diferentes instalações para autenticação, você pode usar um prefixo nas contas.
- Use nome de usuários "case-sensitive" para maior segurança.

Authentication / Accounts	
Select which type of authentication you are using:	<input type="text" value="SQL"/>
Select where you want to store/retrieve user accounts:	<input type="text" value="SQL"/>
SQL encryption type for passwords (default - md5):	<input type="text" value="MD5"/>
Minimum account id (e.g. 500 or 100, etc.):	<input type="text"/>
Maximum account id (e.g. 65535 or 1000000):	<input type="text"/>
User account prefix:	<input type="text"/>
Usernames are casesensitive:	<input type="text" value="Yes"/>
Auto create account records for authenticated users:	<input type="text" value="No"/>
Auto-created user accounts expire:	<input type="text" value="one week"/>
Add auto-created users to this group ('Default' will be attempted if this is empty.):	<input type="text"/>
If no ACL records for user or any group the user is a member of:	<input type="text" value="Deny Access"/>

Se estiver usando LDAP

Se você não pretende utilizar LDAP, não é necessário preencher esses campos. Se você deseja usar LDAP, dê uma olhada em [phpgwapi/doc/ldap/README](#).

If using LDAP:	
Do you want to manage homedirectory and loginshell attributes?:	<input type="button" value="Yes"/>
LDAP Default homedirectory prefix (e.g. /home for /home/username):	<input type="text" value="/home"/>
LDAP Default shell (e.g. /bin/bash):	<input type="text" value="/bin/false"/>
LDAP host:	<input type="text" value="127.0.0.1"/>
LDAP accounts context:	<input type="text" value="dc=accounts,dc=network,dc=loc"/>
LDAP groups context:	<input type="text" value="dc=groups,dc=network,dc=loc"/>
LDAP rootdn:	<input type="text" value="cn=egroupware,dc=network,dc=loc"/>
LDAP root password:	<input type="password"/>
LDAP encryption type:	<input type="button" value="DES"/>
Enable LDAP Version 3:	<input type="button" value="No"/>

Configurações do Mcrypt (exige a extensão mcrypt PHP)

Nem todas as distribuições tem um mcrypt compilado executando nelas por padrão, você precisará verificar isso. Você também terá que experimentar diversas versões para ver qual funciona melhor com o eGroupWare.

Mcrypt Settings (requires mcrypt PHP extension)	
Enter some random text for app session encryption:	<input type="text" value="hjlhdfgilzslfzoayhlchvuzertis"/>
Mcrypt algorithm (default TRIPLEDES):	<input type="button" value="TRIPLEDES"/>
Mcrypt mode (default CBC):	<input type="button" value="CBC"/>

Configurações adicionais

Os valores padrões aqui estão OK.

Additional settings	
Select where you want to store/retrieve filesystem information: (file type, size, version, etc.)	<input type="button" value="SQL"/>
Select where you want to store/retrieve file contents: (Recommended: Filesystem)	<input type="button" value="Filesystem"/>

Quando você terminar, salve sua configuração

7.5.3 Passo 3: Configure as contas dos seus usuários

Aqui você cria a conta de administrador do seu eGroupWare. Não use um nome de usuário administrador como admin, administrador, administrator, root, etc. Para senha use letras, números e caracteres especiais. Não crie contas Demo em ambientes de produção!

7.5.4 Passo 4: Gerenciamento de Idiomas

O idioma padrão que será instalado é o Inglês e o idioma que estiver ativado como padrão em seu navegador. É possível instalar mais idiomas.

✍️ Você pode converter seus caracteres de sistema automaticamente, ex: de iso-8859-1 para UTF-8.

7.5.5 Passo 5: Gerenciamento da Aplicação

Na instalação padrão, todas as aplicações são instaladas. Para desinstalar alguma, selecione-as na caixa de checagem e clique em "Save". Se você receber alguma mensagem de erro referente a dependências, você deve instalar outra aplicação. Por exemplo, felemimail exige emailadmin para funcionar.

Application Data				Actions			
Application Name and Status Information	Application Title	Current Version	Available Version	Install	Upgrade	Resolve	Remove
✓ addressbook-OK - C	Addressbook	0.9.13.002	0.9.13.002	✓	✓		✓
✓ admin-OK - C	admin*	0.9.13.002	0.9.13.002				✓
✓ backup-OK - C	Backup	0.0.1.001	0.0.1.001				✓
✓ bookmarks-OK - C	Bookmarks	0.9.2	0.9.2				✓
✓ calendar-OK - C	calendar*	0.9.16.002	0.9.16.002				✓

8 Inicie uma sessão no eGroupWare (login)

Uma vez que você tenha terminado sua instalação do eGroupWare, você pode iniciar uma nova sessão(login). Digite no seu browser a URL <http://seudominio.com.br/egroupware> .

O primeiro passo como administrador deveria ser, ir para a interface admin e configurar suas preferências, usuários e grupos, e-mail e outras informações necessárias.

9 Solução de problemas (troubleshooting)

9.1 Esqueceu a senha do administrador

Eu esqueci minha senha de administrador e não posso iniciar uma nova sessão(login) com o usuário administrador do eGroupWare



Vá para <http://yourserver.com/egroupware/setup>
Entre em Setup/Config Admin Login
Configure uma nova conta de administrador .

9.2 Administrador ou outro usuário está bloqueado

Não consigo iniciar uma nova sessão de instalação do eGrouWare. Eu recebo: "Blocked, to many attemps." (Bloqueado, muitas tentativas). O que posso fazer?



Na configuração padrão, espere 30 minutos para iniciar de novo a sessão. Esta é uma medida de segurança. Não desative isto!

9.3 Erro de banco de dados: lock(Array, write) failed

Erro de banco de dados: lock(Array, write) failed

MySQL Error 1044 (Access denied for user '@localhost' to database 'groupware')

Function: db::halt / db::lock / config::save_repository / sessions::sessions_ / session_sessions / createobject / include / include
session halted



Verifique as permissões do seu banco de dados. O seu usuário não possui todas as permissões necessárias.

9.4 Verificando as permissões de arquivo

Este erro abaixo está ocorrendo?

Checking file-permissions of ./phpgwapi/images for not worldwritable: hri/users drwx---rwx
./phpgwapi/images is world writable !!!



Mude as permissões do diretório.
chmod 700 images

9.5 Não conseguiu passar da página de verificação da instalação (Check install page)

Não há avisos de erros... Eu já instalei o arquivo "headers.inc.php" com todos os valores corretos , mas continuo retornando para a página "check_install.php..."



Verifique se o servidor web tem permissão para ler o arquivo "header.inc.php" e se o arquivo está no diretório raiz do servidor.

9.6 Não conseguiu passar da página de verificação da instalação (Check install page)

Nós instalamos o eGroupWare em Linux que possuía um servidor proxy instalado

Clientes que estão usando o Microsoft Internet Explorer que têm referência para o servidor proxy, ela, entretanto deve ser ignorada (options->conection->proxy->advanced settings).

Não conseguimos baixar anexos maiores do que 1 MB. No php.ini e http.conf tudo foi aplicado, mas nós ainda não somos capazes de baixar arquivos maiores que 1 MB



Servidores proxy freqüentemente são configurados para bloquear um fluxo maior do que um certo tamanho padrão. Por exemplo, no Squid você precisaria mudar o valor de "request_body_max_size", que tem 1 MB como padrão.

ex: request_body_max_size 20 MB

9.7 (WINDOWS) fudforum/3814*****9): Permissão Negada

Warning:mkdir(D:\Websites\yourwebsite\egroupware\fudforum/3814*****9): Permission denied in D:\Websites\egroupware\fudforum\setup\default_records.inc.php on line 114

ERROR: Failed to create D:\Websites\yourwebsite\egroupware\fudforum/38145*****, please create this directory manually and chmod it 777SiteMgr demo site installed.



Crie o diretório 3814***** dentro do diretório D:\Websites\yourwebsite\egroupware\fudforum e dê permissões de leitura e escrita. Por favor, anote: "3814*****" número será o CRC32 do seu domínio, então isto será diferente em cada máquina.

**Isto é um trecho retirado do arquivo d:\sites\yourwebsite\fudforum\setup\readme - "O arquivo \fudforum\setup\index.php precisará criar vários arquivos dentro do diretório fudforum\. Isto requer que você dê permissão de escrita para o servidor-web para vários arquivos e diretórios (o instalador irá reclamar, caso eles não tenham permissão de escrita). A solução mais simples é dar temporariamente permissão de acesso total e então restaurar aos níveis de permissão anterior (ler e escrever), uma vez que o processo de instalação esteja completo. Se você desejar liberar uns poucos megabytes de espaço, uma vez que o fórum está instalado, você pode remover o diretório base, ele não é mais necessário."

9.8 Sitemgr:mkdir(/sitemgr-link): Permissão negada (Permission denied)

Warning: mkdir(/sitemgr-link): Permission denied in

D:\Websites\calvarycentral\egrouptest\egroupware\sitemgr\setup\default_records.inc.php on line 165

Can't mkdir(/sitemgr-link) !!! sitemgr/sitemgr-link copied to eGroupWare dir and sitemgr-link NOT installed, you need to copy it from egroupware/sitemgr/sitemgr-link to egroupware/sitemgr-link and install.



Copie a pasta sitemgr-link do \egroupware\sitemgr\ que foi criada pelo eGroupWare e coloque-o na pasta raiz do D:\Websites\yourwebsite\egroupware. Isto habilita você a instalá-lo do link "Manage Applications" na página /egroupware/setup/index.php.

10 Software Map

AIDE, Advanced Intrusion Detection System

Plataforma Linux / BSD / *nix

Licença **GPL**

Página <http://sourceforge.net/projects/aide/>

Download

RPM Verifique um de acordo com sua distribuição

DEB [Debian Project](#)

tar.gz [AIDE Project file server](#)

Apache Webserver project

Plataforma Linux / BSD / Win / other

Licença Apache Software License

Página <httpd.apache.org>

Download

RPM Verifique um de acordo com sua distribuição

DEB [Debian Project](#)

tar.gz [Apache Project file server](#)

Win [Apache Project file server](#)

chkrootkit project

Plataforma Linux / BSD

Licença **BSD-Like**

Página www.chkrootkit.org

Download

RPM [creativix chkrootkit page](#)

tar.gz [chkrootkit project](#)

eGroupWare project

Plataforma Linux / BSD / WIN / other

Licença **GPL**

Página www.egroupware.org

Download

RPM [sourceforge.net eGroupWare project](#)

tar.gz [sourceforge.net eGroupWare project](#)

tar.bz2 [sourceforge.net eGroupWare project](#)

zip [sourceforge.net eGroupWare project](#)

logwatch project

Plataforma	Linux / BSD/ other
Licença	GPL
Página	www.logwatch.org
Download	
RPM	logwatch project
tar.gz	logwatch project

logcheck project

Plataforma	Linux / BSD/ other
Licença	GPL
Página	sourceforge project page
Download	
tar.gz	logcheck project

ModSecurity

Plataforma	Linux / BSD / WIN / other
Licença	GPL
Página	http://www.modsecurity.org/
Download	
tar.gz	ModSecurity project
zip	ModSecurity project

NMAP

Plataforma	Linux / BSD / WIN / other
Licença	GPL
Página	http://www.nmap.org/
Download	
RPM	NMAP project
tar.gz	NMAP project
tar.bz2	NMAP project
zip	NMAP project

openssh project

Plataforma	Linux / BSD
Licença	GPL
Página	www.openssh.org
Download	
RPM	OpenBSD project filesaver
tar.gz	OpenBSD project filesaver

php project

Plataforma Linux / BSD / WIN / other

Licença The PHP License

Página www.php.net

Download

RPM Verifique um de acordo com sua distribuição

tar.gz [php project](#)

tar.bz2 [php project](#)

zip [php project](#)

Roxen webserver project

Plataforma Linux / BSD / WIN / other

Licença **GPL**

Página <http://www.roxen.com/products/webserver/>

Download

The Linux package will be installed with a shell script

Turck MMCache

Plataforma Linux / BSD / Win / other

Licença **GPL**

Página sourceforge.net/projects/turck-mmcache

Download

tar.gz [turck-mmcache project](#)

tar.bz2 [turck-mmcache project](#)

zip [turck-mmcache project](#)

11 Próximos passos e Registro de alterações

11.1 Próximos passos para este documento

Para a documentação versão 1.0

- Pré-planejamento de uma instalação do eGroupWare
- Treinando os usuários
- Instalar um servidor LDAP e configurar OpenLDAP / E-mail / SMTP sob *nix
- Instalar um firewall simples no Linux para o eGroupWare

Para depois do lançamento acima

- Mod_log_forensic para Apache
- Ocultar a versão de ssh
- Suporte ao Fedora (YUM, RPM-apt)
- Acrescentar psad para a segurança do HOWTO
- Instalação e configuração do sXad
- Criação de um backup e check-list/howto de recuperação de dados perdidos
- Rsnapshot
- Bastille Linux / LSAD

11.2 Registro de alterações deste documento

*** Domingo – 22 de fevereiro de 2004 - Reiner Jung <r.jung AT creativix DOT net> 0.4**

- Licença alterada para a "creative commons"
- Construído pacotes RPM para o SuSE?
- Segurança e Otimização do Apache
- Possíveis encriptações SQL para senhas de usuários
- A instalação fornece o prefixo do cliente para instalações de LDAP
- Seleção nome de usuários "case sensitive" na instalação
- Correção de erros adicionada
- Torne mais seguro seu eGroupWare com ModSecurity?
- Atualize o arquivo header.inc.php
- Segurança da configuração do PHP atualizada
 - Restrição do open basedir
 - Desativa os logs de erros
- Configuração avançada da detecção de intrusão do sistema
- Alteração do "Quick Install HowTo" para "Express Install Howto" e ampliação.
- Instalar o analisador dos arquivos de log (logcheck)
- Turck-mmcache estendido
 - Manual de como instalar o mmcache no RedHat? Linux
 - Requerimentos para instalar mmcache

*** Domingo - 22 de novembro de 2003 - Reinerer Jung <r.jung AT creativix DOT net> 0.3**

- Atualização do eGroupWare
 - Atualização com pacotes
 - Atualização do CVS
- Instalação do RPM em um outro "path" como /var/www/html
- Mapeamento dos Software
 - Adicionado o software e licença de todas as partes do documento 003
- Alguns tipos de erros consertados
 - Chave do tipo GPG consertada
- Verificação e adição da chave GPG
- Criação de um certificado https
- Garantia a segurança de sua instalação PHP

*** Sexta-feira – 16 de setembro de 2003 - Reiner Jung <r.jung AT creativix DOT net> 0.2**

- Alguns tipos de erros consertados
 - Consertado erro na instalação da documentação de CVS
 - Consertado tipo In nmcache
- Manual do chkrootkit adicionado
 - Amostra do checkrootkit
 - Instalação do check rootkit rpm
 - Instalação do check rootkit tar.gz
- Verifique se seu servidor possui serviços desnecessários / portas abertas
 - Portas necessárias para que o eGW funcione
 - O portscanner
 - Saída para o portscanner
 - Desativar serviços/servidores desnecessários
- Desinstale extensões de softwares desnecessários
- Administração segura (ssh/sshd)
 - Conecte seu servidor com uma sessão segura
 - Trabalhar com pares de chaves ssh
 - Crie um par de chaves de segurança do shell
 - Copie para sua chave pública para o servidor
 - A ferramenta ssh-add
 - Garantindo a segurança do seu cliente ssh
 - Garantindo a segurança do seu sshd

*** Sexta-feira – 12 de setembro de 2003 - Reiner Jung <r.jung AT creativix DOT net> 0.2**

- Início da criação deste documento

12 Voluntários no desenvolvimento deste documento

As pessoas a seguir têm contribuído para o documento Instalação e Configuração - "Install and security howto"

Traduções

Português Brasil:	Roger de Souza Moraes, Leandro Arruda Costa Oliveira Gonçalves, Renato Cintra.
Francês:	Patrice Lallement
Alemão:	Wolfgang Baumgartner, Andreas Wengrzik
Espanhol:	Oscár Manuel Gómez Senovilla
Chinês Tradicional:	Finjon Kiang

Revisão

Inglês:	Jeff Mitchell (v. 0.4)
	Geltmar von Buxhoeveden (v. 0.3)
Português Brasil:	Tales Costa (v.0.4)

Co-Autores

Versão para Windows:	Pastor John W. Brown
----------------------	----------------------

13 Licenças de uso

Attribution-ShareAlike 1.0

You are free:

- Copiar, distribuir, expor e executar este trabalho.
- Produzir trabalhos derivados deste
- Fazer uso comercial deste trabalho

Sob as seguintes condições:



Atribuição. Você deve mencionar os créditos ao autor original.



Compartilhamento. Se você alterar, transformar ou construir sobre este trabalho, você deve distribuir o resultado somente sob licenças idênticas às deste.

- Para qualquer reutilização ou distribuição, você deve deixar claro aos outros os termos da licença deste trabalho.
- Algumas destas condições podem ser negligenciadas se você conseguir uma autorização do autor.

Seu bom uso e outros direitos não são afetados pelos termos acima.

Este é um legítimo sumário do [Legal Code \(the full license\)](#).