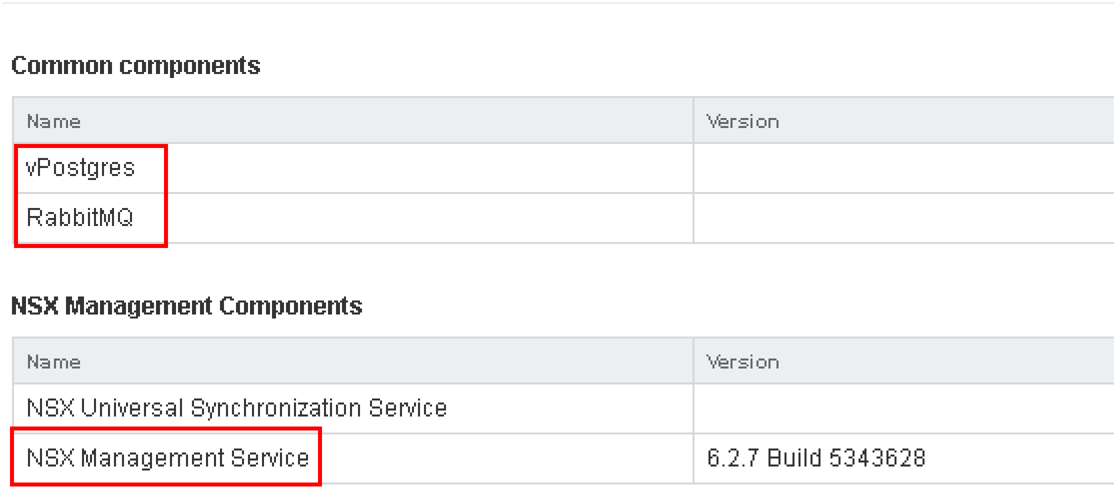
Troubleshooting Guide

1. Failed to add VMware NSX host
   1) Please check configuration or practical examples related with NSVM service in vCenter to make sure if they are deleted first, and please read chapter 13 “Un stall the security module of host” in this file.
   2) Enter into the page of NSX Manager to make sure that if the service status of vPostgres, RabbitMQ and NSX Management Service are correct.



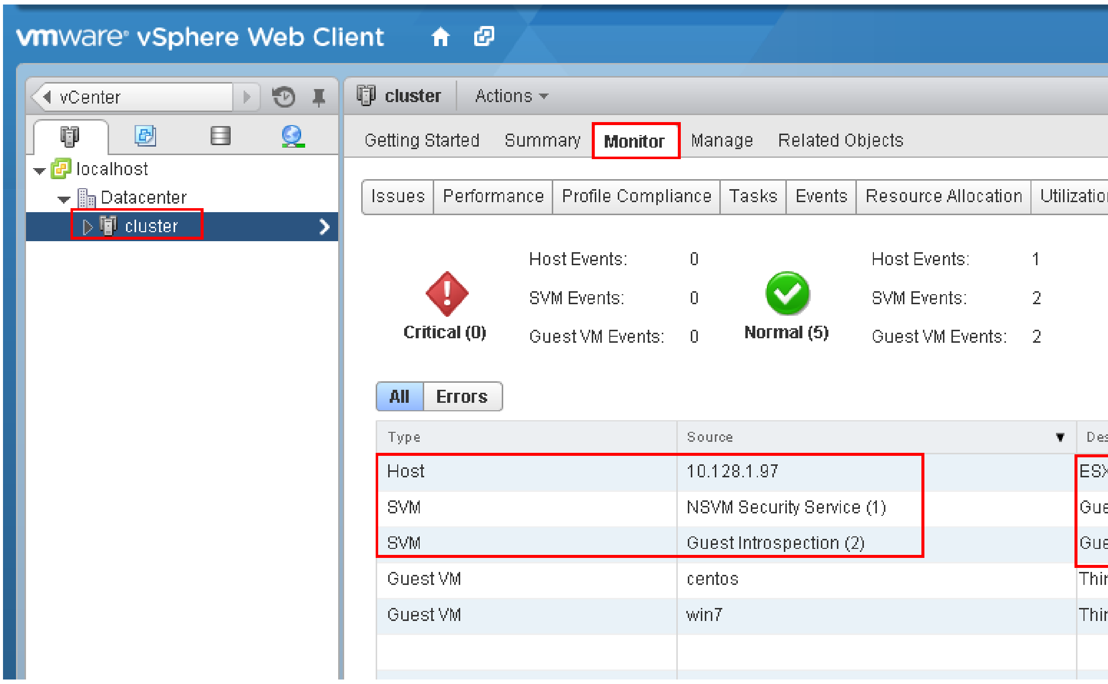
Common components

Name	Version
vPostgres	
RabbitMQ	

NSX Management Components

Name	Version
NSX Universal Synchronization Service	
NSX Management Service	6.2.7 Build 5343628

2. The VM cannot kill virus.
   1) First Login Vcenter Vsphere Web Client, select “cluster” in the page of “ local host and cluster”, then enter into the page of “ Monitor-Guest Introspection”, and check if the description and status of host, NSVM Security Service, Guest Introspection are correct.



Critical (0)	
Host Events:	0
SVM Events:	0
Guest VM Events:	0

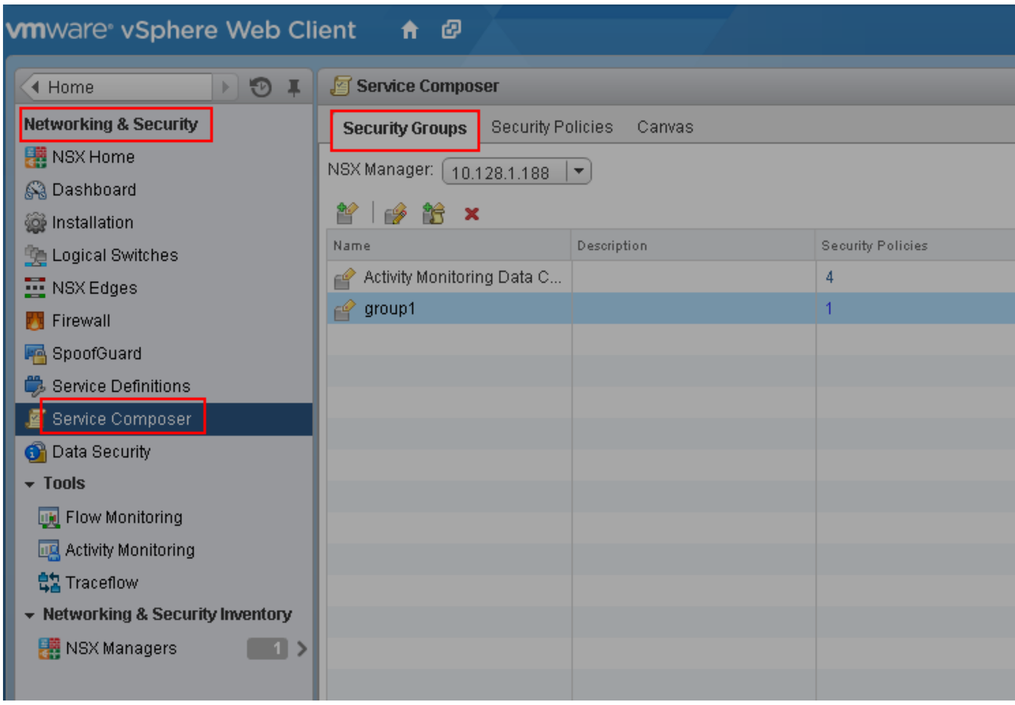
Normal (5)	
Host Events:	1
SVM Events:	2
Guest VM Events:	2

Type	Source	Des
Host	10.128.1.97	ESX
SVM	NSVM Security Service (1)	Gue
SVM	Guest Introspection (2)	Gue
Guest VM	centos	Thir
Guest VM	win7	Thir

2) Then according to the VM operating system for troubleshooting.

- **Windows VM**

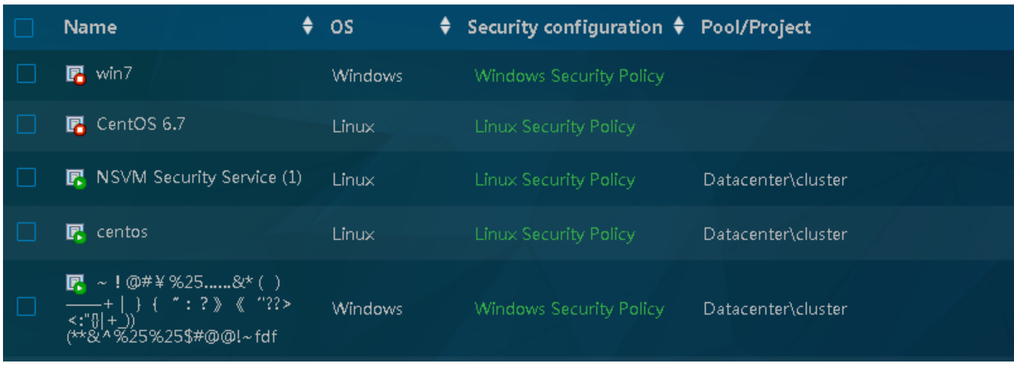
a) Enter into the page of " Networking & Security" –"Service Composer "–"Security Groups" in vCenter vSphere Web Client, and click the value of VM in the Security Groups, then check if the windows VM is included in the security groups in the dialog box.



NSX Manager: 10.128.1.188

Name	Description	Security Policies
Activity Monitoring Data C...		4
group1		1

b) Check if the configuration applied in this windows VM have turned on “ Real-time protection”. Login management center, enter into the page of “ Asset Management- VM/Terminal” to check the status of “ Real-time protection”. If the status is not “ Real-time protection on”, please change the security configuration matched and turn on “ Real-time protection”.

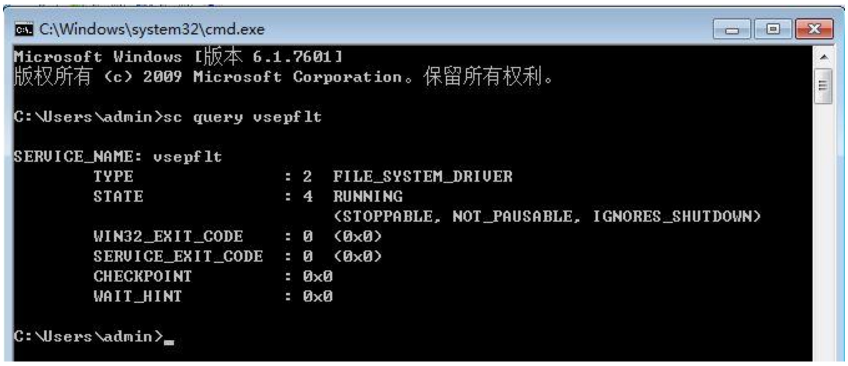


□	Name	OS	Security configuration	Pool/Project
□	win7	Windows	Windows Security Policy	
□	CentOS 6.7	Linux	Linux Security Policy	
□	NSVM Security Service (1)	Linux	Linux Security Policy	Datacenter\cluster
□	centos	Linux	Linux Security Policy	Datacenter\cluster
□	~ ！@#￥%25……&*（ ） ——+ | }{ “ : ?》《 ‘’??> <:"{}|+_)) (**&^%25%25$#@@!~fdf	Windows	Windows Security Policy	Datacenter\cluster

c) Then check if this VM has already installed with VMware tools and “NSX File Introspection Driver” by custom installation.

d) In the command line of VM to run “scquery vsepflt” and check if the service is existing. The following picture1 shows that is normal; the picture2 shows the service is unavailable.

Service is normal：



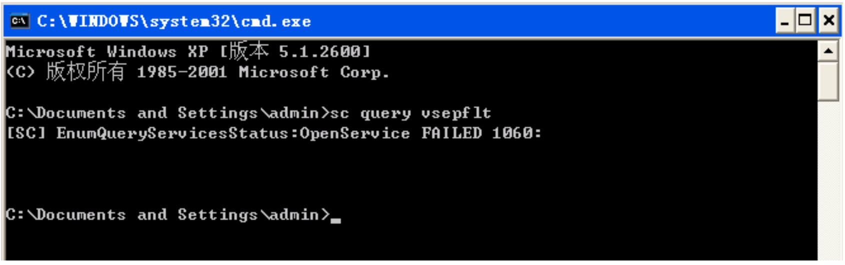
```
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\admin>sc query vsepflt

SERVICE_NAME: vsepflt
        TYPE               : 2  FILE_SYSTEM_DRIVER
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\Users\admin>_
```

Service is unavailable, please install VMware tools again:

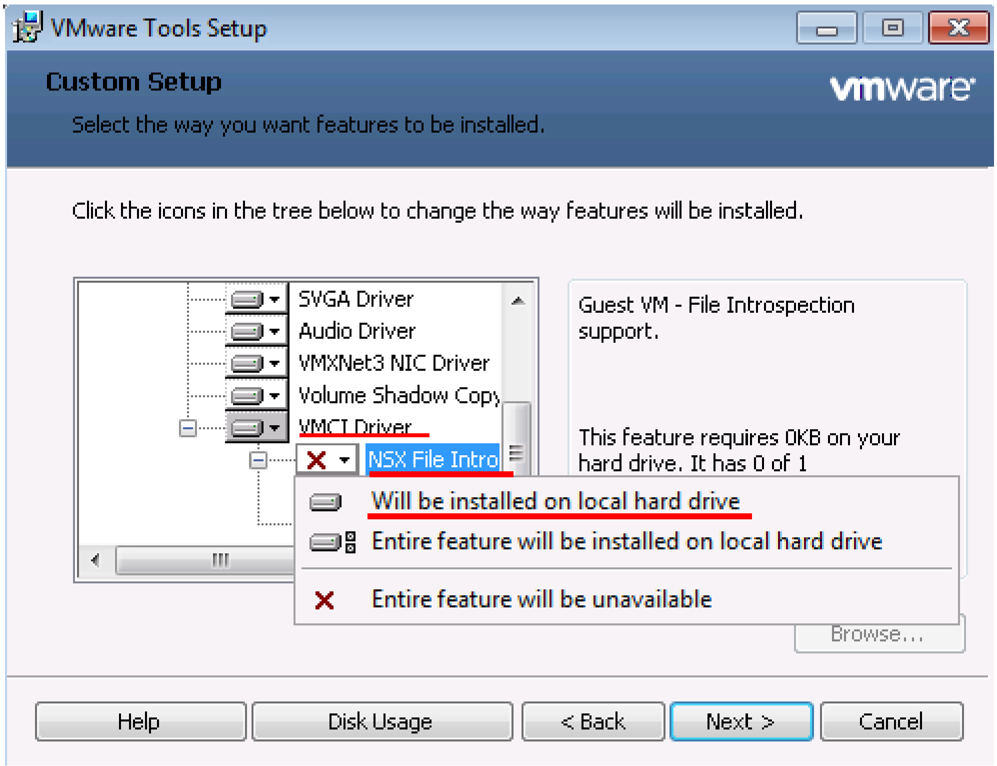


```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\admin>sc query vsepflt
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:


C:\Documents and Settings\admin>_
```

e) If the service is unavailable, please install VMware tools again, and select the driver of NSX File Introspection under “ VMCI driver” by custom installation. After installation, reboot VM and make sure that VMware tools has been installed.



VMware Tools Setup

Custom Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

Guest VM - File Introspection support.

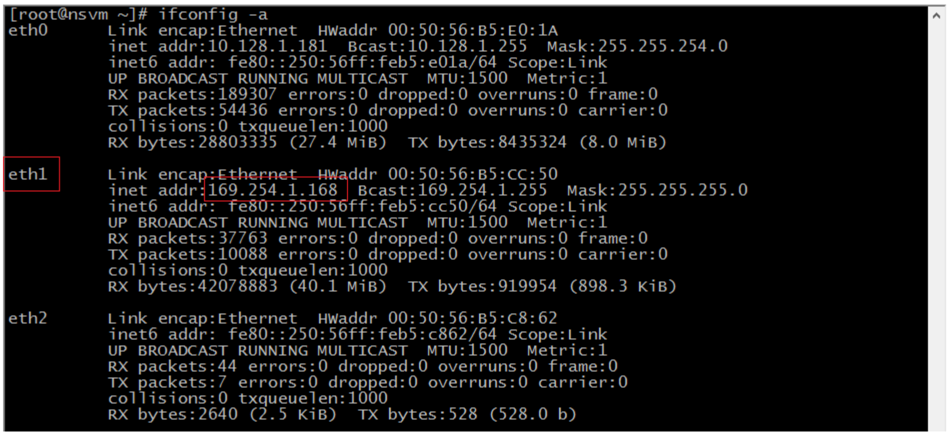
This feature requires 0KB on your hard drive. It has 0 of 1

Versions before vSphere 5.5 U2 should search “VMCI driver”, and select to install “vShield Drivers” to local disk

Find “VMCI driver” and select “vShield Drivers” to install it in local disk.

PS: If there is not “ NSX File Introspection Driver” or the option of “ vShield Drivers” like the picture above in the dialog box of “VM ware Tools”, which means that the version of VMware Tools is old, you need download the new version of VMware Tools. And this is the website: https://packages.vmware.com/tools/esx

f) Check the security VM of host. Login this security VM through console or SSH and execute the command of “ifconfig-a”, and the IP of eth1 is as following:

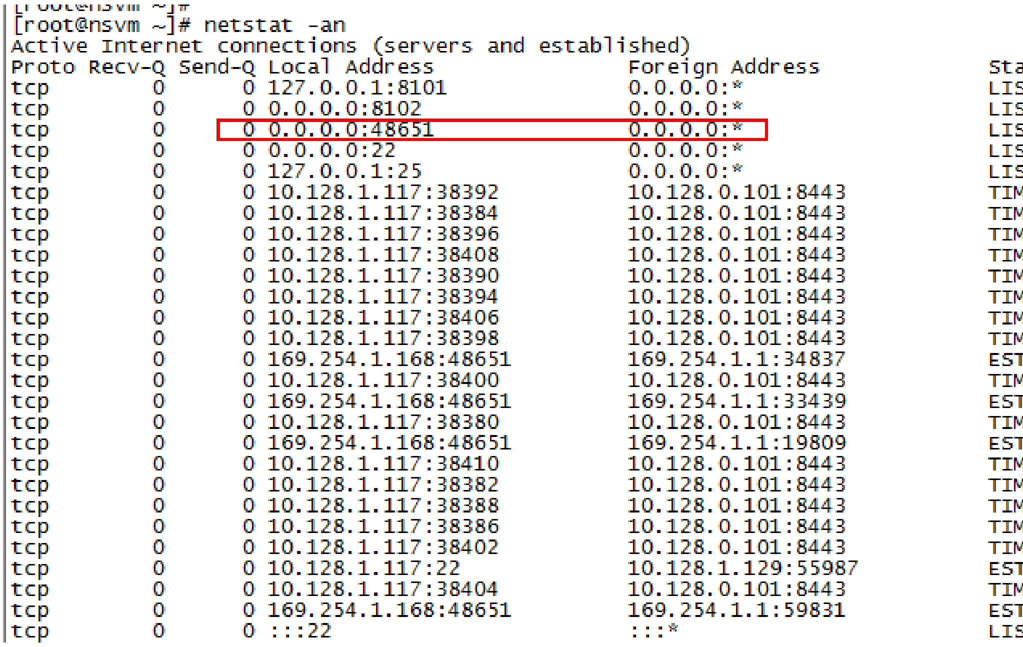


```
[root@nsvm ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:50:56:B5:E0:1A
          inet addr:10.128.1.181  Bcast:10.128.1.255  Mask:255.255.254.0
          inet6 addr: fe80::250:56ff:feb5:e01a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:189307 errors:0 dropped:0 overruns:0 frame:0
          TX packets:54436 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:28803335 (27.4 MiB)  TX bytes:8435324 (8.0 MiB)

eth1      Link encap:Ethernet  HWaddr 00:50:56:B5:CC:50
          inet addr:169.254.1.168  Bcast:169.254.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb5:cc50/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:37763 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10088 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:42078883 (40.1 MiB)  TX bytes:919954 (898.3 KiB)

eth2      Link encap:Ethernet  HWaddr 00:50:56:B5:C8:62
          inet6 addr: fe80::250:56ff:feb5:c862/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:44 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2640 (2.5 KiB)  TX bytes:528 (528.0 b)
```

g) Test security and the communication of VM. You can ping the IP169.254.1.1 of vmsevice-nvmsec-pg from security VM. Security process monitors TCP48651 port of this machine. If the protected VM is enabled, it will connect with local 8000 port.

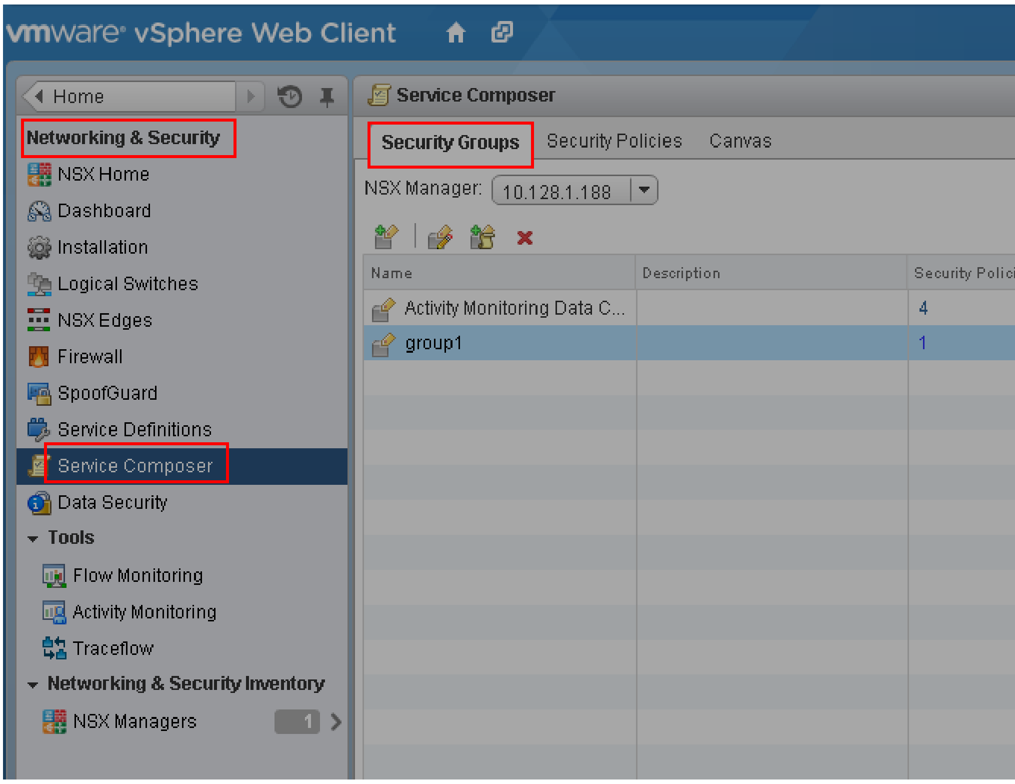


```
[root@nsvm ~]#
[root@nsvm ~]# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             Sta
tcp        0      0 127.0.0.1:8101              0.0.0.0:*                   LIS
tcp        0      0 0.0.0.0:8102                0.0.0.0:*                   LIS
tcp        0      0 0.0.0.0:48651               0.0.0.0:*                   LIS
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LIS
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LIS
tcp        0      0 10.128.1.117:38392          10.128.0.101:8443           TIM
tcp        0      0 10.128.1.117:38384          10.128.0.101:8443           TIM
tcp        0      0 10.128.1.117:38396          10.128.0.101:8443           TIM
tcp        0      0 10.128.1.117:38408          10.128.0.101:8443           TIM
tcp        0      0 10.128.1.117:38390          10.128.0.101:8443           TIM
tcp        0      0 10.128.1.117:38394          10.128.0.101:8443           TIM
tcp        0      0 10.128.1.117:38406          10.128.0.101:8443           TIM
tcp        0      0 10.128.1.117:38398          10.128.0.101:8443           TIM
tcp        0      0 169.254.1.168:48651         169.254.1.1:34837           EST
tcp        0      0 10.128.1.117:38400          10.128.0.101:8443           TIM
tcp        0      0 169.254.1.168:48651         169.254.1.1:33439           EST
tcp        0      0 10.128.1.117:38380          10.128.0.101:8443           TIM
tcp        0      0 169.254.1.168:48651         169.254.1.1:19809           EST
tcp        0      0 10.128.1.117:38410          10.128.0.101:8443           TIM
tcp        0      0 10.128.1.117:38382          10.128.0.101:8443           TIM
tcp        0      0 10.128.1.117:38388          10.128.0.101:8443           TIM
tcp        0      0 10.128.1.117:38386          10.128.0.101:8443           TIM
tcp        0      0 10.128.1.117:38402          10.128.0.101:8443           TIM
tcp        0      0 10.128.1.117:22             10.128.1.129:55987          EST
tcp        0      0 10.128.1.117:38404          10.128.0.101:8443           TIM
tcp        0      0 169.254.1.168:48651         169.254.1.1:59831           EST
tcp        0      0 :::22                       :::*                        LIS
```

- **Linux VM**

a) Make sure if the operating system of linux VM is supported, refer to Appendix-Linux OS lists of support.

b) Enter into the page of " Networking & Security"- "Service Composer"-"Security Groups " in vCenter vSphere Web Client, click the value of "VM" lists in the page of security groups, then check if the Linux VM is included by security groups in the dialog box.



NSX Manager: 10.128.1.188

Name	Description	Security Polici
Activity Monitoring Data C...		4
group1		1

c) Check if the configuration applied in this linux VM have turned on “ Real-time protection”. Login management center, enter into the page of “ Asset Management- VM/Terminal” to check the status of “ Real-time protection”. If the status isn’t “ Real-time protection on”, please change the security configuration matched and turn on “ Real-time protection”.

d) Enter into the command line of linux VM, check through the command of service vseped status if the service status of vseped is correct, and the normal is running.