安全狗·云安全系统

CentOS 6.5 64 位镜像使用说明手册

2017 年 12 月

厦门服云信息科技有限公司
www.safedog.cn

目录

1. 镜像环境及使用说明.....3
1.1. 镜像环境说明.....3
1.2. 镜像安装说明.....3
2. 服务器安全狗 Linux 版介绍.....3
3. 网站安全狗 Nginx 版介绍.....4
4. 安全狗·服云.....4
5. MySQL 数据库密码.....5
5.1. 初始密码存储位置：.....5
5.2. 修改 Mysql 密码.....5
6. 软件目录及配置目录.....6
7. 云主机系统安全体检.....6
8. 软件操作命令汇总.....7
9. 环境配置文件加固.....8
9.1. PHP 环境配置文件加固.....8
10. 加入安全狗“服云”.....9
11. 注意事项.....10
12. 附录.....10

1. 镜像环境及使用说明

1.1. 镜像环境说明

操作系统：Centos 6.5 64 位
防护软件：Linux 服务器安全狗 nginx 网站安全狗
PHP 运行环境：（nginx 1.12.1 - PHP 7.1.12 - mysql 5.5.53）

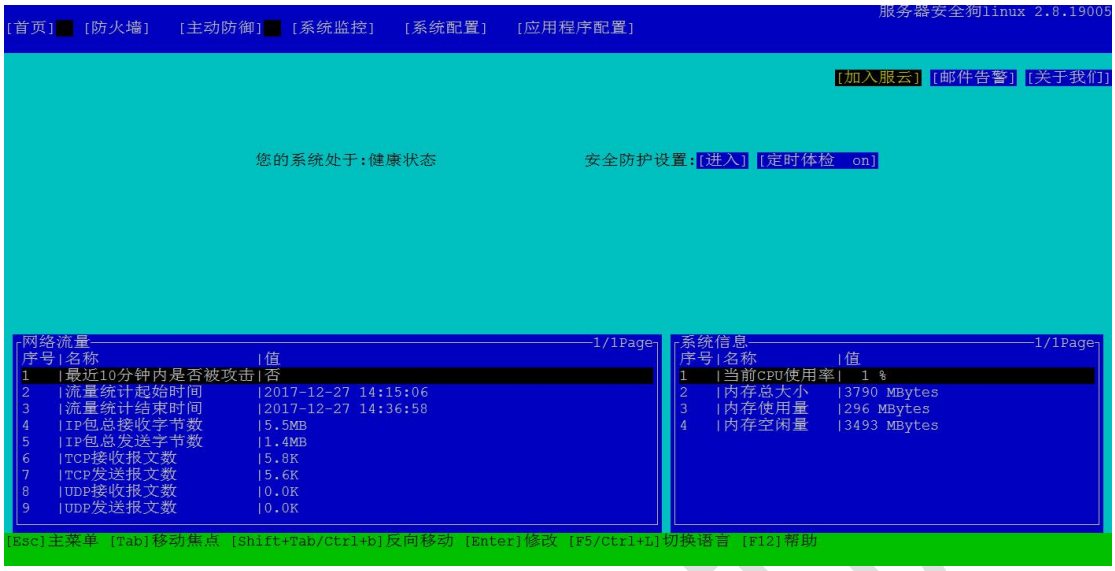
1.2. 镜像安装说明

镜像环境基于安全狗团队多年的安全经验和安全狗软件的防护功能，对 Linux 服务器操作系统进行全面的加固和调优，与华为云主机实现无缝接入；同时集成 MySQL、PHP、Nginx 环境，助您快速搭建数据库及网站环境。

- 融合安全狗专业安全工程师多年运维及 Linux 系统环境搭建经验。
- 默认安装服务器安全狗 Linux 版，并通过安全狗软件进行加固。
- 对 Linux 系统权限、目录权限、应用程序权限、密码强度、网站目录权限、网站应用程序权限、数据库权限进行安全加固。
- 对 Linux 操作系统网络、系统配置等进行全面优化。
- 对 PHP 环境配置、Nginx 环境配置进行加固，禁用相关风险配置。
- 集成开源的 Nginx、PHP、MYSQL，轻松部署数据库及建立网站。

2. 服务器安全狗 Linux 版介绍

服务器安全狗 Linux 版（SafeDog for Linux Server）是为 Linux 服务器开发的一款服务器管理软件，它集成了 DDOS 攻击检测和防御系统、远程登录监控、SSH 防暴力破解、流量统计、帐户监控和设置、系统参数快速设置、系统运行状态展示、系统状态实时监控等功能。其 DDOS 攻击检测和防御系统能够有效防御 CC 攻击，并极大地减少误判。本软件提供纯字符界面下的界面交互接口和详细的操作指引，使得管理员对服务器的状态更加了解，管理和配置服务器也更加简单。



服务器安全狗 Linux 版软件主界面

3. 网站安全狗 Nginx 版介绍

网站安全狗系统（Nginx 版）（以下简称网站安全狗)是为 IDC 运营商、虚拟主机服务商、企业主机、服务器管理者等用户提供服务器安全防范的实用系统，是集网站内容安全防护、网站资源保护及网站流量保护功能为一体的服务器工具。

具有网马/木马查杀、黑链/畸形文件清理、防 SQL 注入、防盗链、防 CC 攻击、网站加速、网站流量监/CPU 监控、下载保护、危险组件防护、禁止执行程序、响应内容保护、IP 黑白名单、网页防篡改（结合安全狗服云使用）等功能模块。为用户提供实时的网站安全防护，同时强大的云端网马引擎与本地智能引擎结合，为用户带来最安全、高效的网马查杀体验，极大降低因黑客攻击带来的损害。目前，网站安全狗已经为百万网站提供了安全保护。

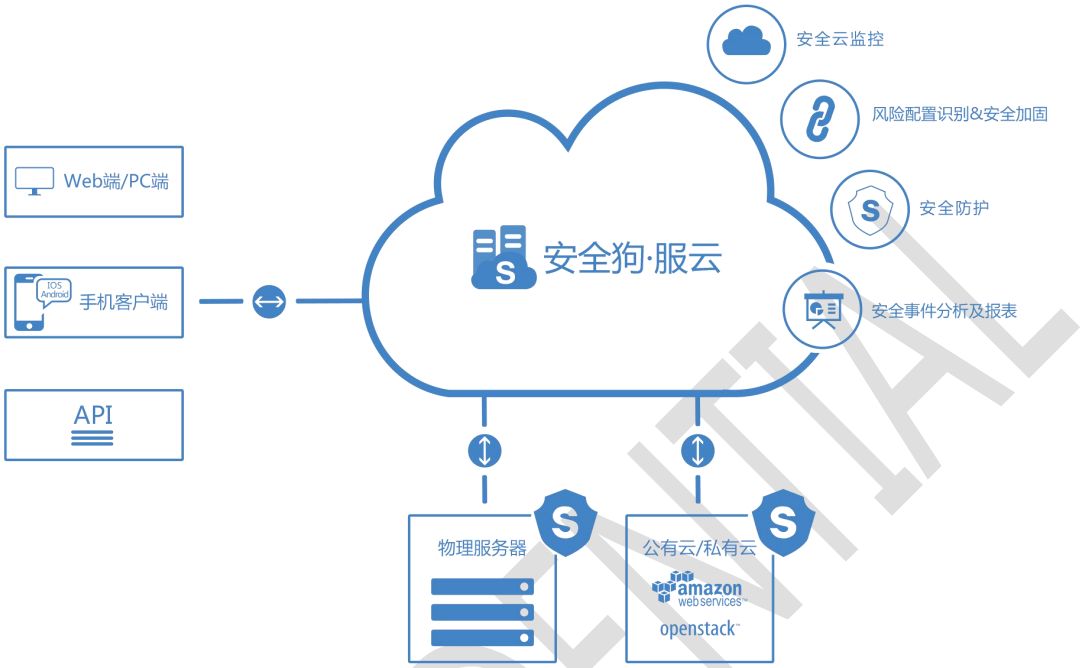
4. 安全狗•服云

云+端的 SAAS 服务模式，自适应各种 IT 架构

安全狗•服云首创云+端的云安全管理平台（SAAS 模式）为用户解决公有云、私有云和混合云环境中可能遇到的安全及管理问题；提供了包含自动化系统风险识别和加固、系统级的安全防护（防黑/防入侵/抗攻击）、云监控（安全监控/性能监控/日志监控）、云管理（多公有管理/混合云管理）以及基于大数据架构的安全事件分析等功能。

安全狗•服云的云安全 SAAS 架构可以很好的适应公有云（包括阿里云、腾讯云、AWS、

微软 AZURE 等）和私有云（包括 VMVARE、OpenStack 等）架构，也可以适应传统的 IT 架构；并且具有快速部署、快速使用方面的优势。



5. MySQL 数据库密码

MySQL 数据库采用安全脚本随机生成密码，安全性更高，用户如有需要，可以随时修改。

5.1. 初始密码存储位置：

帐号:root 密码在/root/mysql_account.log 文件中。
查看密码使用命令：

```
cat mysql_account.txt
```

5.2. 修改 Mysql 密码

用 root 用户登录系统，执行下面命令：

```
mysqladmin -uroot -p oldpassword password newpassword
```

mysqladmin -uroot -p 您的旧密码 password 您的新密码。

6. 软件目录及配置目录

所有软件都采用源代码编译安装，安装目录如下：

Web 主目录：/data/wwwroot

MySQL 主目录：/usr/local/mysql

MySQL 数据目录：/usr/local/mysql/data

MySQL 配置文件：/etc/my.cnf

PHP 主目录：/usr/local/php

PHP 配置文件：/etc/local/php/etc/php.ini

服务器安全狗 Linux 版本：/etc/safedog

网站安全狗 Nginx 版本：/etc/safedog/nginx

PHP 日志：/usr/local/php/log/php-fpm.log

Mysql 日志：/usr/local/mysql/data/error.log

Nginx 日志：/usr/local/nginx/logs

Php 日志：/usr/local/php/log/php-fpm.log

7. 云主机系统安全体检

系统安全体检通过对云服务器进行全方位安全体检，检测各种可能出现的服务器安全漏洞，并提供相应的修复功能，有效的帮助用户提高服务器安全性与稳定性。如下图所示。

服务器优化-服务器体检进度

服务器优化-服务器体检结束

8. 软件操作命令汇总

启动 nginx 命令：
/etc/init.d/nginx start
停止 nginx 命令：
/etc/init.d/nginx stop
重启 nginx 命令：
/etc/init.d/nginx restart

启动 php-cgi 处理进程命令：
/etc/init.d/php-fpm start
停止 php-cgi 处理进程命令：
/etc/init.d/php-fpm stop
重启 php-cgi 处理进程命令：
/etc/init.d/php-fpm restart

启动 mysql 命令：
/etc/init.d/mysql start
停止 mysql 命令：
/etc/init.d/mysql stop
重启 mysql 命令：
/etc/init.d/mysql restart

启动 LINUX 服务器安全狗命令：sdui

即可进入软件操作界面，首次进入 sdui 界面的首页，连续按 F5 或 CTRL+L 组合键，切换到合适的显示文字，按 ESC 键可以切换顶部菜单项，按两下 ESC 键会弹出是否退出 sdui 界面，选择是即退出 LINUX 服务器安全狗。

LINUX 服务器安全狗使用：

查看安全狗服务：service safedog status

启动安全狗服务：service safedog start

停止安全狗服务：service safedog stop

重启安全狗服务：sdstart

重启安全狗云中心命令：runsdcc

在软件的每个界面直接按 F12，可以显示详细的帮助信息。

9. 环境配置文件加固

9.1. PHP 环境配置文件加固

对 Php 配置文件（/usr/local/php/etc/php.ini）做安全加固，屏蔽风险函数

disable_functions =exec,passthru,popen,proc_open,shell_exec,system,phpinfo,assert

文件类型解析漏洞：

配置 php.ini 中 cgi.fix_pathinfo=0

#关闭错误信息提示

display_errors = off

display_startup_errors = off

关闭全局变量

register_globals = off

不允许调用 dl

enable_dl = off

关闭远程文件

allow_url_fopen = off

allow_url_include = off

http only 开启

session.cookie_httponly = 1

https secure 开启

session.cookie_secure = 1

适当的 PHP redirects

cgi.force_redirect = 0

SQL 的安全模式

sql.safe_mode = on

10. 加入安全狗“服云”

1）打开安全狗·服云官网 http://fuyun.safedog.cn，注册并创建安全狗服云账号。

2）登录云主机，打开安全狗软件，软件右上角的【加入服云】，如图所示：

加入服云（软件界面方式）

通过输入服云帐号用户名和密码，自动下载服务器证书，加入服云。

支持两种方式加入服云：

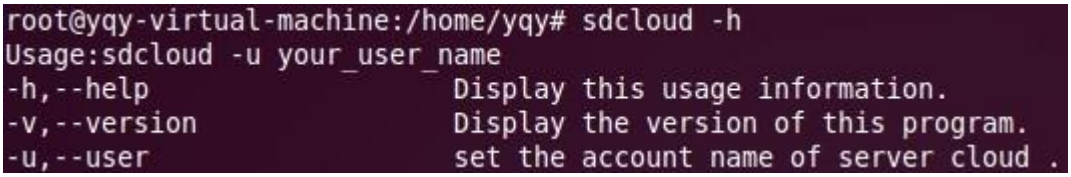
（1）软件界面方式：如上图，在弹出框内输入服云帐户名和密码；

（2）命令行方式：输入命令 **sdcloud -u 用户名**

加入服云（命令行方式）

软件界面不支持中文用户名和中文密码，此类情况通过以上命令加入。

软件可以通过下面的命令查看加入服云的命令使用方法：**sdcloud -h**



查询加入服云的命令方式

3）成功加入服云后，利用同一个服云帐号登录云端（fuyun.safedog.cn），即可方便

享受云端服务器便捷安全管理。

11.注意事项

镜像环境注意事项：

（1）服务器端口开启建议

服务器开启的对外端口越多，风险性就越高，镜像环境只开启 WEB 的 80 端口和远程端口，远程端口做限制 IP 设置，服务器上其他应用可以使用 nginx 转发请求来处理，数据库 3306 端口可以限制下 IP，不要直接对外，可以使用 Linux 服务器狗来屏蔽 IP 或者 iptables 命令。

（2）关于 MYSQL binlog 默认是开启状态

MYSQL binlog 默认是开启状态，要关闭，需修改/etc/my.cnf 配置文件，在这个配置文件中，最后面去掉以下内容：

log-bin=mysql-bin

expire_logs_days = 7

12.附录

教程一：部署网站

1、在使用镜像安装系统后，在/usr/local/nginx/conf/vhost 目录下，我们可以看到一个默认的配置文件 test.conf。

关于如何配置网站，我们可以参考该文件中的内容（#号后面为注释说明）：

```
server
        {
                listen 80 default; #虚拟主机，指定 80 端口
                #listen [::]:80 default ipv6only=on;
                server_name www.test.com; #定义使用域名访问
                index index.html index.htm index.php;
                root   /data/wwwroot/; #定义服务器的默认网站根目录位置
```

```
#error_page     404     /404.html;
location ~ [^/]\.php(/|$)
        {
                # comment try_files $uri =404; to enable pathinfo
                try_files $uri =404;
                fastcgi_pass    unix:/tmp/php-cgi.sock;
                fastcgi_index index.php;
                include fastcgi.conf;
                #include pathinfo.conf;
        }

location /nginx_status {
        stub_status on;
        access_log      off;
}

location ~ .*\.(gif|jpg|jpeg|png|bmp|swf)$
        {
                expires         30d;
        }

location ~ .*\.(js|css)?$
        {
                expires         12h;
        }
```

```
        access_log  /usr/local/nginx/logs/access.log  access;#访问日志
        error_log /usr/local/nginx/logs/error_www.test.com.log; #错误日志
    }
```

2、根据以上默认配置，我们进入网站根目录/data/wwwroot/可以看到 index.html 这个文件。我们直接在浏览器中输入“http://*.*.*.* ”（*.*.*.*为我们服务器的公网 ip），就默认可以访问到 index.html 中的内容。

在/data/wwwroot/目录下，编辑一个探针 phpinfo.php 文件：

```
<?php
echo "OK";
?>
```

我们也可以输入“http://*.*.*.*/index.php”显示访问 index.php 运行后的结果。当然你输入一个不存在的文件访问，就会出现 404 Not Found 的错误。

3、假如我们有个 demo.test.com 的域名的网站需要部署在云主机上。以下我们以部署 phpmyadmin 为例，来详细介绍一下网站的部署：

3.1、首先，我们需要备案此域名。如果没备案域名，此域名会被运营商拉入黑名单不能使用的哦。针对备案问题，您可以以工单的形式反馈，在这里不再过多阐述。

如果您的域名已成功备案，您需要把此域名解析的 ip 地址设置为云主机的公网 ip。demo.test.com 是测试的二级域名，由于此域名是在域名商购买注册的，所以我们登陆到域名的管理后台，在域名管理中，我们增加一个 demo.test.com 的二级域名，记录值即我们域名解析的 ip，这里填写我们云主机的公网 ip。

3.2、然后，我们下载 phpmyadmin 的源码部署我们的站点。具体安装部署命令如下：

以下为部署 phpmyadmin：

wget

http://sourceforge.net/projects/phpmyadmin/files/phpMyAdmin/3.5.8.1/phpMyAdmin-3.5.8.1-all-languages.zip/download

mv download phpMyAdmin-3.5.8.1-all-languages.zip

rm -rf phpMyAdmin-3.5.8.1-all-languages

unzip pphpMyAdmin-3.5.8.1-all-languages.zip

mv phpMyAdmin-3.5.8.1-all-languages /data/wwwroot/phpmyadmin

chown -R www:www /data/wwwroot/phpmyadmin/

3.3、最后，我们需要配置 nginx，并让 nginx 重新启动，即可完成我们网站的配置。

我们可以在默认的配置文件 testconf 中加入以下内容，也可以在/usr/local/nginx/conf/vhost 目录下新建一个 phpmyadmin.conf 文件（文件名必须以.conf 结尾，phpmyadmin 为自取名称，可以为其它名称），并且加入以下内容：

```
server
{
listen 80;
server_name demo.test.com;
index index.php index.html index.htm;
root /data/wwwroot/;
charset gbk;
access_log /usr/local/nginx/logs/access/access_demo.test.com.log combined;
error_log /usr/local/nginx/logs/error_demo.test.com.log;
location ~ .*\.php?$
{
fastcgi_pass 127.0.0.1:9000;
#fastcgi_pass unix:/tmp/php-fcgi.sock;
```

```
#fastcgi_pass php;

fastcgi_index index.php;

fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;

include fastcgi_params;

}

}
```

3.4、最终我们用命令/etc/init.d/nginx restart 完成我们网站的配置。

然后我们也可以用 http://demo.test.com/phpmyadmin 来访问我们部署的 phpmyadmin，用户名和密码输入/data/mysql.txt 中存储我们的 mysql 的用户名及密码：

输入正确的 mysql 用户名及密码后，然后我们就可以访问我们云主机上部署的 mysql 了：

教程二：将网站迁移至数据盘

用镜像生成系统后，网站的数据目录都默认在系统盘的/data/wwwroot/目录下。如果您的应用数据量较大，系统盘默认的 20G 大小可能不够用。这需要我们将网站迁移至数据盘中。

1、首先分区并格式化我们的数据盘。如果已经格式化数据盘，此步可以不用做。

2、以《附录教程一：部署网站》为例，然后我们执行以下命令迁移 phpwind 至数据盘中：

/etc/init.d/nginx stop #首先停止 nginx 服务

cd / #进入根目录下

mount /dev/xvdb1 /mnt/ #将第一块数据盘挂载至 mnt 目录下，也可以根据您自己的需要，挂载至其他数据盘中。这里也可以尝试：mount /dev/xvdb1 /data/wwwroot/ 直接把/data/wwwroot/目录挂载在数据盘中，似乎更加方便。

mkdir -p /mnt/www /mnt/log

cp -a /data/wwwroot//phpmyadmin /mnt/www/ #将数据迁移至数据盘中

3、vi /usr/local/nginx/conf/vhost/phpmyadmin.conf 将：

root /data/wwwroot/;

更改为：

root /data/wwwroot//phpmyadmin

4、启动 nginx 完成迁移：

/etc/init.d/nginx start

教程三：将 mysql 迁移至数据盘中

镜像部署的 mysql 的安装目录及数据目录都存放在系统盘中，同样考虑到系统盘空间不够用的情况，后面如果我们部署的 mysql 数据量很大，这里就需要我们将我们的 mysql 迁移至数据盘中。mysql 迁移至数据盘中，一般指将 mysql 的数据目录迁移至数据盘中。具体操作步骤可以参考如下：

1、首先格式化磁盘，并将数据盘挂载在 mnt 目录下（根据您自己的需求，也可以挂载在其他目录下）

mkdir -p /mnt/data

2、用 mysqldump 命令导出您项目所有的数据，命令参考如下：

mysqldump -p --all-databases > all.sql

3、停止 mysql :

/etc/init.d/mysql stop

4、vi /usr/local/mysql/etc/my.cnf 将文件中“datadir=/usr/local/mysql/var”中的目录地址更改为您迁移至数据盘中的目录地址，即“datadir=/mnt/data”。

5、然后用以下命令初始化一个全新的数据库环境：

/usr/local/mysql/scripts/mysql_install_db --basedir=/usr/local/mysql --datadir=/mnt/data --user=mysql

值得注意的是 datadir 为您 mysql 的数据目录。

6、启动 mysql，然后将数据还原至新的数据盘中：

/etc/init.d/mysql start

mysql < all.sql

/etc/init.d/mysql restart

教程四：如何配置 mysql 远程连接

很多用户反馈，用镜像生成系统后，云主机本地能够连接 mysql，为何远程连接不上 mysql 呢？这是因为默认安装的 mysql，出于安全考虑，只能本地连接。如果您需要远程连接，这里就需要设置一下 mysql 的权限表。具体设置的步骤如下：

1、在您的云主机上连接进入 mysql。

2、执行以下 mysql 命令：

use mysql #打开 mysql 数据库

#将 host 设置为%表示任何 ip 都能连接 mysql，当然您也可以将 host 指定为某个 ip

update user set host='%' where user='root' and host='localhost';

flush privileges; #刷新权限表，使配置生效

然后我们就能远程连接我们的 mysql 了。

3、如果您想关闭远程连接，恢复 mysql 的默认设置（只能本地连接），您可以通过以下步骤操作：

use mysql #打开 mysql 数据库

#将 host 设置为 localhost 表示只能本地连接 mysql

update user set host='localhost' where user='root';

flush privileges; #刷新权限表，使配置生效

备注：您也可以添加一个用户名为 safedog，密码为 123456，权限为%（表示任意 ip 都能连接）的远程连接用户。命令参考如下：

grant all on *.* to 'safedog'@'%' identified by '123456';

flush privileges;

教程五：PHP 限制执行路径

出于安全考虑，镜像中安装的 PHP 默认限制执行路径，只允许/data/wwwroot/下的 PHP 文件。

具体配置/usr/local/php/etc/php.ini 如下：

open_basedir = /tmp:/data/wwwroot/

那如何增加路径呢，我们只需将上述配置文件增加相应路径，比如：要增加/home/web001，把“open_basedir = /tmp:/data/wwwroot/”改为

“open_basedir = /tmp:/data/wwwroot/:/home/web001”

然后重启 PHP 进程，命令：/etc/init.d/php-fpm restart，即可。

关于如何配置 php 和 nginx，这里不做过多介绍，这块网络上有很多教程，大家自行参考。