
Deployment experiences with EL9 at MWT2

Farnaz Golnaraghi, Lincoln Bryant, Fengping Hu
David Jordan, Judith Stephen

US ATLAS Computing Facilities Face-to-Face meeting
SLAC National Accelerator Laboratory
12/01/2022



MANIAC LAB



ENRICO FERMI
INSTITUTE

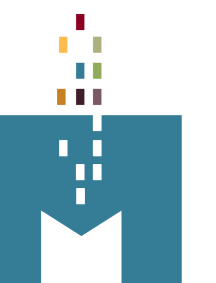


Motivation

- CentOS 7 is the predominant OS in MWT2.
 - CentOS 7 reaches its End of Lifetime in 2024.
 - CentOS-Stream 8 End of Lifetime is also 2024.
- ➔ MWT2-UC plans to upgrade from CentOS 7 to some flavor of EL9 in the near future.

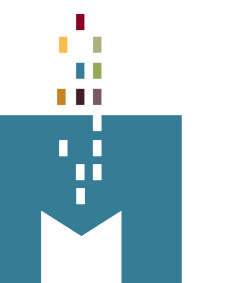
End of Lifetime (EOL) Dates		
	CentOS Linux 7	CentOS Stream 8
Full Updates ¹	2020-08-06	2024-05-31
Maintenance Updates ²	2024-06-30	2024-05-31

<https://wiki.centos.org/About/Product>



Outline

- Installation via Cobbler:
 - Cobbler changes from 2.x to 3.x
 - Cobbler support for EL9
- Changes in EL9:
 - Security
 - Networking



Installation via Cobbler

- Cobbler is a Linux installation server.
- Decided to install CentOS-Stream 9 via Cobbler on a number of machines as a test run.
- Our current Cobbler version is 2.8.5 which runs on our bootstrap server with CentOS 7.
- When attempting to install CentOS-Stream 9 via Cobbler 2.8.5 we faced the following problems:
 - The boot options such as `ks`, `ksendmac`, and `lang` are deprecated in EL9.
 - Any boot option specific to installation must start with `inst.`.

- Boot options are hard-coded in Cobbler.

➔ Cobbler 3.x needed for updated boot options.

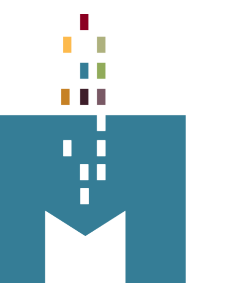
- Cobbler 3.x official rpm is available for EL8 and EL9.



<https://cobbler.github.io>

```
[ 256.390867] dracut-initqueue[1592]: Warning: ##### Anaconda installer errors begin #####
[ 256.393257] dracut-initqueue[1592]: Warning: #
[ 256.396237] dracut-initqueue[1592]: Warning: It seems that the boot has failed. Possible causes include
[ 256.399091] dracut-initqueue[1592]: Warning: missing inst.stage2 or inst.repo boot parameters on the
[ 256.401941] dracut-initqueue[1592]: Warning: kernel cmdline. Please verify that you have specified
[ 256.402058] dracut-initqueue[1592]: Warning: inst.stage2 or inst.repo.
[ 256.404989] dracut-initqueue[1592]: Warning: Please also note that the 'inst.' prefix is now mandatory.
[ 256.407949] dracut-initqueue[1592]: Warning: #
[ 256.410762] dracut-initqueue[1592]: Warning: #### Installer errors encountered during boot: ####
[ 256.410916] dracut-initqueue[1592]: Warning: #
[ 256.413389] dracut-initqueue[1592]: Warning: 'lang' is deprecated and has been removed.
[ 256.416217] dracut-initqueue[1592]: Warning: All usage of Anaconda boot arguments without 'inst.' prefix was removed. Please use inst.lang instead.
[ 256.418957] dracut-initqueue[1592]: Warning: 'ks' is deprecated and has been removed.
[ 256.421698] dracut-initqueue[1592]: Warning: All usage of Anaconda boot arguments without 'inst.' prefix was removed. Please use inst.ks instead.
[ 256.421920] dracut-initqueue[1592]: Warning: 'ksendmac' is deprecated and has been removed.
[ 256.424551] dracut-initqueue[1592]: Warning: All usage of Anaconda boot arguments without 'inst.' prefix was removed. Please use inst.ks.sendmac instead.
[ 256.427383] dracut-initqueue[1592]: Warning: #
[ 256.429672] dracut-initqueue[1592]: Warning: ##### Anaconda installer errors end #####
```

➔ You need at least EL8 to get EL9 installed because Cobbler needs EL8+



Changes from Cobbler 2.x to Cobbler 3.x

- **kickstarts** (/var/lib/cobbler/kickstarts) → **templates** (/var/lib/cobbler/templates)
- **ks_mirror** (/var/www/cobbler/ks_mirror) → **distro_mirror** (/var/www/cobbler/distro_mirror)
- **config** (/var/lib/cobbler/config) → **collections** (/var/lib/cobbler/collections)
- `kickstart` argument for profiles (i.e., distribution + additional specialized options) is now called `autoinstall`.
- If migrating from an older Cobbler to 3.x, there are scripts available under `/usr/share/cobbler/bin` to transfer your data and settings:

```
[root@bootstrap-el8-test bin]# ls  
migrate-data-v2-to-v3.py  migrate-settings.sh  settings-migration-v1-to-v2.sh
```



Cobbler 3.3.x and EL9 support

- Latest Cobbler rpm: 3.3.3.
 - Needs patches to support EL9 (<https://github.com/cobbler/cobbler/issues/3068>).
- `tftpgen.py` (generates files provided by TFTP server) uses `kssendmac` for boot options.
- `sample.ks` (sample kickstart file) uses `install` which is deprecated and not needed anymore.
- The patches are available on Cobbler's Github.
 - Will be included in Cobbler 3.4.
- **Boot-loaders** might be missing from `/var/lib/cobbler/loaders` and **pxeboot would hang** (<https://github.com/cobbler/cobbler/issues/2844>).
 - Copy them from `syslinux (/usr/share/syslinux {ldlinux.c32, libcom32.c32, libutil.c32, menu.c32, pxelinux.0})` to `/var/lib/cobbler/loaders`.
- Run `cobbler sync`.

```
autoinstall_templates/sample.ks
@@ -34,8 +34,6 @@ selinux --disabled
34 34 skipx
35 35 # System timezone
36 36 timezone America/New_York
37 - # Install OS instead of upgrade
38 - install
39 37 # Clear the Master Boot Record
40 38 zerombr
41 39 # Allow anaconda to partition the system as needed

cobbler/tftpgen.py
@@ -1022,7 +1022,7 @@ def build_kernel_options(
1022 1022
1023 1023         if distro.breed is None or distro.breed == "redhat":
1024 1024
1025 -         append_line += " kssendmac"
1025 +         append_line += " inst.kssendmac"
```

<https://github.com/cobbler/cobbler/commit/2dd4f3386817c771cef81a0613ee224b6650164e>



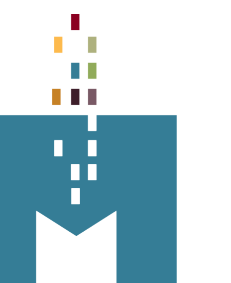
Security changes in EL9

- SCP protocol is deprecated, and now is replaced by SSH file transfer protocol (SFTP).
 - SCP Protocol is decades old, has known security issues, and is not readily fixed.
 - The API is still available.
 - One of the differences between SCP and SFTP protocol is the expansion of **~-based** path processing.
 - Not supported in earlier versions of OpenSSH (<8.7).
 - Copying folders from a new version of RHEL to an old one is going to fail if `~` path processing is used. In such cases, the recommended fix is to provide absolute paths.
 - Usage of SCP protocol can be restored by adding a **-O** option.
- SSH root login with password is disabled by default.
 - Can be restored by adding `PermitRootLogin yes` to `sshd_config`



iptables deprecation

- `iptables-nft` packages are deprecated, but still supported.
- Using `iptables`, `ip6tables`, `ipset` will result in the following warnings in the logs:
 - Warning: `<module_name>` - this driver is not recommended for new deployments. It continues to be supported in this RHEL release, but it is likely to be removed in the next major release. Driver updates and fixes will be limited to critical issues. Please contact Red Hat Support for additional information.
- Resolution: Use `nftables` package to manage firewall rules.



SHA-1 deprecation

- Official packages are not affected as they are signed by SHA-256.
 - Third party packages might be affected.
 - Dell packages are affected.
 - IGTF CAs are affected.

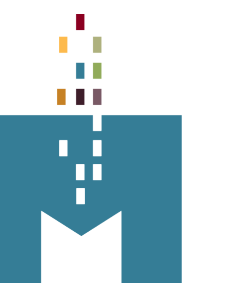
```
warning: Signature not supported. Hash algorithm SHA1 not available.  
error: /tmp/GPG-KEY-2091818-zegPJh: key 1 import failed.  
GPG-KEY import failed.
```

- Crypto policy can be set to DEFAULT:SHA1 or legacy, if SHA-1 signed package is needed.

```
# update-crypto-policies --set DEFAULT:SHA1
```

```
# update-crypto-policies --set LEGACY
```

- If using `ssh-rsa` keys:
 - ssh from EL9 to EL7 will fail since ssh-rsa uses SHA-1.



Networking

- network-scripts is removed in EL9.
 - The package was deprecated in EL8.
- **ifcfg** files (`/etc/sysconfig/network-scripts`) are no longer the primary storage for network configuration.
- By default, NetworkManager stores the network configuration files in `/etc/NetworkManager/system-connections` in a **key-file format**.

ifcfg-rh format

```
DEVICE=eno1.3606
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.170.231.52
NETMASK=255.255.255.192
GATEWAY=192.170.231.1
USERCTL=no
VLAN=yes
DNS1=128.135.247.50
DNS2=128.135.249.50
MTU=9000
IPV6INIT=yes
NETWORKING_IPV6=yes
IPV6_AUTOCONF=no
IPV6_DEFAULTGW=2605:9a00:10:200b::1
IPV6ADDR=2605:9a00:10:200b:266e:96ff:fe02:b600
```

key-file format

```
[connection]
id=eno1.3606
uuid=4165f457-0452-087b-0835-1dbdb3f02bbd
type=vlan

[ethernet]
mtu=9000
mac-address=24:6E:96:02:B6:00

[vlan]
flags=1
id=3606
parent=eno1

[ipv4]
address1=192.170.231.52/26,192.170.231.1
dns=128.135.247.50;128.135.249.50;
method=manual

[ipv6]
address1=2605:9a00:10:200b:266e:96ff:fe02:b600/64,2605:9a00:10:200b::1
method=manual

[proxy]
```

- The net-tools package which includes `ifconfig`, `netstat`, `route`, etc. is still available for EL9.

Methods to configure network

- nmcli API.
- Edit files directly under `/etc/NetworkManager/system-connections`.
- Write into `/etc/sysconfig/network-scripts` (ifcfg-rh).

nmcli examples

- Add a new ethernet connection:

```
nmcli connection add con-name eno1 ifname eno1 type ethernet ipv4.addresses 192.168.131.52
ipv4.method manual connection.autoconnect yes ethernet.mtu 9000 ipv4.never-default no mac
24:6E:96:02:B6:00
```

- Modify a connection: `nmcli connection modify eno1 ipv4.addresses 192.168.131.40`

- Get the status of interfaces: `nmcli dev status`

```
[[root@river-s022 ~]# nmcli dev status
DEVICE    TYPE    STATE    CONNECTION
eno1.3606  vlan    connected eno1.3606
eno1      ethernet connected eno1
eno3      ethernet connected eno3
tunl0     iptunnel disconnected --
eno2      ethernet unavailable --
eno4      ethernet unavailable --
lo        loopback unmanaged  --
```

- List all connections: `nmcli connection show`

```
[[root@river-s022 ~]# nmcli connection show
NAME      UUID                                  TYPE    DEVICE
eno1.3606 27d18546-a4ee-4755-9982-e8a2b4bc3a20  vlan    eno1.3606
eno1      43a5b0dd-0dda-4274-b367-0826da3099f4  ethernet eno1
eno3      09b7f8b8-67f5-48c6-b115-082f2f981246  ethernet eno3
eno2      817b4111-afca-4789-8083-8461928b0bc6  ethernet --
eno4      4853824f-175a-4795-bc64-b90a1b2a6f25  ethernet --
```

- Activate and deactivate a connection: `nmcli connection up/down <connection name>`

```
[[root@river-s022 ~]# nmcli connection up eno3
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/6)
[[root@river-s022 ~]# nmcli connection down eno3
Connection 'eno3' successfully deactivated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/6)
```

Editing key-files directly

- Edit key-files under `/etc/NetworkManager/system-connections:`

```
[connection]
id=en01.3606
uuid=4165f457-0452-087b-0835-1dbdb3f02bbd
type=vlan

[ethernet]
mtu=9000
mac-address=24:6E:96:02:B6:00

[vlan]
flags=1
id=3606
parent=en01

[ipv4]
address1=192.170.231.52/26,192.170.231.1
dns=128.135.247.50;128.135.249.50;
method=manual

[ipv6]
address1=2605:9a00:10:200b:266e:96ff:fe02:b600/64,2605:9a00:10:200b::1
method=manual

[proxy]
```

- Tell NetworkManager to reread the configuration files:

```
nmcli connection reload
```


Using ifcfg scripts

- **ifcfg** scripts can still be used.
- **/etc/NetworkManager/NetworkManager.cfg** contains a line to accept ifcfg files.
 - **plugins=keyfile,ifcfg-rh.**
- Configure network by setting up ifcfg files and restarting NetworkManager.
 - `ifup`, `ifdown` will not work.
 - Use `nmcli connection down/up [connection name]`.
- If there are two files, one under `system-connections` and under `network-scripts` for the same interface, `nmcli` will write into the one in **system-connections**.

Support for EL9

- puppet → Supported
- ganglia → Not supported yet
- HEPOSLibs → Supported
- OSG → Packages will be available for testing in 2 months.
- K8S → EL7 is the latest they support (?!)
- dcache/java → Supported

Conclusions

- EL9 can be installed via Cobbler with a few minor patches. The patches will be officially included in Cobbler 3.4 release.
- SHA-1 is deprecated and third party packages using SHA-1 will be affected.
- NetworkManager uses the key-file format by default to store the network configurations. The ifcfg files can still be used.
- We plan to upgrade from EL7 to some flavor of EL9 based on the community preference and needs in the near future.