DDS Operating System Administration

The Deployable Defensive System (DDS) is a modular fly-away computing cluster that is purpose-built for conducting Defensive Cyber Operations (DCO) missions. This kit provides a platform with hardware and software for the US Army and its DoD mission partners.

Operating system administration

System administration is based upon Red Hat Enterprise Linux (RHEL), a lightweight, enterprise-supported Linux Operating System (OS) developed by Red Hat. This OS gives users the flexibility of the Linux environment while also maintaining a level of support, security, and stability for production purposes.

Common administration commands

When using RHEL, there are many commands, concepts, and tools to familiarize yourself with as operators. These commands will be common across RHEL and RHVH Operating Systems. However, other distributions of Linux may vary. Within this section, we've created a cheat sheet of commands related to common administration tasks operators may need to perform.

Common CLI commands

Command	Use
`ssh [ip or hostname]`	Secure shell, an encrypted network protocol allowing for remote login and command execution.
`sudo [command] Sudo –s`	Run a command with root permissions. Switch to root user mode
`pwd`	Print working directory
`whoami`	Displays the logged in user id
`cd /cd [target]`	Change the directory to "target" directory
`cd /cure/ansible_main`	Change the directory to the root of the filesystem
`Ls`	View list of files in directory
`Clear`	Clears the terminal screen
`cat [filename] cat passwords.yml`	Displays the contents of filename to standard out
`cp [source_file] [target file]`	Copies a specific file to a target location
`mkdir my_directory`	Create a directory "my_directory"
`rm mymistake.txt`	Removes a file 'mymistake.txt'
`mv [source_file] [target_file]`	Move a file or directory

Command	Use
`ip a` `ip -4 a`	View network interface information. View only network interfaces with IPV4 address
`ifup [nic]` `ifup p1p1` `ifdown p1p1`	Turn on specified network interface card, Turn on Sonnet Thunderbolt, Turn off Sonnet Thunderbolt
`find . -name [file]`	Find file or directory by name
`subscription-manager [command]`	Red Hat Subscription Manager use -help for list of commands
`systemctl start name.service`	Start a service
`systemctl stop name.service`	Stop a service
`systemctl enable name.service`	Enable service (persists reboots)
`systemctl disable name.service`	Disable service (persists reboots)
`systemctl shutdown`	System shutdown
`systemctl restart`	System restart

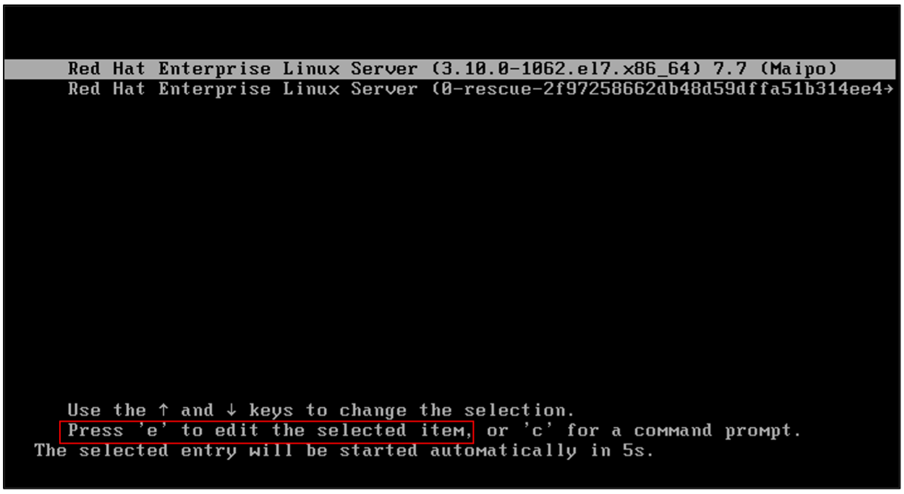
User management

User and password management is critical for maintaining kit operations and access to all infrastructure, services, and tools. Passwords for all infrastructure and services deployed by automation are stored in **/opt/test/ansible_main/passwords.yml**. The majority of users should be managed within **IdM** to enable authentication across the cluster. Operators should not change local user passwords or application passwords unless necessary; they are randomly generated upon install. However, the loss of a root password requires a specific set of tasks to recover.

Reset root password

If the root password is known, simply login as root and use the `passwd` command to enter a new root password. However if the root password is lost, create a new one by doing the following:

1. Reboot or power on the system and press `‘e’` to edit the installed OS bootloader, (1st boot option), when the boot menu displays



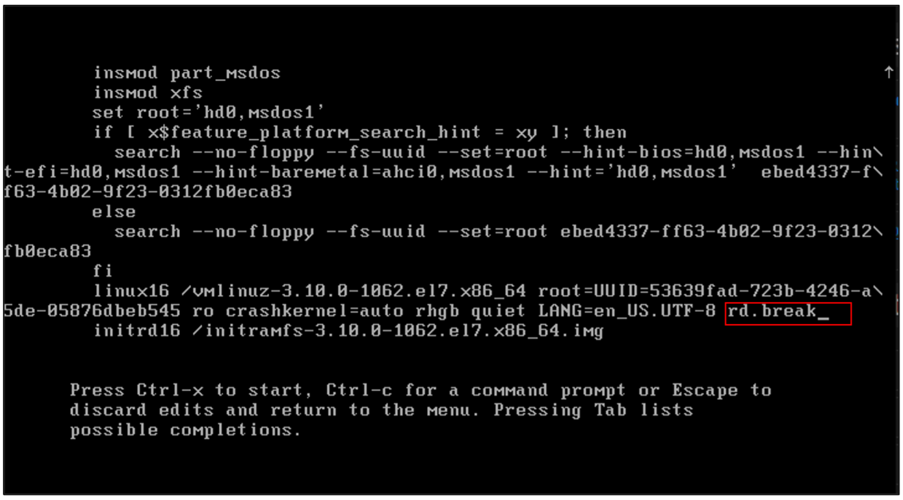
```
    Red Hat Enterprise Linux Server (3.10.0-1062.el7.x86_64) 7.7 (Maipo)
    Red Hat Enterprise Linux Server (0-rescue-2f97258662db48d59dffa51b314ee4→




    Use the ↑ and ↓ keys to change the selection.
    Press 'e' to edit the selected item, or 'c' for a command prompt.
  The selected entry will be started automatically in 5s.
```

RHEL Boot Selector

2. Towards the bottom of the page, locate the grub options (indicated by the `'linux16 /vmlinuz-\<kernel>'` precursor) and add the `rd.break` option to the end of the line. This will allow edits to the initial ramdisk (`initrd`) environment.



```
      insmod part_msdos
      insmod xfs
      set root='hd0,msdos1'
      if [ x$feature_platform_search_hint = xy ]; then
        search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hin\
t-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 --hint='hd0,msdos1'  ebed4337-f\
f63-4b02-9f23-0312fb0eca83
      else
        search --no-floppy --fs-uuid --set=root ebed4337-ff63-4b02-9f23-0312\
fb0eca83
      fi
      linux16 /vmlinuz-3.10.0-1062.el7.x86_64 root=UUID=53639fad-723b-4246-a\
5de-05876dbeb545 ro crashkernel=auto rhgb quiet LANG=en_US.UTF-8 rd.break_
      initrd16 /initramfs-3.10.0-1062.el7.x86_64.img


     Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
     discard edits and return to the menu. Pressing Tab lists
     possible completions.
```

RHEL Edit Boot Options

3. Press **Ctrl-x** to boot with the option you added, allowing access to a root shell within `initramfs`.

4. Once the shell has been accessed, remount the `/sysroot` partition with read/write permissions. (It is currently mounted with read-only permissions):

```
switch_root:/# mount -o remount,rw /sysroot
```

5. After the partition is remounted, change the root directory of the process to `/sysconfig` with the chroot command:

```
switch_root:/# chroot /sysroot
```

6. Reset the root user password.

⚠ **Do NOT reboot! The next step is vital to maintaining a working system**.

7. By default, SELinux is running and will need to be updated after the password has been created. To fix the `/etc/shadow` file, enter the following command:

```
sh-4.2# touch /.autorelabel
```

8. Finally, exit the chroot and initram shells. Login with the new root password after the host boots into RHEL.

```
sh-4.2# exit
exit
switch_root:/# exit
logout
```

Network management

Networking is a vital part of the RHEL 7.7 OS and can be configured numerous ways. The most common administrative tasks are described below.

Viewing IP address information

1. To view current network configuration, for all interfaces, use the following command:

```
[user@host ~]# ip addr
```

2. To find information regarding a specific interface, add the interface name after the command, example:

```
[user@host ~]# ip addr eth0
```

Configuring network interfaces

In RHEL, network address configuration is stored within the following directory:

```
/etc/sysconfig/network-scripts/
```

Each interface should have its own `ifcfg-<interface>` file that stores all relevant configuration persistent across reboots. After editing this file, restart the network for the changes to take effect. Below is an example file for an interface named `eth0` with a static IP address of `10.1.51.50`:

```
DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
IPADDR=10.1.51.50
NETMASK=255.255.255.0
GATEWAY=10.1.51.1
DNS1=10.1.51.10
```

✎ **Note**: the `ONBOOT=yes` option must be included if the interface should be activated after a reboot or network restart. If set to `‘no’`, the interface will not automatically display!