BOSTON, MA
JUNE 23-26, 2015

IKEA vs. Shellshock: 1-0

Magnus Glantz,
Product Responsible, Linux, IKEA IT

Mattias Haern,
Solution Architect, Red Hat

2015-06-24

redhat.

Reenactment
24th of September, 2014
Sweden

redhat.

Ingvar Kamprad Elmtaryd Agunnarud

redhat.

IKEA
IKEA
IKEA
IKEA
Entrance
Entrance
IKEA
Home Furnishings
IKEA
IKEA
IKEA
IKEA
IKEA
IKEA
IKEA
IKEA
IKEA
IKEA
宜家家居
IKEA
Home furnishings
ايكيا

redhat.

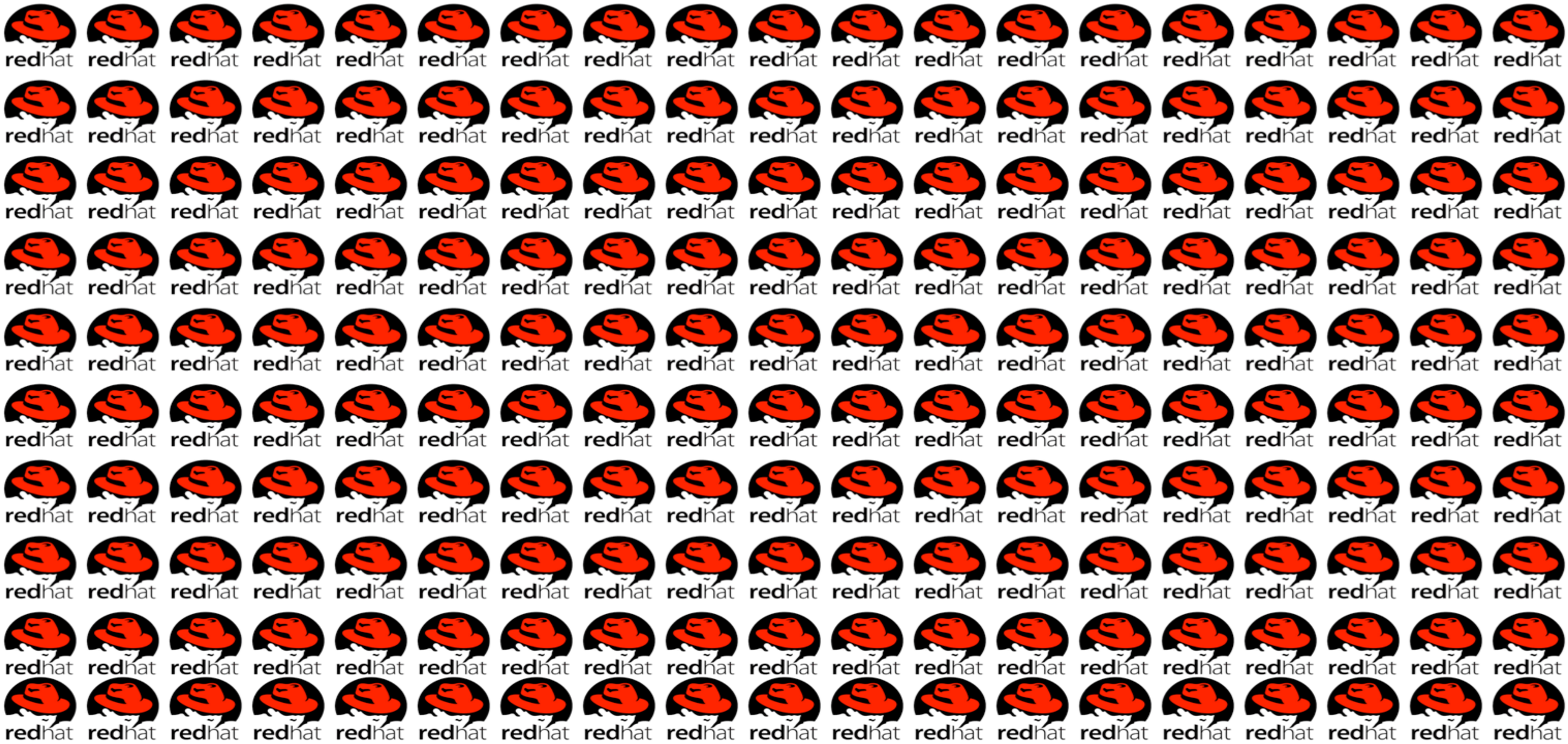
We have many Red Hat Enterprise Linux servers

I mean

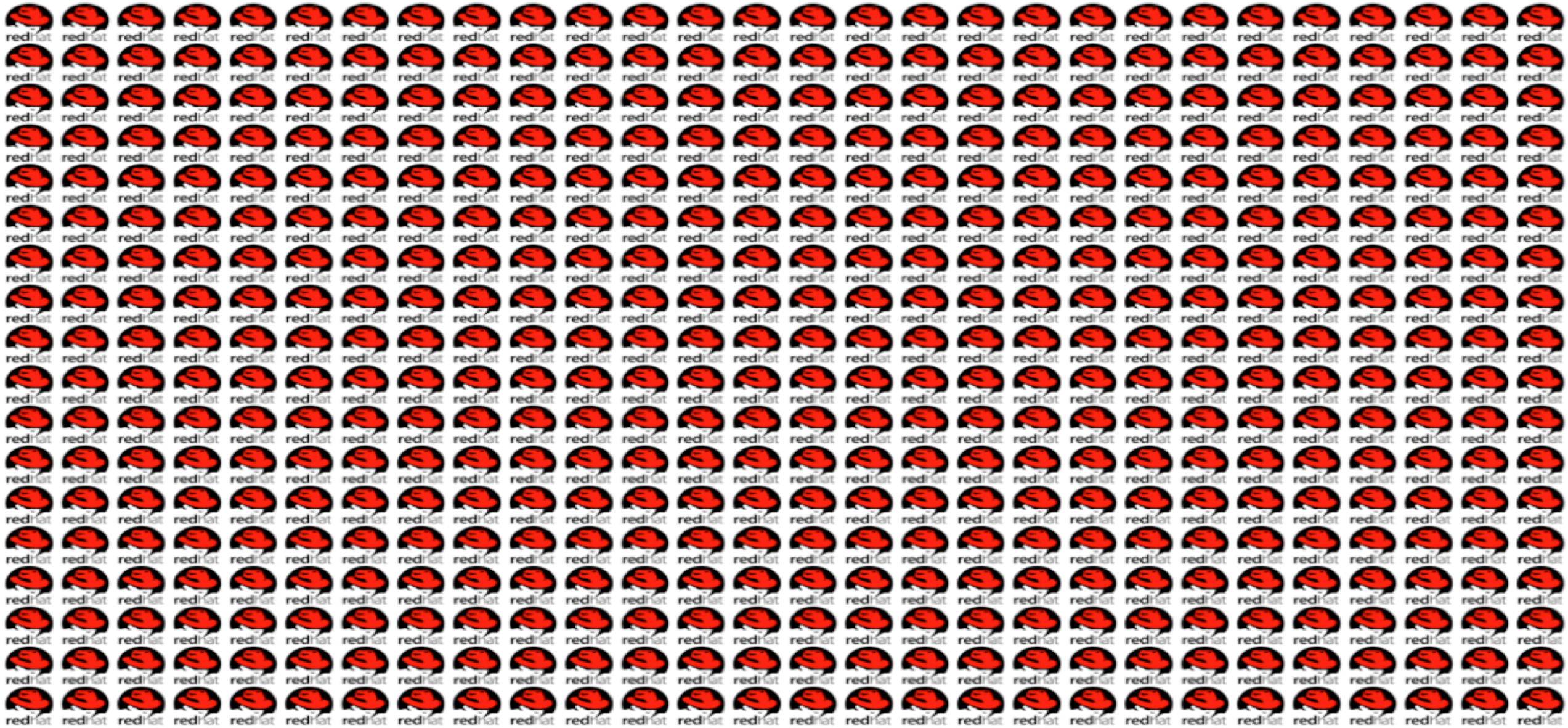
redhat.

Very

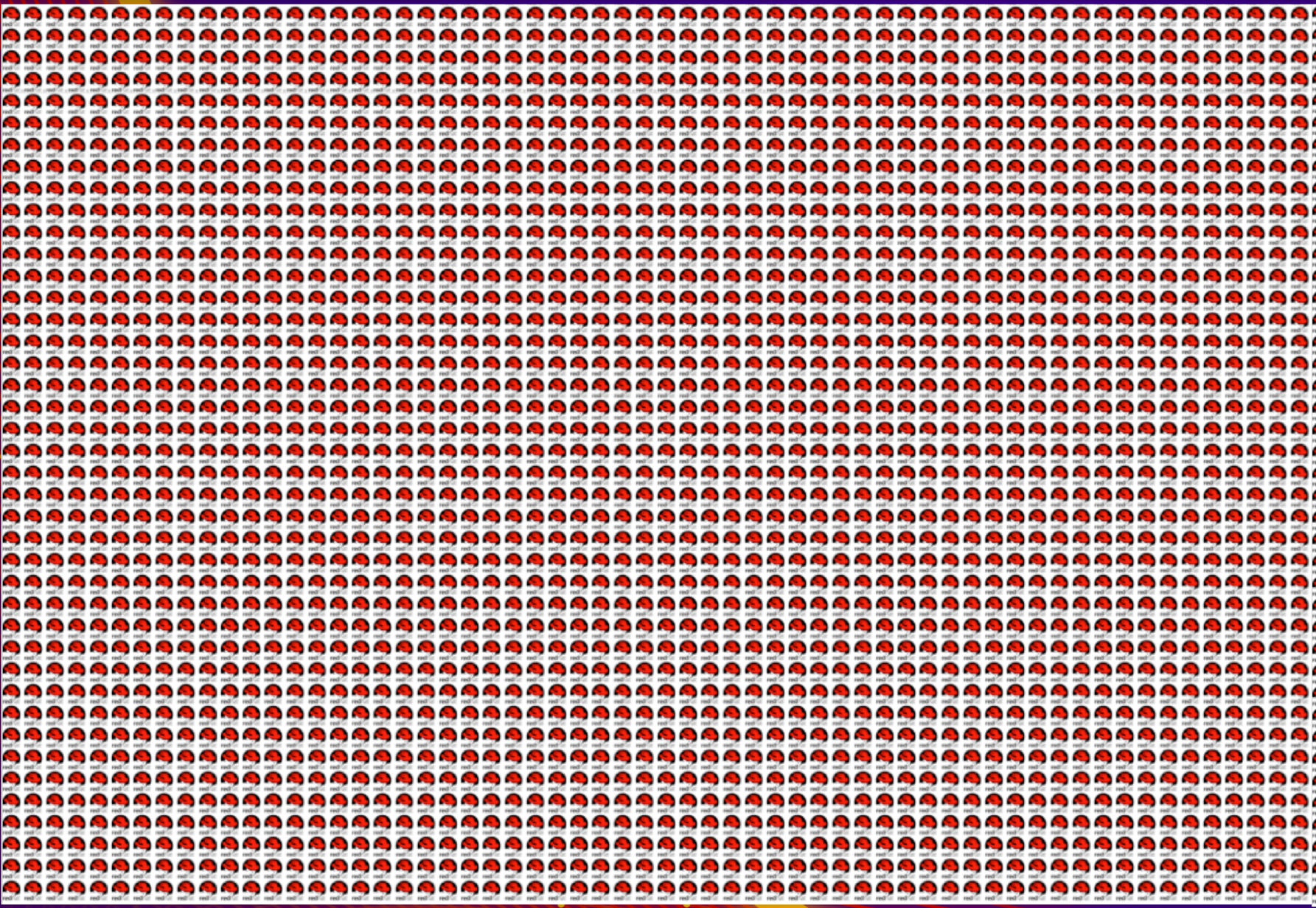
very



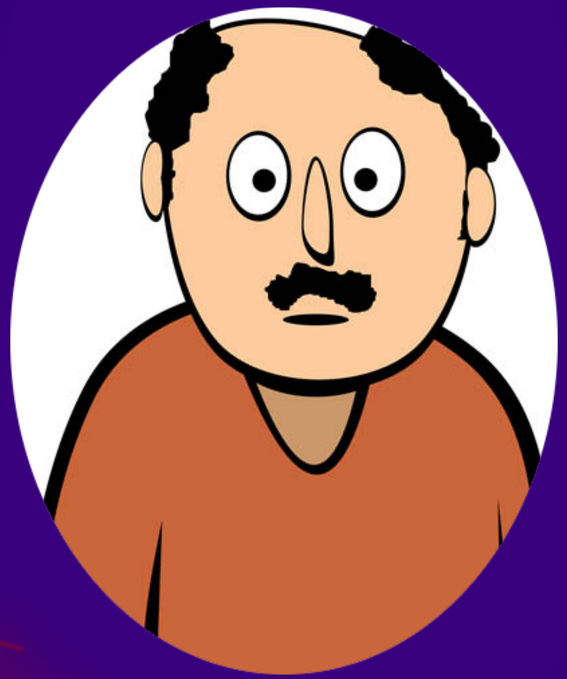
very



very many



redhat.



redhat.

..Red Hat Enterprise Linux servers.

redhat.

And this is how we patched all 3500 servers for shellshock..
..in 2 ½ hours.

redhat.

```
[me@ingvar5 ~]$ ./patch
Wed Sep 24 23:14:15 UTC 2014: Issuing 'yum -y update bash' to all servers..
Wed Sep 25 01:44:15 UTC 2014: Done.
[me@ingvar5 ~]$
```


redhat.

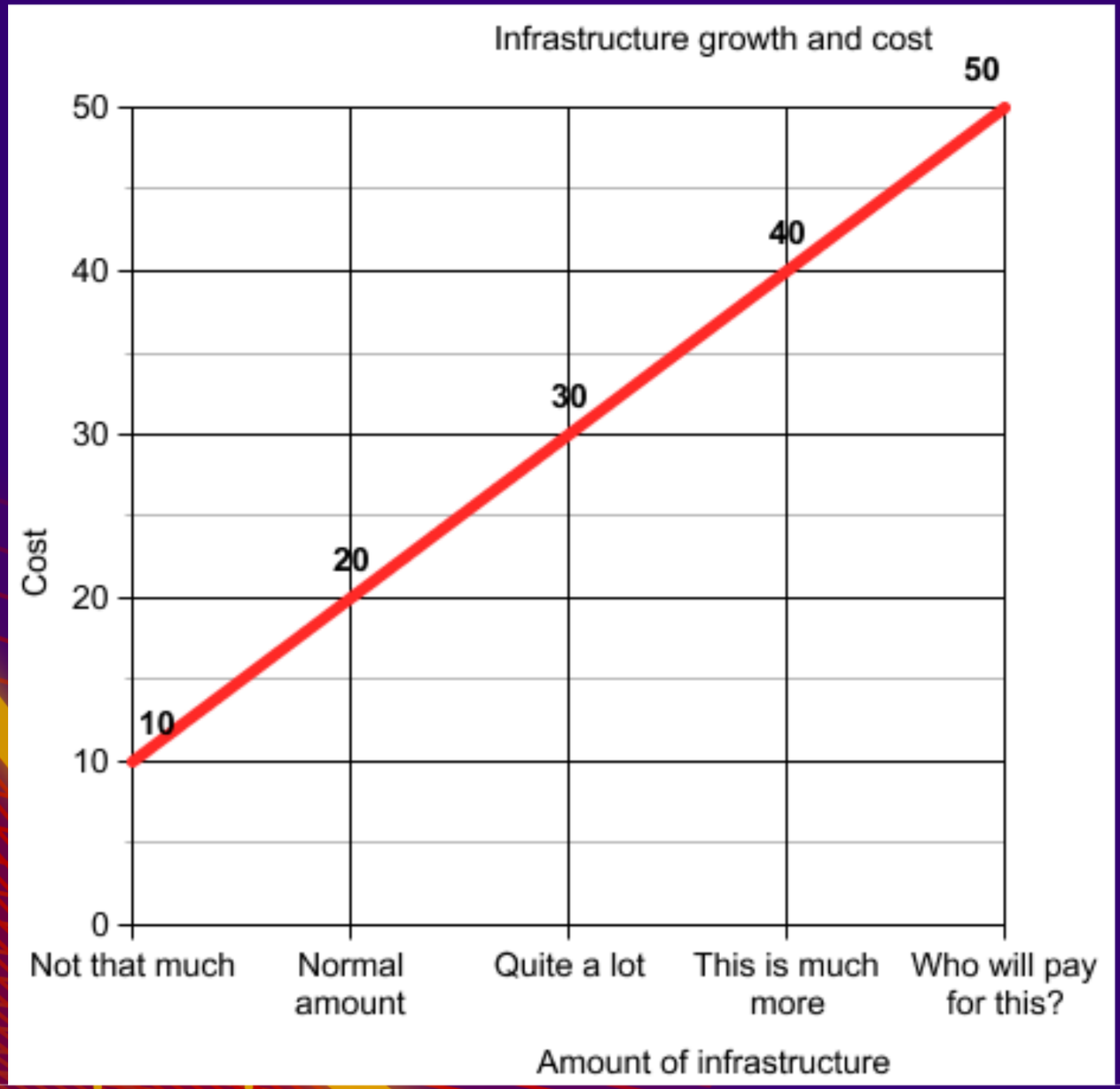
LEARN. NETWORK.
EXPERIENCE OPEN SOURCE.

redhat.

We used to run mainly old school UNIX and mainframes

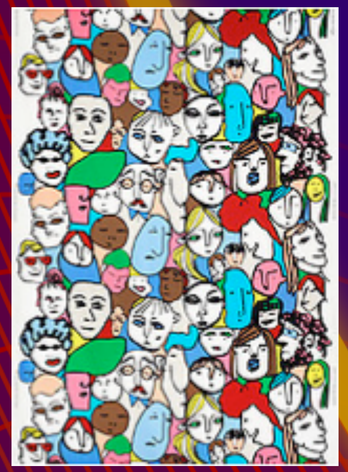
redhat.

But

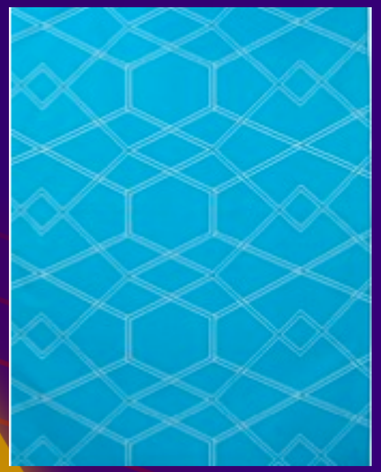

Infrastructure growth and cost
50
40
30
20
10
0
Cost
10
20
30
40
50
Not that much
Normal amount
Quite a lot
This is much more
Who will pay for this?
Amount of infrastructure

redhat.

Many different systems



ITSM



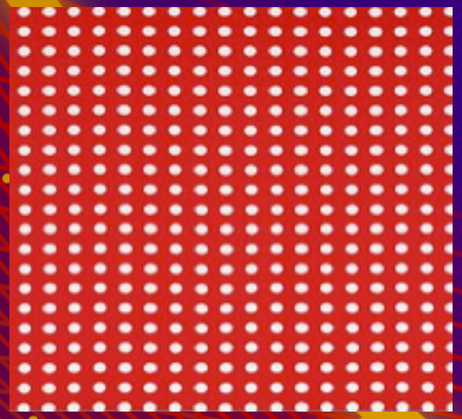
Databases

App servers

In-house

Network mgmt

Log mgmt



IP services

Integration

Directory

redhat.

On many different platforms

redhat.

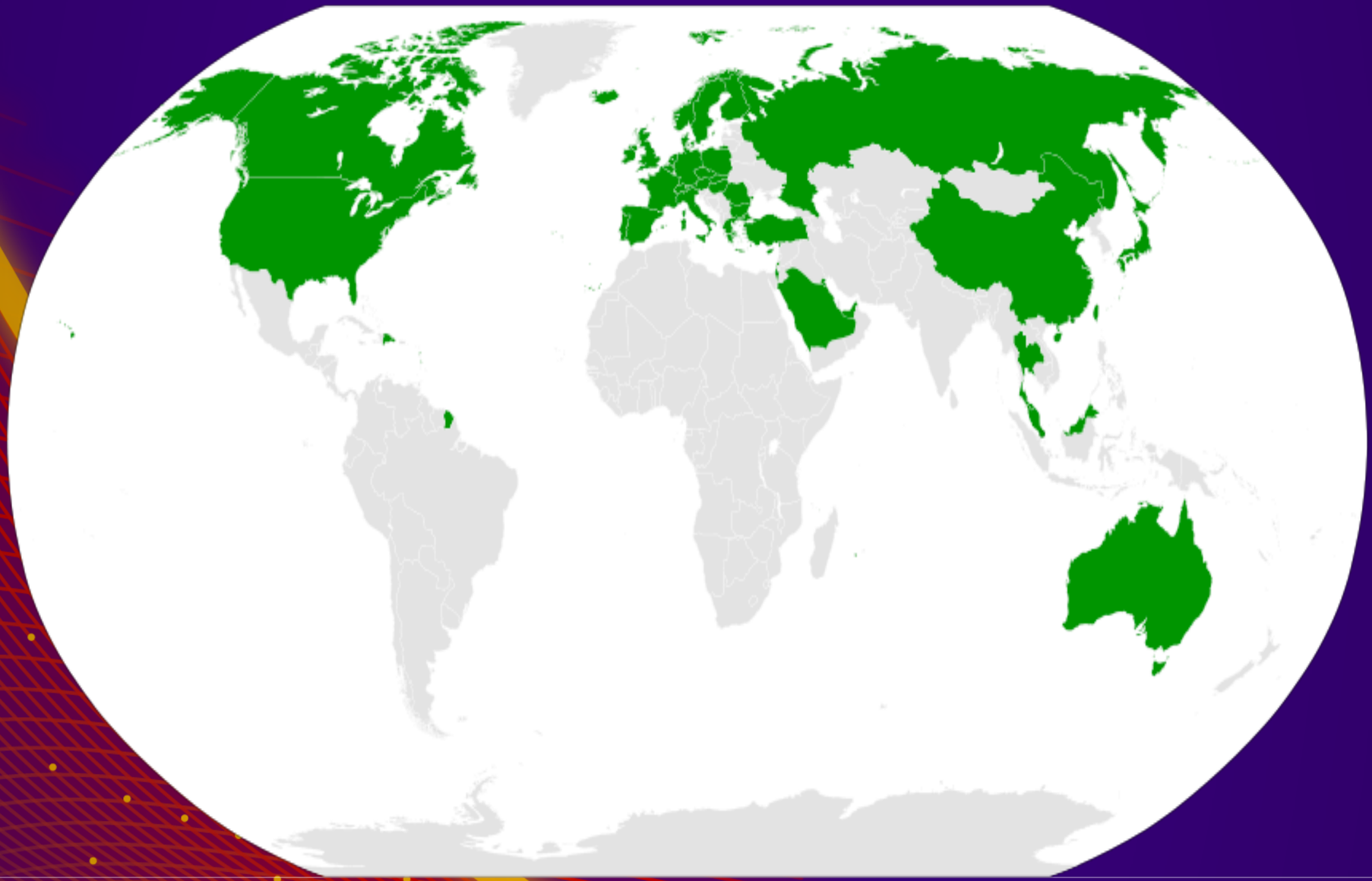
On 400+ different sites

redhat.

In 35+ different countries

redhat.

On 4 different continents

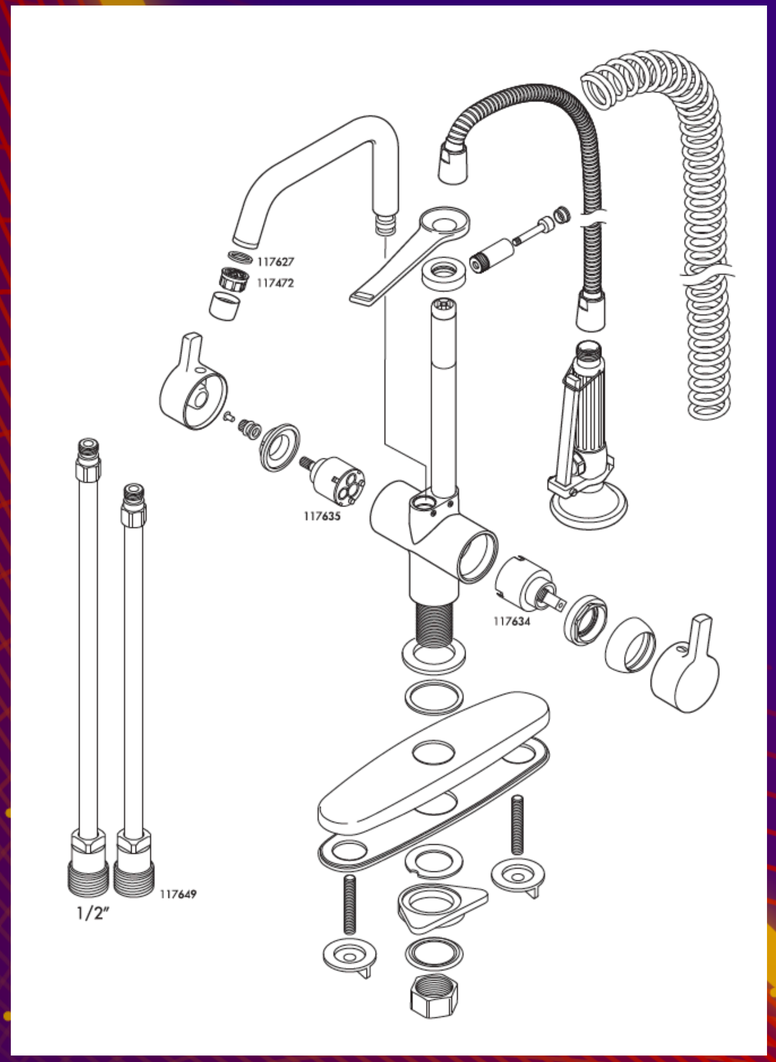


redhat.

“One does not simply” patch a server

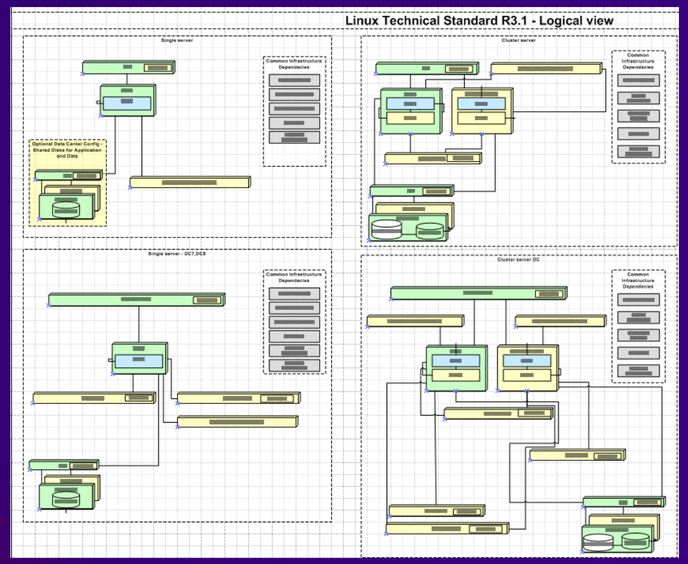
redhat.

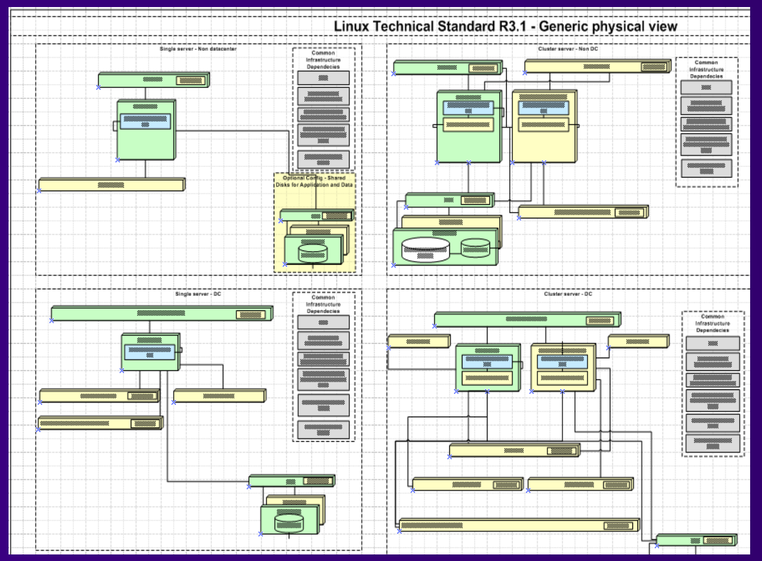
You have to create a well defined product (SOE) (..and follow some simple instructions)

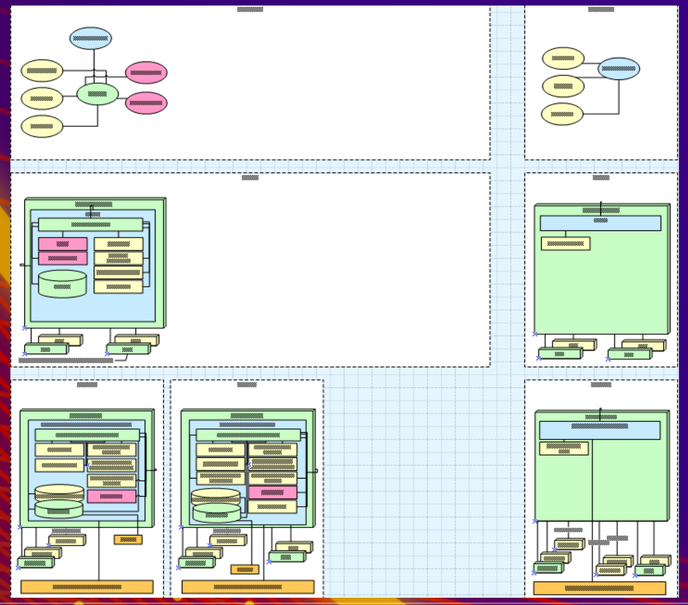


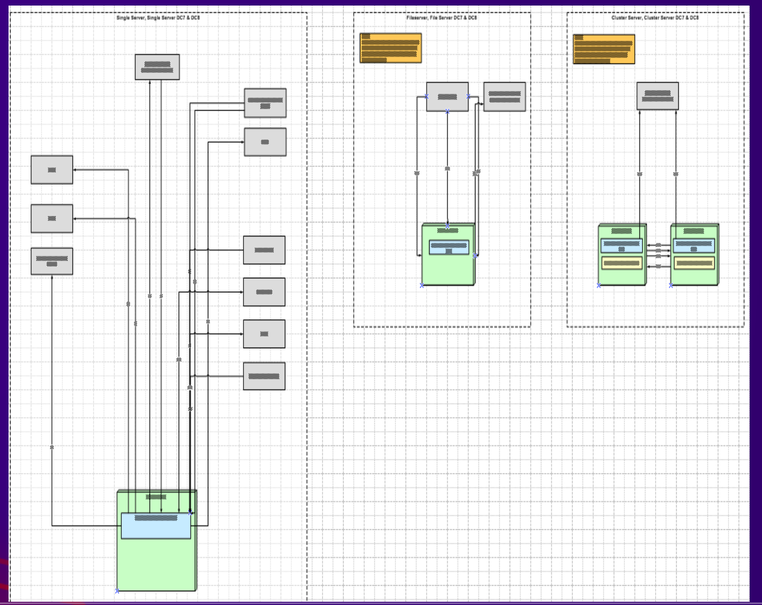
redhat.

Architectural model



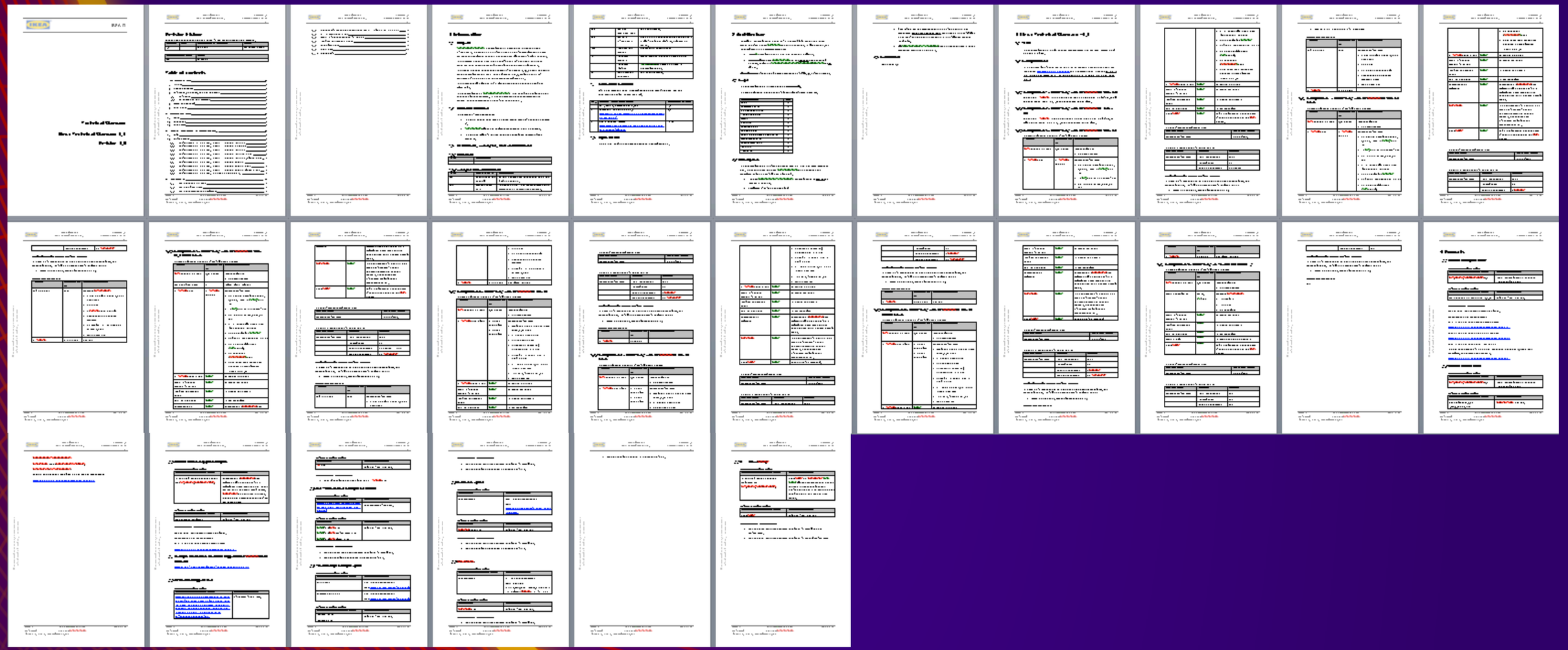






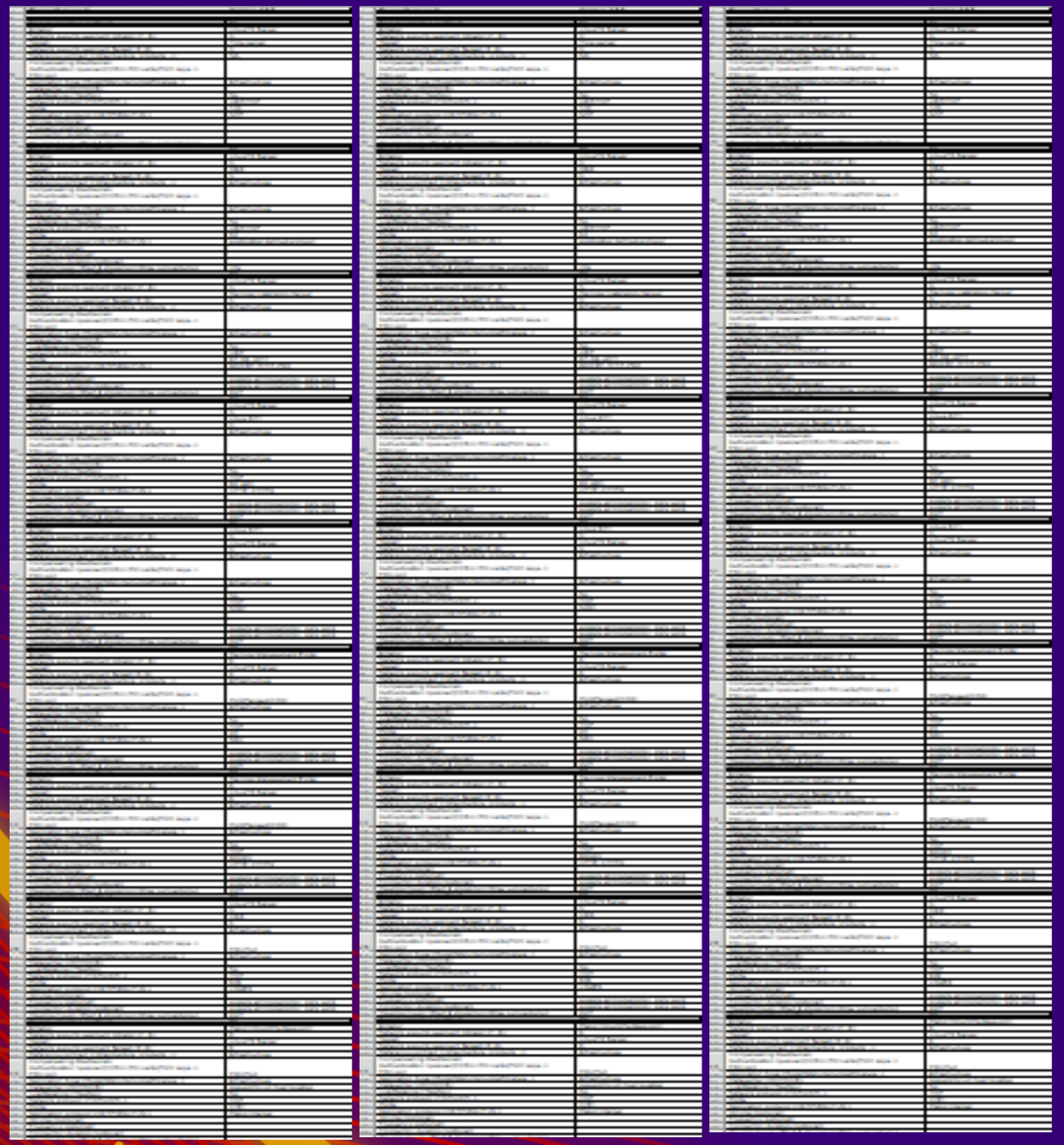
redhat.

Product description



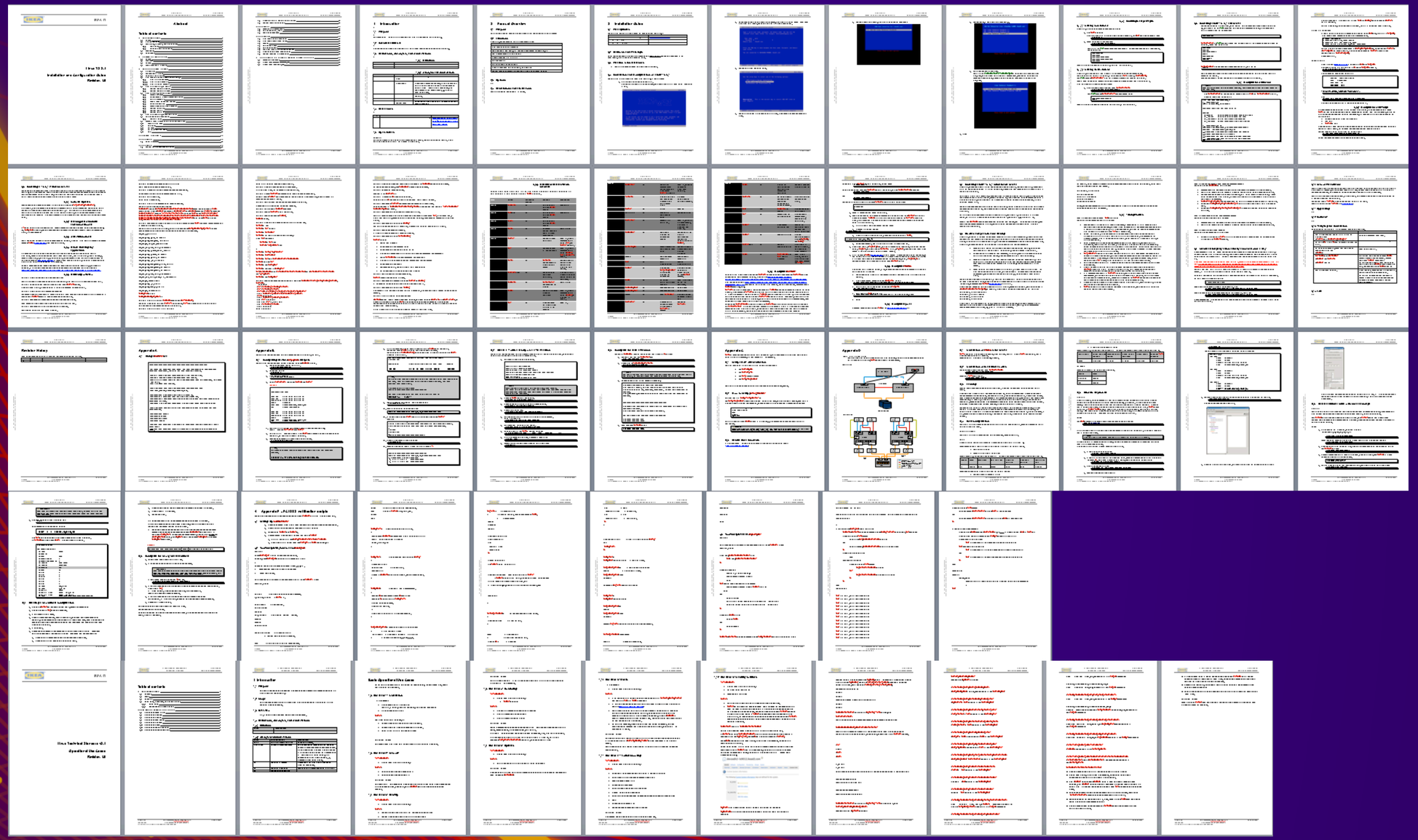
redhat.

Communication contract



redhat.

Installation and Configuration manual

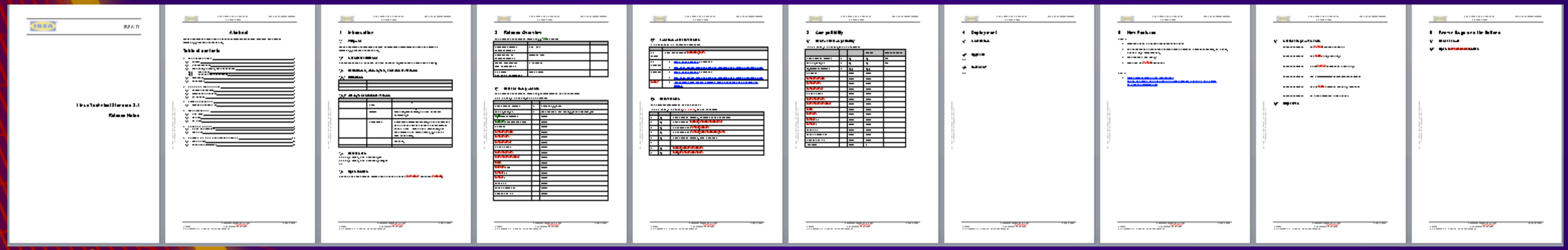


redhat.

Test cases

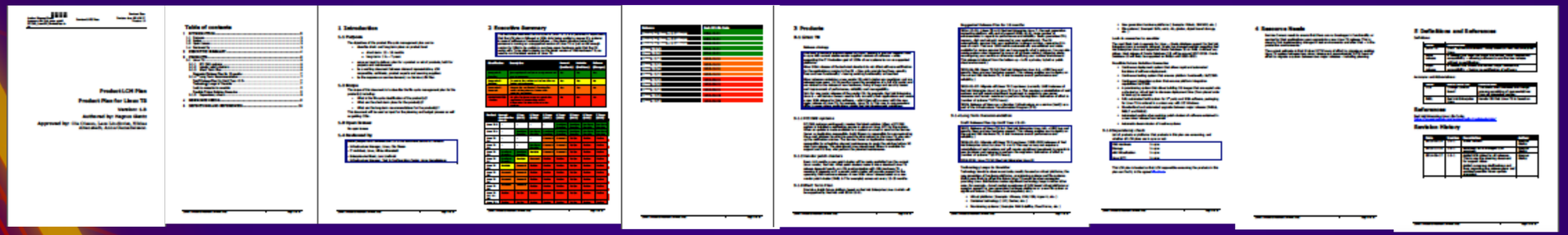
redhat.

Release notes



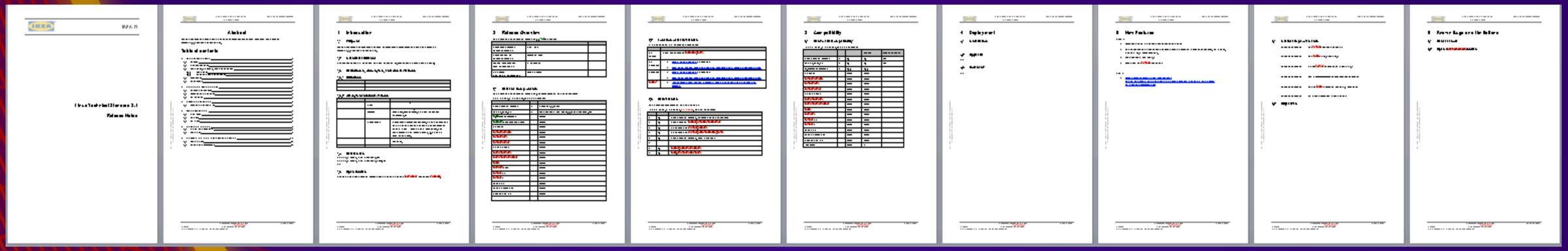
redhat.

Life Cycle Management Plan



redhat.

Delivery Plan

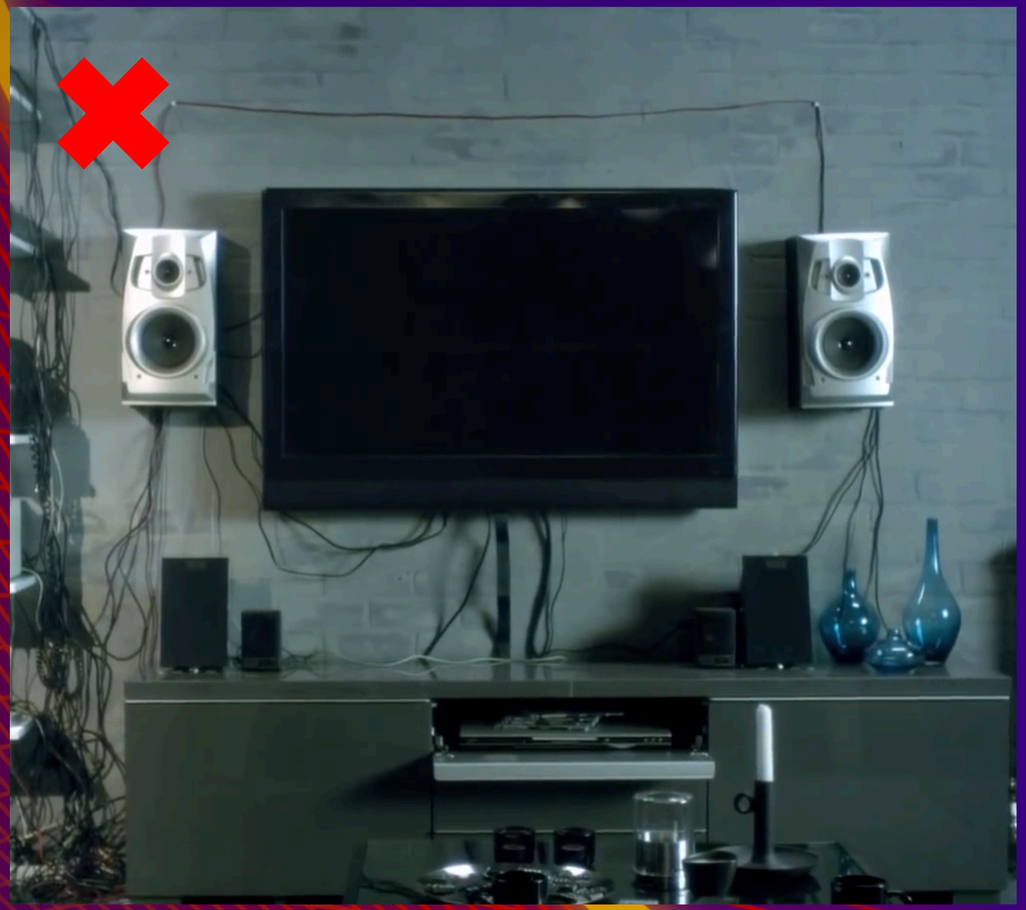


redhat.

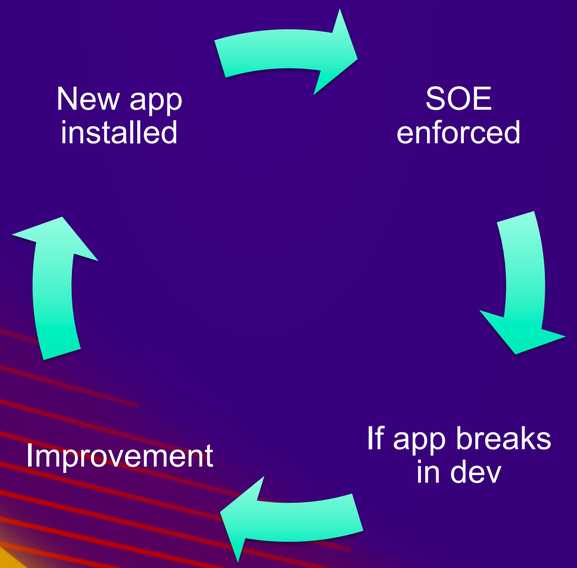
Create an organized release management process

redhat.

Make it a requirement to use latest versions



Enforce your SOE!



redhat.

Oh, I thought this would be a technical talk...

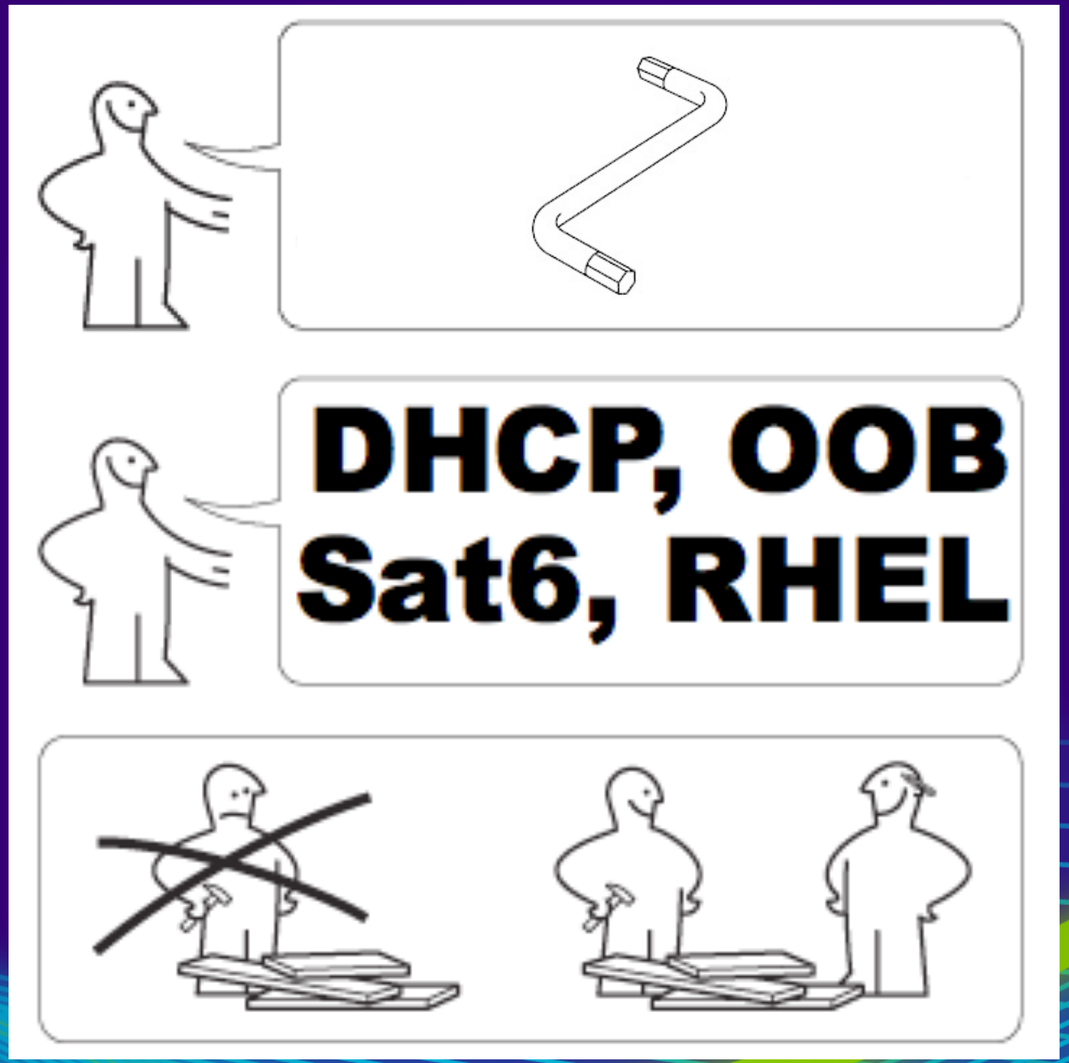
redhat.

-Yeah. Can we please have some technical slides?

redhat.

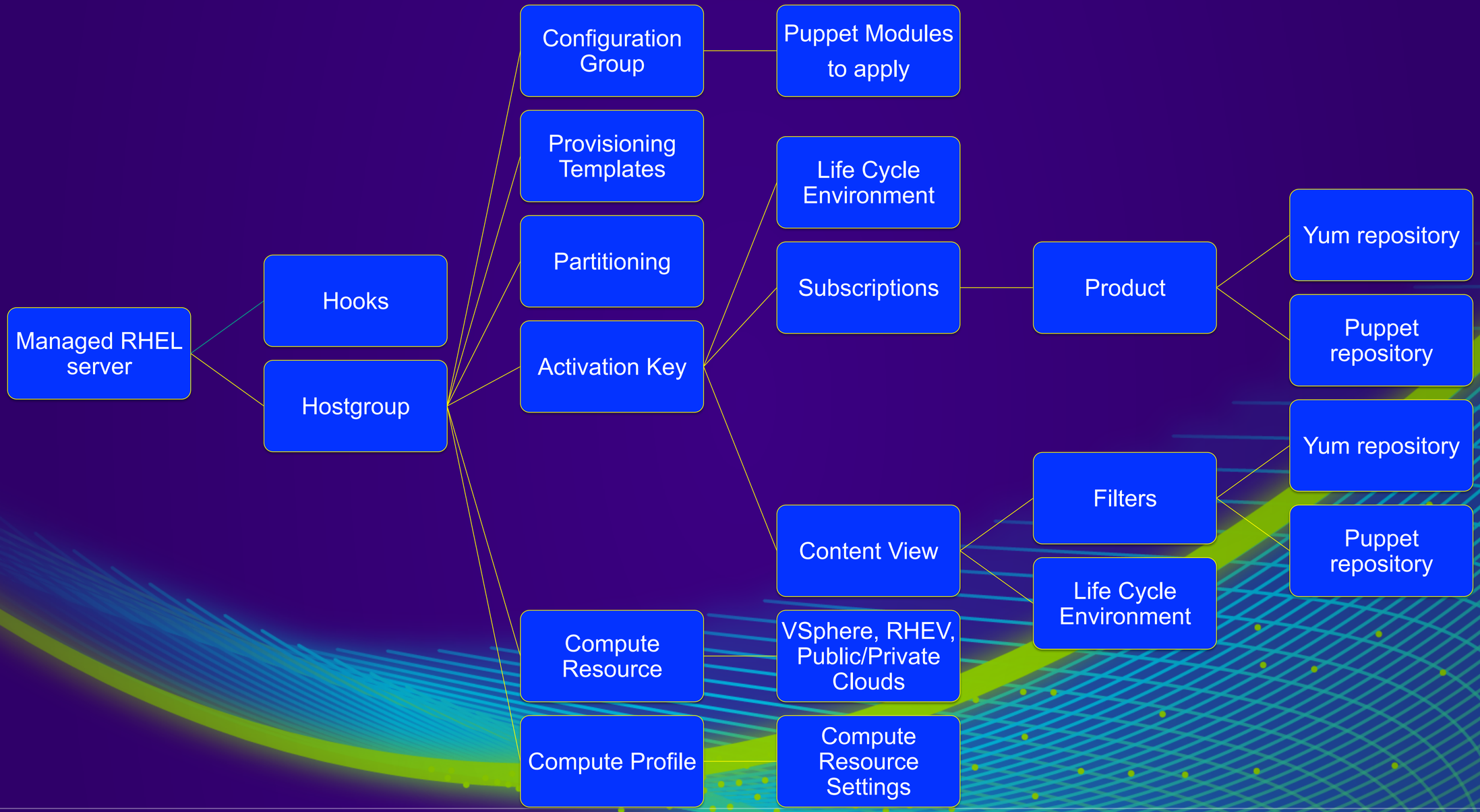
Red Hat Enterprise Linux 7 SOE with Red Hat Satellite 6.0

redhat.



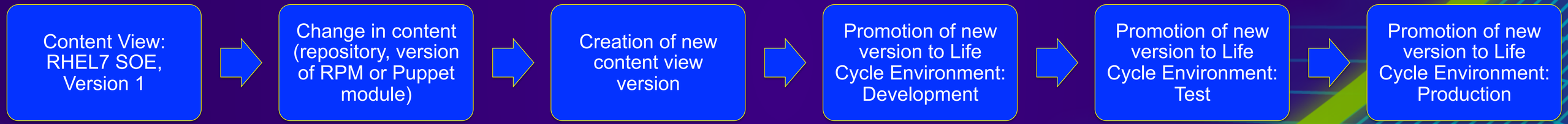
redhat.

Red Hat Satellite 6.0 components – Simplified view



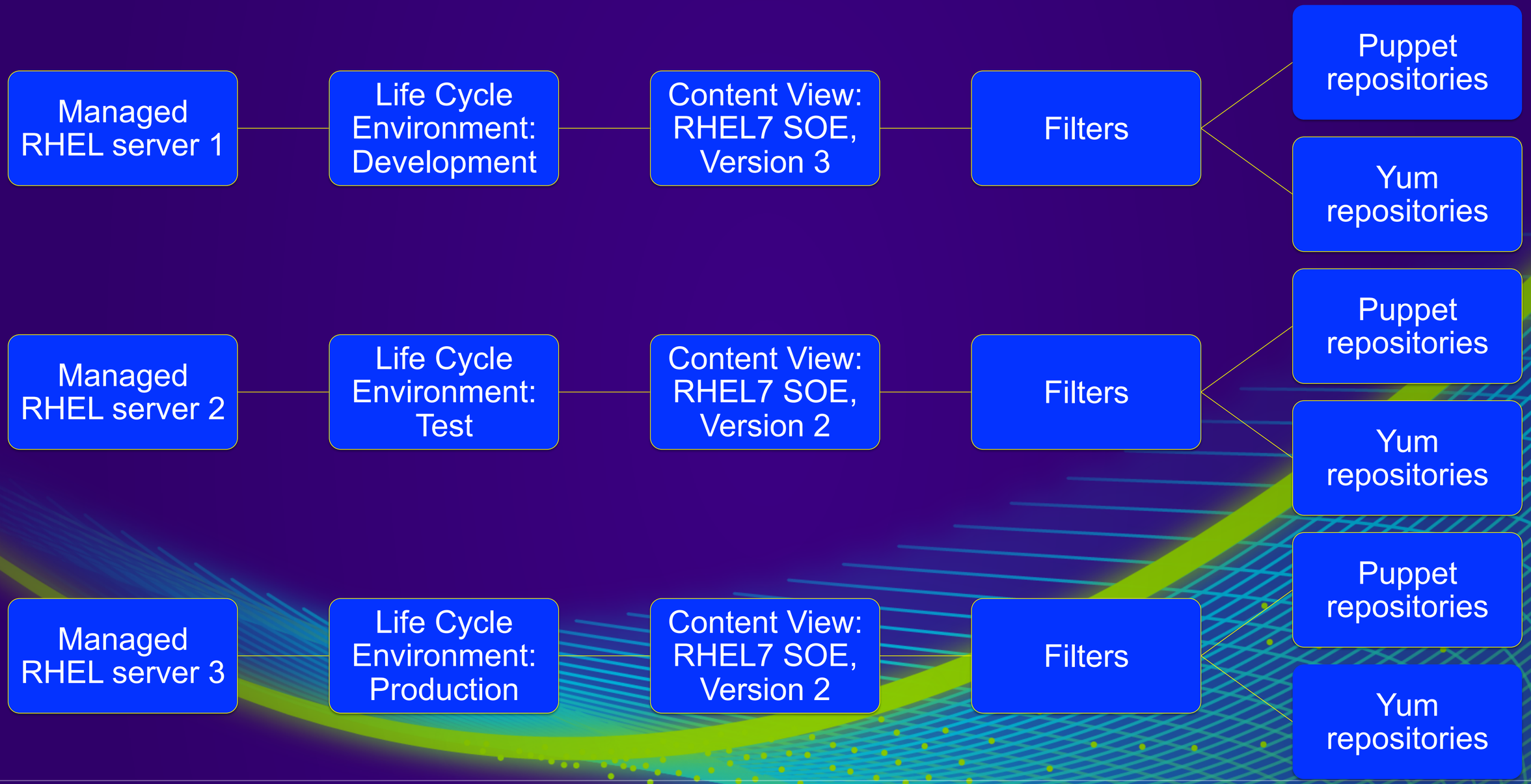
redhat.

Red Hat Satellite 6.0 components – Simplified view



redhat.

Red Hat Satellite 6.0 components – Simplified view



redhat.

Overview - Deployment of VM with RH Satellite 6.0

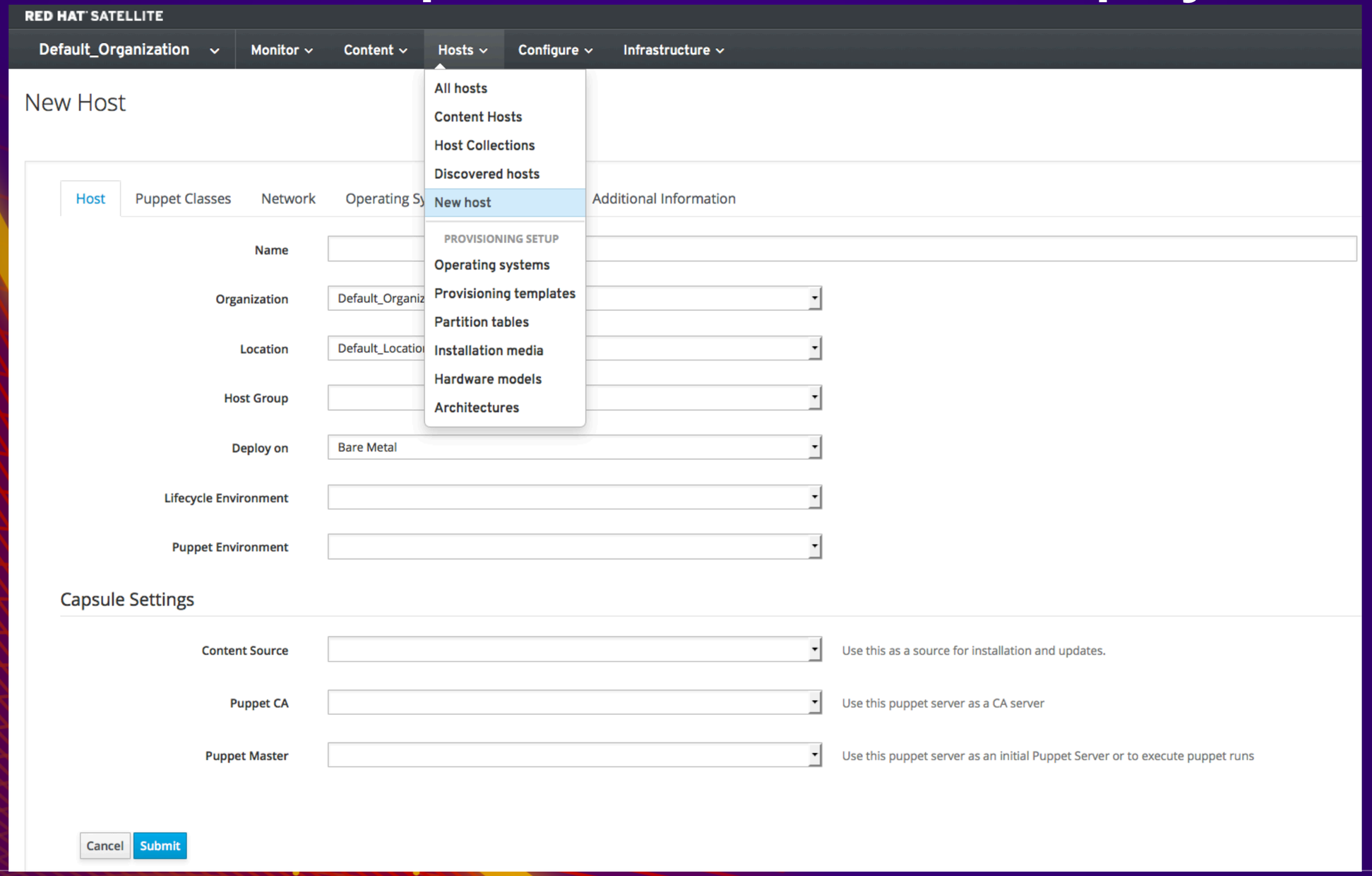
redhat.

Finish scripts for template deployed servers:
Firstboot script: What's my name?

```
SATELLITE_SERVER=https://satellite6-server.domain/api/v2/
VMINFO_FILE=/var/tmp/vm_info.txt

function jsonValue() {
    KEY=$1
    FILE=$2
    cat $FILE | awk -F"[,:}]" '{for(i=1;i<=NF;i++){if($i~/\042'$KEY'\042/){print $(i+1)}}}' | tr -d '"'
}


getMAC(){
    NIC=$1
    ip addr show $NIC |  awk -F'ether' '/ether/ {print $2}' | sed 's/ //' | awk '{print $1}'
}

getHostname(){
        jsonValue name $VMINFO_FILE
}

getVMInfo(){
    curl -s -o $VMINFO_FILE –user theuser:thepass -H "Content-Type:application/json" -H "Accept:application/
json" -k ${SATELLITE_SERVER}hosts?search="$(getMAC eth0)”
    result=$(getHostname)
    if [ -z $result ]; then
        echo "$MAC : is not known to the Satellite 6 server"
        exit 1
    fi
}

getVMInfo; setupNetworking $(getHostname)
```

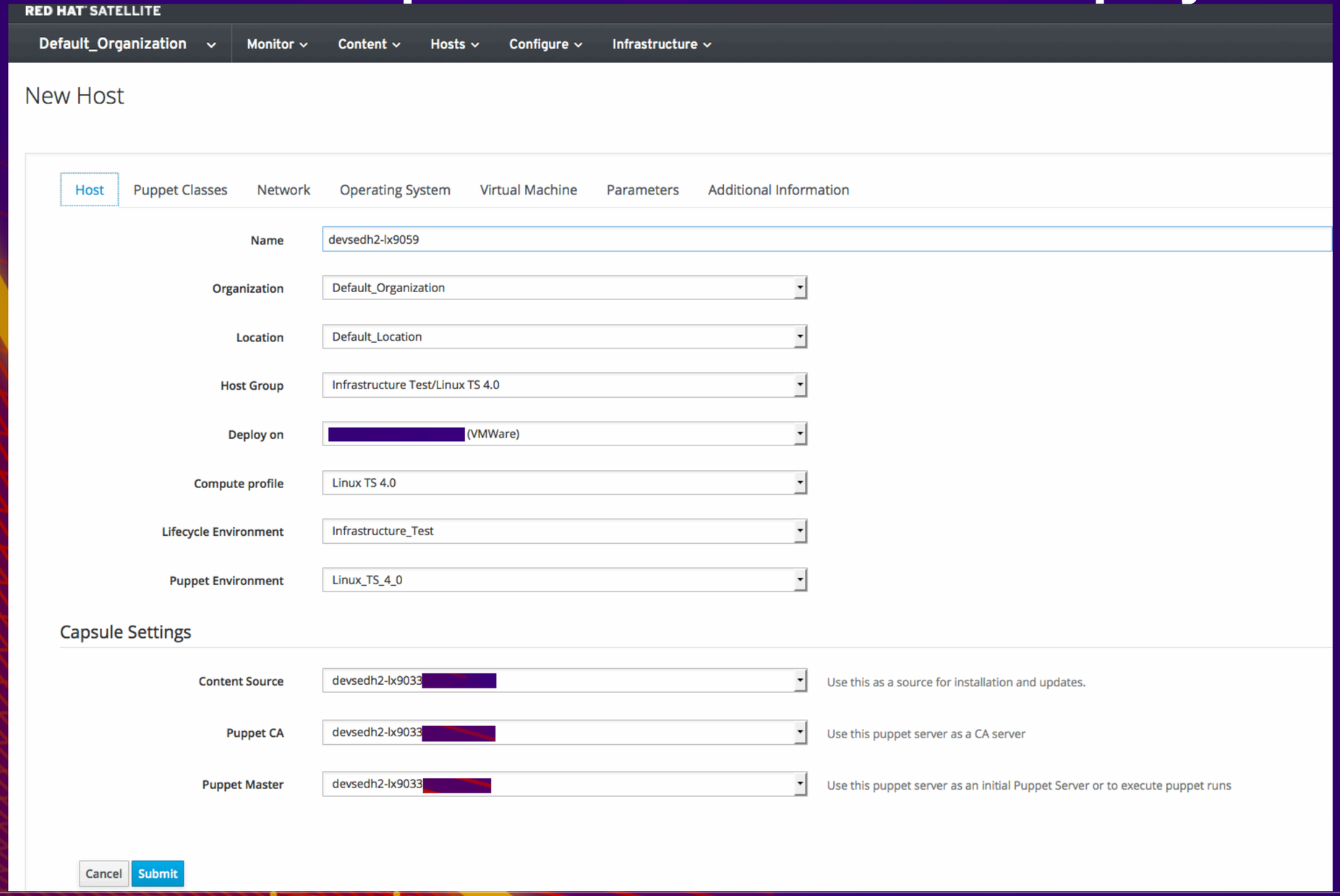

redhat.

Red Hat Enterprise Linux 7 SOE VM Deployment



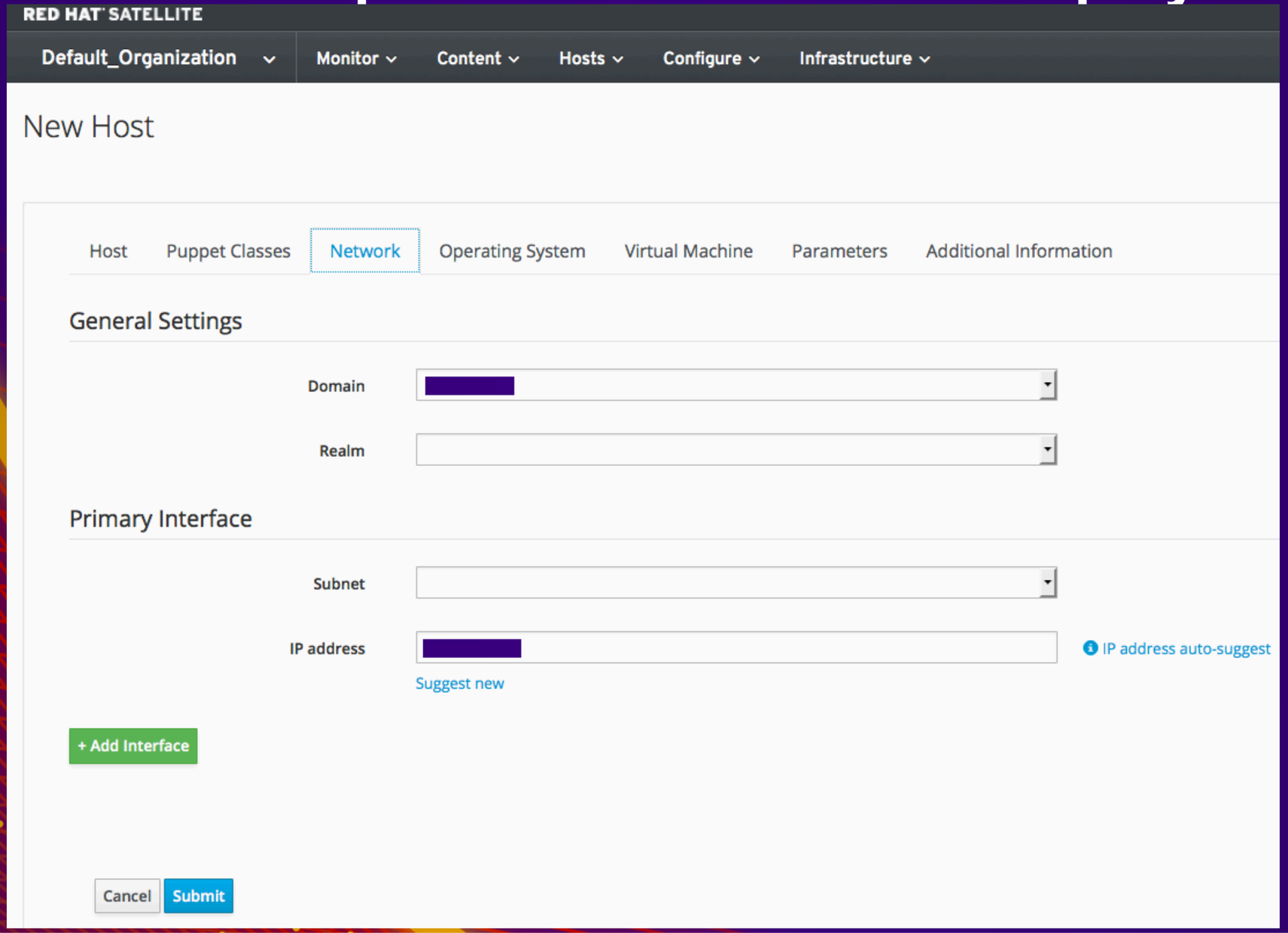
redhat.

Red Hat Enterprise Linux 7 SOE VM Deployment



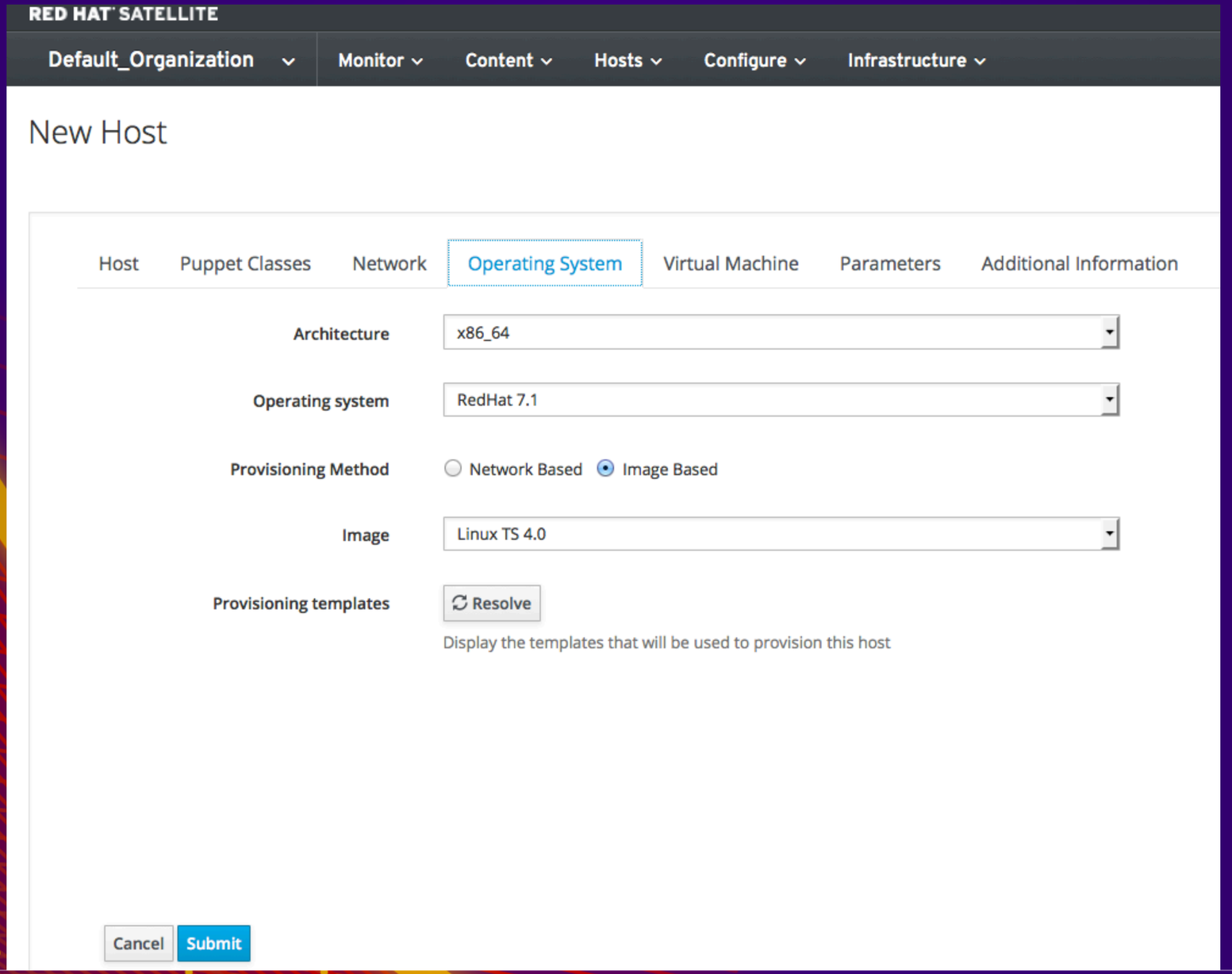
redhat.

Red Hat Enterprise Linux 7 SOE VM Deployment



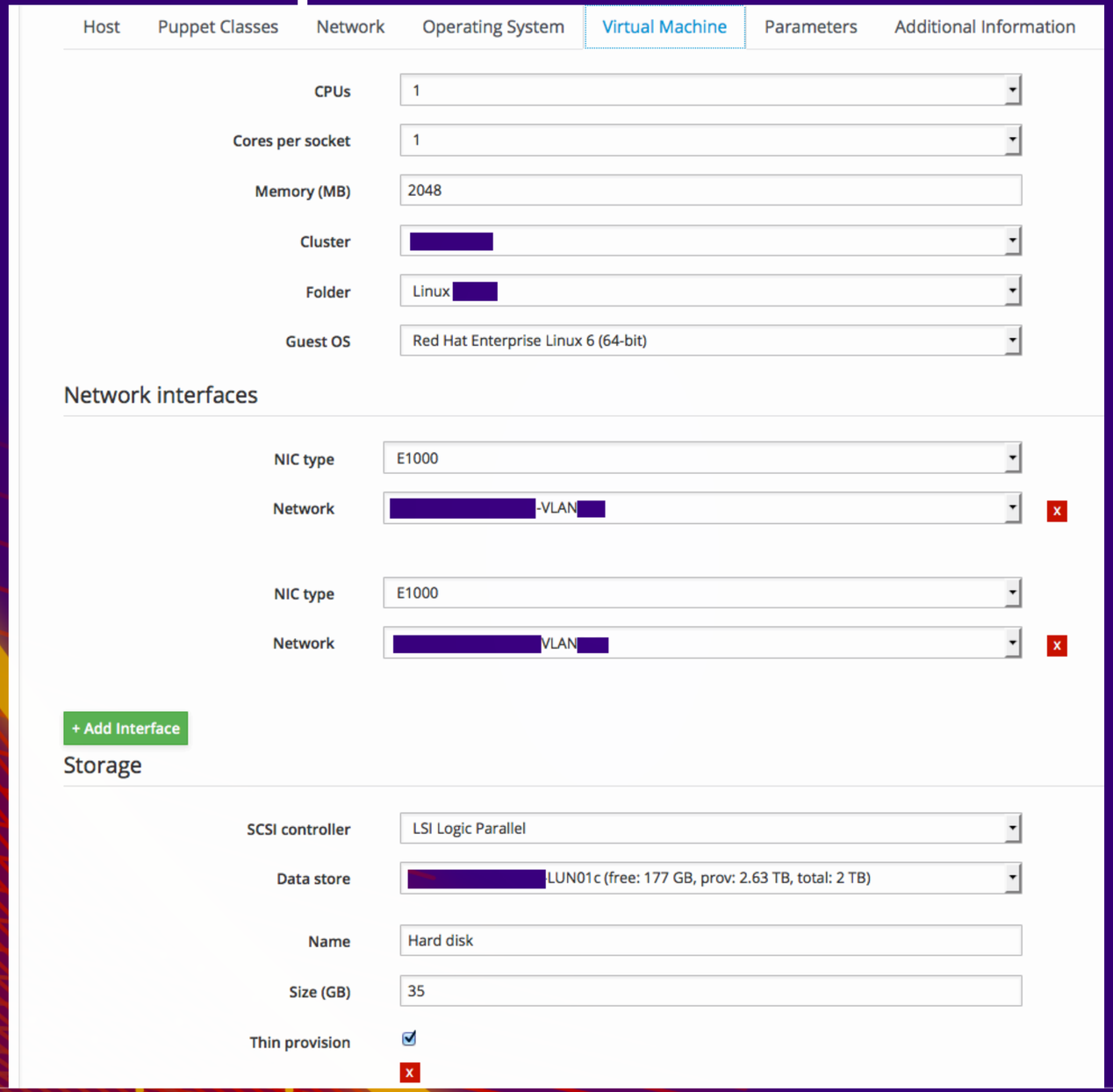
redhat.

Red Hat Enterprise Linux 7 SOE VM Deployment



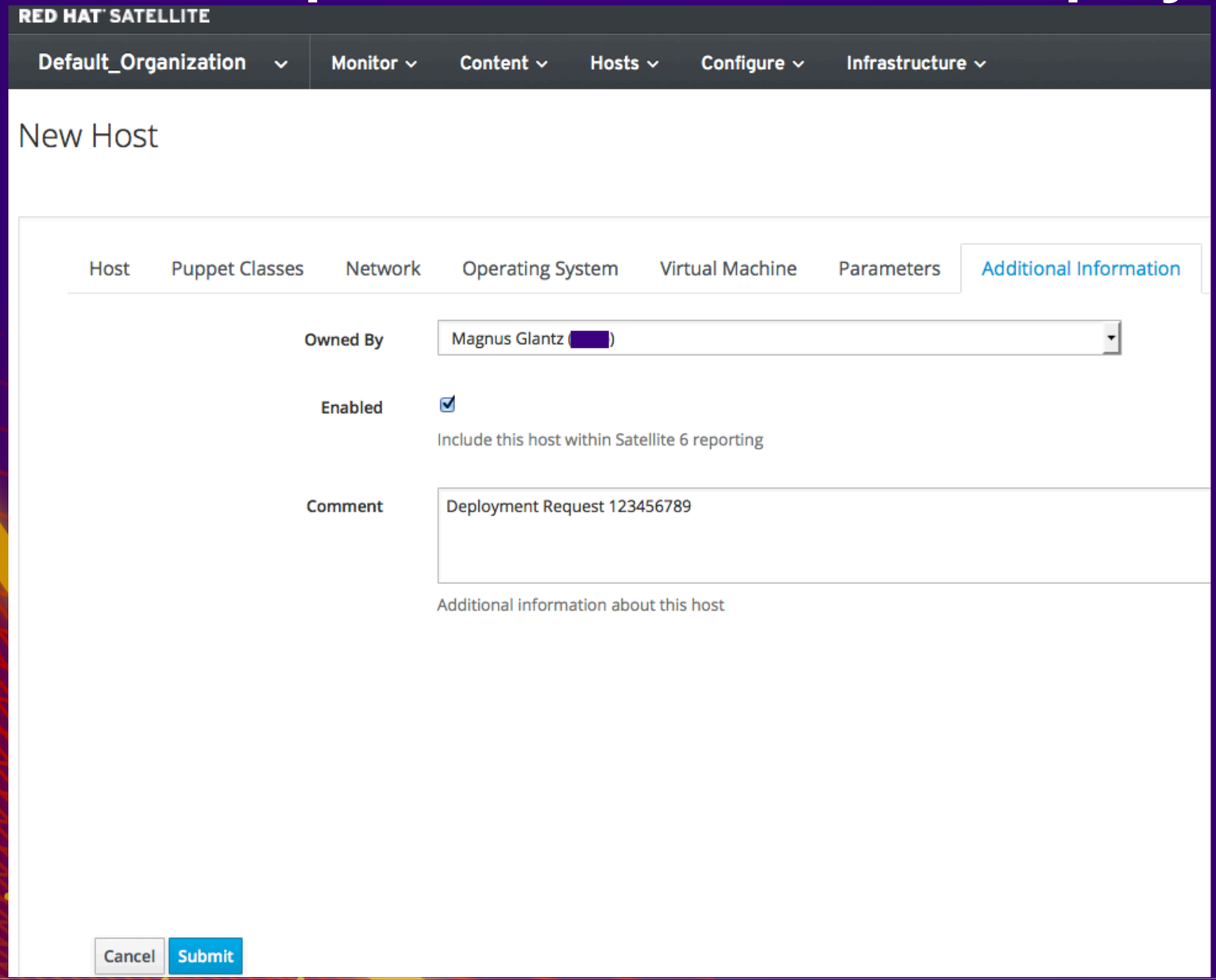
redhat.

Red Hat Enterprise Linux 7 SOE VM Deployment



redhat.

Red Hat Enterprise Linux 7 SOE VM Deployment

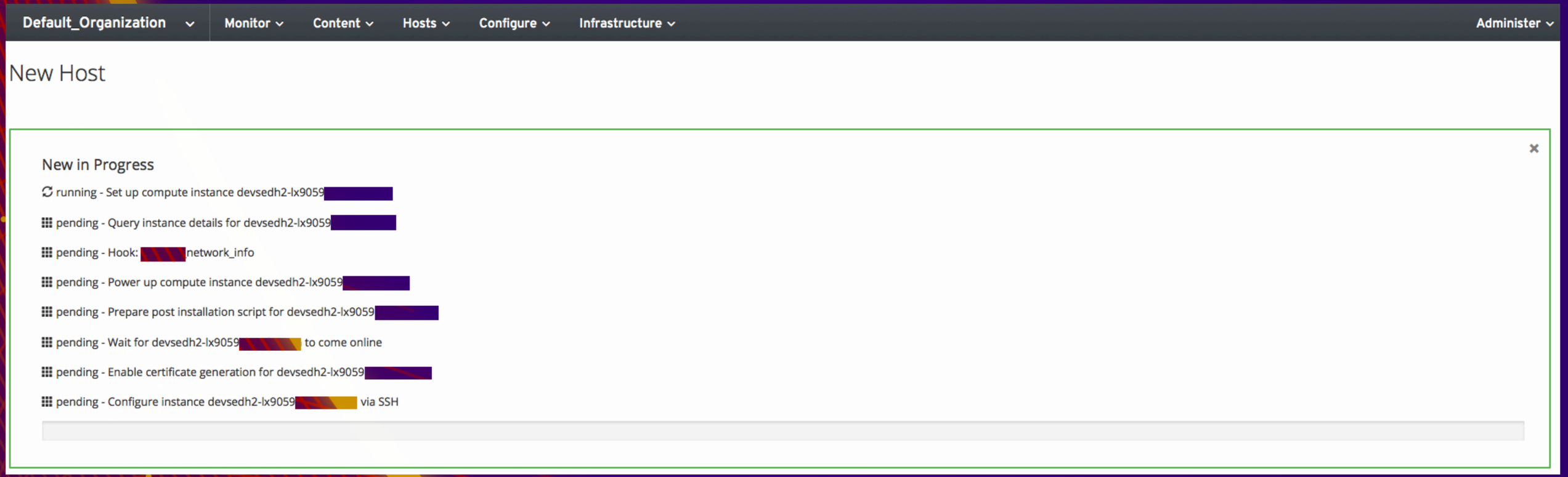


redhat.

80 seconds

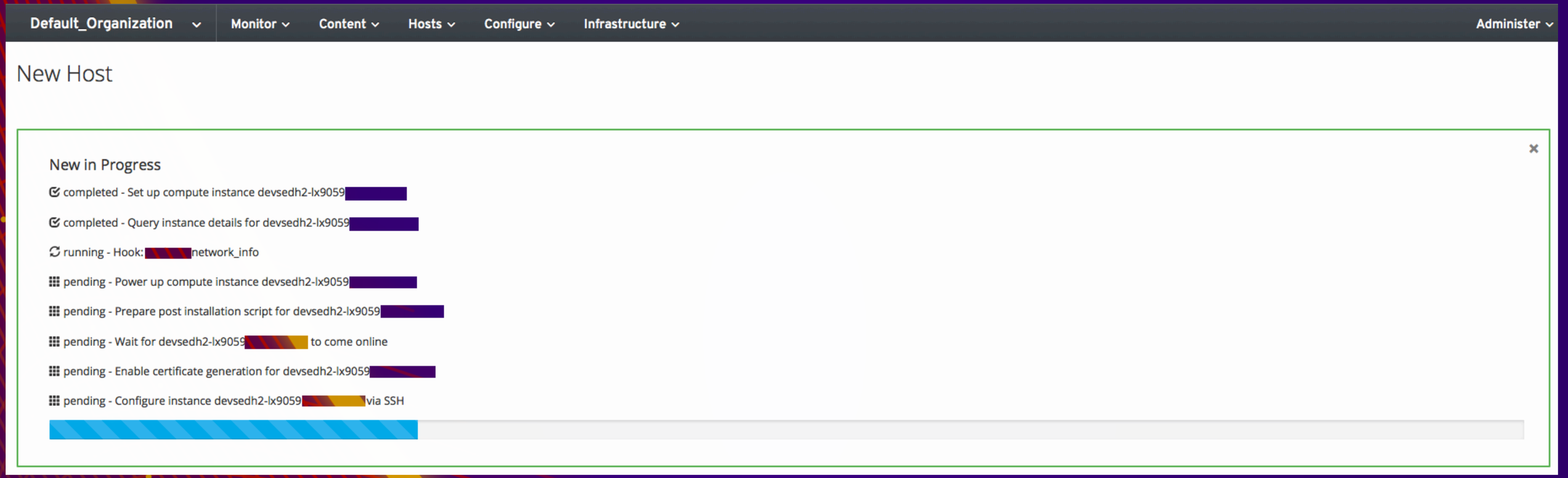
redhat.

Red Hat Enterprise Linux 7 SOE VM Deployment



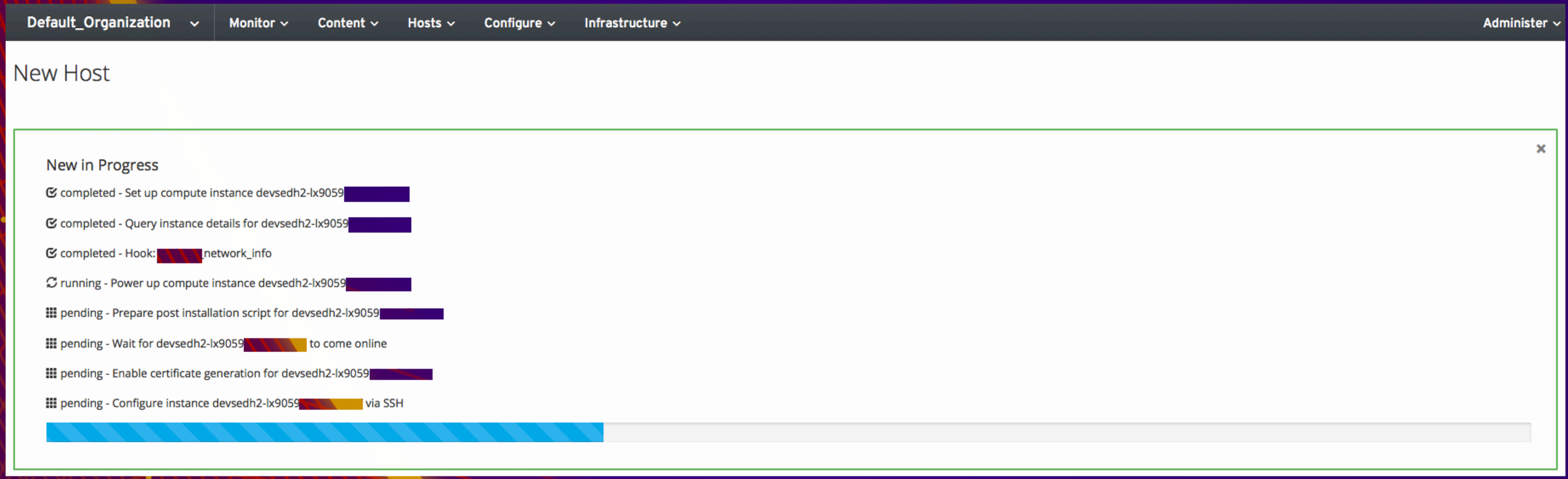
redhat.

Red Hat Enterprise Linux 7 SOE VM Deployment



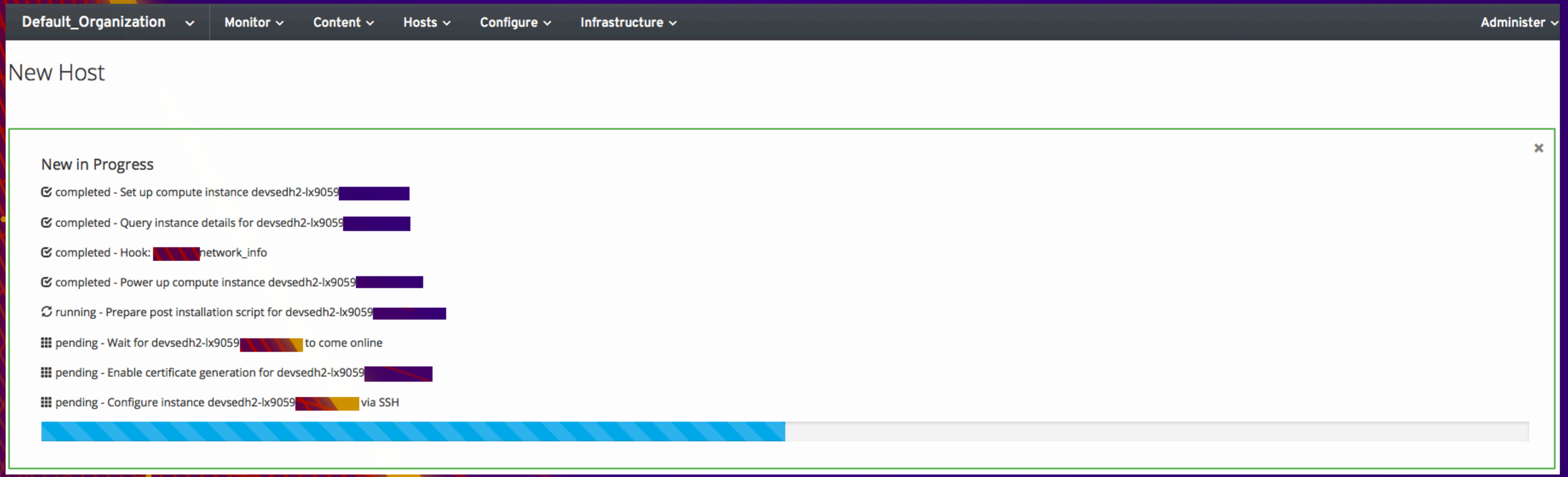
redhat.

Red Hat Enterprise Linux 7 SOE VM Deployment



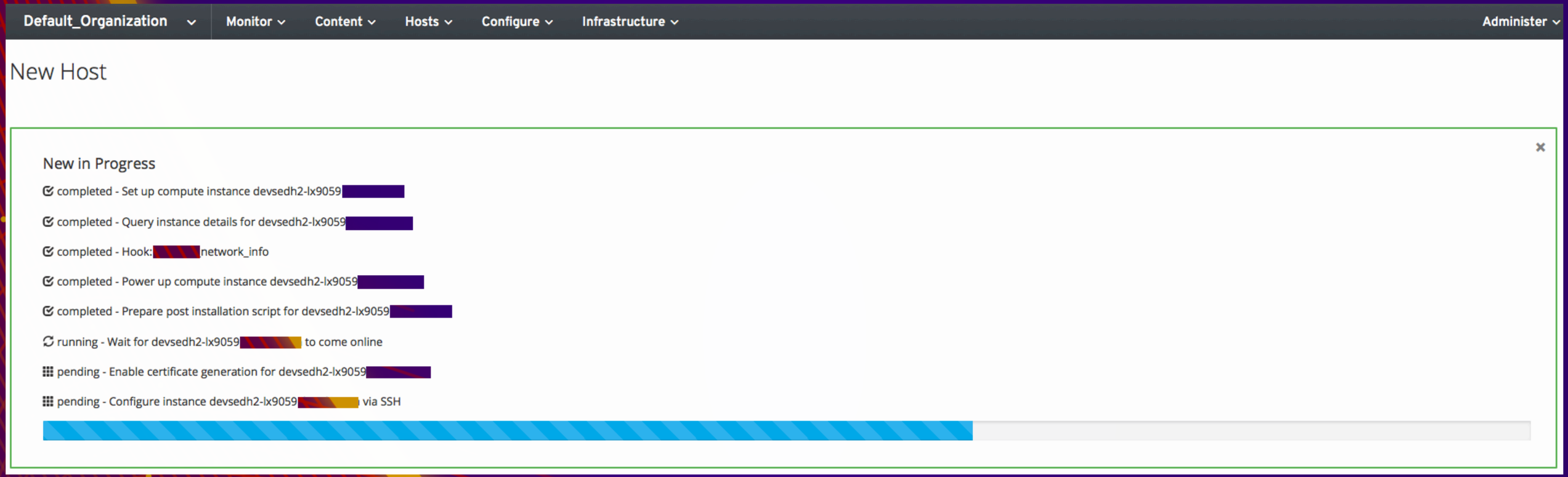
redhat.

Red Hat Enterprise Linux 7 SOE VM Deployment



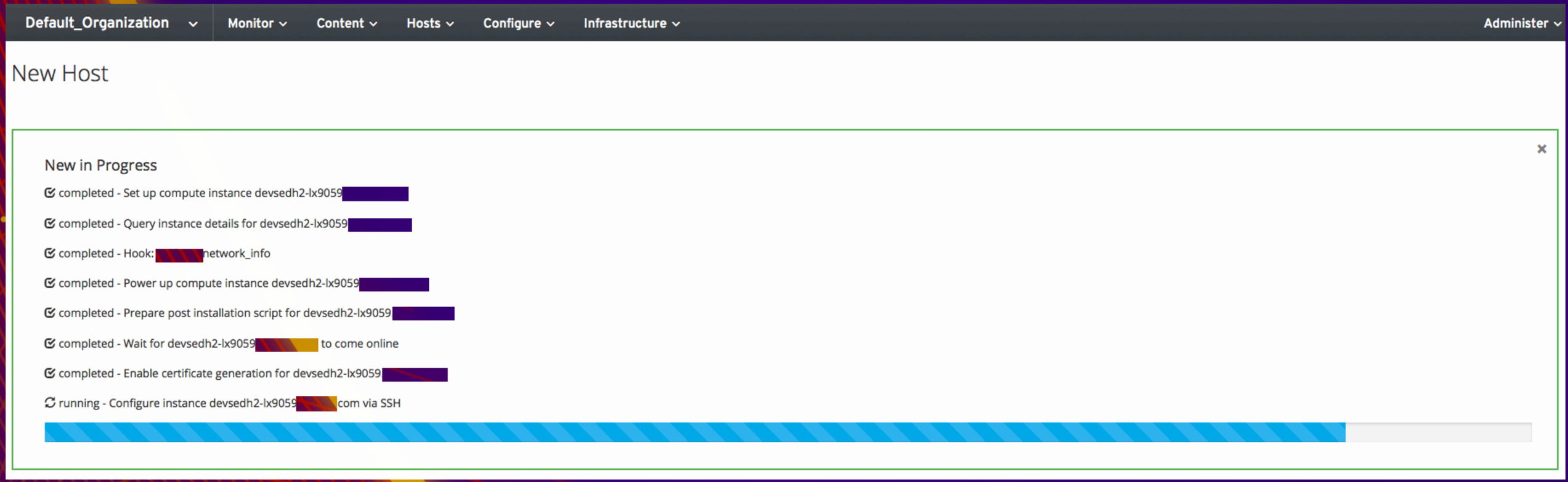
redhat.

Red Hat Enterprise Linux 7 SOE VM Deployment



redhat.

Red Hat Enterprise Linux 7 SOE VM Deployment



redhat.

Red Hat Enterprise Linux 7 SOE VM Deployment

Default_Organization | Monitor | Content | Hosts | Configure | Infrastructure | Administer

devsedh2-lx9059[redacted]

Reports from the last [ ] days - 2 reports found

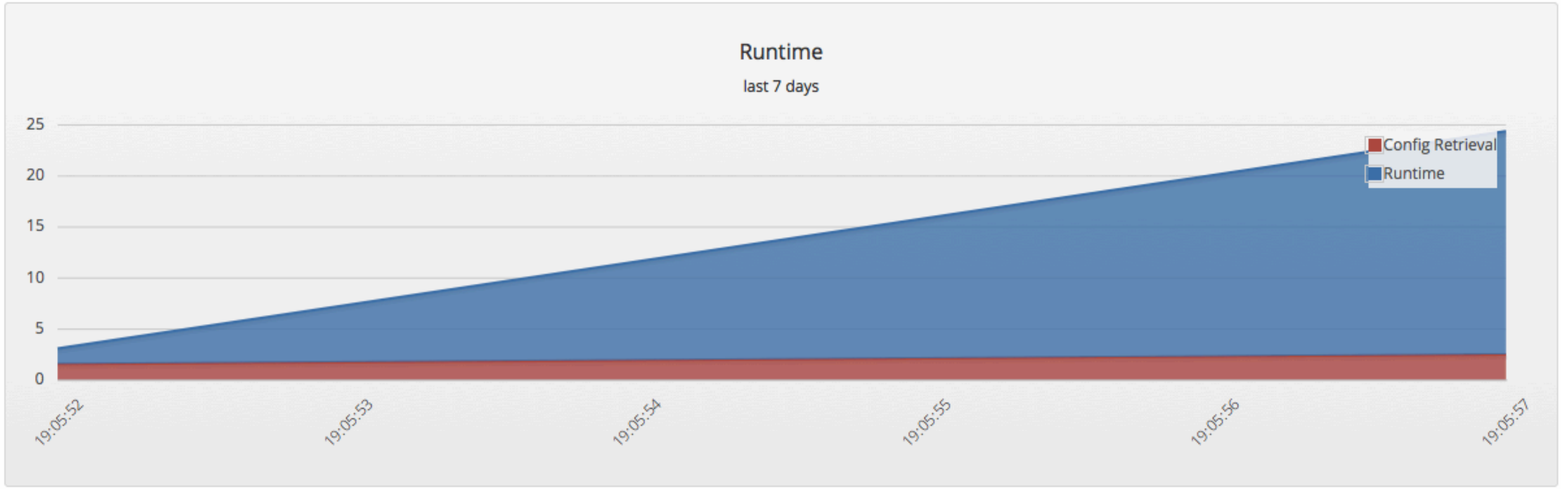
Boot disk | Edit | Build | Power Off | Console | Run puppet | Delete

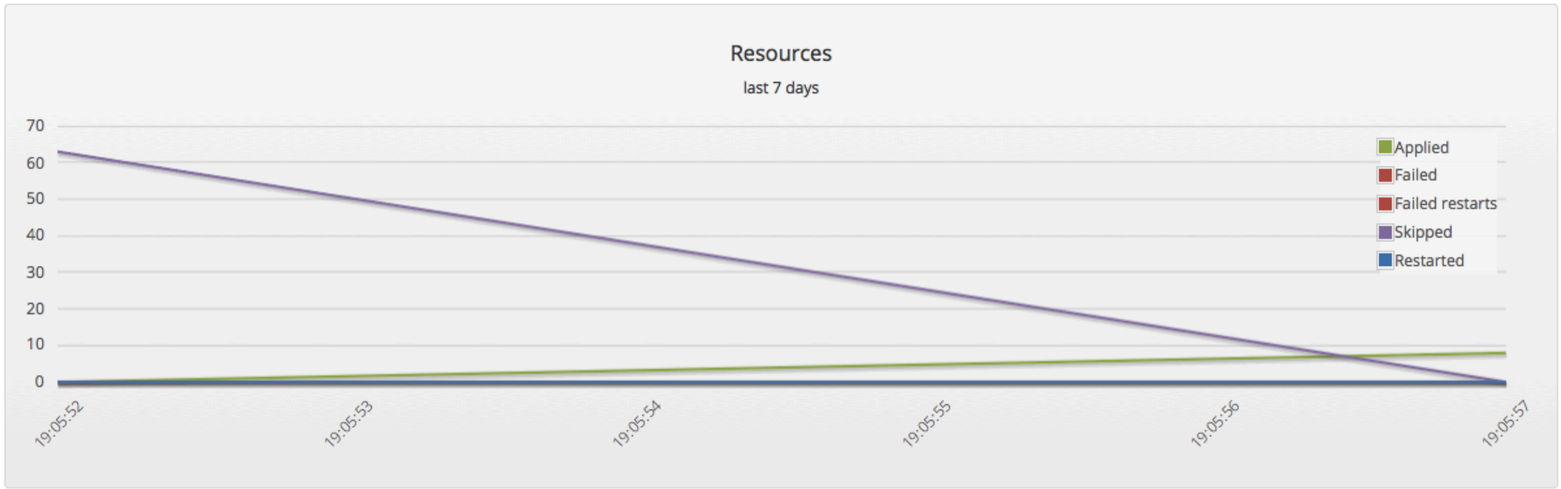
Details

Audits | Facts | Reports | YAML | Content

Properties | Metrics | Templates | VM

Properties	
Subscription status	valid
Domain	[redacted]
Realm	
IP Address	10[redacted]
MAC Address	00:[redacted]
Puppet Environment	KT_Default_Organization_Infrastructure_Test_Linux_TS_4_0_23
Host Architecture	x86_64
Operating System	RedHat 7.1
Host group	Infrastructure Test/Linux TS 4.0
Location	Default_Location
Organization	Default_Organization
Owner	Magnus Glantz



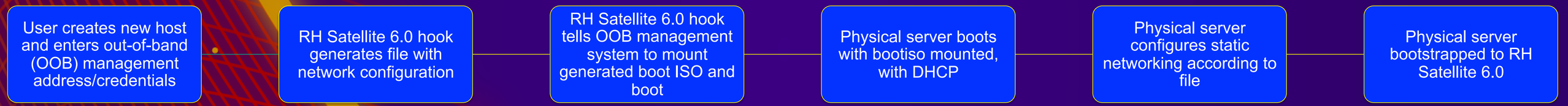


redhat.

-Wow. This is great.

redhat.

Overview - Deployment of physical server with RH Satellite 6.0



redhat.

Satellite 6.0 OOB Hook Concept
Provision physical server (after_commit hook)

```
LOGFILE=/some/place/$2.log
VMINFO_FILE=/some/place/$2.vminfo
NICINFO_FILE=/some/place/$2.nicinfo
BUILDFILE=/some/place/$2.new # Created by a separate ‘create’ hook (just ‘touch $BUILDFILE’).
if [ ! -f $BUILDFILE ]; then
    exit 0 # Prevents further execution for hosts that are not in build mode.
fi
# jsonValue function to extract info from $VMINFO_FILE ..

curl -s -o $VMINFO_FILE --user theuser:thepass-H "Content-Type:application/json" -H "Accept:application/
json" -k https://satellite6-server/api/v2/hosts?search="$2"

if [ -f $BUILDFILE]; then
    rm -f /var/www/html/pub/hooks/info/$2.new
    if grep -i vmware $VMINFO_FILE >/dev/null 2>&1; then
        exit 0 # Exit if it’s not a physical server
    else
        curl -s -o $NICINFO_FILE --user theuser:thepass -H "Content-Type:application/json" -H
"Accept:application/json" -k https://satellite6-server/api/v2/hosts/$(jsonValue id $VMINFO_FILE)/interfaces

        if grep "Nic::BMC" $NICINFO_FILE >/dev/null; then
            sudo foreman-rake bootdisk:generate:full_host NAME=$2 OUTPUT=/var/www/html/some/place/$2.iso >>
$LOGFILE 2>&1 # full_host requires ruby193-rubygem-foreman_bootdisk-3.2.1>
            sudo /bin/chmod a+r /var/www/html/some/place/$2.iso
            # Code here to extract OOB details from $NICINFO_FILE and put into variables
            oob_integration_script $OOB_IP $OOB_USER $OOB_PASS ..
        fi
    fi
fi
exit 0
```

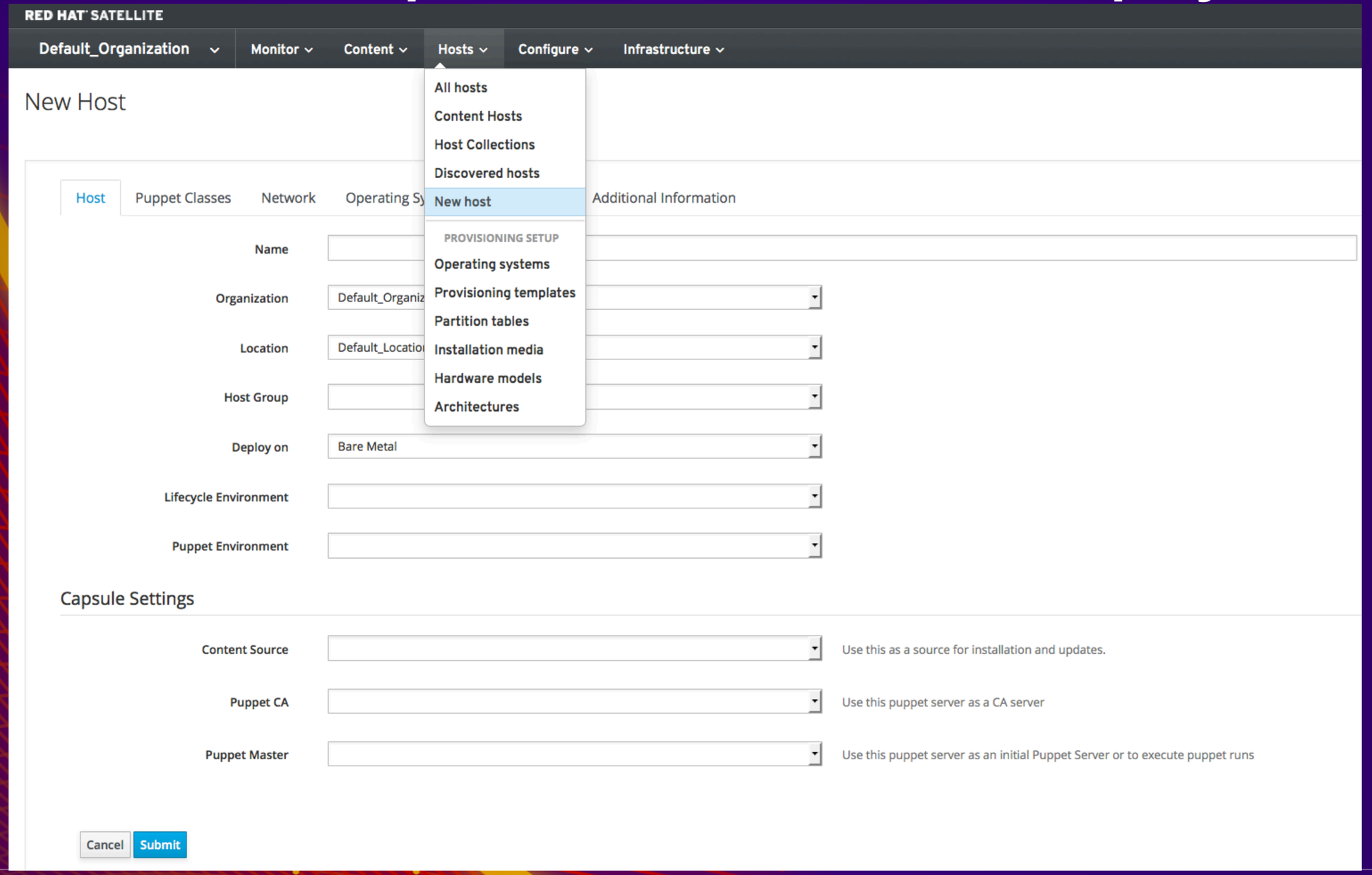

redhat.

Kickstart %POST
Set hostname, register and install/run stuff

```
THEHOSTNAME="<%= @host.name %>"
hostname $THEHOSTNAME

# Fetch network configuration from Satellite 6 generated by host create hook andand setup proper static network
setupNetwork $THEHOSTNAME

# Subscription manager stuff
# Add: --force to subscription-manager command to get reinstallations working

# Update system to latest available errata
yum -t -y -e 0 update

# Mimic Satellite 5 activation keys
HOSTGROUP="<%= @host.hostgroup.to_s %>"

case $HOSTGROUP in
        *aaa)
            yum -t -y -e 0 install nmap-ncat perf screen
            ;;
        *bbb)
            yum -t -y -e 0 install httpd tomcat6
            ;;
esac

# Execute in case some RPM (usually related to a hostgroup) drops it off
if [ -x /tmp/post-script ]; then
    /tmp/post-script
fi
```

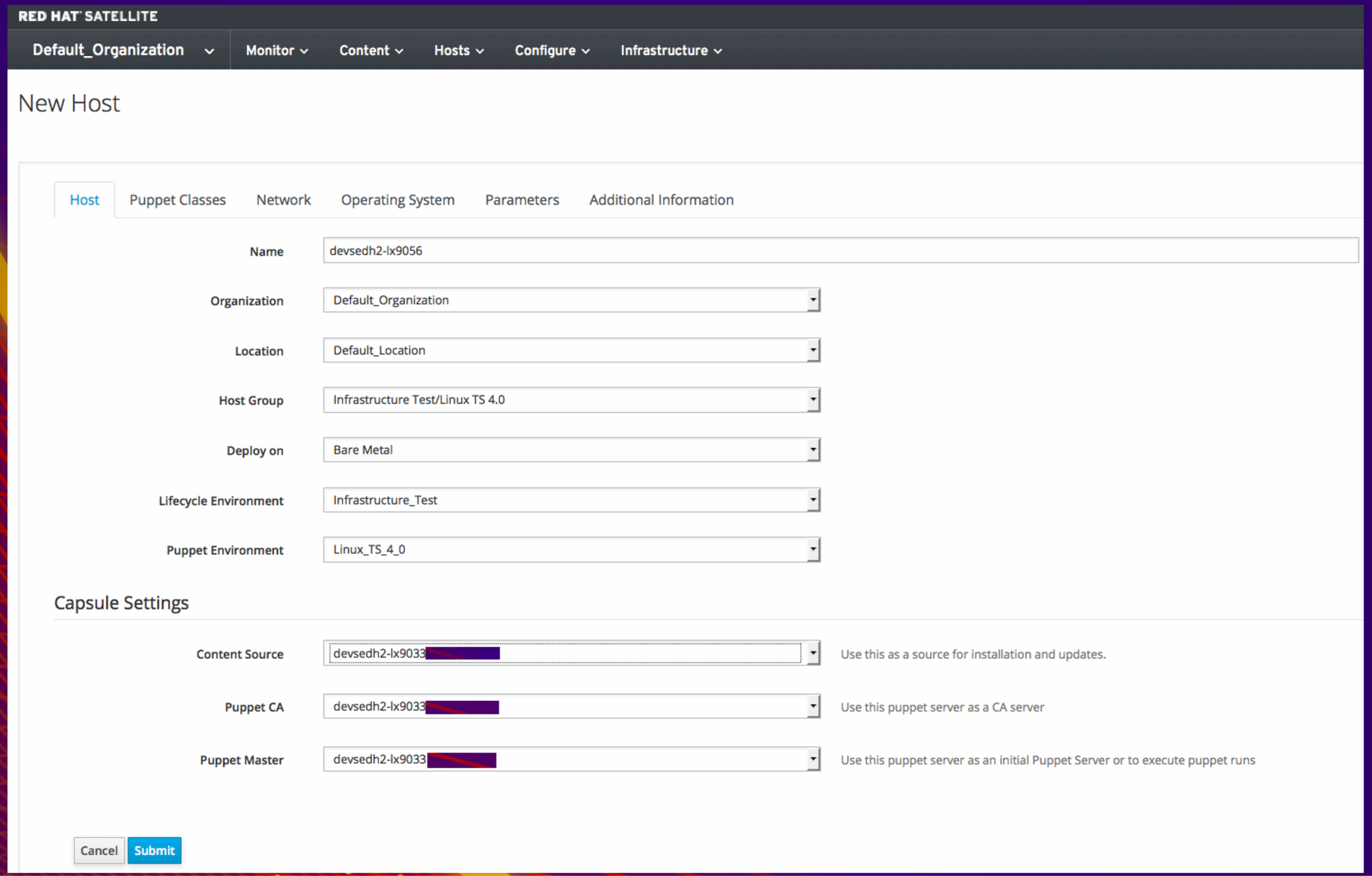

redhat.

Red Hat Enterprise Linux 7 SOE PHY Deployment



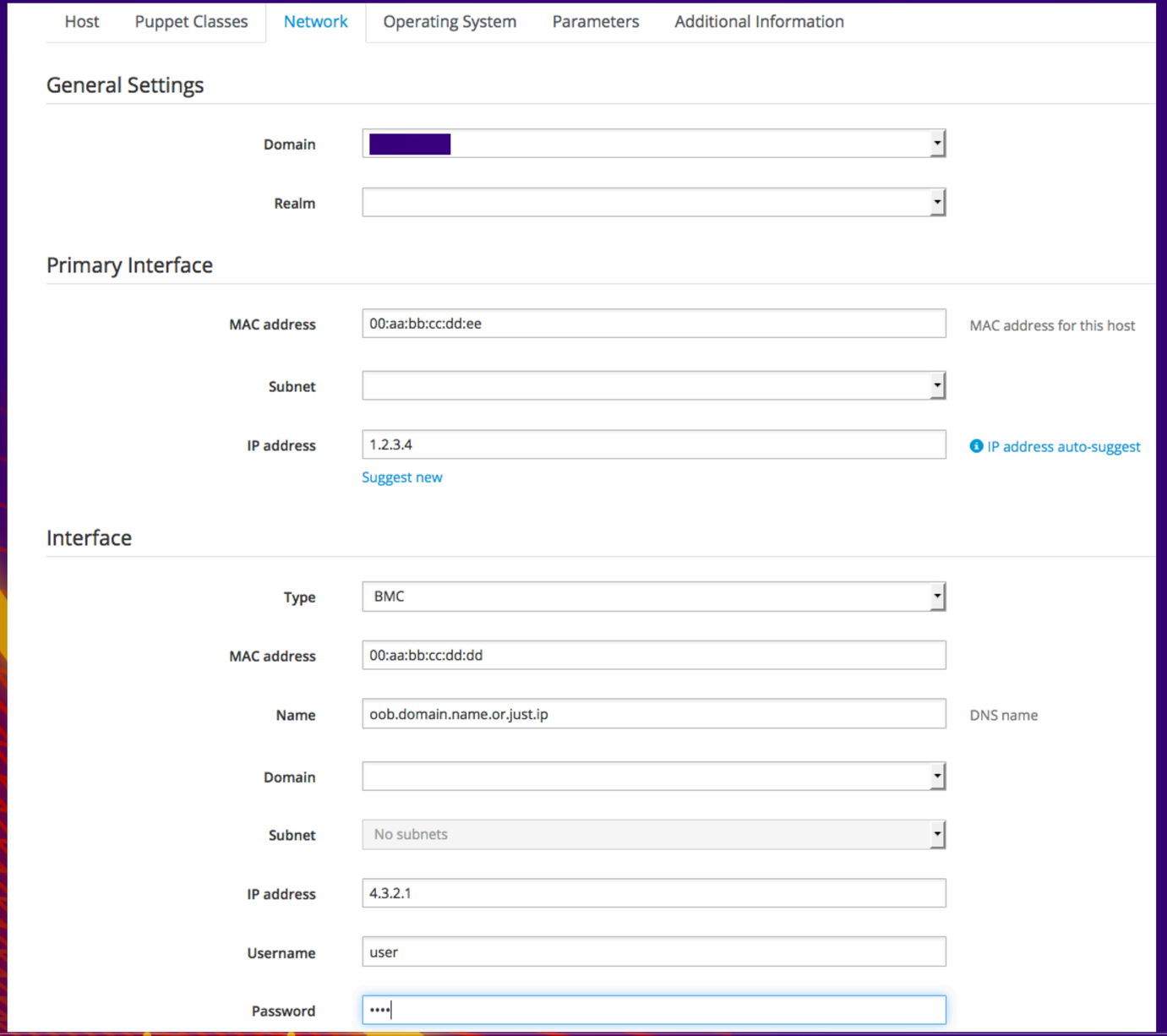
redhat.

Red Hat Enterprise Linux 7 SOE PHY Deployment



redhat.

Red Hat Enterprise Linux 7 SOE PHY Deployment



redhat.

Red Hat Enterprise Linux 7 SOE PHY Deployment

```
Tue May 26 12:07:41 UTC 2015: Completed gathering network information for: devsedh2-lx9056
Tue May 26 12:07:42 UTC 2015: Detected that devsedh2-lx9056 is in build mode.
Tue May 26 12:07:42 UTC 2015: devsedh2-lx9056 is a non-VMware host.
Tue May 26 12:07:42 UTC 2015: Initializing generation of bootiso for: devsedh2-lx9056
Size of boot image is 4 sectors -> No emulation
 24.34% done, estimate finish Tue May 26 12:08:16 2015
 48.73% done, estimate finish Tue May 26 12:08:16 2015
 73.03% done, estimate finish Tue May 26 12:08:16 2015
 97.44% done, estimate finish Tue May 26 12:08:16 2015
Total translation table size: 2048
Total rockridge attributes bytes: 0
Total directory bytes: 2048
Path table size(bytes): 22
Max brk space used 0
20539 extents written (40 MB)
Wrote /var/www/html/ /devsedh2-lx9056 .iso
Tue May 26 12:08:17 UTC 2015: generated bootiso for: devsedh2-lx9056
Tue May 26 12:08:17 UTC 2015: ILO DNS name not set on ILO interface.
ILO info for devsedh2-lx9056
ILODNS:
ILOIP: 10
ILOUSER:
ILOPASS: **********
ISO: /var/www/html/ /devsedh2-lx9056 .iso
Tue May 26 12:08:17 UTC 2015: Working network connection to devsedh2-lx9056 ILO (10 ) on port 443.
>>> my_ilo.hold_pwr_btn()
>>> my_ilo.insert_virtual_media(device="cdrom", image_url="http:// /devsedh2-lx9056 .iso")
>>> my_ilo.set_vm_status(device="cdrom", boot_option="boot_once")
>>> my_ilo.set_host_power()
Tue May 26 12:08:43 UTC 2015: ILO integration executed successfully.
```


redhat.

-I’m so happy right now.

redhat.

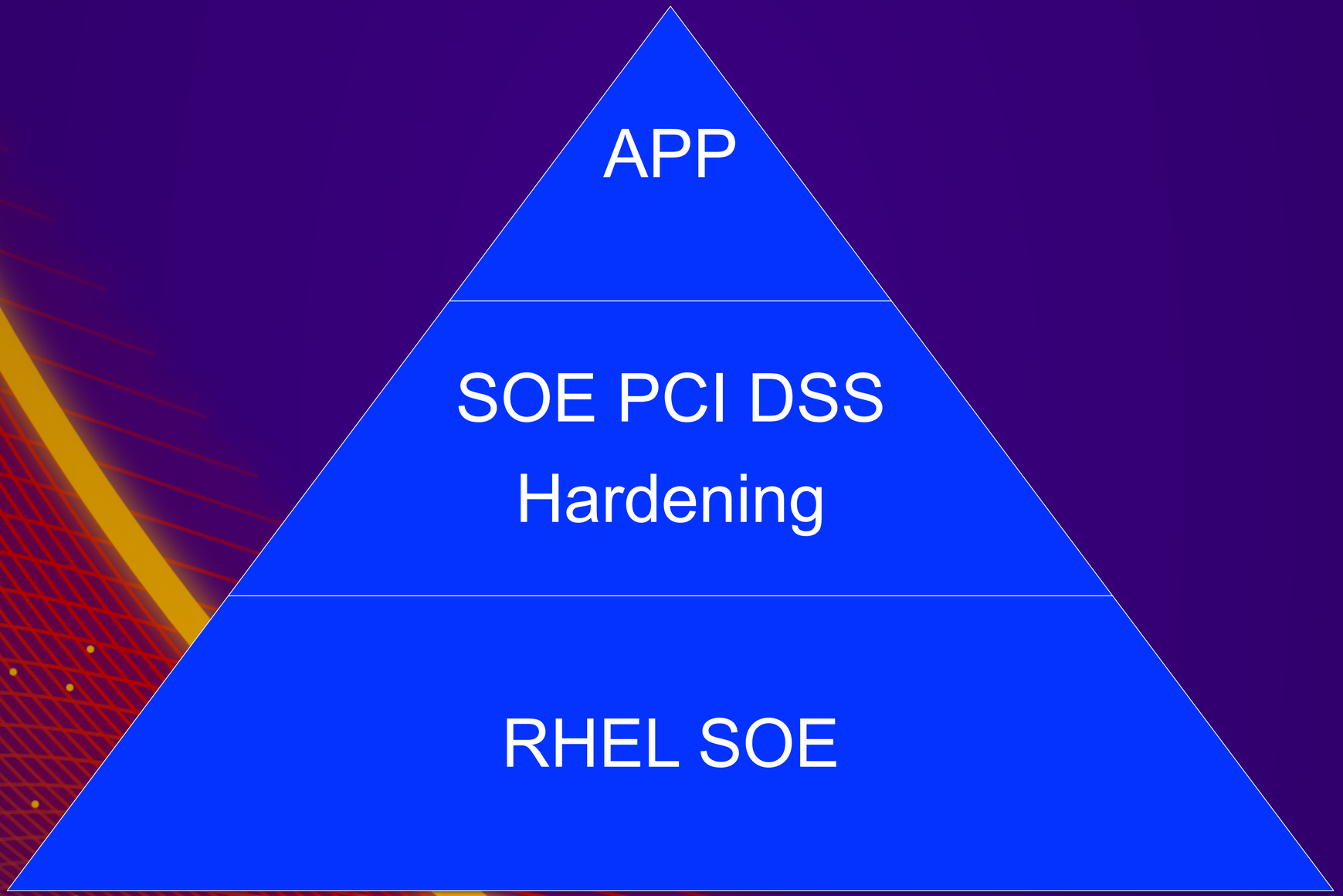
The ~~Red Hat Enterprise Linux~~ IKEA ABI

redhat.

Payment Card Industry Data Security Standard
PCI DSS
[Imagine dramatic music being played]

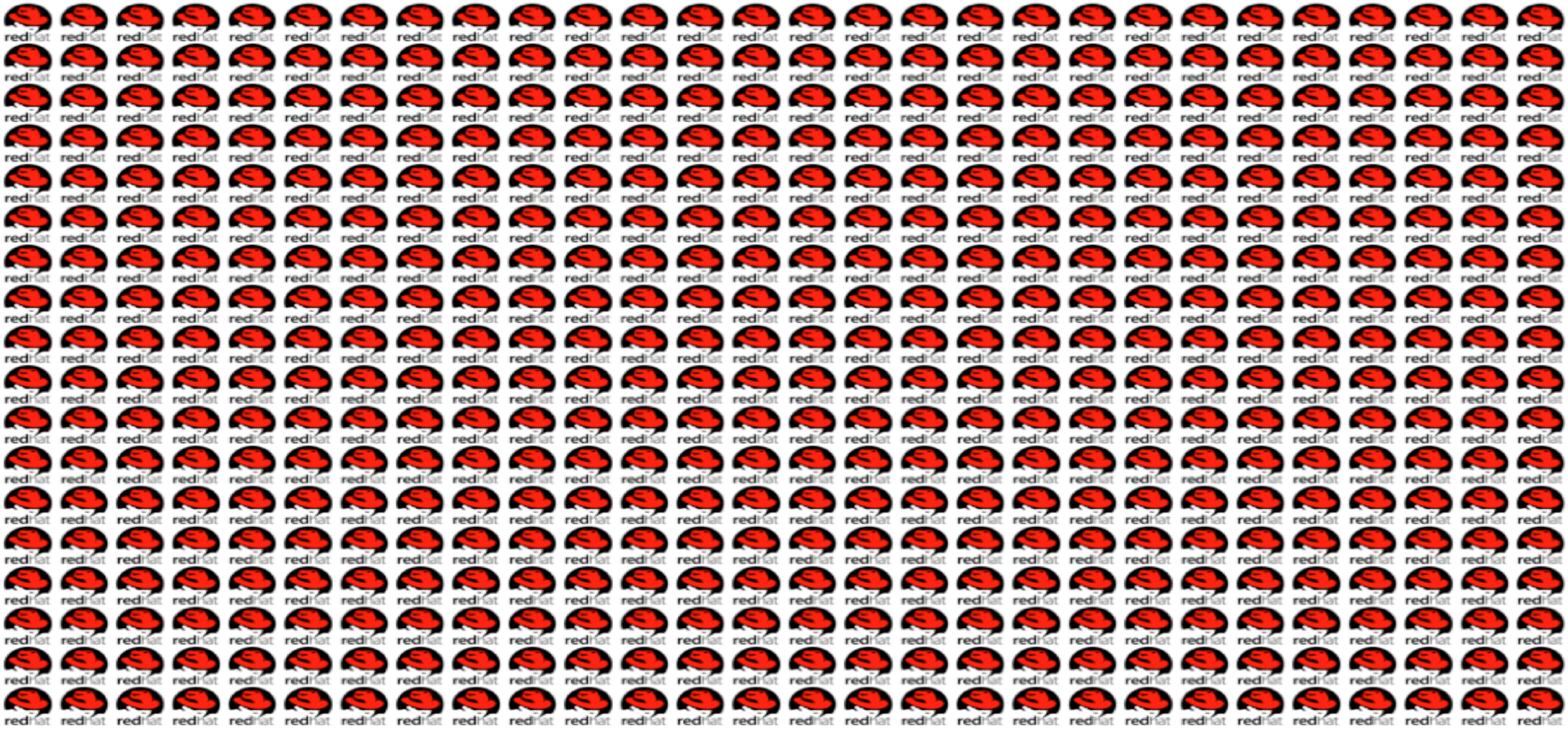
redhat.

PCI DSS configuration of SOE is required for all systems affected

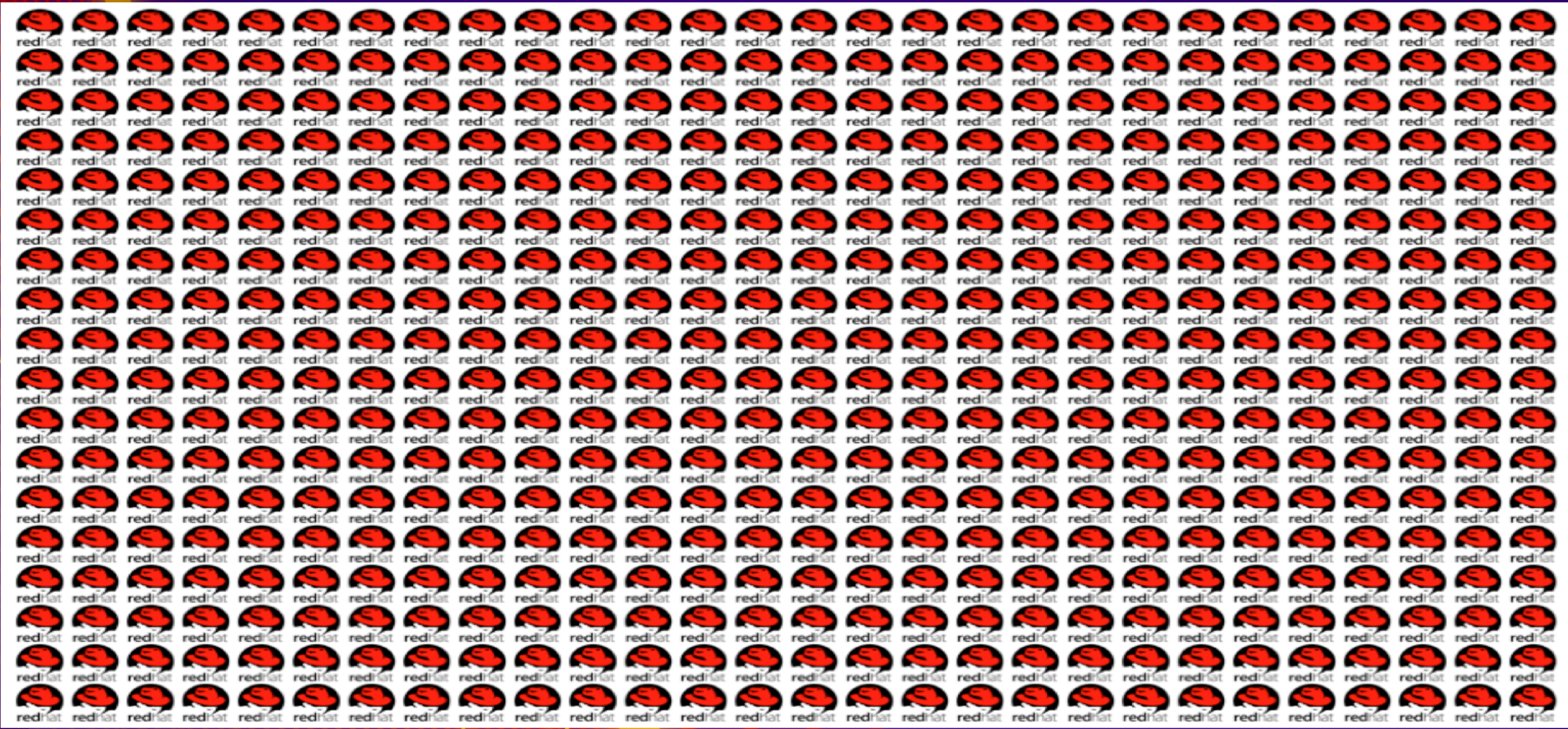


redhat.

Number of systems affected by PCI DSS compliance



Number of systems patched to RHEL-latest every 30 days



redhat.

Number of people required for patching 3500 servers ..in 2 ½ hours:

Me and Briju

redhat.

Total number of people working with Linux at IKEA IT

redhat.

Red Hat personnel

Account Manager

Technical Account Manager

Solution Architects (Regularly)

Consultants (on a need-to basis)

redhat.

Would it be an army of people..

BILLY

Bookcase, white

~~$59.99~~ **$1,000,000.99**

The price reflects selected options

Article Number: 836.882.10

Adjustable shelves can be arranged according to your needs. A simple unit can be enough storage for a limited space or the foundation for a larger storage solution if your needs change. Read more

Color

white

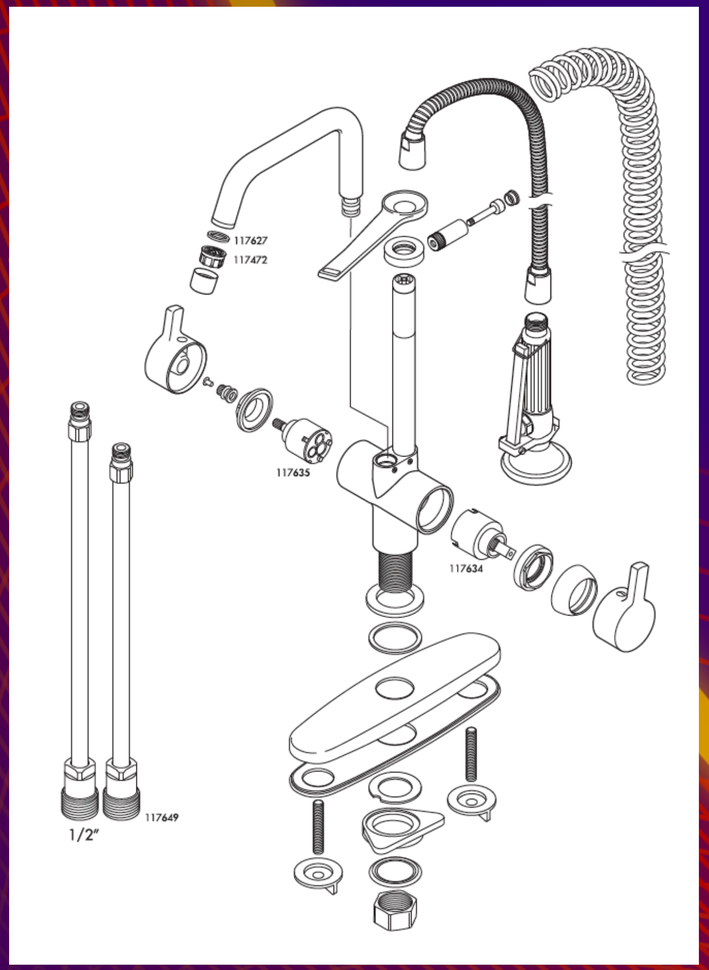
Size

31 1/2x11x79 1/2 "

1 **Buy online** **Save to list**

Coordinating Products

View all coordinating products



+

redhat

+

```
[me@ingvar5 ~]$ ./patch
Wed Sep 24 23:14:15 UTC 2014: Issuing 'yum -y update bash' to all servers..
Wed Sep 25 01:44:15 UTC 2014: Done.
[me@ingvar5 ~]$
```


redhat.

LEARN. NETWORK.
EXPERIENCE OPEN SOURCE.

redhat.