RHCSA 系列（九）：安装、配置及加固一个 Web 和 FTP 服务器

2015-9-24 14:11 收藏: 8

原文：http://www.tecmint.com/rhcsa-series-install-and-secure-apache-web-server-and-ftp-in-rhel/ 作者： Gabriel Cánepa
译文：LCTT https://linux.cn/article-6286-1.html 译者： FSSlc

Web 服务器（也被称为 HTTP 服务器）是在网络中将内容（最为常见的是网页，但也支持其他类型的文件）进行处理并传递给客户端的服务。

FTP 服务器是最为古老且最常使用的资源之一（即便到今天也是这样），在身份认证不是必须的情况下，它可通过客户端在一个网络访问文件，因为 FTP 使用没有加密的用户名和密码，所以有些情况下不需要验证也行。

在 RHEL 7 中可用的 web 服务器是版本号为 2.4 的 Apache HTTP 服务器。至于 FTP 服务器，我们将使用 Very Secure Ftp Daemon (又名 vsftpd) 来建立用 TLS 加固的连接。

RHCSA: 安装，配置及加固 Apache 和 FTP 服务器 – Part 9

在这篇文章中，我们将解释如何在 RHEL 7 中安装、配置和加固 web 和 FTP 服务器。

安装 Apache 和 FTP 服务器

在本指导中，我们将使用一个静态 IP 地址为 192.168.0.18/24 的 RHEL 7 服务器。为了安装 Apache 和 VSFTPD，运行下面的命令：

```
# yum update && yum install httpd vsftpd
```

当安装完成后，这两个服务在开始时是默认被禁用的，所以我们需要暂时手动开启它们并让它们在下一次启动时自动地开启它们：

```
# systemctl start httpd
# systemctl enable httpd
# systemctl start vsftpd
# systemctl enable vsftpd
```

另外，我们必须打开 80 和 21 端口，它们分别是 web 和 ftp 守护进程监听的端口，为的是允许从外面访问这些服务：

```
# firewall-cmd --zone=public --add-port=80/tcp --permanent
# firewall-cmd --zone=public --add-service=ftp --permanent
# firewall-cmd --reload
```

为了确认 web 服务工作正常，打开你的浏览器并输入服务器的 IP，则你应该可以看到如下的测试页面：

对于 ftp 服务器，在确保它如期望中的那样工作之前，我们必须进一步地配置它，我们将在几分钟后来做这件事。

配置并加固 Apache Web 服务器

Apache 的主要配置文件位于 `/etc/httpd/conf/httpd.conf` 中，但它可能依赖 `/etc/httpd/conf.d` 中的其他文件。

尽管默认的配置对于大多数的情形都够用了，但熟悉在 官方文档 <http://httpd.apache.org/docs/2.4/> 中介绍的所有可用选项是一个不错的主意。

同往常一样，在编辑主配置文件前先做一个备份：

```
# cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.$(date +%Y%m%d)
```

然后用你钟爱的文本编辑器打开它，并查找下面这些变量：

- `ServerRoot` ： 服务器的配置，错误和日志文件保存的目录。
- `Listen` ： 通知 Apache 去监听特定的 IP 地址或端口。
- `Include`：允许包含其他配置文件，要包含的文件必须存在，否则，服务器将会失败。它恰好与 IncludeOptional 相反，假如特定的配置文件不存在，它将静默地忽略掉它们。
- `User` 和 `Group` ： 运行 httpd 服务的用户/组的名称。
- `DocumentRoot` ： Apache 为你的文档所服务的目录。默认情况下，所有的请求将在这个目录中被获取，但符号链接和别名可能会被用于指向其他位置。
- `ServerName` ： 这个指令将设定用于识别它自身的主机名（或 IP 地址）和端口。

安全措施的第一步将包含创建一个特定的用户和组（如 tecmint/tecmint）来运行 web 服务器，以及更改默认的端口为一个更高的端口（在这个例子中为 9000）（LCTT 译注：如果你的 Web 服务器对外公开提供服务，则不建议修改为非默认端口。）：

```
ServerRoot "/etc/httpd"
Listen 192.168.0.18:9000
User tecmint
Group tecmint
DocumentRoot "/var/www/html"
ServerName 192.168.0.18:9000
```

你可以使用下面的命令来测试配置文件：

```
# apachectl configtest
```

假如一切 OK，接着重启 web 服务器。

```
# systemctl restart httpd
```

并别忘了在防火墙中开启新的端口（并禁用旧的端口）：

```
# firewall-cmd --zone=public --remove-port=80/tcp --permanent
# firewall-cmd --zone=public --add-port=9000/tcp --permanent
# firewall-cmd --reload
```

请注意，由于 SELinux 策略，你只能给给 web 服务器使用如下命令所返回的端口。

```
# semanage port -l | grep -w '^http_port_t'
```

假如你想让 httpd 服务使用另一个端口（如 TCP 端口 8100），你必须将它加到 SELinux 的端口上下文：

```
# semanage port -a -t http_port_t -p tcp 8100
```

添加 Apache 端口到 SELinux 策略

为了进一步加固你安装的 Apache，请遵循以下步骤：

1. 运行 Apache 的用户不应该拥有访问 shell 的能力：

```
# usermod -s /sbin/nologin tecmint
```

2. 禁用目录列表功能，这是为了阻止浏览器展示一个未包含 index.html 文件的目录里的内容。

   编辑 `/etc/httpd/conf/httpd.conf` (以及虚拟主机的配置文件，假如有的话)，并确保出现在顶层的和Directory 块中的 Options 指令都被设置为 None：

```
Options None
```

3. 在 HTTP 响应中隐藏有关 web 服务器和操作系统的信息。像下面这样编辑文件 `/etc/httpd/conf/httpd.conf` ：

```
ServerTokens Prod
ServerSignature Off
```

现在，你已经做好了从 `/var/www/html` 目录开始服务内容的准备了。

配置并加固 FTP 服务器

和 Apache 的情形类似， Vsftpd 的主配置文件 `/etc/vsftpd/vsftpd.conf` 带有详细的注释，且虽然对于大多数的应用实例，默认的配置应该足够了，但为了更有效率地操作 ftp 服务器，你应该开始熟悉相关的文档和 man 页 `man vsftpd.conf` （对于这点，再多的强调也不为过！）。

在我们的示例中，使用了这些指令：

```
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_std_format=YES
chroot_local_user=YES
allow_writeable_chroot=YES
listen=NO
listen_ipv6=YES
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
```

通过使用 `chroot_local_user=YES` ，（默认情况下）本地用户在登录之后，将被限制在以用户的家目录为 chroot 监狱的环境中。这意味着本地用户将不能访问除其家目录之外的任何文件。

最后，为了让 ftp 能够在用户的家目录中读取文件，设置如下的 SELinux 布尔值：

```
# setsebool -P ftp_home_dir on
```

现在，你可以使用一个客户端例如 Filezilla 来连接一个 ftp 服务器：

查看 FTP 连接

注意， `/var/log/xferlog` 日志将会记录下载和上传的情况，这与上图的目录列表一致：

监视 FTP 的下载和上传情况

另外请参考： **在 Linux 系统中使用 Trickle 来限制应用使用的 FTP 网络带宽 <https://linux.cn/article-5517-1.html>**

总结

在本教程中，我们解释了如何设置 web 和 ftp 服务器。由于这个主题的广泛性，涵盖这些话题的所有方面是不可能的（如虚拟主机）。因此，我推荐你也阅读这个网站中有关 **Apache <http://www.google.com/cse?cx=partner-pub-2601749019656699:2173448976&ie=UTF-8&q=virtual+hosts&sa=Search&gws_rd=cr&ei=Dy9EVbb0IdHisASnroG4Bw#gsc.tab=0&gsc.q=apache>** 的其他卓越的文章。

---

via: **http://www.tecmint.com/rhcsa-series-install-and-secure-apache-web-server-and-ftp-in-rhel/ <http://www.tecmint.com/rhcsa-series-install-and-secure-apache-web-server-and-ftp-in-rhel/>**

作者：**Gabriel Cánepa <http://www.tecmint.com/author/gacanepa/>** 译者：**FSSlc <https://github.com/FSSlc>** 校对：**wxy <https://github.com/wxy>**

本文由 **LCTT <https://github.com/LCTT/TranslateProject>** 原创翻译，**Linux中国 <file:///root/github/my-notes/Manual/Linux.cn/RHCSA/RHCSA%E7%B3%BB%E5%88%97%E5%AE%89%E8%A3%85%E3%80%81%E9%85%8D%E7%BD%AE%E5%8F%8A%E5%8A%A0%E5%9B%BA%E4%B8%80%E4%B8%AA%20Web%20.html>** 荣誉推出

> 原文：**http://www.tecmint.com/rhcsa-series-install-and-secure-apache-web-server-and-ftp-in-rhel/ <http://www.tecmint.com/rhcsa-series-install-and-secure-apache-web-server-and-ftp-in-rhel/>**
>
> 作者： Gabriel Cánepa
>
> 译文：**LCTT <http://lctt.github.io/> https://linux.cn/article-6286-1.html <https://linux.cn/article-6286-1.html>** 译者： FSSlc

本文导航

相关阅读

RHCSA

- RHCSA 系列（八）：加固 SSH，设定主机名及启用网络服务 2015-9-23
- RHCSA 系列（十）：Yum 包管理、Cron 自动任务计划和监控系统日志 2015-9-26
- RHCSA 系列（七）：使用 ACL（访问控制列表）和挂载 Samba/NFS 共享 2015-9-22
- RHCSA 系列（十一）：使用 firewalld 和 iptables 来控制网络流量 2015-9-29
- RHCSA 系列（十二）：使用 Kickstart 完成 RHEL 7 的自动化安装 2015-10-2
- RHCSA 系列（十三）：在 RHEL 7 中使用 SELinux 进行强制访问控制 2015-10-3