GETTING TO KNOW
RED HAT ENTERPRISE LINUX 7

CHRISTOPH DOERBECK
Principal Solutions Architect
cdoerbec@redhat.com
Agenda

Review new GUI installer

- Walk through decision points
- Discuss improved features

Hands-on Activities

- Installing a Webserver:
  - Package installation
  - Storage Management with SSM
  - Web Services Configuration (systemd, httpd configuration)
  - Security with SELinux & Firewalld
  - Performance Tuning with “tuned” profiles
The NEW RHEL 7 Installer

Highlights

● Fewer Questions
● Background Installation
● Support for Complex Network Configurations
● Support for Complex Storage Configurations
● Reset partitioning without rebooting

Let's examine a few screenshots...
Network
Destination
Partitioning

New Red Hat Enterprise Linux 7.0 Installation

You haven't created any mount points for your Red Hat Enterprise Linux 7.0 installation yet. You can:

- Click here to create them automatically.
- Create new mount points by clicking the +
  - Standard Partition
  - Btrfs
  - LVM
  - LVM Thin Provisioning

When you create mount points for your Red Hat Enterprise Linux 7.0 installation, you'll be able to view their details here.
Software Selection

**Base Environment**

- Minimal Install
  - Basic functionality.
- Infrastructure Server
  - Server for operating network infrastructure services.
- File and Print Server
  - File, print, and storage server for enterprises.
- Basic Web Server
  - Server for serving static and dynamic internet content.
- Virtualization Host
  - Minimal virtualization host.
- **Server with GUI**
  - Server for operating network infrastructure services, with a GUI.

**Add-Ons for Selected Environment**

- **Backup Server**
  - Software to centralize your infrastructure's backups.
- **DNS Name Server**
  - This package group allows you to run a DNS name server (BIND) on the system.
- **Directory Server**
  - Machine and user identity servers.
- **E-mail Server**
  - Allows the system to act as a SMTP and/or IMAP e-mail server.
- **FTP Server**
  - Allows the system to act as an FTP server.
- **File and Storage Server**
  - CIFS, SMB, NFS, iSCSI, iSER, and iSNS network storage server.
- **Hardware Monitoring Utilities**
  - A set of tools to monitor server hardware.
- **Identity Management Server**
  - Centralized management of users, servers and authentication policies.
- **InfiniBand Support**
  - Software designed for supporting clustering and grid connectivity using RDMA-based InfiniBand and iWARP fabrics.
Conventions

1. Don't like typing? Use the lab helper ex: lab-helper-####
2. Consult attendee portal for URL info
   SAMPLE
   Host URL: CLIENT-01
   Login: student
   Password: n0boundaries!
   ** CLIENT-02 provides jumphost option
3. Commands are in BOLD
4. Call-outs are highlighted in yellow
5. Just about everything we do will be as “root” but keep an eye on the prompt
6. Are you on the right host?
Log In via SIAB / SSH

1. CONNECTION INFORMATION
   - Host URL: CLIENT-01
   - Login: student
   - Password: n0boundaries!

2. Don't forget "sudo -i"

3. Source the Lab Helpers
   - **NOTE** **The command starts with a period** `.`
   - . helper-g2k
Install Webserver Software

1. Use "yum" to install package group
2. On occasion we will cut out the boring messages with "<...snip...>"
Configure HTTP

1. We are leveraging config file management from a local RH Satellite Server
2. This is the config file we are interested in
3. Inspect the config file

Defines DocumentRoot as: /var/www/html/example_corp
Understanding SSM

- **System Store Manager**
- **Single CLI to manage storage technologies**

**Examples:**
- Device Mapper (dm), Encryption
- Logical Volume Manager (LVM), Snapshots
- Multiple Devices (MD), RAID
- More...
Exploring SSM

1. Install SSM
2. Single Command:
   - Creates VG/Pool
   - Creates LV
   - Formats FS
   - Mounts FS

```
root# yum install -y system-storage-manager
root# ssm list volumes

Volume        Pool          Volume size  FS      FS size       Free  Type    Mount point
-------------------------------------------------------------------------
/dev/rhel_pwob-r7/swap  rhel_pwob-r7      1.00 GB                              linear
/dev/rhel_pwob-r7/root  rhel_pwob-r7      8.51 GB  xfs     8.50 GB    6.57 GB  linear  /
/dev/vda1                               500.00 MB  xfs   496.67 MB  375.54 MB  part    /boot
-------------------------------------------------------------------------

root# mkdir -p /mnt/test
root# ssm -f create --fstype ext4 /dev/vdb1 /mnt/test
Physical volume "/dev/vdb1" successfully created
Volume group "lvm_pool" successfully created

root# df /mnt/test
Filesystem                   1K-blocks  Used Available Use% Mounted on
/dev/mapper/lvm_pool-lvol001    118867  1550    108430   2% /mnt/test

root# ssm -f remove /mnt/test lvm_pool

root# pvremove /dev/vdb1
```
Setup HTML Storage with SSM

1. Create Mount Point

2. Create Mirrored Filesystem
   - size: 50MB
   - vg/lv name: webvg/html
   - raid: 1 (mirror)
   - fstype: ext4
   - devices: vdb1, vdc1
   - mount: /var/www/html

3. Restore SELinux contexts

4. Verify RAID Syn+c status

5. Add Mount to fstab
Download HTML Content

1. Change directory to `/var/www/html`
2. Retrieve HTML content from `http://sat5.example.com/pub`
3. Don't forget to unpack the tarball
Understanding Firewalld

Still IPTables underneath

Why Firewalld:

- Realtime rule changes without interruption
- Separate network traffic & rules by interface or zones
- GUI and CLI tools
- System configs in /usr/lib/firewalld/*
- Custom config in /etc/firewalld/*
Exploring Firewalld

1. Check firewalld status
2. Enable firewalld service with systemd
3. Show all firewalld services
4. Disable unwanted firewalld service
   - add `--permanent` to persist after system reboot
Secure HTTP with Firewalld

1. Enable http(s) services
   
   - `add --permanent` to persist after system reboot

2. Check enabled firewalld services

```
root# firewall-cmd --add-service http --add-service https
success

root# firewall-cmd --add-service http --add-service https --permanent
success

root# firewall-cmd --list-all
public (default, active)
   interfaces: eth0
   sources: services: http https siab ssh
   ports: masquerade: no
   forward-ports: icmp-blocks:
   rich rules:
```
Understanding SELinux

Standard Security = Discretionary Access Controls
- Owner, group, world/read, write, execute
- Enhanced with Access Control Lists (ACLs)

Security-enhanced Linux = Mandatory Access Controls
- Framework allows definition of permissions for how all processes (called subjects) interact with other parts of the system such as files, devices, sockets, ports, and other processes (called objects in SELinux).

SELinux was introduced in RHEL 4
Exploring SELinux

1. Check SELinux Status
2. Set SELinux to Enforcing
3. To set persistant SELinux mode, edit config file /etc/sysconfig/selinux

*Note*
- SELinux Mode
- SELinux Type (Policy)
Secure HTTP with SElinux

1. Check SELinux Status
   *Note* how current and persistent configuration do not match

2. Examine SELinux security contexts

3. Change security context on some files
   changing `httpd_sys_content_t` to `tmp_t`
Understanding Tuned

Tuned provides recommended configurations for common workloads

- Easy to apply
- Easy to customize
- Persists across reboots

Installed and enabled with RHEL 7

Available for RHEL 6 as well
“tuned” provides complete tuning profiles for common work-loads

Change the configured tuning profile for the system

Verify active profile

1. `tuned-adm list`
2. `tuned-adm profile throughput-performance`
3. `tuned-adm active`
Tune HTTP with Tuned

1. Change tuning profile for the system
2. Verify active profile

```
root# tuned-adm profile network-throughput

root# tuned-adm active
Current active profile: network-throughput
```
Understanding Systemd

Prior to RHEL 7, you had a SysV Init style "Upstart"

- Remember initd, innittab, rc scripts, run levels and who can forget rc.local?

Systemd replaces SysV Init

- Controls “units” rather than just daemons
- Handles dependency with service information
- Tracks processes with service information
- Services are owned by a cgroup
- Simple to configure “SLAs” based on CPU memory
- Properly kills daemons (zombies are for tv & movies, not the Enterprise)
- Minimize boot times
- Debuggability – no early boot messages are lost
- Easy to learn and backwards compatible.
Exploring Systemd

Look how much info systemd provides:

1. List configured services
2. Disable an unwanted service (postfix)

1. service status
2. active since
3. pid & ppid
4. cgroup info
5. more...

1. root# systemctl status sshd
2. systemctl -t service
3. systemctl disable postfix
4. systemctl stop postfix
Enable HTTP with Systemd

1. Use systemd to enable httpd
2. Use systemd to start httpd
3. Check httpd status

```
cgroup slice httpd.service
```

```
root# systemctl enable httpd
In -s '/usr/lib/systemd/system/httpd.service'
'/etc/systemd/system/multi-user.target.wants/httpd.service'

root# systemctl start httpd

root# systemctl status httpd
httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled)
   Active: active (running) since Fri 2014-10-24 22:48:53 EDT; 8min ago
  Process: 2577 ExecStop=/bin/kill -WINCH $MAINPID (code=exited, status=0/SUCCESS)
Main PID: 2581 (httpd)
   Status: "Total requests: 15; Current requests/sec: 0; Current traffic: 0 B/sec"
   CGroup: /system.slice/httpd.service
      └─2583 /usr/sbin/httpd -Dforeground
           └─2584 /usr/sbin/httpd -Dforeground

<...snip...>
```
Understanding CGroups

Cgroups provide Resource Management

- Manages CPU, Memory, Network and Block i/o consumption
- Reduce process contention, increase throughput and predictability

Systemd replaces SysV Init

- system.slice – contains system services
- user.slice – contains user sessions
- machine.slice – contains virtual machines and containers

Services can be promoted to their own slice if needed
Exploring CGroups

1. Broad look at cgroup configuration
2. Apply change to subsequent httpd starts
3. Apply change to current running httpd
Configure HTTP with CGroups

1. Download systemd unit file for httpd

   **Provided here by Satellite Configuration Management**

2. Inspect the unit file

   Restart=Always
   CPUShares=2048
   OOMScoreAdjust=-1000
Understanding Journald

• Does NOT replace rsyslog in RHEL 7
  Continue using rsyslog for traditional logging w/ enterprise features

• The journal is not persistent by default
• Collects event metadata
• Stored in key-value pairs
• Simple (or complex) filtering
• Indexed
• Formatted
• Message Verification – source authenticity
Exploring Journald

1. Display messages in "pager mode" starts at top of log (oldest)
2. Display messages in "pager mode" starts at end of log (newest)
3. Display messages for (unit) httpd
4. Reverse order
5. Since yesterday
Validate Webserver Setup
Use the URL provided

CONNECTION INFORMATION
Host URL: CLIENT-01 AUX

*Note*
Webpage is incomplete
All of the images are missing

Recall that we changed the security context of the files in the unpacked tarball
Revisiting SELinux

```
root# cd /var/www/html
root# restorecon -R example_corp/images
root# ls -Z example_corp/images
```

-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 banner.jpg
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 business-people.jpg
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 pic01.jpg
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 pic02.jpg
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 pic03.jpg
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 pic04.jpg
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 pic05.jpg
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 pic06.jpg
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 pic07.jpg
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 pic08.jpg
- rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 pic09.jpg
- rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 pic10.jpg

1

1. Restore SELinux Security Context
Revisiting Systemd

1. Check httpd status with systemd
2. Abruptly kill httpd processes
3. Examine httpd logs with journald

*Note*
httpd exited
httpd restarted

Now you can reload the web page
Validate Webserver Setup
Use the URL provided
QUESTIONS?