Cheatsheet Enterprise Linux

# CentOS – Firewall controls

* firewall-cmd --status : status van de firewall
* firewall-cmd –list-all(-zones) : overzicht van alle services en poorten die worden gefilterd (per zone).
* firewall-cmd [--permanent] [--zone=naamZone] --add-service=[naamService] : een service toelaten doorheen de firewall.
* firewall-cmd [--permanent] [--zone=naamZone] --add-port=[naamPort bv 80/tcp] : een poort openzetten.
* Om te verwijderen add 🡪 remove

# CentOS – Services controls

* sudo systemctl [start/stop/restart] [naam-service].service : de genoemde service starten/stoppen/herstarten.
* sudo systemctl status [naam-service].service : de status van de service opvragen.
* sudo systemctl [enable/disable] [naam-service].service : de service wel/niet opstarten bij het booten.

# Bind-Utils

* dig @[ip-of-dnsServer] [FQDN] [NS/A] : vraagt het IP-adres op van de server die geregistreerd staat met deze FQDN. De laatste parameter is optioneel en vraagt de specifieke records op.
* dig @[ip-of-dnsServer] –x [ip-adres]: vraagt de FQDN op van de server met

het gegeven ip adres.

# CentOS – Log files

* journalctl \_COMM=[naam-Service]: Geeft de log file weer van de opgegeven service.
* journalctl \_COMM=[naam-Service] --since "10:00" --until "11:00": idem maar je kan ook filteren op tijdstip.
* \_COMM 🡪 voor services, je kan ook zoeken op \_PID= of \_UID= of zelfs \_SELINUX\_CONTEXT=

# CentOS – Configuratie testen

* named-checkconf [locatie conf]: configuratie testen named.conf
* named-checkzone [naam-zone-file] [locatie-zone-file]: configuratie van zone-file testen.
* testparm : controleert configuratie van Samba config file.

# SELinux

* getsebool –a: toont alle booleans die SELinux bevat en hun status.
* setsebool -P [naamBoolean] [0/1]
* setenforce [0/1]: uit of aanschakelen van SELinux

# CentOS – Locaties

|  |  |
| --- | --- |
| Locatie | Uitleg |
| /etc/named.conf | Bind config file |
| /var/named/[zone name] | Bind zone file |
| /etc/dhcp/dhcpd.conf | DHCP config file |
| /etc/vsftpd/vsftpd.conf | VSFTP config file |
| /etc/samba/smb.conf | SMB config file |
| /etc/pki/tls/certs | SSL certificaat locatie |
| /etc/pki/tls/private/ca.key /etc/pki/tls/private/ca.csr | SSL locatie private key |
| /etc/httpd/conf.d/ssl.conf | SSL config file |
| /etc/httpd/conf/httpd.conf | http config file |
| /etc/httpd/conf.d/wordpress.conf | Secundaire configs (vn wordpress bv) |
| /etc/sysconfig/network-scripts | In deze map staan de config files voor alle netwerkinterfaces |
| - /var/log/messages (hoofd-log)  – /var/log/audit/audit.log (SELinux)  – /var/log/httpd/\*  – /var/log/samba/\*  – /var/log/vsftpd/\* | Oude logfile locaties |

# Checklist troubleshooting a fileserver (SMB/FTP)

Gebruik Bottom-Up strategy!

1. FYSIEK: Check kabel en power 🞎
2. DATA LINK: check statusparameters en evt LED’s (in virtualbox: status netw int) 🞎
3. NETWERK:
   1. IP stack juist 🞎
   2. De interfaces staan aan 🞎
   3. De interfaces zijn goed geconfigureerd 🞎
   4. Draaien de diensten op het juiste adres 🞎
   5. Zijn de diensten juist geconfigureerd hiervoor 🞎
4. TRANSPORT:
   1. Worden de services van de server niet geblokkeerd door de firewall? 🞎
   2. Kan mijn host-systeem de server vinden via Explorer 🞎
5. APPLICATIE:
   1. Zijn de permissies geregeld op Samba-niveau 🞎
   2. Zijn de permissies geregeld qua bestandspermissies 🞎
   3. Zijn de permissies geregeld voor SELinux 🞎