Day 03 系统安全保护 配置用户环境 配置高级连接 防火墙策略管理

1. 系统安全保护
2. SELinux概述

· Security-Enhanced Linux

- 美国NSA国家安全局主导开发，一套增强Linux系统安全的强制访问控制体系

- 集成到Linux内核（2.6及其以上）中运行

- RHEL7基于SELinux体系针对用户、进程、目录和文件提供了预设的保护策略，以及管理工具

· SELinux的运行模式

- enforcing(强制)、permissive(宽松)

|

|重启

|reboot

V

- disable(彻底禁用)

查看SELinux状态：getenforce

· 切换运行模式

- 临时切换：setenforce 1|0

- 固定配置：/etc/selinux/config 文件

1. 防火墙策略管理

· 作用：隔离

- 硬件防火墙

- 软件防火墙

· 搭建web

- 服务端：server0.example.com

1. 安装服务端软件 httpd(完善，均衡) Nginx(并发量高，自动化运维) Tomcat(Java)

[root@server0 ~]# yum -y install httpd

1. 启动httpd服务，设置为开机自启

[root@server0 ~]# systemctl restart httpd

[root@server0 ~]# systemctl enable httpd

1. 写自己的主页

默认网页文件路径：/var/www/html

默认网页文件的名字：index.html

默认书写网页内容的语言：html

- 客户端：desktop0.example.com

· 搭建ftp

- 服务端：server0.example.com

1) 安装服务端软件

[root@server0 ~]# yum -y install vsftpd

2) 启动vsftpd服务，设置为开机自启

[root@server0 ~]# systemctl restart vsftpd

[root@server0 ~]# systemctl enable vsftpd

3 默认共享路径：/var/ftp

- 客户端：desktop0.example.com

· 防火墙：firewalld服务基础

1. RHEL7的防火墙体系

a) 系统服务：firewalld

b) 管理工具：firewall-cmd、firewall-config

c) 预设安全区域

· 根据所在的网络场所区分，预设保护规则集

- public：仅允许访问本机的sshd等少数几个服务

- trusted：允许任何访问

- block：阻塞任何来访请求

- drop：丢弃任何来访的数据包

- ......

· 配置规则的位置

- 运行时 (runtime)

- 永久配置选项 (-permanent)

· 匹配规则：原则 匹配即停止

· 防火墙判定进入哪一个区域的规则：

1) 查看客户端请求数据包中，源ip地址，查看自己所有的区域，哪一个区域有该源ip地址进入哪一个区域

2) 如果规则1不符合则进入默认区域

· 预设安全区域

- public：仅允许访问本机的sshd等少数几个服务

- trusted：允许任何访问

- block：阻塞任何来访请求（明确拒绝，客户端会接收到拒绝信息）

- drop：丢弃任何来访的数据包（直接丢弃，节省服务器的资源）

d) 防火墙对源ip地址的控制

· 方式1-宽松模式：默认区域未trusted，将想要拒绝的源ip地址放入到block或drop中

· 方式2-严格模式：默认区域未block或drop，将想要允许的源ip地址放入到trusted中

1. 端口：数字 编号，用来标识进程或程序
2. 默认端口号

· http：80

· ftp：21

1. 端口转发

· 利用防火墙进行对指定端口的转发

1. 配置高级连接
2. 配置高级连接（聚合连接 网卡绑定 链路聚合）

· 热备份（activebackupo）连接冗余（活跃状态 备份状态）

eth1 eth2

team0虚拟网卡

1. 制作网卡绑定
   1. 制作虚拟网卡team0
2. IPv6地址
3. IPv4地址：32个二进制 点分隔4个部分 十进制表示
4. IPv6地址：128个二进制 冒号分隔8个部分 十六进制表示