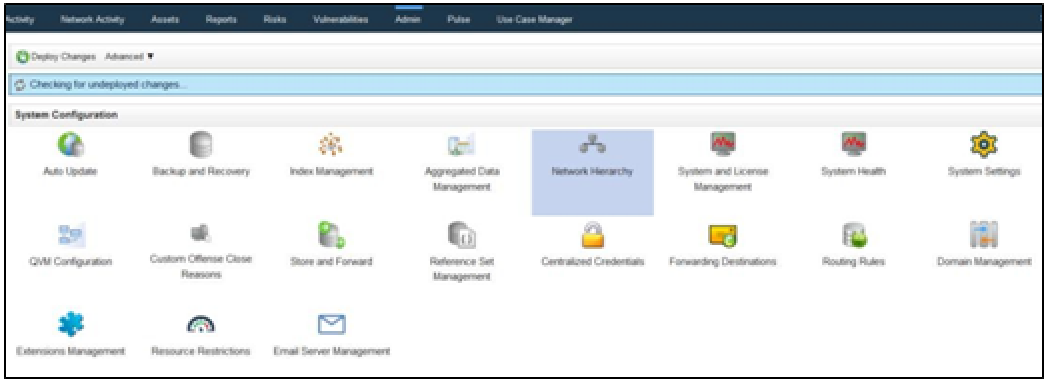
Using the Network Hierarchy

Using the Network Hierarchy

In this lab, we will explore the Network Hierarchy feature of Qradar. We will create and view a Network Hierarchy Object.

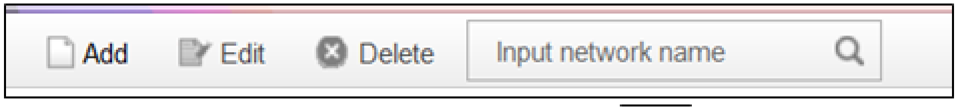
Create a Network Object

1. Navigate to the **Admin** tab and click the **Network Hierarchy** icon in the System configuration section.



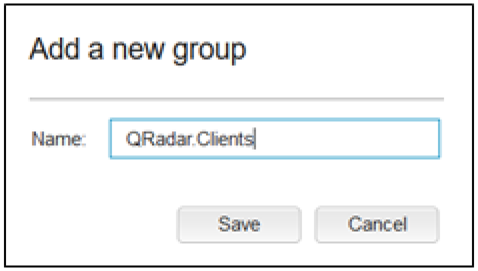
Checking for undeployed changes...

2. Click **Add.**



3. In the Add network window, click the ⚙ **Yellow gear wheel** icon.

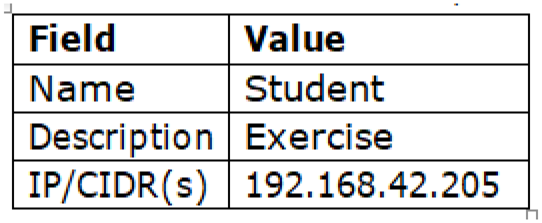
4. For **Name** in the Add a new Group window, enter the following text. QRadar.Clients and Click **Save.**



Add a new group

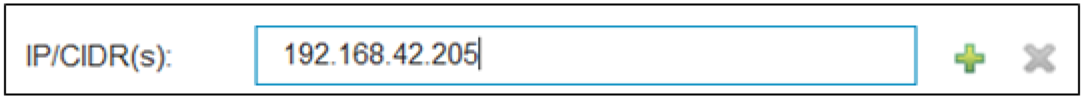
Name: QRadar.Clients

5. In the Add network Window, enter the values shown below.



Field	Value
Name	Student
Description	Exercise
IP/CIDR(s)	192.168.42.205

6. Make sure you click the plus icon to add the IP/CIDR(s) value to the object’s list.

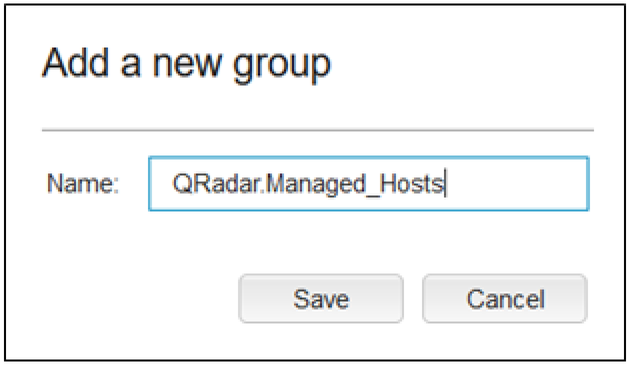


IP/CIDR(s): 192.168.42.205

7. Using the similar process from steps 2 to 6, add a new network object as per the below data.

a. In the Add network window, click the ⚙ **Yellow gear wheel icon.**

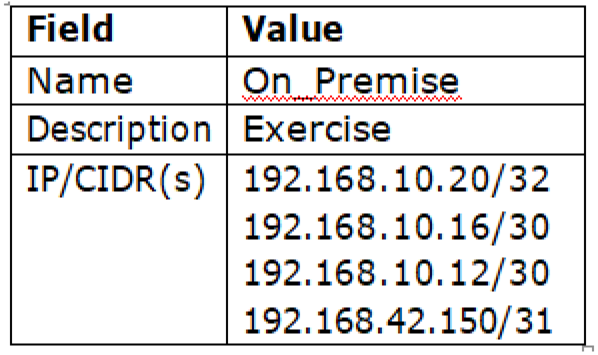
b. In the Name field, enter QRadar.Managed_Hosts. Click **Save.**



Add a new group

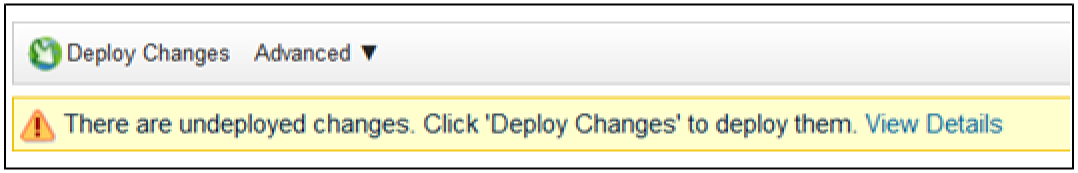
Name: QRadar.Managed_Hosts

c. In the add network window, enter the values shown as below.



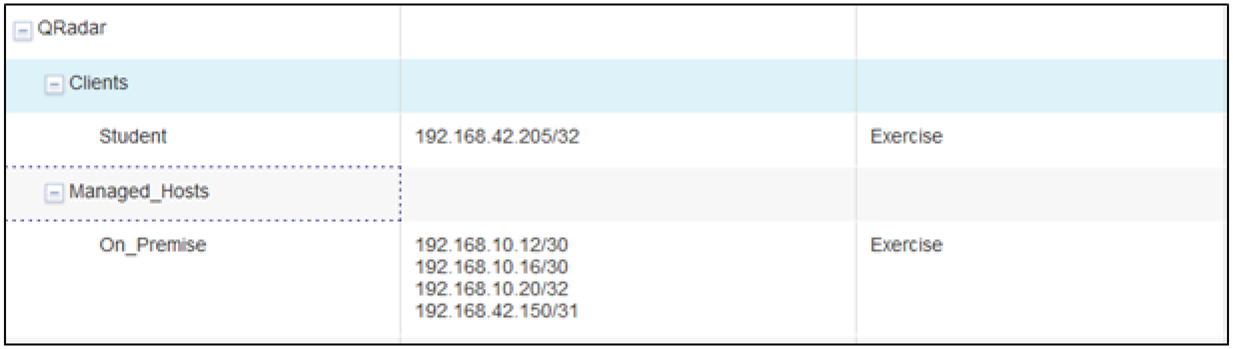
Field	Value
Name	On_Premise
Description	Exercise
IP/CIDR(s)	192.168.10.20/32 192.168.10.16/30 192.168.10.12/30 192.168.42.150/31

8. Close the Network Hierarchy Window and Click **Deploy Changes.**



There are undeployed changes. Click 'Deploy Changes' to deploy them.

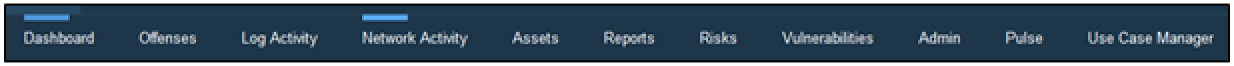
Open the Network hierarchy tab and verify that the **Student** and **On_Premise** network objects are listed.



QRadar		
Clients		
Student	192.168.42.205/32	Exercise
Managed_Hosts		
On_Premise	192.168.10.12/30 192.168.10.16/30 192.168.10.20/32 192.168.42.150/31	Exercise

View Network Objects in Flow

1. To view incoming flows, double-click the **Network Activity** tab.



Note: The double-click resets the tab to its default settings.

2. Wait until you see flows with the IP addresses 192.168.42.150 and 192.168.42.205.

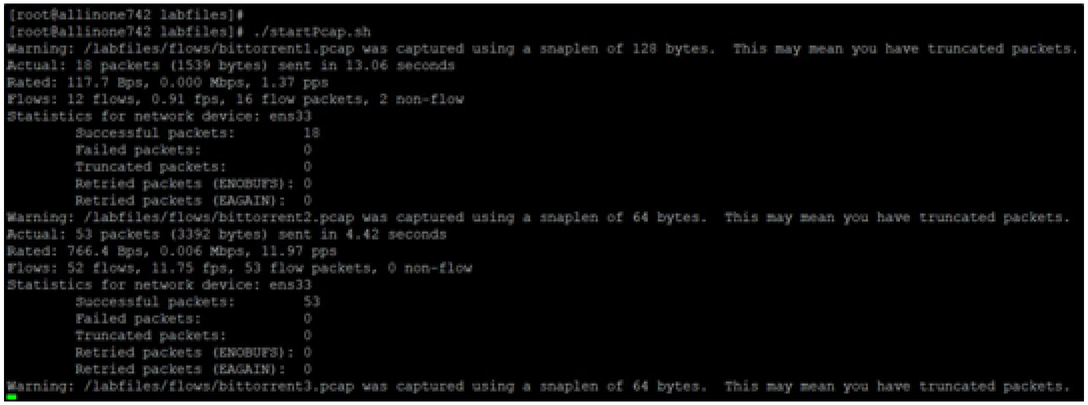
3. To pause the incoming events, click the **Pause** ⏸ icon in the upper-right corner of the QRadar user interface.

4. Hover the mouse over either of the IP addresses and review the Network field information.

5. Open a remote shell to the QRadar VM. And run the following commands:

```
cd /labfiles

./startPcap.sh
```



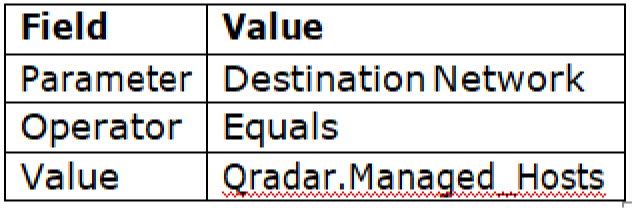
```
[root@allinone742 labfiles]#
[root@allinone742 labfiles]# ./startPcap.sh
Warning: /labfiles/flows/bittorrent1.pcap was captured using a snaplen of 128 bytes.  This may mean you have truncated packets.
Actual: 18 packets (1539 bytes) sent in 13.06 seconds
Rated: 117.7 Bps, 0.000 Mbps, 1.37 pps
Flows: 12 flows, 0.91 fps, 16 flow packets, 2 non-flow
Statistics for network device: ens33
        Successful packets:        18
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
Warning: /labfiles/flows/bittorrent2.pcap was captured using a snaplen of 64 bytes.  This may mean you have truncated packets.
Actual: 53 packets (3392 bytes) sent in 4.42 seconds
Rated: 766.4 Bps, 0.006 Mbps, 11.97 pps
Flows: 52 flows, 11.75 fps, 53 flow packets, 0 non-flow
Statistics for network device: ens33
        Successful packets:        53
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
Warning: /labfiles/flows/bittorrent3.pcap was captured using a snaplen of 64 bytes.  This may mean you have truncated packets.
```

6. In the browser return to the Network Activity Tab.

7. If refresh of the Network Activity tab is paused, press the **Play** button in the upper-right corner of the QRadar user interface. Wait for at least one minute.

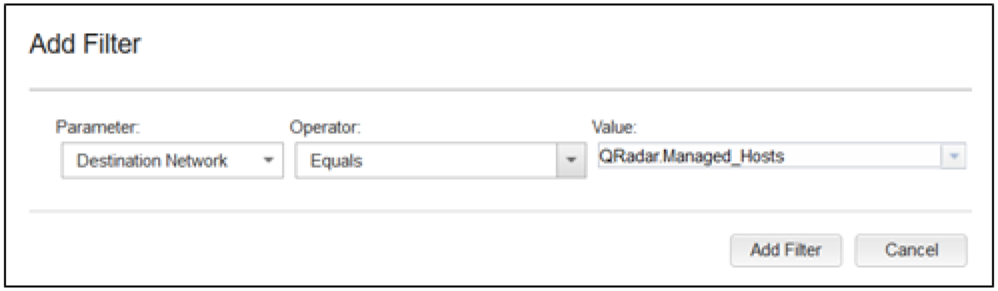
8. To display only flows with destination IP addresses part of the network objects you created, click **Add Filter** Add Filter.

a. In the Add Filter window, enter the values shown below.



Field	Value
Parameter	Destination Network
Operator	Equals
Value	Qradar.Managed_Hosts

b. Click **Add Filter.**



Add Filter

Parameter: Destination Network

Operator: Equals

Value: QRadar.Managed_Hosts

9. If there are no rows with a Destination Network of **On_Premise** listed.

10. Change the View to show the **Last Hour.**

11. Change the Display to **Destination Network.**

12. Use the right-click option menu on the Destination IP column to apply **Filter on Destination IP is not 192.168.42.150.**

13. Verify that you only see rows with Destination IP 192.168.10.12.

14. However the mouse over the Destination IP address and review the **Network** Field Information.

15. Navigate to the **Admin** tab, click the **Network Hierarchy** icon in the System Configuration section.

a. Click the plus signs in front of Qradar and Managed_Hosts.

b. Double click **On_Premise.**

c. Select **192.168.10.12/30** from the IP/CIDR(s) list and click the red **X.**

d. Click **Save.**

e. Close the **Network Hierarchy** Window.

f. Click **Deploy Changes.**

16. Return to the Network Activity page.

a. Hover the mouse over the Destination IP address and review the **Network** field information to verify that it no longer displays **QRadar.Managed_Hosts.On_Premise.**

b. Clear the **Destination Network is QRadar.Managed_Hosts** filter.

c. Reapply the **Destination Network is QRadar.Managed_Hosts** filter.

d. Verify that the result set is now empty.