Cheatography

RHEL command list Cheat Sheet

by cyphox90 via cheatography.com/192992/cs/40221/

Version, Kernel & Package details

Verify RHEL installed version	cat /etc/r-edhat--release
Verify RHEL has the correct version of SLES installed. Log in as root user.	cat /etc/S-uSE-re-lease
Display the RHEL kernel version	uname-r
Display the RHEL kernel version	uname -mrs
Display the RHEL kernel version	uname -a
List all packages with RPM	rpm --query --all
List all installed RPM packages	rpm -qa
List all installed YUM packages	yum list installed
List all installed DNF packages	dnf list installed
View current firewall settings	firewall--config

Notes for SSH

Use SSH Public Key based login	~
Disable root user login	add users to a SUDO group
Disable password based login	AuthenticationMethods publickey PubkeyAuthen-tication yes
Limit users SSH access	AllowUsers first lastname
Disable empty passwords	PermitEmptyPasswords no
Firewall SSH TCP port #22	~
Configure idle log out timeout interval	ClientAliveInterval 300 ClientAliveCountMax 0

RHEL firewalld

View the current status of firewalld	firewall-cmd --state or systemctl status firewalld
View current firewalld settings in window	firewall-config
View current firewalld settings via CLI	firewall-cmd --list-all
View what services are allowed in the current firewalld zone	firewall-cmd --list-services

SSH & Hostnamectl identification

Identify Port number in OpenSSH server config file	grep Port /etc/ssh/ssh-d_config
Identify Port number in OpenSSH client config file	grep Port /etc/ssh/ssh-_config
Identify system wide OpenSSH config file for client	cat /etc/ssh_ssh_config
View all hostna-mectl	hostnamectl status
Confirm SSH password authentication	grep sshd -T | grep PasswordAuthentication
Find all failed SSH login attempts	grep "Failed password" /var/log/auth.log
Find all failed SSH login attempts	cat /var/log/auth.log | grep "Failed password
List all IP adddresses that attempted login & failed	grep "Failed password" /var/log/auth.log | awk '{print $11}' | uniq -c | sort -nr
(1) Finding failed SSH login attempts	grep "authentication failure" /var/log/secure

SSH & Hostnamectl identification (cont)

(1) Finding failed SSH login attempts	grep -E -i 'authenti-cation failure|Invalid user' /var/log/secure | grep sshd
(1) Finding failed SSH login attempts	grep -E 'sshd.*Faile-d|Invalid|Did|failure' /var/log/secure
(1) Finding failed SSH login attempts	grep -E 'sshd.*Faile-d|Invalid|Did|failure' /var/log/auth.log
(2) Finding failed SSH login attempts (awk print statement may need to be changed)	grep "authentication failure" /var/log/-secure | awk '{ print $13 }' | cut -b7- | sort | uniq -c
Testing SUDO access	sudo -i
Identify sudoers with authorisation	cat /etc/sudoers

Basic SELinux settings

Display current SELinux state mode	getenforce
Check SELinux SELINUX variable to persist across rebots	cat /etc/s-eli-nux/config-
Identify if NTP is installed	chkconfig --list ntpd
Identify if ntpd is running	ntpq -p
Check NTP sync status	timeda-tectl
Check NTP sync status	timeda-tectl status

By **cyphox90**
cheatography.com/cyphox90/

Not published yet.
Last updated 9th September, 2023.