

Install NetYCE on RHEL/Centos 7

This installation guide installs NetYCE version 7.x on a Redhat 7 or Centos 7 physical or virtual x86_64 platform.

References to EL or RHEL refer to RedHat Enterprise Linux or CentOS Linux. All OS versions and packages are required to use the x86_64 architecture, that is x86 processors running 64-bit. The installation applies to both physical and virtual platform deployments.

Introduction

The choice of operating system (Redhat or CentOS), disk filesystem layout, installed packages, and security hardening are mostly defined by the customers common practice. NetYCE does have some requirements on disk-usage and directory-trees that may warrant filesystem allocations, and we do rely on a specific functional user, yce that requires some sudo permissions.

A basic set of packages should be installed which will later be amended by specific NetYCE software. The basic OS installation can easily be realized by the customer, but we recommend the NetYCE software installation and configuration to be a joint effort.

During the first install of the NetYCE software packages, the configuration preferences and details of the NetYCE system and its architecture will be defined and initialized. Subsequent software upgrades and patches can be installed by the application manager using the NetYCE front-end without requiring system privileges. Only on some major upgrades will those be required.

The NetYCE software installation consists of two self-installing packages, YCE and YCEperl, a sample database and a license file. The installation depends on MariaDB (mysql server), apache (http server), fping and some standard distribution packages (openssl, tftp, ftp, ssh, telnet, gtar, etc). Mysecureshell is a non standard distribution package we use for sftp jail functionality.

System specification

The hardware requirements of NetYCE are moderate by itself although much depends on the intended level of use and the application architecture selected.

In general we suggest to deploy two NetYCE servers in different data centers attached to Network Management (NMS) networks. These systems will provide both front-end (user and network facing) functions AND a database function. These functions can be configured to provide live failover and backup services by means of master-master replication. The front-end functions support 10-20 simultaneous users and can execute several thousand config changes per hour.

For such deployments a physical or virtual x86 server needs to have at least two CPU cores and 4 GB of memory, but 4 cores and 8 GB memory is recommended.

Disk space can be local or SAN based and should not exceed 100 GB. This disk space is allotted to a single filesystem or split across several, depending on system management preferences.

```
/ - 4 to 15 GB (OS root, bin, usr, lib, opt, etc)
/opt/yce - 500 MB
/opt/nms - 500 MB
/opt/yce/lib - 800 MB
/var/opt/yce - 3 to 8 GB (logs and working data)
/var/opt/shared - 6 to 12 GB (os-files)
/var/opt/mysql - 4 to 16 GB (mysql data)
```

The provided image has an expanding virtual disk of 500G.

Centos

- root password: NetYCE01
- Group: nms, gid: 8000
- User: yce, uid: 1000, password: NetYCE01
- Timezone: Europe/Amsterdam
- firewall: disabled

partition layout

- sda1: /boot, xfs, 2G, primary
- sda2: lvm, 1x PV, 1x VG
 - swap 4G, name: swap
 - /, xfs, rest of disk, name: rootvol

After initial OS install

First we make sure the 'yce' user exists. Any step afterwards is to be executed by the 'yce' user, unless stated otherwise.

Change user/group

```
groupadd -g 8000 nms
adduser -g nms -u 1000 -N -p
'$6$0u7BTBsmCa/hZ$qIbX6BATWHAL26mXR2vfqFenev8K26KMQC1YZbeq2JG27CA0Hmd2WSUF1F
JyLiMDTV.2WVksKxl0dZLvZtDuW/' yce
passwd -i -l yce

# "Changing yce user group to nms"
usermod -g nms -G '' -c "NetYCE user" yce
# "Removing temporary group yce"
groupdel yce
```

```
adduser -M -g nms -u 1000 -d /var/opt/shared -s /bin/MySecureShell -o -N -p
'$6$DepSUhWyIC60x$2w.jWJx7Qxd2wWkeMfhcFwGJNqC7DcJUkkw8B5Ukgey8rawN4f2gDn52nM
pyAn0Kzj3J1opmbu9dpdryLouq00' ycycle
passwd -i -l ycycle
```

Log out and log in with the 'yce' user.

Packages

```
sudo /usr/bin/yum install -y epel-release

sudo /usr/bin/yum install -y bzip2 crontabs curl dhcp dkms findutils fping
ftp git httpd iproute iputils less man man-pages MariaDB-client MariaDB-
server mtr mysecureshell nano net-snmp net-snmp-utils nfs-utils nfs4-acl-
tools ntp ntpdate openssh-clients openssh-server openssl php postfix
python2-pip python3 python3-pip rpcbind rsync sed sudo syslog-ng syslog-ng-
libdbi tar telnet tftp traceroute unzip vim-enhanced vsftpd wget which yum-
utils zip mod_ssl

sudo /usr/bin/yum -y update

sudo /usr/bin/yum clean all
```

Files

All files have 644 permissions and 'yce:nms' owned unless stated otherwise.

This is a file, since it contains special characters.

bash_profile

```
/home/yce/.bash_profile
.bash_profile
```

bashrc

```
/home/yce/.bashrc
```

```
# .bashrc

# User specific aliases and functions

# Source global definitions
if [ -f /etc/bashrc ]; then
    . /etc/bashrc
fi
```

```
# Uncomment the following line if you don't like systemctl's auto-paging
feature:
# export SYSTEMD_PAGER=

# Source alias definitions
if [ -f ~/.shell_aliases ]; then
    . ~/.shell_aliases
fi
```

shell_aliases

/home/yce/.shell_aliases and /root/.shell_aliases

```
export PAGER="less"
export EDITOR="vim"
alias l='ls -lF'
alias ll='ls -lhF'
alias llt='ls -latrF'
alias lr='ls -latrF'
alias la='ls -ahF'
alias lla='ls -lahF'
alias lc='ls -CaF'
alias p='ping'
alias pst='ps axjf'
alias t='telnet'
alias n='nslookup'
alias o='less'
if [ -x /usr/bin/vim ]; then
    alias vi='vim'
fi
alias grep='grep --color=auto'
alias gerp='grep --color=auto'
alias ip='ip --color'
alias ip4='ip -4 --color --brief addr | grep -v UNKNOWN'
alias ip6='ip -6 --color --brief addr | grep -v UNKNOWN'
```

vimrc

/home/yce/.vimrc

```
set ts=4
set sw=4
set ai
set noerrorbells
set formatoptions-=r
```

sudo

/etc/sudoers.d/yce, root:root, 600

```
# Yce
Cmdn_Alias YCE = /opt/yce/system/init/yce_tftpd,
/opt/yce/system/init/yce_netmon

# Services
Cmdn_Alias SERVICES = /usr/bin/systemctl, /sbin/service, /sbin/chkconfig

# Installation and management of software
Cmdn_Alias SOFTWARE = /bin/rpm, /usr/bin/up2date, /usr/bin/yum

# Processes
Cmdn_Alias PROCESSES = /bin/nice, /bin/kill, /usr/bin/kill,
/usr/bin/killall, /usr/bin/pkill

# Networking
Cmdn_Alias NETWORKING = /usr/sbin/ss, /usr/sbin/ip, /bin/ping,
/usr/sbin/dhclient, /usr/sbin/iptables, /usr/sbin/ifstat, /usr/sbin/ethtool

# Storage
# Cmdn_Alias STORAGE = /sbin/fdisk, /sbin/sfdisk, /sbin/parted,
/sbin/partprobe, /bin/mount, /bin/umount

# Delegating permissions
Cmdn_Alias DELEGATING = /usr/sbin/visudo, /usr/bin/chown, /usr/bin/chmod,
/usr/bin/chgrp

Defaults    !requiretty

#==== YCE user group 'nms'
# Below are a few examples.
# For production the MINIMUM profile might be a good start.
# For testing, the MAINTENANCE is regularly used.

# MINIMUM
# No password required for YCE applications, ALL other applications are
allowed with a password.
# %nms ALL = PASSWD:ALL, NOPASSWD:YCE, SERVICES

# MAINTENANCE
# No password required for YCE applications and services and processes. NO
other applications are allowed to run at all!
%nms ALL = PASSWD:ALL, NOPASSWD:YCE, SERVICES, PROCESSES

# Same, but all applications are allowed if you know the password.
# %nms ALL = PASSWD:ALL, NOPASSWD:YCE, SERVICES, PROCESSES
```

```
# DEVELOPMENT
# %nms ALL = PASSWD:ALL, NOPASSWD:SOFTWARE, YCE, SERVICES, PROCESSES
# %nms ALL = PASSWD:ALL, NOPASSWD:DELEGATING, NETWORKING, SOFTWARE, YCE, SERVICES, PROCESSES
```

bash_profile (root)

/root/.bash_profile

```
# .bash_profile
#
# NetYCE, 2021
#

# Get the aliases and functions
if [ -f ~/.bashrc ]; then
    . ~/.bashrc
fi

# User specific environment and startup programs
if [ -r "/opt/yce/system/go" ]; then
    source "/opt/yce/system/go"
else
    echo "Skipping 'go'"
fi

PATH=$PATH:$HOME/bin

PATH=/usr/local/sbin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin:/root/bin:/opt/yce/bin:/opt/yce/system
export PATH

export PS1='\e[32m\u@\h\e[0m \w\n# '

if [ -f /etc/DIR_COLORS ]; then
    alias ls='ls -N --color=tty -T 0 '
fi

echo " "
if [ -x "/opt/yce/system/net_setup.pl" ]; then
    /opt/yce/system/net_setup.pl -w
else
    echo "ERROR: cannot start net_setup.pl"
fi

echo " "
echo " You can setup the networking by logging in "
echo " as 'root' and using"
```

```
echo " /opt/yce/system/net_setup.pl"
echo " "
echo " YCE setup can be restarted as 'yce' user using"
echo " /opt/yce/system/yce_setup.pl"
echo " "
```

bashrc (root)

/root/.bashrc

```
# .bashrc

# User specific aliases and functions

# alias rm='rm -i'
# alias cp='cp -i'
# alias mv='mv -i'

# Source global definitions
if [ -f /etc/bashrc ]; then
    . /etc/bashrc
fi

# Uncomment the following line if you don't like systemctl's auto-paging
# feature:
# export SYSTEMD_PAGER=

# Source alias definitions
if [ -f ~/.shell_aliases ]; then
    . ~/.shell_aliases
fi
```

General

All files need to be changed with root privileges.

/etc/systemd/journald.conf

```
# or your desired value
SystemMaxUse=200M
```

/etc/environment

```
LANG=en_US.utf-8
LC_ALL=en_US.utf-8
```

/etc/sysconfig/ntpdate

```
SYNC_HWCLOCK=yes
```

/etc/sysconfig/clock

```
ZONE="Europe/Amsterdam"  
UTC="yes"
```

/etc/selinux/config

```
SELINUX=disabled
```

Yce dirs

```
sudo mkdir -p /var/opt  
sudo mkdir -p /var/opt/shared  
sudo mkdir -p /opt  
sudo mkdir -p /etc/systemd/system/mariadb.service.d/  
sudo mkdir -p /etc/systemd/system/httpd.service.d/  
sudo mkdir -p /etc/systemd/system/chronyd.service.d/
```

```
sudo mkdir -p /var/opt/mysql  
sudo mkdir -p /opt/yce/lib  
sudo mkdir -p /opt/yce  
sudo mkdir -p /opt/nms  
sudo mkdir -p /var/opt/yce/backup  
sudo mkdir -p /var/opt/yce/backup/.tmp  
sudo mkdir -p /var/opt/yce/configs  
sudo mkdir -p /var/opt/yce/download  
sudo mkdir -p /var/opt/yce/jobs  
sudo mkdir -p /var/opt/yce/logs  
sudo mkdir -p /var/opt/yce/configs  
sudo mkdir -p /var/opt/yce/output  
sudo mkdir -p /var/opt/yce/download/users  
sudo mkdir -p /var/opt/yce/download/documentation  
sudo mkdir -p /var/opt/yce/download/.tmp  
sudo mkdir -p /var/opt/yce/download/client  
sudo mkdir -p /var/opt/yce/shared  
sudo mkdir -p /var/opt/shared/public/acs  
sudo mkdir -p /var/opt/shared/public/os  
sudo mkdir -p /var/opt/shared/public/previous  
sudo mkdir -p /var/opt/shared/public/users  
sudo mkdir -p /var/opt/shared/public/.tmp  
sudo mkdir -p /home/yce/.ssh
```

```
sudo chown yce:nms /var/opt/mysql  
sudo chown yce:nms /opt/yce/lib  
sudo chown yce:nms /opt/yce
```



```
sudo chown yce:nms /opt/nms
sudo chown yce:nms /var/opt/yce/backup
sudo chown yce:nms /var/opt/yce/backup/.tmp
sudo chown yce:nms /var/opt/yce/configs
sudo chown yce:nms /var/opt/yce/download
sudo chown yce:nms /var/opt/yce/jobs
sudo chown yce:nms /var/opt/yce/logs
sudo chown yce:nms /var/opt/yce/configs
sudo chown yce:nms /var/opt/yce/output
sudo chown yce:nms /var/opt/yce/download/users
sudo chown yce:nms /var/opt/yce/download/documentation
sudo chown yce:nms /var/opt/yce/download/.tmp
sudo chown yce:nms /var/opt/yce/download/client
sudo chown yce:nms /var/opt/yce/shared
sudo chown yce:nms /var/opt/shared/public/acs
sudo chown yce:nms /var/opt/shared/public/os
sudo chown yce:nms /var/opt/shared/public/previous
sudo chown yce:nms /var/opt/shared/public/users
sudo chown yce:nms /var/opt/shared/public/.tmp
sudo chown yce:nms /home/yce/.ssh
```

Repositories

Create the files with root privileges.

/etc/yum.repos.d/MySecureShell.repo

```
[MySecureShell]
baseurl = http://mysecureshell.free.fr/repository/index.php/centos/6.4/
enabled = 1
gpgcheck = 0
name = MySecureShell
```

/etc/yum.repos.d/MariaDB.repo

```
[MariaDB]
baseurl = http://yum.mariadb.org/10.3/centos7-amd64
enabled = 1
gpgcheck = 1
gpgkey = https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
name = http://downloads.mariadb.org/mariadb/repositories/
```

Packages

```
sudo yum install -y bzip2 crontabs curl dhcp dkms findutils file fping ftp
git httpd iproute iputils less man man-pages MariaDB-client MariaDB-server
mod_ssl mtr mysecureshell nano net-snmp net-snmp-utils nfs-utils nfs4-acl-
```

```
tools ntp ntpdate openssh-clients openssh-server openssl php postfix  
python2-pip python3 python3-pip rpcbind rsync sed sudo syslog-ng syslog-ng-  
libdbi tar telnet tftp traceroute unzip vim-enhanced vsftpd wget which yum-  
utils zip
```

```
sudo yum remove -y rsyslog
```

```
sudo python2 -m pip install -U pip==20.3.4 pexpect
```

```
sudo python3 -m pip install -U pip setuptools
```

as yce user:

```
python3 -m pip install -U xmltodict ncclient PyYAML pexpect pymysql netyce  
requests
```

If running VMware:

```
sudo yum install -y open-vm-tools  
sudo systemctl enable vmtoolsd
```

If running HyperV:

```
/etc/dracut.conf.d/hyperv.conf, root:root, 644
```

```
add_drivers+="hv_vmbus hv_storvsc hv_netvsc hv_utils hv_balloon hyperv-  
keyboard hyperv_fb hid-hyperv"
```

```
sudo dracut -f
```

yce perl

as yce user:

```
wget https://wiki.netyce.com/lib/exe/fetch.php/downloads:yceperl_7.0.2.bin -  
O /tmp/yceperl.bin  
chmod +x /tmp/yceperl.bin  
/tmp/yceperl.bin  
  
rm /tmp/yceperl.bin
```

yce license

```
mkdir /opt/yce/etc  
wget
```

```
https://wiki.netyce.com/lib/exe/fetch.php/downloads:system_updates:genesis_license_v7.txt -0 /opt/yce/etc/yce_license
```

Install NetYCE

Download the desired version from the [download page](#).

```
sh $downloaded_file
rm $downloaded_file
```

Service setup

```
sudo ln -s /opt/yce/system/init/mariadb.service.d-yce.conf
/etc/systemd/system/mariadb.service.d/yce.conf
sudo ln -s /opt/yce/system/init/httpd.service.d-yce.conf
/etc/systemd/system/httpd.service.d/yce.conf
sudo cp /opt/yce/system/init/yce_psmon.service
/etc/systemd/system/yce_psmon.service
sudo chmod 664 /etc/systemd/system/yce_psmon.service

sudo systemctl daemon-reload
```

/etc/snmp/snmpd.conf, root:root, 600

```
# Map 'readsys' community to the 'ConfigUser'
# Map 'readall' community to the 'AllUser'
#      sec.name          source          community
com2sec ConfigUser      default        readsys
com2sec AllUser         default        readall

# Map 'ConfigUser' to 'ConfigGroup' for SNMP Version 2c
# Map 'AllUser' to 'AllGroup' for SNMP Version 2c
#      sec.model         sec.name
group  ConfigGroup      v2c          ConfigUser
group  AllGroup         v2c          AllUser

# Define 'SystemView', which includes everything under .1.3.6.1.2.1.1 (or
.1.3.6.1.2.1.25.1)
# Define 'AllView', which includes everything under .1
#      incl/excl        subtree
view   SystemView      included     .1.3.6.1.2.1.1
view   SystemView      included     .1.3.6.1.2.1.25.1.1
view   AllView         included     .1

# Give 'ConfigGroup' read access to objects in the view 'SystemView'
# Give 'AllGroup' read access to objects in the view 'AllView'
```

#		context	model	level	prefix	read	
write	notify						
access	ConfigGroup	""	any	noauth	exact	SystemView	none
none							
access	AllGroup	""	any	noauth	exact	AllView	none
none							

/etc/syslog-ng/syslog-ng.conf, root:root, 600

```
@version:3.5
@include "scl.conf"

# RHEL7 syslog-ng configuration file for NetYCE.
#
# This should behave pretty much like the original syslog on RedHat.
# See syslog-ng(8) and syslog-ng.conf(5) for more information.
#
# Note: it also sources additional configuration files (*.conf)
#       located in /etc/syslog-ng/conf.d/

options {
    flush_lines (0);
    time_reopen (10);
    log_fifo_size (1000);
    chain_hostnames (off);
    use_dns (yes);
    use_fqdn (yes);
    create_dirs (no);
    keep_hostname (yes);
    keep-timestamp (no);
};

source net {
    tcp();
    udp();
};

source s_sys {
    system();
    internal();
    # udp(ip(0.0.0.0) port(514));
};

destination d_logs {
    file(
        "/var/opt/yce/logs/syslog-ng.log"
        owner("yce")
        group("nms")
        perm(0644)
    )
};
```

```
);
};

destination d_cons { file("/dev/console"); };
destination d_mesg { file("/var/log/messages"); };
destination d_auth { file("/var/log/secure"); };
destination d_mail { file("/var/log/maillog" flush_lines(10)); };
destination d_spol { file("/var/log/spooler"); };
destination d_boot { file("/var/log/boot.log"); };
destination d_cron { file("/var/log/cron"); };
destination d_kern { file("/var/log/kern"); };
destination d_mlal { usertty("*"); };

filter f_kernel { facility(kern); };
filter f_default {
    level(info..emerg) and
    not (facility(mail)
    or facility(authpriv)
    or facility(cron));
};
filter f_auth { facility(authpriv); };
filter f_mail { facility(mail); };
filter f_emergency { level(emerg); };
filter f_news {
    facility(uucp) or
    (facility(news)
    and level(crit..emerg));
};
filter f_boot { facility(local7); };
filter f_cron { facility(cron); };

log { source(net); destination(d_logs); };
log { source(s_sys); filter(f_kernel); destination(d_kern); };
#log { source(s_sys); filter(f_kernel); destination(d_cons); };
log { source(s_sys); filter(f_default); destination(d_mesg); };
log { source(s_sys); filter(f_auth); destination(d_auth); };
log { source(s_sys); filter(f_mail); destination(d_mail); };
log { source(s_sys); filter(f_emergency); destination(d_mlal); };
log { source(s_sys); filter(f_news); destination(d_spol); };
log { source(s_sys); filter(f_boot); destination(d_boot); };
log { source(s_sys); filter(f_cron); destination(d_cron); };

# Source additional configuration files (.conf extension only)
@include "/etc/syslog-ng/conf.d/*.conf"
```

/etc/logrotate.d/syslog-ng

```
/var/opt/yce/logs/syslog-ng.log {
    missingok
    notifempty
```

```
start 0
rotate 9
nodateext
nocompress
maxsize 50M
daily
create 0644 yce nms
postrotate
    /bin/kill -HUP `cat /var/run/syslogd.pid` >/dev/null 2>/dev/null ||
true
    /bin/kill -USR2 `cat /var/opt/yce/jobs/yce_events.pid` >/dev/null
2>/dev/null || true
endscript
}
```

/etc/logrotate.d/vsftpd

```
#
# NetYCE 2020
# see /etc/vsftpd/vsftpd.conf
#
/var/opt/yce/logs/ftpxfer.log
/var/opt/yce/logs/vsftpd.log
{
    missingok
    notifempty
    start 0
    rotate 9
    nodateext
    nocompress
    maxsize 2M
    daily
    create 0644 yce nms
    postrotate
        /usr/bin/pkill -HUP /usr/sbin/vsftpd >/dev/null 2>/dev/null || true
    endscript
}
```

/etc/vsftpd/vsftpd.conf

```
#
# NetYCE 2016, 2020
#
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=002
dirmessage_enable=YES
connect_from_port_20=YES
```

```
chroot_list_enable=YES
listen=NO
listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES

xferlog_enable=YES
xferlog_std_format=YES
dual_log_enable=YES
userlist_log=YES
log_ftp_protocol=YES
xferlog_file=/var/opt/yce/logs/ftpxfer.log
vsftpd_log_file=/var/opt/yce/logs/vsftpd.log

local_root=/var/opt/shared
secure_chroot_dir=/var/opt/shared
chown_username=yce.nms
guest_enable=NO
force_dot_files=NO
hide_file={.yce_prop}
delete_failed_uploads=YES
```

/etc/vsftpd/chroot_list

```
ycicle
```

/etc/ssh/sshd_config

```
# $OpenBSD: sshd_config,v 1.80 2008/07/02 02:24:18 djm Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

# Disable legacy (protocol version 1) support in the server for new
# installations.  In future the default will change to require explicit
# activation of protocol 1
Protocol 2
```

```
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 1h
#ServerKeyBits 1024

# Logging
# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile .ssh/authorized_keys
#AuthorizedKeysCommand none
#AuthorizedKeysCommandRunAs nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication yes

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
```



```
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
#KerberosUseKuserok yes

# GSSAPI options
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
#UsePAM no
UsePAM yes

# Accept locale-related environment variables
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY
LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding no
#X11DisplayOffset 10
#X11UseLocalhost yes
#PrintMotd yes
PrintLastLog yes
#TCPKeepAlive yes
#UseLogin no
#UsePrivilegeSeparation yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#ShowPatchLevel no
#UseDNS yes
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
```

```
# no default banner path
#Banner none

# Set Ciphers and MACs
Ciphers aes128-ctr,aes192-ctr,aes256-ctr
MACs hmac-ripemd160,hmac-sha2-256,hmac-sha2-512,hmac-ripemd160@openssh.com

# no reverse lookups
UseDNS no

# override default of no subsystems
Subsystem sftp /usr/libexec/openssh/sftp-server
# Subsystem sftp internal-sftp

Match User ycicle
    AllowTCPForwarding no
    X11Forwarding no
# ChrootDirectory /var/opt/shared
# ForceCommand internal-sftp
# ForceCommand /opt/yce/bin/cpsh.pl
```

/etc/ssh/sftp_config

```
## MySecureShell Configuration File ##
#Default rules for everybody
<Default>
    GlobalDownload 0 #total speed download for all clients
                        # o -> bytes k -> kilo bytes m -> mega bytes
    GlobalUpload 0 #total speed download for all clients (0 for
unlimited)
    Download 0 #limit speed download for each connection
    Upload 0 #unlimit speed upload for each connection
    StayAtHome true #limit client to his home
    VirtualChroot true #fake a chroot to the home account
    LimitConnection 50 #max connection for the server sftp
    LimitConnectionByUser 50 #max connection for the account
    LimitConnectionByIP 2 #max connection by ip for the account
#ey Home /home/$USER #override home of the user but if you want
you can use
                        # environment variable (ie: Home /home/$USER)
    IdleTimeOut 5m #(in second) disconnect client is idle too long time
    ResolveIP true #resolve ip to dns
# IgnoreHidden true #treat all hidden files as if they don't
exist
# DirFakeUser true #Hide real file/directory owner (just change
displayed permissions)
# DirFakeGroup true #Hide real file/directory group (just change
displayed permissions)
# DirFakeMode 0400 #Hide real file/directory rights (just change
```

```
displayed permissions)
        #Add execution right for directory if read right is set
    HideNoAccess      true      #Hide file/directory which user has no
access
#   MaxOpenFilesForUser 20 #limit user to open x files on same time
#   MaxWriteFilesForUser 10 #limit user to x upload on same time
#   MaxReadFilesForUser 10 #limit user to x download on same time
    DefaultRights     0640 0750 #Set default rights for new file and new
directory
#   MinimumRights      0400 0700 #Set minimum rights for files and dirs

    ShowLinksAsLinks  false #show links as their destinations
#   ConnectionMaxLife  1d #limits connection lifetime to 1 day

#   Charset            "ISO-8859-15" #set charset of computer
#EY
    Shell              /opt/yce/bin/cpsh.pl
    Home               /var/opt/shared/
</Default>

<User ycycle>
    Shell              /opt/yce/bin/cpsh.pl
    Home               /var/opt/shared/
    VirtualChroot      true
    ResolveIP          false
    IgnoreHidden       true
    ShowLinksAsLinks  false
</User>

#Rules only for group ftp
#<Group ftp>
#   Download           25 k/s
#   LogFile            /var/log/sftp-server_ftp.log #Change logfile
#   ExpireDate         "2007-02-28 18:31:01"
#</Group>

#<Group sftp_administrator>
#   IsAdmin            true #can admin the server
#   VirtualChroot      false #you must disable chroot to have a full
support of admin
#   StayAtHome         true
#   IdleTimeOut        0
#</Group>

#<Group old_client>
#   SftpProtocol        3 #force protocol SFTP
#   DisableAccount     true #disable account
#</Group>

#Rules only for group ftpnolimit
#<Group ftpnolimit>
```

```
# Download 0 #0 = unlimited
# IdleTimeout 0 #no timeout
# DirFakeUser false #show real user on file/directory
# DirFakeGroup false #show real group on file/directory
# DirFakeMode 0 #show real rights on file/directory
# MaxReadFilesForUser 0 #0 = unlimited but still have the restriction
MaxOpenFilesForUser
#</Group>

#<IpRange 192.168.0.1-192.168.0.5>
# ByPassGlobalDownload true #bypass GlobalDownload restriction
# ByPassGlobalUpload true #bypass GlobalUpload restriction
# Download 0
# DisableAccount false #enable account
# IdleTimeout 0 #disable timeout
# LimitConnectionByIP 0 #no limit
#</IpRange>

#<Group trusted_users>
# Shell /bin/tcsh #give a shell access to TRUSTED clients !!!
#</Group>

#<VirtualHost *:22>
# DirFakeUser false #show real user on file/directory
# DirFakeGroup false #show real group on file/directory
# DirFakeMode 0 #show real rights on file/directory
# HideNoAccess false
# IgnoreHidden false
#</VirtualHost>

#Include /etc/my_sftp_config_file #include this valid configuration file
```

/etc/systemd/system/chronyd.service.d/yce

```
[Service]
PrivateTmp=no
```

MySQL

copy the [mysql_10.3.tgz](#) to the system

```
systemctl stop mariadb.service
rm -rf /var/opt/mysql
tar xzpf mysql_10.3.tgz -C /var/opt
chown -R yce:nms /var/opt/mysql
```

net_setup & yce_setup

```
sudo /opt/yce/system/net_setup.pl  
  
/opt/yce/system/yce_setup.pl
```

Service activation

```
sudo systemctl enable postfix  
sudo systemctl enable yce_psmon  
sudo systemctl enable sshd  
sudo systemctl enable syslog-ng  
sudo systemctl enable rpcbind  
sudo systemctl enable rpcbind.socket  
sudo systemctl enable snmpd  
sudo systemctl disable firewalld  
sudo systemctl start postfix  
sudo systemctl start yce_psmon  
sudo systemctl start sshd  
sudo systemctl start syslog-ng  
sudo systemctl start rpcbind  
sudo systemctl start rpcbind.socket  
sudo systemctl start snmpd
```

Mysql repair

```
/opt/yce/system/mysql_repair.sh
```

Verify mysql is running else execute again.

Install yce_patches

```
cd /opt/yce/system  
./patch_install.pl
```

csv_api.ini optional

```
wget  
https://wiki.netyce.com/lib/exe/fetch.php/maintenance:downloads:system_updates:csv_api.ini -O /opt/yce/etc/csv_api.ini
```

cleanup, if needed

```
rm /opt/yce/etc/ignore_*
```

reboot

```
sudo reboot
```

From:
<https://yce-wiki.netyce.com/> - Yce-Wiki version 7

Permanent link:
https://yce-wiki.netyce.com/doku.php/maintenance:general:installing_netyce_on_rhel7

Last update: **2021/04/13 13:54**

