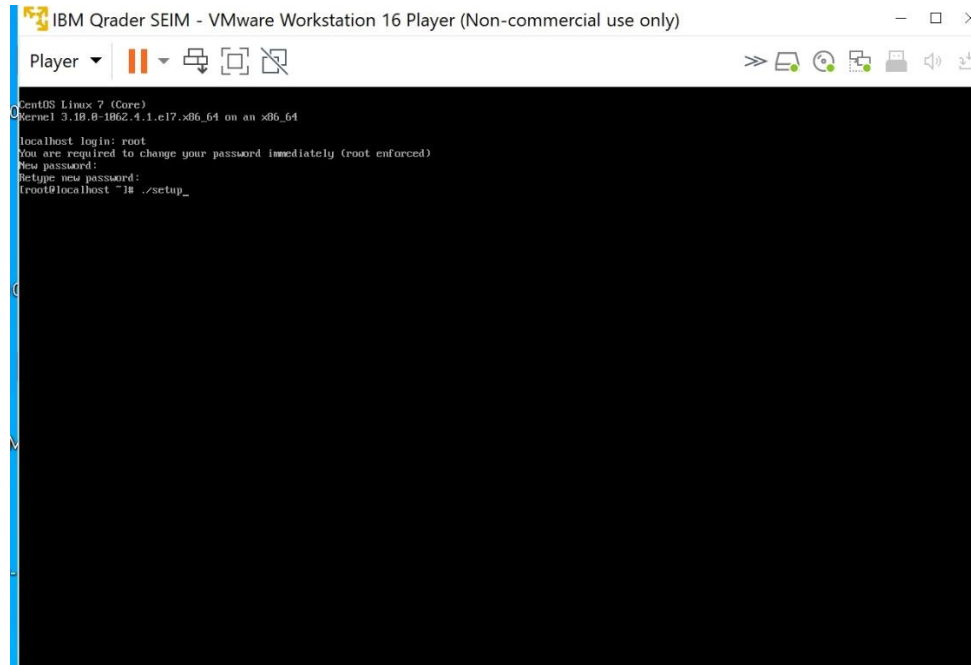


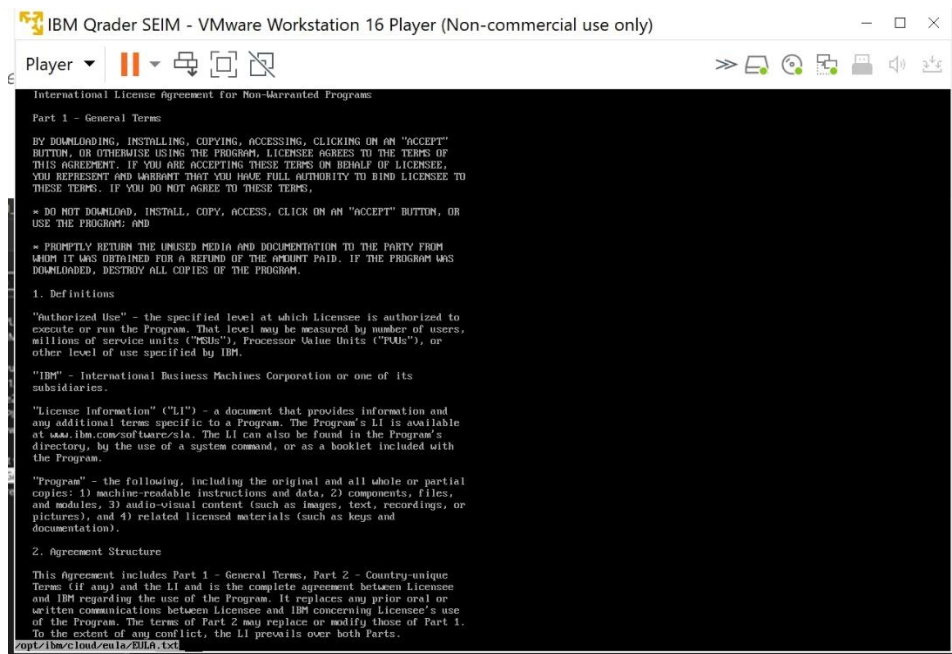
Lab 12-5-1: How to install Qrader SEIM in ICS

Installation Guide



```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.4.1.el7.x86_64 on an x86_64

localhost login: root
You are required to change your password immediately (root enforced)
New password:
Retype new password:
(root@localhost ~) # ./setup_
```



```
International License Agreement for Non-Warranted Programs

Part 1 - General Terms

BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN "ACCEPT"
BUTTON, OR OTHERWISE USING THE PROGRAM, LICENSEE AGREES TO THE TERMS OF
THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF LICENSEE,
YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE TO
THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,

= DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN "ACCEPT" BUTTON, OR
USE THE PROGRAM; AND

= PROMPTLY RETURN THE UNUSED MEDIA AND DOCUMENTATION TO THE PARTY FROM
WHICH IT WAS OBTAINED FOR A REFUND OF THE AMOUNT PAID. IF THE PROGRAM WAS
DOWNLOADED, DESTROY ALL COPIES OF THE PROGRAM.

1. Definitions

"Authorized Use" - the specified level at which Licensee is authorized to
execute or run the Program. That level may be measured by number of users,
millions of service units ("MSUs"), Processor Value Units ("PVUs"), or
other level of use specified by IBM.

"IBM" - International Business Machines Corporation or one of its
subsidiaries.

"License Information" ("LI") - a document that provides information and
any additional terms specific to a Program. The Program's LI is available
at www.ibm.com/software/sla. The LI can also be found in the Program's
directory, by the use of a system command, or as a booklet included with
the Program.

"Program" - the following, including the original and all whole or partial
copies: 1) machine-readable instructions and data, 2) components, files,
and modules, 3) audio-visual content (such as images, text, recordings, or
pictures), and 4) related licensed materials (such as keys and
documentation).

2. Agreement Structure

This agreement includes Part 1 - General Terms, Part 2 - Country-unique
Terms (if any) and the LI and is the complete agreement between Licensee
and IBM regarding the use of the Program. It replaces any prior oral or
written communications between Licensee and IBM concerning Licensee's use
of the Program. The terms of Part 2 may replace or modify those of Part 1.
To the extent of any conflict, the LI prevails over both Parts.

/opt/ibm/cloud/elastic/ELA.txt
```

IBM Qrader SEIM - VMware Workstation 16 Player (Non-cc -

Player ▾



```
Installing Qrader changes...
Activating system with key 3Q765S-5A4J6L-3D584Q-34891X.
Appliance ID is 388.
Installing 'QRadar Community Edition' with id 388.
Configuring network...
Setting current date and time.
Restarting postgresql-qrdr
Running changeQraderPassword
Stopping hostcontext
Stopping httpd
Stopping tomcat
```

IBM Qrader SEIM - VMware Workstation 16 Player (Non-cc -

Player ▾



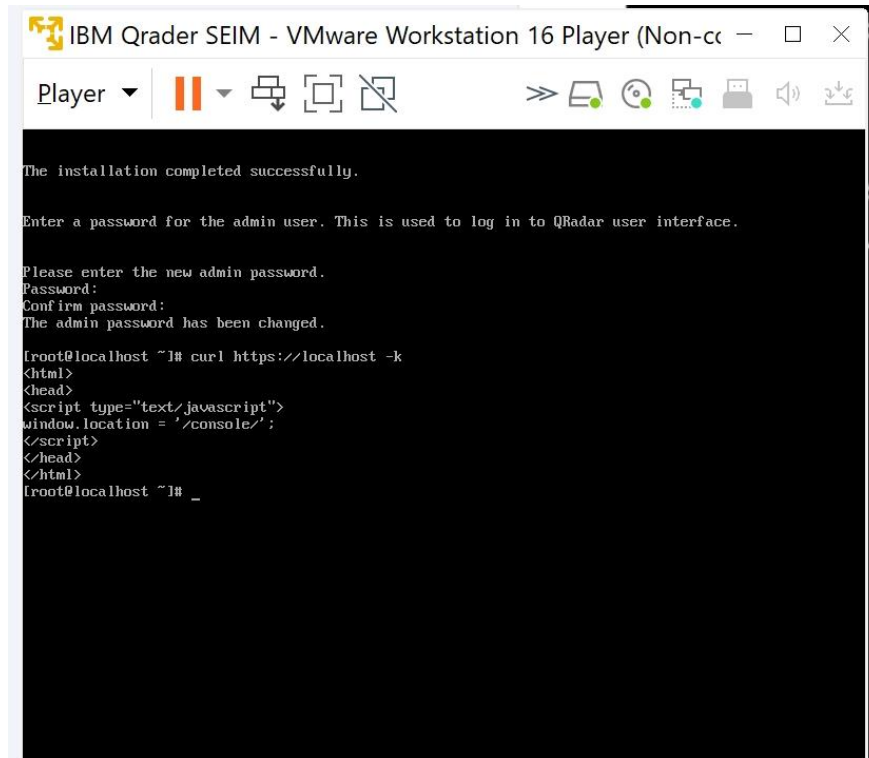
```
The installation completed successfully.

Enter a password for the admin user. This is used to log in to QRadar user interface.

Please enter the new admin password.
Password:
Confirm password:
The admin password has been changed.

[root@localhost ~]#
```

Verify the QRadar CE Installation

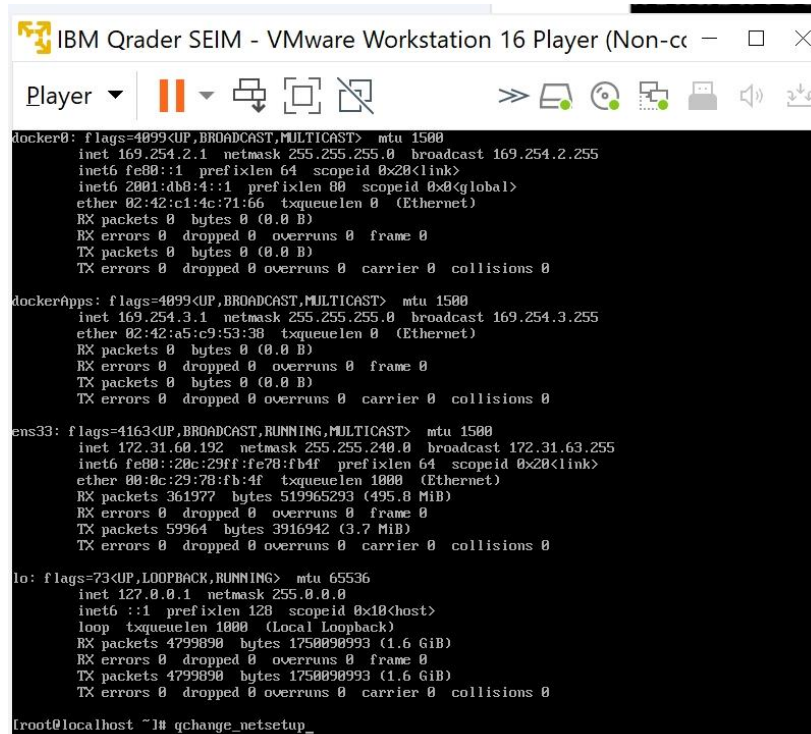


```
IBM QRadar SEIM - VMware Workstation 16 Player (Non-cc)
Player
The installation completed successfully.

Enter a password for the admin user. This is used to log in to QRadar user interface.

Please enter the new admin password.
Password:
Confirm password:
The admin password has been changed.

[root@localhost ~]# curl https://localhost -k
<html>
<head>
<script type="text/javascript">
window.location = '/console/';
</script>
</head>
</html>
[root@localhost ~]# _
```



```
IBM QRadar SEIM - VMware Workstation 16 Player (Non-cc)
Player
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 169.254.2.1 netmask 255.255.255.0 broadcast 169.254.2.255
    inet6 fe80::1 prefixlen 64 scopeid 0x20<link>
    inet6 2001:db8:4::1 prefixlen 80 scopeid 0x0<global>
    ether 02:42:c1:4c:71:66 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

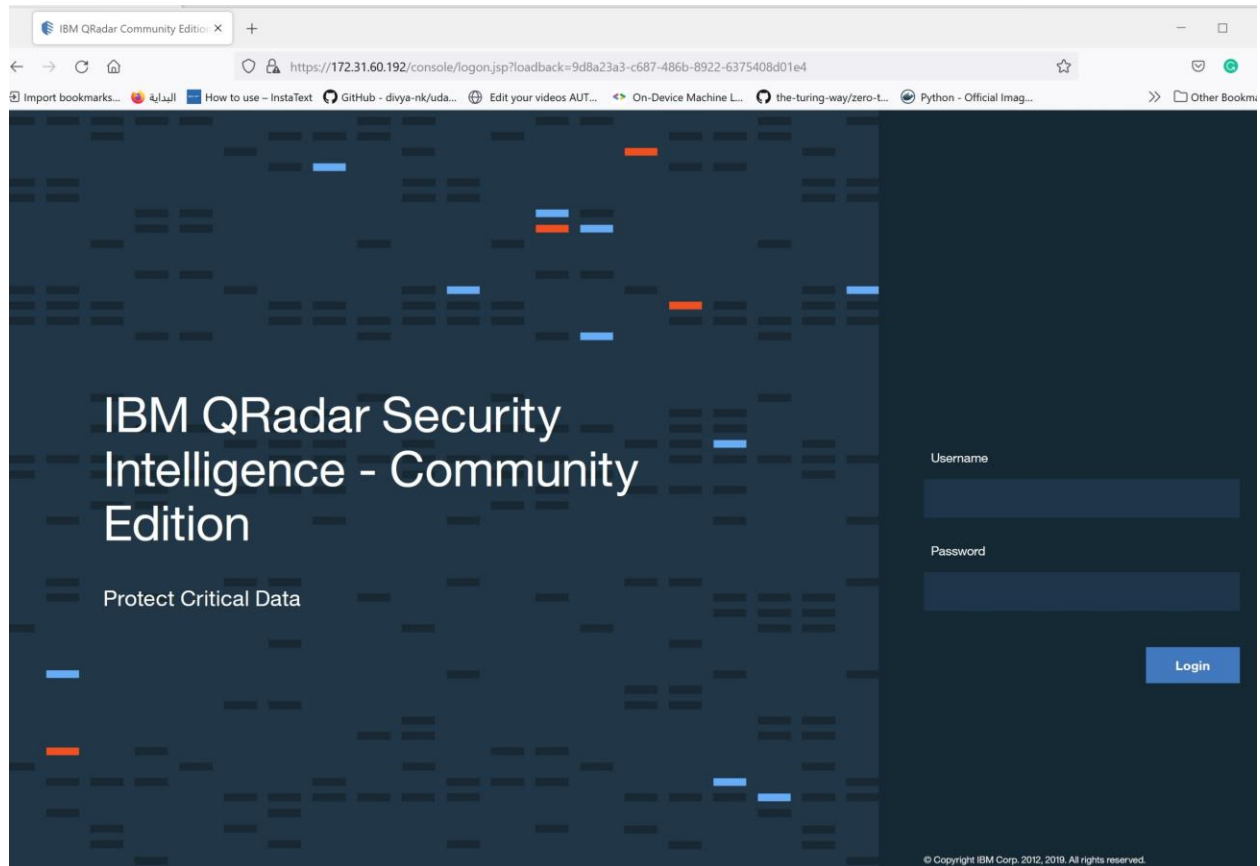
dockerapps: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 169.254.3.1 netmask 255.255.255.0 broadcast 169.254.3.255
    ether 02:42:a5:c9:53:38 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

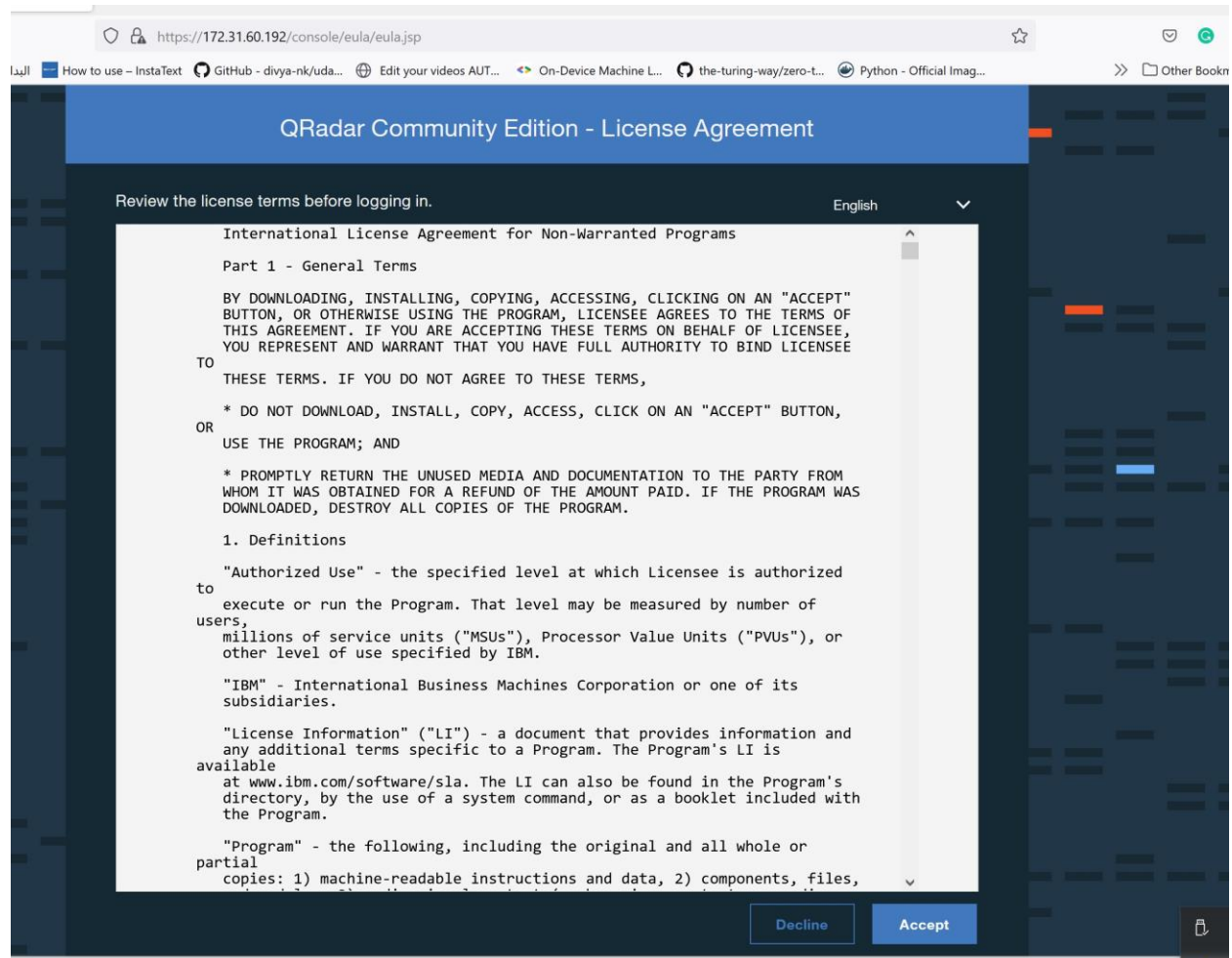
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.31.60.192 netmask 255.255.240.0 broadcast 172.31.63.255
    inet6 fe80::28c:29ff:fe78:fb4f prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:78:fb:4f txqueuelen 1000 (Ethernet)
    RX packets 361977 bytes 519965293 (495.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 59964 bytes 3916942 (3.7 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

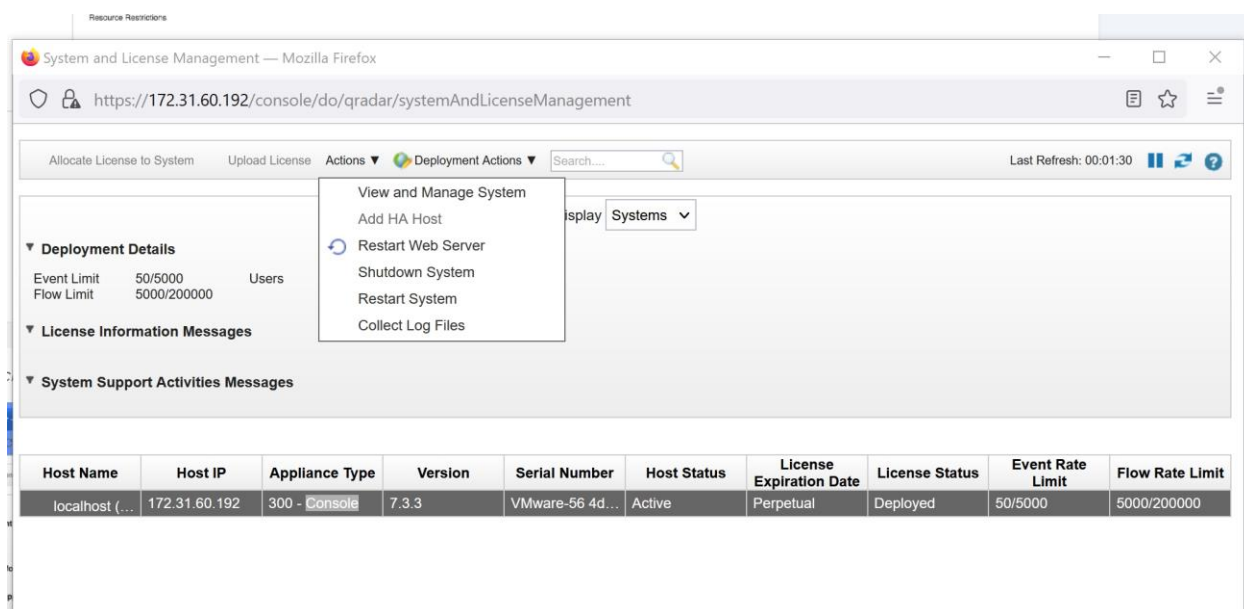
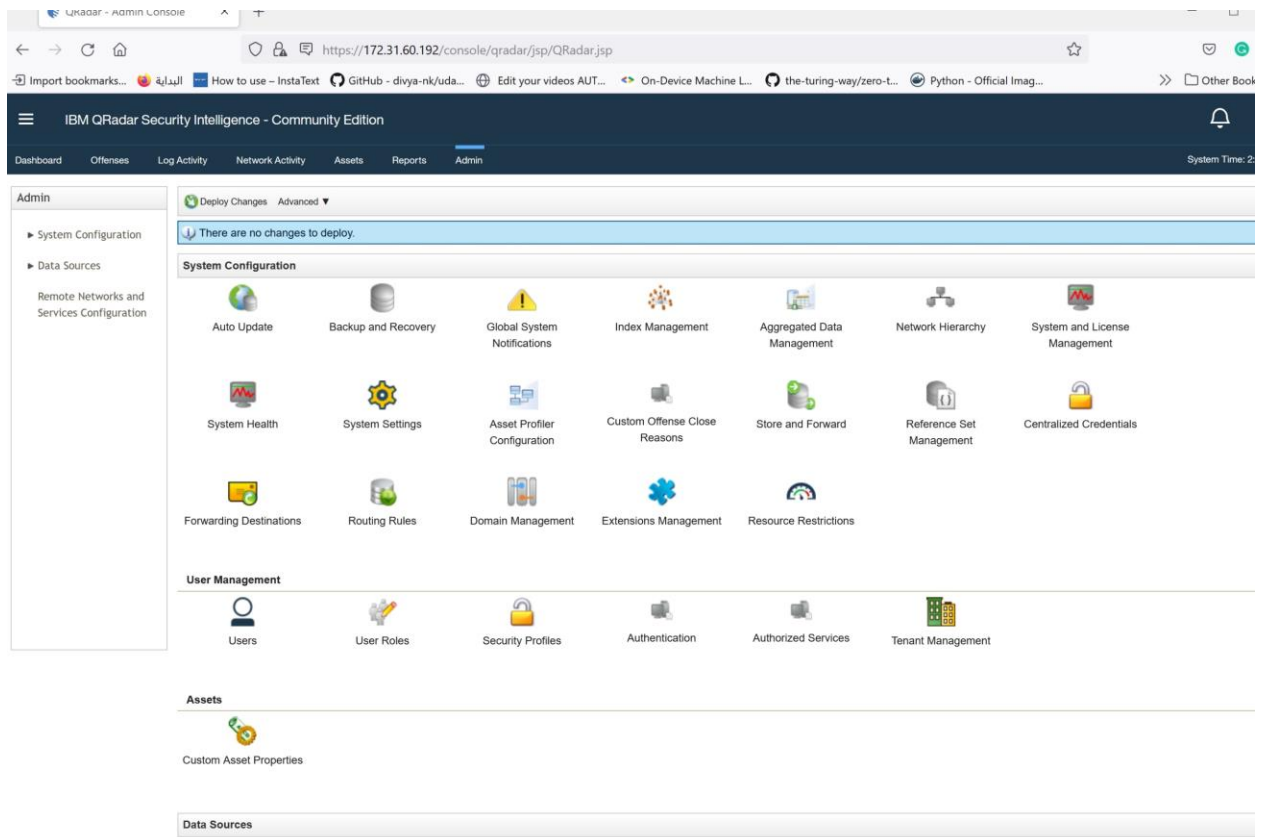
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4799890 bytes 1750090993 (1.6 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4799890 bytes 1750090993 (1.6 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

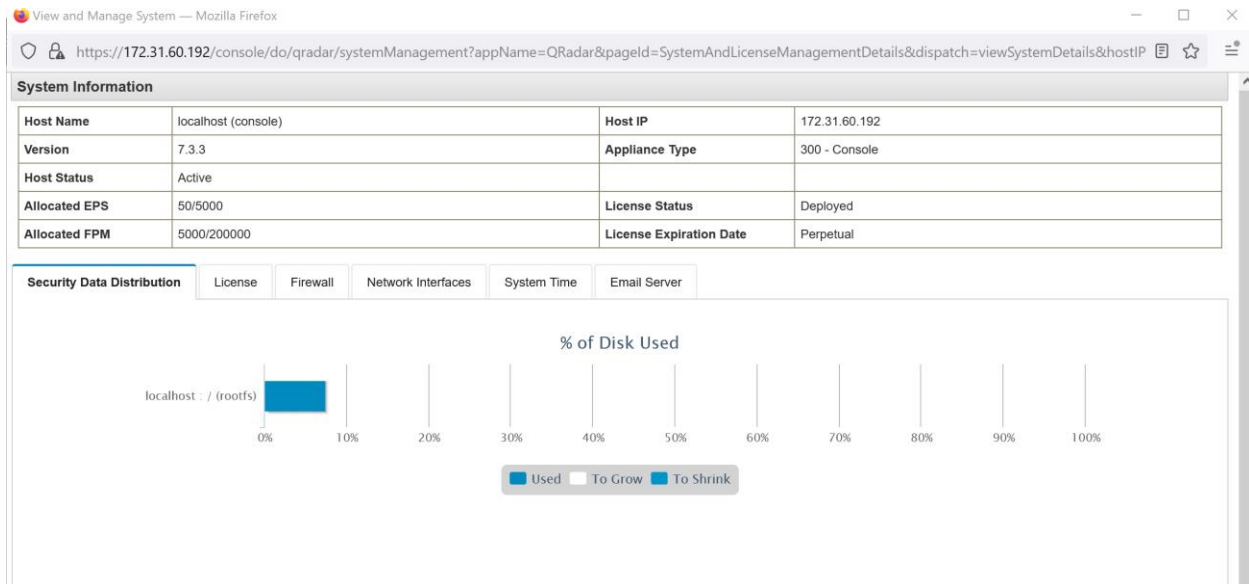
[root@localhost ~]# qchange_netsetup_
```

```
-bash: curl: command not found
[root@localhost ~]# curl https://172.31.60.192 -k
<html>
<head>
<script type="text/javascript">
window.location = '/console/';
</script>
</head>
</html>
[root@localhost ~]#
```









View and Manage System — Mozilla Firefox

https://172.31.60.192/console/do/qradar/systemManagement?appName=QRadar&pagelId=SystemAndLicenseManagementDetails&dispatch=viewSystemDetails&hostIP

System Information

Host Name	localhost (console)	Host IP	172.31.60.192
Version	7.3.3	Appliance Type	300 - Console
Host Status	Active		
Allocated EPS	50/5000	License Status	Deployed
Allocated FPM	5000/200000	License Expiration Date	Perpetual

Security Data Distribution

License Firewall Network Interfaces **System Time** Email Server

Time Zone:

(UTC+03:00) Asia/Riyadh

☒ Set time manually:

Date: 2/27/2022 Time: 3:03 AM

☐ Specify NTP servers:

Add four or more NTP servers to get the most accurate time.

+ Add More

Save

https://172.31.60.192/console/do/qradar/systemManagement?appName=QRadar&pagelId=SystemAndLicenseManagementDetails&dispatch=viewSystemDetails&hostIP

System Information

Host Name	localhost (console)	Host IP	172.31.60.192
Version	7.3.3	Appliance Type	300 - Console
Host Status	Active		
Allocated EPS	50/5000	License Status	Deployed
Allocated FPM	5000/200000	License Expiration Date	Perpetual

Security Data Distribution License Firewall Network Interfaces **System Time** Email Server

Time Zone:
(UTC+03:00) Asia/Riyadh

Services are restarted when you change the time setting, which interrupts data collection and causes the user interface to be unavailable for several minutes. Are you sure that you want to change the system time?

OK Cancel

☐ Specify NTP servers:

Add four or more NTP servers to get the most accurate time.

Add More

Save

View and Manage System — Mozilla Firefox

https://172.31.60.192/console/do/qradar/systemManagement?appName=QRadar&pagelId=SystemAndLicenseManagementDetails&dispatch=viewSystemDetails&hostIP

System Information

Host Name	localhost (console)	Host IP	172.31.60.192
Version	7.3.3	Appliance Type	300 - Console
Host Status	Active		
Allocated EPS	50/5000	License Status	Deployed
Allocated FPM	5000/200000	License Expiration Date	Perpetual

Security Data Distribution License Firewall Network Interfaces **System Time** Email Server

System Time is updated successfully. Services will now restart.

Time Zone:
(UTC+03:00) Asia/Riyadh

☒ Set time manually:

Date: 2/27/2022 Time: 3:17 AM

☐ Specify NTP servers:

Add four or more NTP servers to get the most accurate time.

Add More

Save