CentOS - Systems Administration and Security Cheat Sheet

by Bayan (Bayan.A) via cheatography.com/122738/cs/44041/

Install Apache / Verify Status

Install HTTPD service	`yum install httpd`
Check httpd status	`systemctl status httpd.s ervice`

Configuring Apache HTTP Server

Inspect Control Script	`less /etc/s yst emd /sy ste m/m ult i-u ser.ta rge t.w ant s/h ttp d.s ervice`
	displays the contents of the httpd.service file for the Apache HTTP server in the systemd multi-user target.
Get default start-up state	`systemctl get-de fault`
	shows the default target (runlevel) that the system boots into.
Find config file	`find / -name httpd.conf`
Inspect config file	`nano /etc/h ttp d/c onf /ht tpd.conf`
	nano [location of config file found using `find`]
`.htaccess & .htpasswd`	Note that these are hidden by default, to prevent files being viewed by web clients
`ErrorLog`	Find and take note of where the errorlog is located (usually `logs/e rro r_log`)
`Docume ntRoot`	The web document location is usually the `/var/w ww/html`

Investigate Processes, Make & Test Apache

List processes and filters for those related to httpd	`ps -ef ¦ grep httpd`
Rules for incoming traffic	`iptables -L INPUT`
Create index.html file	1) Navigate to appropriate directory
	e.g.: `cd /var/w ww/html`
	2) create and edit file using nano
	e.g.: `sudo nano index.html`
View access log	`cat /var/l og/ htt pd/ acc ess_log`
Request local page	`curl http:/ loc alhost`

MySQL/MariaDB Installation, Start & Status

MariaDB Installation	`yum install mariad b-s erver`
Confirm MySQL/MariaDB is installed	`find / -name mysql`
Start MariaDB	`systemctl start mariadb`
Check MariaDB Status	`systemctl status mariadb`
Confirm servers are running	`ps -ef`
	This produces a list of running servers, where you will search for `mysql` in the far left column(the UID(User ID))
Set new password for mysqladmin root	`mysqladmin -u root password [INSERT PASSWORD]`

MySQL Config file & Data Directory	
Find config file (my.cnf) location	`sudo find / -name my.cnf ¦ less`
Navigate to config file directory	`cd [INSERT DIRECTORY]`
	e.g. in my case, my.cnf was located found to be /etc/my.cnf, so `cd /etc` is used
View contents of config file	`cat my.cnf`
Locate MySQL Daemon	`find / -name mysqld`

Create & Populate Database	
Enter MariaDB Server	`mysql -h localhost -u root -p`
	Then enter password created previously. Note, password will not show any typing.
Create database	`CREATE DATABASE [database name];
	e.g. `CREATE DATABASE food;`
Change to created database	`USE [database]`
	e.g. `USE food'
Exit MariaDB	`quit`
Confirm database was created outside of MariaDB	Change to appropriate directory `cd /var/l ib/ mysql`
	Display contents of current directory using `ls`
Create Table	`CREATE TABLE restaurant (name VARCHA R(40), type VARCHA R(40), location VARCHA R(4));`
	VARCHAR(n) defines variable length
Insert values into restaurant table	`INSERT INTO restaurant (name, type, location) values ("Pi zza hut ", " Ita lia n", " -SW1 0");`
Show table	`SHOW TABLES; DESCRIBE restau rant; SELECT * FROM restau rant;`
Delete value from table	`DELETE FROM restaurant WHERE name="P izz a"& &l oca tio n="S W10 ";`
Create new user	`GRANT SELECT ON food.r est aurant TO bayan@ loc alhost IDENTIFIED BY " bay ans _pa ss w ord ";`

Firewalls	
Confirm firewalld is running	`systemctl status firewalld`
Check firewall conifiguration	`firewa ll-cmd --list-all`
Display firewall rules	`iptables -L'
Services/ports available for sshd	`systemctl status sshd`
Services/ports available for httpd	`systemctl status httpd`
Services/ports available for vsftp	`systemctl status vsftp`
	if not installed, use yum install. e.g. `yum install vsftpd`
Stop firewalld, then check if running to confirm it is infact stopped	`systemctl stop firewalld`
Start firewalld	`systemctl start firewalld`

Firewalls (cont)

Add http service to firewall configuration	`firewa ll-cmd --add- service http`
Add ftp service to firewall configuration	`firewa ll-cmd --add- service ftp`
iptables rules for accepting traffic for ports 22(SSH), 80(HTTP), and 21 (FTP)	`iptables -A INPUT -p tcp --dport 22 -j ACCEPT`
	`iptables -A INPUT -p tcp --dport 80 -j ACCEPT`
	`iptables -A INPUT -p tcp --dport 21 -j ACCEPT`
Add rules to output chain	`iptables  -A OUTPUT -m state --state ESTABL ISHED, RELATED -j ACCEPT`
Dropping default rules for INPUT and OUTPUT traffic	`iptables -P INPUT DROP`
	`iptables -P OUTPUT DROP`

SELinux

Install setroubleshoot and httpd	`sudo yum install setrou ble shoot httpd`
Enable httpd	`systemctl enable httpd`
Start httpd	`systemctl start httpd`
Check default directory for HTML files	`cat /etc/h ttp dco nf/ htt pd.conf | grep Docume - ntRoot`
Check SELinux permissions / context	`ls -lZ index.html`
Temporarily disable SELinux enforcement for troubleshooting or testing without changing the permanent configuration.	`setenforce 0`
Re-enable SELinux enforcement after it has been disabled, restoring its security policies.	`setenforce 1`
Apply default SELinux to a file:	`/sbin/ res torecon -v /var/w ww/ htm l/s ecr et.h tml`