IMPLEMENTATION GUIDE



Security Solution Implementation Installation Guide

Intel Corporation Datacenter Network Solutions Group

Authors

Eduardo Castro Solution Software Engineer, Intel Corporation

Tarek Radi Lead Technical Program Manager, Intel Corporation





1.0 Introduction

Cerner Corporation, Intel Corporation, and Midokura have teamed up to deliver a complete Red Hat Enterprise OpenStack Platform*-based virtual security solution that provides visibility and control against malicious activities within the software-defined data center of Cerner Corporation, securing east-west traffic.

Cerner Corporation is providing its services with private clouds. One of the results of the strict security policy in Cerner is the use of physical devices with intrusion prevention systems (IPS) and intrusion detection systems (IDS), located at the edge of the data centers. Currently, any traffic at Cerner's private cloud must be redirected to remote, physical IPS/IDS devices for packet inspection.

Even if two interconnected virtual machines (VMs) are located on the same physical host, the traffic from the source VM is redirected via the Midokura Enterprise MidoNet* virtual switch to the router and the gateway at the edge of the cloud, to reach IPS/IDS devices. Then it is sent back through the gateway to the cloud, and through the router and vSwitch to the target VM. Such behavior is known as a trombone effect and has a significant, negative impact on the overall latency.

The proposed solution eliminates the trombone effect and minimizes latency because traffic is inspected locally within the cloud through the use of virtual security functions. In this solution, we do not replace the physical IPS/IDS appliances. These are still used to inspect the north-south and east-west traffic coming from outside the cloud. To support inspection of the east-west traffic within the same cloud, we installed virtual IPS (vIPS) functions at each compute node of the cloud.

This Solution Implementation installation document presents the installation and configuration of the software components of this virtualized security solution. The setup is based on the Red Hat Enterprise Linux* 7.1 operating system and the Red Hat OpenStack Platform 7 for the orchestration of the cloud infrastructure, enabling better scalability and automated deployment of virtual functions. The level of security and performance of the cloud solution is at least as good as that of physical IPS appliances.

The primary audiences for this document are architects and engineers who are interested in implementing security protection mechanisms in an SDN/NFV environment; however, the presented solution is by no means a large-scale, general-purpose solution that can be applied to any NFV use case. Readers should use this document as a demonstration of how effective protection against internal-to-internal attacks is possible in SDN/NFV. They can follow the steps documented herein to build their own proof-of-concept topology and scale it.

It is important to note that the details contained herein are just an example of one way of applying security functions for a customer. Intel does not aim to promote or recommend any specific hardware, software, or supplier mentioned in this document. In addition, Intel does not aim to tie customers to any specific software and hardware stack.

For an overview of this security solution, including the hardware and software components used, please refer to the Security Solution Implementation Summary.

Table of Contents

1.0 Introduction	1
2.0 Solution Configuration	3
3.0 Installation Guide	4
3.1 Prerequisites to Installation of Red Hat Enterprise Linux 7.1	4
3.2 Installation of Red Hat OpenStack Platform* 7	5
3.3 Installing Midokura Enterprise MidoNet	5
3.3.1 OpenStack Networking* Integration	6
3.3.2 Apache ZooKeeper* Installation	7
3.3.3 Apache Cassandra* Installation	8
3.3.4 Midokura Enterprise MidoNet Cluster Installation	9
3.3.5 Midokura Enterprise MidoNet CLI Installation.	9
3.3.6 MidoNet Agent* (Midolman) Installation	9
3.4 Adding a Compute Node to OpenStack with MidoNet	0
3.4.1 Testing the New Compute Node1	2
3.5 Adding Uplink to an External (Public) Network1	3
3.6 Midokura Enterprise MidoNet Analytic Installation1	6
3.6.1 Prerequisites	6
3.6.2 Quickstart	6
3.6.3 Configuration	7
3.6.4 Files and Directories	9
3.6.5 Usage1	9
3.6.6 Update the OpenStack EndPoints1	9
3.7 OpenStack Deployment—Create Tenants	20
3.8 Creating and Testing a Web Server	2
3.9 Windows* VM Configuration	2
3.10 Network Security Manager Installation	2 4
3.11 Open Security Controller (OSC) Installation	27
3.12 F5 Load Balancer Installation	31
4.0 Demo Setup: Cross-Tenant Cross-Machine Attack3	;4
Appendix A: The PackStack Answer File	57
Appendix B: Updating the vIPS Sensor Image (Upgrade Version)	0
Appendix D: Abbreviations	11

2.0 Solution Configuration

This section provides the data definitions specific to the setup and configuration that appear as examples in this installation guide. This section lists all relevant configuration items, such as network Internet Protocol (IP addresses), IP ranges, ports, and interfaces, in the form of a data dictionary and is intended to help you plan in advance the configuration of your setup.

Disclaimer: Please note that not all the data specific to the setup were listed in this section. Some type of data, including various kinds of IDs, labels, and so on might have been generated automatically or are not editable; however, such data will be present in the installation steps of this guide. For these kinds of commands and outputs, you will experience different values, specific to the setup.

For the setup presented in this installation guide, each node is connected to three different networks:

- External network (herein also called a Public network) is used as an external gateway. This network is needed for the uplink in Midokura Enterprise MidoNet.
- Management Network is the network where OpenStack is installed; however, in this document, for the sake of simplification and easier connectivity to the OpenStack Dashboard*, we use the same external network as the management network. This means that in this setup two network interfaces are connected to the same external network per server.
- **Data network** where the virtual extensible local area network (VxLAN) tunnels are allocated.

	CONTROLLER/COMPUTE1	COMPUTE2	СОМРИТЕЗ	ANALYTIC SERVER
Host	host0	host1	host2	
Host name	MultinodeController.ch.intel.com	CernerMidonet	MultinodeCompute1.ch.intel.com	AnalyticServer
Gateway	10.250.101.1			
DNS1	10.248.2.1			
DNS2	10.2.71.6			
DNS3	10.19.1.4			

Table 1. Basic host and connectivity information.

Table 2. Physical network interface addresses.

	EXTERNAL NETWORK	MANAGEMENT NETWORK	DATA NETWORK
Subnet ID	10.250.101.0	10.250.101.0	172.16.10.0
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0

Table 3. Physical network interface devices.

NETWORK	CONTROLLER/COMPUTE1	COMPUTE2	COMPUTE3	MIDONET ANALYTIC SERVER	
External	enp4s0f3	enp4s0f0	ens20f0	ens20f0	
Management	enp4s0f0	enp4s0f3	ens20f1	ens20f1	
Data	ens787f0	ens787f0	enp133s0f0	enp133s0f0	

Table 4. Physical network interface addresses.

NETWORK	CONTROLLER/COMPUTE1	COMPUTE2	COMPUTE3	MIDONET ANALYTIC SERVER
External	10.250.101.11	10.250.101.13	10.250.101.15	10.250.101.16
Management	10.250.101.10	10.250.101.12	10.250.101.14	10.250.101.17
Data	172.16.10.10	172.16.10.12	172.16.10.14	172.16.10.16

Table 5. Floating IP address pool ranges for External Network.

Start with IP address	10.250.101.133
End with IP address	10.250.101.149

Figure 1 explains the physical network connections and OpenStack deployment.



Figure 1. Network connectivity for the target setup.

3.0 Installation Guide

This chapter contains instructions for installation and configuration of the software stack.

3.1 Prerequisites to Installation of Red Hat Enterprise Linux 7.1

Note that the instructions for installing Red Hat Enterprise Linux 7.1 are not within the scope of this document; however, this section contains some information that a user needs to follow during OS installation or configuration.

To help ensure a successful installation process, make sure that the following steps occur:

- Create a RAID 0 virtual disk from all the physical disks.
- Create custom partitioning as presented in Table 6:

Table 6. Partitioning schema.

PARTITION	SIZE
Biosboot	2 MB
/boot	5 GB
/swap	Double the size of physical memory
/ (root partition)	Remaining space

Perform the following steps to install the operating system and configure the network interfaces on all the machines in the setup.

- 1. Install Red Hat Enterprise Linux 7.1 and set the following:
 - Hostname: /etc/hostname
 - Hosts: /etc/host
- 2. Disable and stop the firewall.
 - # systemctl disable firewalld
 - # systemctl stop firewalld
- 3. Configure all of the network interfaces using files in the /etc/sysconfig/network-scripts/ directory. In this setup, all of the nodes have three network interfaces. The following example is presented for the ens20f0 interface of the controller. In this case, the configuration file name is ifcfg-ens20f0.

Note: The example below shows the configuration specific to the setup presented in this installation guide. IP addresses, device names, and universally unique identifier (UUID) should be respectively changed for a different setup.

TYPE=Ethernet BOOTPROTO=static IPADDR=10.250.101.10 NETMASK=255.255.255.0 GATEWAY=10.250.101.1 DNS1=10.248.2.1 DNS2=10.2.71.6 DNS3=10.19.1.4 DEFROUTE=yes PEERDNS=yes PEERROUTES=yes IPV4 FAILURE FATAL=yes IPV6INIT=no IPV6_AUTOCONF=yes IPV6_DEFROUTE=yes IPV6 PEERDNS=yes IPV6 PEERROUTES=yes IPV6 FAILURE FATAL=no NAME=ens20f0 UUID=633b582e-7696-4e43-ad1d-ac53bf074250 DEVICE=ens20f0 ONBOOT=ves NM CONTROLLED=no

- 4. Disable and stop the NetworkManager service, enable/ start the network service, and bring up all the configured network interfaces with the following commands. Note that in the listing below only the interface ens20f0 is brought up.
 - # yum install net-tools
 - # systemctl disable NetworkManager
 - # systemctl stop NetworkManager
 - # systemctl start network
 - # chkconfig network on
 - # ifup ens20f0

3.2 Installation of Red Hat OpenStack Platform* 7

For this implementation, PackStack was used to create a multi-host test environment to showcase the security implementation. However, a production deployment would require high availability of the control plane as well as other considerations such as Secure Socket Layer (SSL) endpoints. Red Hat OpenStack Platform Director* is Red Hat's solution to meet the needs of provisioning production environments. You can consult Red Hat production documentation for more information on Director. In addition, a reference architecture for a highly available deployment can be found at:

https://access.redhat.com/articles/1610453

Installation of Red Hat Open Stack Platform 7 must be performed on all of the machines in the setup.

- 1. Register and subscribe to the Red Hat and Open Stack Platform 7.
 - # subscription-manager register
 - # subscription-manager subscribe --auto
 - # subscription-manager list --consumed
- Clear the initially set-up repositories and enable the appropriate ones.
 - # subscription-manager repos --disable=*
 - # subscription-manager repos
 - --enable=rhel-7-server-rpms
 - # subscription-manager repos
 - --enable=rhel-7-server-rh-common-rpms
 - # subscription-manager repos
 - --enable=rhel-7-server-openstack-7.0-rpms
- 3. Install the PackStack installer.

yum install openstack-packstack

- 4. Create PackStack answer file and save it on the disk. In this example, the /home/myanswerfile.txt file is used. The answer file used in this setup is presented in Appendix A: The PackStack Answer File.
- 5. Run PackStack on the created answer file.

packstack --answer-file=/home/
myanswerfile.txt

6. Increase the number of open files in MySQL*.

\$ mkdir -p /etc/systemd/system/mariadb. service.d/ \$ cat /etc/systemd/system/mariadb. service.d/limits.conf [Service] LimitNOFILE=10000

\$ systemctl daemon-reload

\$ systemctl restart mariadb

7. Verify the open files limit in MySQL.

\$ mysql
SHOW VARIABLES LIKE 'open%';

3.3 Installing Midokura Enterprise MidoNet

Note: The following steps were taken from Midokura's installation guide, which is available at http://docs.midokura.com/docs/latest-en/quick-start-guide/rhel-7_kilo-osp/content/index.html, with respective changes tailored to the setup presented in this guide.

Uninstall the Open vSwitch agent in OpenStack Networking* and install MidoNet, following these steps to integrate ingredients for MidoNet with PackStack. Steps 1 and 2 can be done before OpenStack is installed, so the yum upgrade will include the Midokura and DataStax repositories.

1. Verify that the yum repositories have the midokura.repo.

cat /etc/yum.repos.d/midokura.repo
[mem]
name=MEM
baseurl=http://username:password@repo.

midokura.com/mem-5/stable/e17/
enabled=1
gpgcheck=1
gpgkey=https://repo.midokura.com/midorepo.
key

[mem-openstack-integration] name=MEM OpenStack Integration baseurl=http://repo.midokura.com/ openstack-kilo/stable/el7/ enabled=1 gpgcheck=1 gpgkey=https://repo.midokura.com/midorepo. key

[mem-misc]
name=MEM 3rd Party Tools and Libraries
baseurl=http://repo.midokura.com/misc/
stable/el7/
enabled=1
gpgcheck=1
gpgkey=https://repo.midokura.com/midorepo.
key

2. Enable DataStax repository.

```
# cat /etc/yum.repos.d/datastax.repo
# DataStax (Apache Cassandra)
[datastax]
name = DataStax Repo for Apache
Cassandra
baseurl = http://rpm.datastax.com/
community
enabled = 1
gpgcheck = 1
gpgkey = https://rpm.datastax.com/rpm/
repo key
```

Change the OpenStack Compute* configuration in all the compute nodes with the following steps.

3. Configure libvirt. Edit the /etc/libvirt/qemu.conf file to contain the following.

```
user = "root"
group = "root"
cgroup_device_acl = [
   "/dev/null", "/dev/full", "/dev/zero",
   "/dev/random", "/dev/urandom",
   "/dev/ptmx", "/dev/kvm", "/dev/kqemu",
   "/dev/rtc","/dev/hpet", "/dev/vfio/vfio",
   "/dev/net/tun"
]
```

- 4. Add all the permissions to the folder /dev/net/tun to root user and OpenStack Compute service.
- 5. Restart the libvirt service.

```
# systemctl restart libvirtd.service
```

6. Install nova-rootwrap network filters.

yum install openstack-nova-network
systemctl disable openstack-novanetwork.service

7. Restart the OpenStack Compute service.

systemctl restart openstack-novacompute.service

3.3.1 OpenStack Networking* Integration

Note: The following steps should be executed on the controller/neutron node.

1. Verify that all these components are installed.

yum install openstack-neutron openstackutils openstack-selinux python-neutronplugin-midonet

 Set the OpenStack Networking plug-in. Edit the /etc/ neutron/neutron.conf file, and configure the following keys in the [DEFAULT] section.

```
[DEFAULT]
...
core_plugin = midonet.neutron.plugin_
v2.MidonetPluginV2
...
dhcp_agent_notification = False
...
allow overlapping ips = True
```

- 3. Comment all other plug-ins different from core plugin.
- 4. Create the directory for the MidoNet plug-in.

```
mkdir /etc/neutron/plugins/midonet
```

5. Create the /etc/neutron/plugins/midonet/midonet. ini file, and edit it to contain the following.

> [DATABASE] sql_connection = mysql://neutron:NEUTRON_ DBPASS@controller/neutron

```
[MIDONET]
# Midonet API URL
midonet_uri = http://controller:8181/
midonet-api
# Midonet administrative user in Keystone
username = midonet
password = MIDONET_PASS
# Midonet administrative user's tenant
project id = services
```

6. Create a symbolic link to direct OpenStack Networking to the Midonet configuration.

ln -s /etc/neutron/plugins/midonet/
midonet.ini /etc/neutron/plugin.ini

7. Create the OpenStack Networking database.

\$ mysql -u root -p

CREATE DATABASE neutron character set utf8; GRANT ALL PRIVILEGES ON neutron.* TO 'neutron'@'localhost' IDENTIFIED BY 'NEUTRON_DBPASS'; GRANT ALL PRIVILEGES ON neutron.* TO 'neutron'@'%' IDENTIFIED BY 'NEUTRON_ DBPASS'; FLUSH PRIVILEGES; quit

8. Run the neutron-db-manage command.

```
# neutron-db-manage \
    --config-file /usr/share/neutron/neutron-
dist.conf \
    --config-file /etc/neutron/neutron.conf \
    --config-file /etc/neutron/plugin.ini \
    upgrade head
```

9. Run the midonet-db-manage command.

midonet-db-manage upgrade head

- 10. If the command midonet-db-manage has issues with extra fields (such as alembic), perform the next steps.
 - Install the most recent version of python-neutronplugin-midonet.<version>.noarch.rpm
 - Remove any Open vSwitch installation (on all compute and controller nodes).

yum erase openstack-neutron-openvswitch openvswitch python-openvswitch

3.3.2 Apache ZooKeeper* Installation

Note: ZooKeper should be installed in at least one NSDB physical machine.

1. Install the Apache ZooKeeper packages.

- # yum install java-1.7.0-openjdk-headless
- # yum install zookeeper zkdump nmap-ncat

Common Configuration

2. Configure Apache ZooKeeper. Edit the /etc/zookeeper/ zoo.cfg file to contain the following:

> server.1=nsdb1:2888:3888 server.2=nsdb2:2888:3888 server.3=nsdb3:2888:3888

3. Create the data directory.

mkdir /var/lib/zookeeper/data
chown zookeeper:zookeeper /var/lib/

zookeeper/data

Note: For production deployments, it is recommended to configure the storage of snapshots in a different disk than the commit log. This can be set by changing the parameter **dataDir** in zoo.cfg to a different disk.

Node-Specific Configuration

1. NSDB Node 1: Create the /var/lib/zookeeper/data/ myid file, and edit it to contain the host's ID.

echo 1 > /var/lib/zookeeper/data/myid

NSDB Node 2: Create the /var/lib/zookeeper/ data/myid file, and edit it to contain the host's ID.

echo 2 > /var/lib/zookeeper/data/myid

NSDB Node 3: Create the /var/lib/zookeeper/ data/myid file, and edit it to contain the host's ID.

echo 3 > /var/lib/zookeeper/data/myid

2. Create the Java* symbolic link.

mkdir -p /usr/java/default/bin/
ln -s /usr/lib/jvm/jre-1.7.0-openjdk/
bin/java /usr/java/default/bin/java

3. Enable and start Apache ZooKeeper.

systemctl enable zookeeper.service

- # systemctl start zookeeper.service
- 4. Verify Apache ZooKeeper operation (use 127.0.0.1 only if you are testing it from the controller; otherwise, use the public IP address of the controller).

After installation of all nodes has been completed, verify that Apache ZooKeeper is operating properly.

A basic check can be done by executing the ruok (Are you ok?) command on all nodes. This will reply with imok (I am ok.) if the server is running in a non-error state.

```
$ echo ruok | nc 127.0.0.1 2181
imok
```

More detailed information can be requested with the stat command, which lists statistics about performance and connected clients.

```
$ echo stat | nc 127.0.0.1 2181
Zookeeper version: 3.4.5--1, built on
06/10/2013 17:26 GMT
Clients:
 /127.0.0.1:34768[0]
(queued=0,recved=1,sent=0)
 /192.0.2.1:49703[1](queued=0,recved=1053,se
nt=1053)
Latency min/avg/max: 0/4/255
Received: 1055
Sent: 1054
Connections: 2
Outstanding: 0
Zxid: 0x260000013d
Mode: follower
Node count: 3647
```

3.3.3 Apache Cassandra* Installation

Perform Apache Cassandra installation on the controller node.

1. Add the Apache Cassandra repository to the /etc/yum. repos.d/datastax.repo.

```
# DataStax (Apache Cassandra)
[datastax]
name = DataStax Repo for Apache
Cassandra
baseurl = http://rpm.datastax.com/
community
enabled = 1
gpgcheck = 1
gpgkey = https://rpm.datastax.com/rpm/
repo_key
```

- 2. Install the Apache Cassandra packages.
 - # yum install java-1.7.0-openjdk-headless
 # yum install dsc20

Common Configuration

3. Edit the /etc/cassandra/conf/cassandra.yaml file to contain the following items.

```
# The name of the cluster.
cluster_name: 'midonet'
```

```
# Addresses of hosts that are deemed
contact points.
seed_provider:
    - class_name: org.apache.cassandra.
locator.SimpleSeedProvider
    parameters:
    - seeds: "nsdb1,nsdb2,nsdb3"
```

Node-Specific Configuration

4. NSDB Node 1: Edit the /etc/cassandra/conf/ cassandra.yaml file to contain the following:

> # Address to bind to and tell other Cassandra nodes to connect to. listen_address: nsdb1

```
...
# The address to bind the Thrift RPC
service.
```

rpc_address: nsdb1

NSDB Node 2: Edit the /etc/cassandra/conf/cassandra.yaml file to contain the following:

Address to bind to and tell other Cassandra nodes to connect to. listen_address: nsdb2 ... # The address to bind the Thrift RPC service. rpc_address: nsdb2 NSDB Node 3: Edit the /etc/cassandra/conf/cassandra.yaml file to contain the following:

```
# Address to bind to and tell other
Cassandra nodes to connect to.
listen_address: nsdb3
...
# The address to bind the Thrift RPC
service.
rpc address: nsdb3
```

5. Edit the service's init script.

On installation, the /var/run/cassandra directory is created, but because it is located on a temporary file system, it will be lost after system reboot. As a result, it is not possible to stop or restart the cassandra service anymore.

To avoid this, edit the /etc/init.d/cassandra file to create the directory on service start.

```
[...]
case "$1" in
start)
    # Cassandra startup
    echo -n "Starting Cassandra: "
    mkdir -p /var/run/cassandra
    chown cassandra:cassandra /var/run/
cassandra
    su $CASSANDRA_OWNR -c "$CASSANDRA_
PROG -p $pid_file" > $log_file 2>&1
    retval=$?
[...]
```

- 6. Enable and start Apache Cassandra.
 - # systemctl enable cassandra.service
 - # systemctl start cassandra.service
- 7. Verify that Apache Cassandra is operating properly (use 127.0.0.1 only if you are testing it from the controller; otherwise use the public IP address of the controller).
- Note: If Apache Cassandra fails to start and prints a "buffer overflow" error message in its log file, try associating 127.0.0.1 with the hostname in etc/hosts (so that hostname -i will show 127.0.0.1). This may solve the Apache Cassandra start problem.

A basic check can be done by executing the nodetool status command. This will reply with UN (Up / Normal) in the first column if the servers are running in a non-error state.

\$ nodetool -host 127.0.0.1 status [...] Status=Up/Down // State=Normal/Leaving/Joining/Moving -- Address Load Tokens Owns Host ID Rack UN 192.0.2.1 123.45 KB 256 33.3% UN 192.0.2.2 234.56 KB 256 33.3% 2222222-3333-4444-5555-6666666666666 rack1 UN 192.0.2.3 345.67 KB 256 33.4%

3.3.4 Midokura Enterprise MidoNet Cluster Installation

Perform the following steps in controller node.

1. Install the midonet-cluster package.

yum install midonet-cluster

2. Set up mn-conf. Edit the /etc/midonet/midonet. conf to point mn-conf to the Apache ZooKeeper cluster (The nsdb1, nsdb2, and nsdb3 should be the actual IP addresses of the servers.):

```
[zookeeper]
zookeeper_hosts = nsdb1:2181,nsdb2:2181,ns
db3:2181
```

3. Configure access to the NSDB.

This step needs to happen only once; it will set up access to the NSDB for the MidoNet cluster and agent nodes.

Run the following command to set the cloud-wide values for the Apache ZooKeeper and Apache Cassandra server addresses (The nsdb1, nsdb2, and nsdb3 should be the actual IP addresses of the servers.):

```
$ cat << EOF | mn-conf set -t default
zookeeper {
   zookeeper_hosts = "nsdb1:2181,nsdb2:2181
,nsdb3:2181"
}
cassandra {</pre>
```

```
servers = "nsdb1,nsdb2,nsdb3"
}
EOF
```

Run the following command to set the Apache Cassandra replication factor.

\$ echo "cassandra.replication_factor : 3"
| mn-conf set -t default

4. Configure OpenStack Identity* access. This step needs to happen only once; it will set up access to OpenStack Identity for the MidoNet cluster node(s).

This step will configure the local MidoNet cluster node to be able to use OpenStack Identity.

```
$ cat << EOF | mn-conf set -t default
cluster.auth {
    provider_class = "org.midonet.cluster.
    auth.keystone.v2_0.KeystoneService"
    admin_role = "admin"
    keystone.tenant_name = "admin"
    keystone.admin_token = "ADMIN_TOKEN"
    keystone.host = controller
    keystone.port = 35357
}
EOF</pre>
```

5. Start the MidoNet cluster.

```
# systemctl enable midonet-cluster.
service
```

systemctl start midonet-cluster.service

3.3.5 Midokura Enterprise MidoNet CLI Installation

Perform the following steps in controller node.

1. Install the MidoNet CLI package.

```
# yum install python-midonetclient
```

2. Configure MidoNet CLI. Create the ~/.midonetrc file and edit it to contain the following:

```
[cli]
api_url = http://MultinodeController.
ch.intel.com:8181/midonet-api
username = admin
password = ADMIN_PASS
project id = admin
```

3.3.6 MidoNet Agent* (Midolman) Installation

Note: The following steps should be executed on compute nodes.

The MidoNet Agent (Midolman) has to be installed on all nodes where traffic enters or leaves the virtual topology; in this guide these are all of three compute nodes.

1. Install the Midolman package.

yum install java-1.8.0-openjdk-headless
yum install midolman

2. Set up mn-conf. Edit the /etc/midolman/midolman.conf file to point mn-conf to the Apache ZooKeeper cluster.

[zookeeper] zookeeper_hosts = nsdb1:2181,nsdb2:2181,ns db3:2181

3. Configure resource usage. Run these steps on each agent host in order to configure resource usage.

Note: For production environments the large templates are strongly recommended.

Midolman resource template

Run the following command to configure the Midolman resource template.

\$ mn-conf template-set -h local -t
TEMPLATE_NAME

Replace TEMPLATE_NAME with one of the following templates:

- agent-compute-large
- agent-compute-medium
- agent-gateway-large
- agent-gateway-medium
- default

Java Virtual Machine (JVM) resource template

Replace the default /etc/midolman/midolman-env.sh file with one of the following to configure the JVM resource template:

- /etc/midolman/midolman-env.sh.compute.large
- /etc/midolman/midolman-env.sh.compute.medium
- /etc/midolman/midolman-env.sh.gateway.large
- /etc/midolman/midolman-env.sh.gateway.medium

4. Configure MidoNet metadata proxy for all agents.

This step needs to happen only once; it will set up MidoNet metadata proxy for all MidoNet Agent nodes.

Run the following commands to set the cloud-wide values for the Midonet Metadata Proxy.

```
$ echo "agent.openstack.metadata.
nova_metadata_url : \"http://
MultinodeController.ch.intel.com:8775\"" |
mn-conf set -t default
$ echo "agent.openstack.metadata.shared_
secret : shared_secret" | mn-conf set -t
default
$ echo "agent.openstack.metadata.enabled
: true" | mn-conf set -t default
```

MultinodeController.ch.intel.com, 8775, and shared_secret should be replaced with the appropriate values. They need to match with the corresponding OpenStack Compute metadata API configuration.

MultinodeController.ch.intel.com and 8775 specify the address on which OpenStack Compute accepts Metadata API requests. shared_secret has to be the same as specified by the metadata_proxy_shared_ secret field in the neutron section of the nova.conf file.

The OpenStack Compute side of the configuration for the metadata service is the same as when using OpenStack Networking metadata proxy. See the OpenStack documentation for details:

Cloud Administrator Guide: Configure Metadata

The metadata proxy creates an interface named "metadata" on the hypervisor hosts. When using iptables it may be necessary to add a rule to accept traffic on that interface.

iptables -I INPUT 1 -i metadata -j ACCEPT

5. Start Midolman.

systemctl enable midolman.service
systemctl start midolman.service

MidoNet Host Registration

6. Launch the Midonet command line interface (CLI).

\$ midonet-cli midonet>

7. Create a tunnel zone.

MidoNet supports the VxLAN and Generic Routing Encapsulation (GRE) protocols to communicate to other hosts within a tunnel zone.

To use the VxLAN protocol, create the tunnel zone with type vxlan.

midonet> tunnel-zone create name tz type
vxlan
tzone0

To use the GRE protocol, create the tunnel zone with type gre.

midonet> tunnel-zone create name tz type gre tzone0 **Note:** Make sure to allow GRE/VxLAN traffic for all hosts that belong to the tunnel zone. For VxLAN MidoNet uses User Datagram Protocol (UDP) port 6677 as default. To add hosts to the tunnel zone:

midonet> list tunnel-zone tzone tzone0 name tz type vxlan

midonet> list host host host0 name MultinodeController. ch.intel.com alive true host host1 name CernerMidonet alive true host host2 name MultinodeCompute1. ch.intel.com alive true

midonet> tunnel-zone tzone0 add member host host0 address 172.16.10.10 zone tzone0 host host0 address 172.16.10.10

midonet> tunnel-zone tzone0 add member host host1 address 172.16.10.14 zone tzone0 host host1 address 172.16.10.14

midonet> tunnel-zone tzone0 add member host host2 address 172.16.10.12 zone tzone0 host host2 address 172.16.10.12

3.4 Adding a Compute Node to OpenStack with MidoNet

On the compute node:

1. Clean up any previous installation of OpenStack.

```
# yum -y remove openstack-glance
# yum -y remove openstack-glance
# yum -y remove openstack-cinder.noarch
# yum -y remove openstack-dashboard
# yum -y remove openstack-swift*
# yum -y remove openstack-packstack*
# yum -y remove openstack-ceilometer-
alarm.noarch
# yum -y remove openstack-ceilometer-api.
noarch
# yum -y remove openstack-ceilometer-
central.noarch
# yum -y remove openstack-ceilometer-
collector.noarch
# yum -y remove openstack-ceilometer-
notification.noarch
# yum -y remove openstack-keystone.noarch
# yum -y remove openstack-neutron-lbaas.
noarch
# yum -y remove openstack-neutron-
midonet.noarch
# yum -y remove openstack-neutron-ml2.
noarch
# yum -y remove openstack-nova-api.noarch
# yum -y remove openstack-nova-cert.
noarch
# yum -y remove openstack-nova-conductor.
noarch
# yum -y remove openstack-nova-console.
noarch
```

yum -y remove openstack-novanovncproxy.noarch # yum -y remove openstack-nova-scheduler. noarch

- # yum -y remove rabbitmq-server.noarch
- 2. Clean up any previous MidoNet installation.
 - # yum -y remove cassandra20
 - # yum -y remove zookeeper
 - # yum -y remove python-midonetclient
 - # yum –y remove midolman
 - # yum -y remove midonet-cluster
 - # rm /etc/yum.repos.d/midokura.repo
 - # rm /etc/yum.repos.d/datastax.repo
 - # rm /etc/midolman
 - # rm /etc/midonet_host_id.properties
- 3. Keep or install the following components:
 - openstack-ceilometer-common.noarch
 - openstack-ceilometer-compute.noarch
 - openstack-neutron-common.noarch
 - openstack-neutron.noarch
 - openstack-nova-common.noarch
 - openstack-nova-compute.noarch
 - openstack-selinux.noarch
 - openstack-utils.noarch
- 4. Remove any Open vSwitch bridges (that is, br-ex) and make static IP addresses directly in the networks interfaces' scripts.
- 5. Copy the yum repositories from the current compute nodes (any node that is currently running).
 - # scp root@10.250.101.12:/etc/yum.repos.d/
 midokura.repo \
 - /etc/yum.repos.d/
- 6. Install Midolman.

yum —y midolman

- 7. Copy the MidoNet configuration file.
 - # scp root@10.250.101.12:/etc/midolman/
 midolman.conf \

/etc/midolman/

8. Copy the configuration file for OpenStack Compute and libvirt.

scp root@10.250.101.12:/etc/nova/* /etc/ nova/ # scp root@10.250.101.12:/etc/libvirt/* / etc/libvirt/ # scp root@10.250.101.12:/etc/libvirt/ gemu/* /etc/libvirt/gemu/

9. Replace the property vncserver_proxyclient_ address in /etc/nova.conf and set the name of the new compute node.

> vncserver_proxyclient_ address=MultinodeCompute1.ch.intel.com

10. Enable Midolman.

systemctl enable midolman

11. Enable OpenStack Compute.

systemctl enable openstack-nova-compute

12. Reboot the machine.

On the controller node:

13. Open the MidoNet console.

midonet-cli

14. List the host in the setup.

midonet> list host

The output should be similar to the following:

host host0 name MultinodeController. ch.intel.com alive true addresses fe80:0:0:0:900e:a9ff:fef7:f5d2,fe80:0:0:0:c8a7 :1ff:fe6b:e70b,fe80:0:0:0:30ef:a0:ec9d:18ff:fe0 7:8abf,fe80:0:0:0:443f:e9ff:fe7b:cf01,fe80:0:0 :0:50ef:3aff:fed3:8011,fe80:0:0:0:21e:67ff:fec b:efaa,10.250.101.10,127.0.0.1,0:0:0:0:0:0:0ffe cb:efa9,172.16.10.10,fe80:0:0:0:e443:19ff:feaa :1ff0,fe80:0:0:0:c086:ddff:fe82:e60e,fe80:0:0:0 :5034:dff:fe53:d499,fe80:0:0:0:46c:24ff:fe09:b 323,5:6d35,172.16.101.2,fe80:0:0:0:147e:92ff:fe f9:a539,fe80:0:0:0:50c9:5bff:fe7e:4afc,169.254 .169.254,fe80:0:0:0:2c46:11ff:fe2e:d6d5,fe80:0 :0:0:f4c3:4fff

host host1 name CernerMidonet alive true addresses

fe80:0:0:0:2c1a:5ff:fed5:24cc,fe80: 0:0:0:225:90ff:fefd:4708,169.254.169. 254,fe80:0:0:0:8d2:4ff:f:3ff:fe00:60 be,127.0.0.1,0:0:0:0:0:0:0:1,192.168.122-

.1,10.250.101.14,fe80:0:0:0:225:90ff:fefd:4709 host host2 name MultinodeCompute1.ch.intel.

com alive true addresses

127.0.0.1,0:0:0:0:0:0:1,fe80:0:0:0:18f5:1ff:f e46:e8a4,10.250.101.12,fe80:0:0:00:0:0:0:8c6f: 1aff:fe4e:9af8,10.250.101.12,fe80:0:0:0:21e:67f f:fecf:c09f,fe80:0:0:0:b4d7:58ff:fef1:e383,fe8 0:0:0:0:1812:33ff:fe77:3bb,fe80:0:0:0:7c85:69.2 54,fe80:0:0:0:74c7:4ff:feba:cf28,fe80:0:0:0:8 0f6:93ff:fe0f:8601,fe80:0:0:0:21e:67ff:fec5:508 5,172.16.101.3,fe80:0:0:0:d8bd:b7ff:fe6e:15d8

- 15. Get the host name from the previous list; in this case it is host1.
- 16. Get the tunnel zone list.

midonet> tunnel-zone list

The output should be similar to the following:

tzone tzone0 name vxlan type vxlan

- 17. Get the tunnel zone name; in this case it is: tzone0.
- 18. Get the list of member in the tunnel zone.

midonet> tunnel-zone tzone0 member list

The output should be similar to the following:

zone tzone0 host host2 address 172.16.10.12 zone tzone0 host host0 address 172.16.10.10 zone tzone0 host host1 address 172.16.10.14 19. If the member already exists with a different IP, it is possible to remove it with this command.

midonet> tunnel-zone tzone0 delete
member host host1

20. Add the new host machine to the members of the tunnel.

midonet> tunnel-zone tzone0 add member host host1 address 10.250.101.10

21. Check whether the new host is a member of the tunnel zone with the command for checking the tunnel list.

Но	st Aggregat	es		Filter	۹	+ Create Host Age	gregate	Delet	e Host Aggrega	ites
	Name Availability Zone Hos		losts	Metadata			Actions			
	new-Compute Compute3 Cer		CernerMidonet	availability_zone = Compute3			Edit Host Aggregate		•	
Displa	ying 1 item									
Av	ailability Zor	nes					Filter			۹
Avail	ability Zone Name		Hosts						Available	
Compute3 CernerMidonet (Services Up)						Yes				
interr	nal		MultinodeCo	ntroller.ch.intel.co	m (Services Down)				Yes	
nova MultinodeController.ch.intel.com (Services Up) MultinodeCompute1.ch.intel.com (Services Up)						Yes				
Displa	ying 3 items									

3.4.1 Testing the New Compute Node

- 1. Create new host aggregates. Add only the new server as an availability zone.
- 2. Create a new instance. Check that the availability zone is set to the new server.
- 3. Ping machines in other availability zones as well as the floating IP addresses.

Project & User * Details * Access & Security	Networking * Pos	t-Creation
Advanced Options		
Availability Zone	Specify the details for I	aunching an instance.
Compute3	The chart below shows	the resources used by this project
Any Availability Zone	in relation to the project	's quotas.
nova	Flavor Details	
	Name	m1.tiny
Flavor * O	VCPUs	1
m1.tiny •	Root Disk	1 GB
Instance Count * 😧	Ephemeral Disk	0 GB
1	Total Disk	1 GB
Instance Boot Source * 9	RAM	512 MB
Select source	Project Limits	
	Number of Instances	5 of 20 Use
	Number of VCPUs	20 of 47 Use
	Total RAM	34,816 of 51,200 MB Use

3.5 Adding Uplink to an External (Public) Network

1. Create an OpenStack network that will be mapped to a physical network. Usually that is done with the following command: # neutron net-create Public --provider:network_type flat --provider:physical_network enp4s0f3 --router:external=True

Created a new network:	
+	-+
Field	Value
+	-+
admin_state_up	True
id	9209b2c6-0803-4ba9-98b5-5ade96afe0e0
name	Public
<pre>port_security_enabled</pre>	True
router:external	True
shared	False
status	ACTIVE
subnets	
tenant_id	a88f84c8ab2e4841b7579518502c1e78
+	-+
allocation-pool start=10. Created a new subnet:	250.101.133,end=10.250.101.149enable-dhcp=False
Fleid	value
+	+
ailocation_pools	10.250.101.0/24
dns nameservers	10.230.101.0/24
enable dhcp	False
gateway ip	
host routes	
id	c9ae94e8-44d1-42c1-8bcd-904c22d0ace6
ip version	4
ipv6 address mode	
ipv6 ra mode	
name	public subnet
network id	9209b2c6-0803-4ba9-98b5-5ade96afe0e0
subnetpool_id	
tenant id	a88f84c8ab2e4841b7579518502c1e78

+_____

Take the ID of the network; in this case: id 9209b2c6-0803-4ba9-98b5-5ade96afe0e0 and create a port. # midonet-cli -e bridge 9209b2c6-0803-4ba9-98b5-5ade96afe0e0 port create 3da71887-d49f-4199-8a4d-10e7ba3b6387

That gives a port id; in this case (3da71887-d49f-4199-8a4d-10e7ba3b6387). Execute: # midonet-cli -e host <host-id> add binding interface <interface> port <port-id>

The host id is on /etc/midonet_host_id.properties.

cat /etc/midonet_host_id.properties
#Fri Nov 06 23:53:25 MST 2015
host_uuid=09a1ee22-0faf-4560-a823-f386ed0ef94f

Thus, the adding bind should be as follows:

midonet-cli -e host 09a1ee22-0faf-4560-a823-f386ed0ef94f add binding interface enp4s0f3
port 3da71887-d49f-4199-8a4d-10e7ba3b6387

At least one compute node should have two network interfaces connected to the same external network, and in the midonet-cli the host and the interface should come from that compute node.

2. Modify the routing rules in MidoNet for the uplink connection.

In order to avoid sending the traffic outside to the external gateway, we have to set some routing rules that will identify the traffic between the floating IP address range and use the tunnel. To do that, access midonet-cli and run these commands.

router router0 add route dst 10.250.101.0/24 src 0.0.0.0/0 type normal port router0:port0
router router1 add route dst 10.250.101.0/24 src 0.0.0.0/0 type normal port router1:port0
router router2 add route dst 10.250.101.0/24 src 0.0.0.0/0 type normal port router2:port0

midonet-cli

midonet> host list

host host0 name MultinodeController.ch.intel.com alive true addresses fe80:0:0:0:4066:a3ff:fe b2:c157,fe80:0:0:0:5cad:60ff:feef:f391,fe80:0:0:0:b491:3dff:fe0b:89dc,127.0.0.1,0:0:0:0:0:0:0:1,10.250 .101.10,fe80:0:0:0:21e:67ff:fecb:efa9,fe80:0:0:0:a803:42ff:fe2c:872b,172.16.101.2,fe80:0:0:0:9cab:22ff: fe45:5544,fe80:0:0:0:5c3a:a0ff:feb3:e125,fe80:0:0:0:6cbd:2ff:febe:5ffb,fe80:0:0:0:20f0:6dff:fe89:9696, fe80:0:0:0:c0f8:adff:fe38:fc58,fe80:0:0:0:21e:67ff:fecb:efaa,10.250.101.11,fe80:0:0:0:bc19:ddff:fe4d:3 9c2,172.16.10.10,fe80:0:0:0:3efd:feff:fe9e:7570,fe80:0:0:0:a046:27ff:fe07:c5da,169.254.169.254,fe80:0:0: 0:e0fa:42ff:fe61:c015 flooding-proxy-weight 1

host host1 name CernerMidonet alive true addresses 127.0.0.1,0:0:0:0:0:0:0:0:1,fe80:0:0:0:2882:adff :fe93:e61e,10.250.101.15,fe80:0:0:0:225:90ff:fefd:4709,fe80:0:0:0:70bd:8ff:fecd:6c7f,169.254.169.254,fe8 0:0:0:0:a490:f3ff:fe78:b824,192.168.122.1,fe80:0:0:0:e486:1eff:fe67:b961,fe80:0:0:0:583e:50ff:fe6b:d2f8, fe80:0:0:0:5c2e:c0ff:fe5d:fb43,fe80:0:0:0:e0bc:89ff:fe49:4d3b,fe80:0:0:0:2035:f7ff:feef:d35a,fe80:0:0:0 :4c19:33ff:fe7f:d60c,fe80:0:0:0:225:90ff:fefd:4708,10.250.101.14,fe80:0:0:0:884e:a2ff:fee4:d630,172.16.10 .14,fe80:0:0:0:3efd:feff:fe9e:7238,fe80:0:0:0:0:70d7:f7ff:fee8:c5c7,fe80:0:0:0:54dc:9dff:fed7:d89f,fe80:0: 0:0:100f:a4ff:fefe:1ede,fe80:0:0:0:8422:2aff:fea7:7b0d flooding-proxy-weight 1

```
host host2 name MultinodeCompute1.ch.intel.com alive true addresses
```

127.0.0.1,0:0:0:0:0:0:0:1,fe80:0:0:8f3:46ff:fe7e:8e6f,fe80:0:0:0:cca7:89ff:fe9f:4333,fe80:0:0:0:30f1:2 9ff:fe12:48c0,172.16.10.12,fe80:0:0:0:3efd:feff:fe9e:77d8,169.254.169.254,fe80:0:0:0:6cf6:dcff:fe08:f6a 5,fe80:0:0:0:9cfa:3bff:fe79:8b66,10.250.101.13,fe80:0:0:0:5412:5eff:fef0:175,fe80:0:0:0:98b7:beff:fe02:8 265,172.16.101.3,fe80:0:0:0:8c32:8aff:fe03:a501,fe80:0:0:0:d4ae:2cff:fef8:dbb1,fe80:0:0:0:2ca0:2cff:fe2 4:e53c,fe80:0:0:0:6831:3dff:fe8c:61be,fe80:0:0:0:c03d:ebff:fe30:a260,fe80:0:0:0:4c39:11ff:fec4:8c7e,10 .250.101.12,fe80:0:0:21e:67ff:fecf:c09e,fe80:0:0:0:7c04:beff:fea6:9c79,fe80:0:0:0:6893:aeff:fed8:9e00 flooding-proxy-weight 1

```
midonet> host host0 binding list
```

```
host host0 interface tapa8ddb6b3-b7 port bridge0:port0
host host0 interface tapa0eef80-7b port bridge0:port1
host host0 interface tap06e55253-36 port bridge1:port0
host host0 interface enp4s0f3 port bridge2:port0
host host0 interface tap36af40a5-dc port bridge3:port0
host host0 interface tap48ae50e0-2d port bridge0:port2
host host0 interface tap28d5d5edc-d7 port bridge4:port0
host host0 interface tap3af79871-4f port bridge3:port10
host host0 interface tap17e40252-30 port bridge0:port3
host host0 interface tap20c3c61-9a port bridge4:port1
host host0 interface tap3456ac90-e3 port bridge5:port0
host host0 interface tap3456ac90-e3 port bridge5:port0
```

```
midonet> bridge list
```

bridge bridgel name Tenant2-net state up bridge bridge0 name Data state up bridge bridge5 name DataCache state up bridge bridge2 name Public state up bridge bridge7 name vsf-inspection-net state up bridge bridge3 name Mgmt_BKP state up bridge bridge4 name Client state up bridge bridge6 name vsf-mgmt-net state up

midonet> bridge bridge2 port list port port0 device bridge2 state up plugged yes vlan 0 port port1 device bridge2 state up plugged no vlan 0 port port2 device bridge2 state up plugged no vlan 0 peer router0:port0

port port3 device bridge2 state up plugged no vlan 0 peer router1:port0 port port4 device bridge2 state up plugged no vlan 0 peer router2:port0 midonet> router list router router2 name Router state up infilter chain0 outfilter chain1 asn -1 router router1 name Router state up infilter chain2 outfilter chain3 asn -1 router router0 name Router state up infilter chain4 outfilter chain5 asn -1 midonet> router router0 route list route route0 src 0.0.0.0/0 dst 10.250.101.134 port router0:port0 weight 100 learned false route route1 type normal src 0.0.0.0/0 dst 10.250.101.0/24 port router0:port0 weight 0 learned false route route2 type normal src 0.0.0.0/0 dst 172.16.36.0/24 port router0:port1 weight 100 learned false route route3 src 0.0.0.0/0 dst 172.16.36.1 port router0:port1 weight 100 learned false midonet> router router1 route list route route0 src 0.0.0.0/0 dst 10.250.101.140 port router1:port0 weight 100 learned false route route1 type normal src 0.0.0.0/0 dst 0.0.0/0 gw 10.250.101.1 port router1:port0 weight 100 learned false route route2 type normal src 0.0.0.0/0 dst 172.16.58.0/24 port router1:port1 weight 100 learned false route route3 src 0.0.0.0/0 dst 172.16.58.1 port router1:port1 weight 100 learned false route route4 type normal src 0.0.0.0/0 dst 172.16.24.0/24 port router1:port2 weight 100 learned false route route5 src 0.0.0.0/0 dst 172.16.24.1 port router1:port2 weight 100 learned false route route6 type normal src 0.0.0.0/0 dst 172.16.65.0/24 port router1:port3 weight 100 learned false route route7 src 0.0.0.0/0 dst 172.16.65.1 port router1:port3 weight 100 learned false midonet> router router0 port list port port0 device router0 state up plugged no mac fa:16:3e:6f:6d:9d address 10.250.101.134 net 10.250.101.0/24 peer bridge2:port2 port port1 device router0 state up plugged no mac fa:16:3e:6a:bf:67 address 172.16.36.1 net 172.16.36.0/24 peer bridge6:port1 midonet> router router0 add route dst 10.250.101.0/24 src 0.0.0.0 type normal port router0:port0 router0:route4 midonet> router router0 route list route route0 src 0.0.0.0/0 dst 10.250.101.134 port router0:port0 weight 100 learned false route route1 type normal src 0.0.0.0/0 dst 0.0.0.0/0 gw 10.250.101.1 port router0:port0 weight 100 learned false route route4 type normal src 0.0.0.0/0 dst 10.250.101.0/24 port router0:port0 weight 0 learned false route route2 type normal src 0.0.0.0/0 dst 172.16.36.0/24 port router0:port1 weight 100 learned false route route3 src 0.0.0.0/0 dst 172.16.36.1 port router0:port1 weight 100 learned false midonet> router router1 add route dst 10.250.101.0/24 src 0.0.0.0 type normal port router1:port0 router0:route8 midonet> router router2 route list route route0 src 0.0.0.0/0 dst 10.250.101.141 port router2:port0 weight 100 learned false route route1 type normal src 0.0.0.0/0 dst 0.0.0.0/0 gw 10.250.101.1 port router2:port0 weight 100 learned false route route2 type normal src 0.0.0.0/0 dst 172.16.90.0/24 port router2:port1 weight 100 learned false route route3 src 0.0.0.0/0 dst 172.16.90.1 port router2:port1 weight 100 learned false midonet> router router2 add route dst 10.250.101.0/24 src 0.0.0.0 type normal port router2:port0

router2:route4

3.6 Midokura Enterprise MidoNet Analytic Installation

Note: The following steps were taken from the Midokura's installation guide, which is available at http://docs.midokura.com/docs/latest-en/quick-start-guide/rhel-7_kilo-osp/content/index.html, with respective changes tailored to the setup presented in this guide.

3.6.1 Prerequisites

The Analytics Node must contain a deployment of Logstash* (version 1.5) and Elasticsearch* (version 1.7), as well as the elasticsearch-curator tool, before the installation of the midonet-analytics package.

Elastic* (https://www.elastic.co/) provides both 'deb' and 'rpm' packages for easy installation of the required packages:

- Logstash (v1.5.4): https://www.elastic.co/guide/en/ logstash/1.5/package-repositories.html
- Elasticsearch (v1.7.3):

https://www.elastic.co/guide/en/elasticsearch/ reference/1.7/setup-repositories.html

3. The elasticsearch-curator tool can be installed with the pip command.

yum install -q python-pip
pip install U plastisseersh su

- # pip install -U elasticsearch-curator
- 4. In the controller node we need to have midonetcluster-mem installed. This can be done with the following command.

yum install midonet-cluster-mem

5. In the compute nodes, the midonet-jmxscraper packages should be installed. To install the midonetjmxscraper package in the agent nodes (compute nodes), execute the following command as root.

yum install midonet-jmxscraper

6. The analytic node is a single dedicated node containing the data analytics services as well as the data storage and search engine. The data storage and search engine services are provided by Logstash and Elasticsearch respectively, which have to be installed in advance, according to the instruction in the Prerequisites section.

It is also recommended to install the midonet-tools package in the analytic node; this makes the mn conf command available in the analytic node, facilitating its configuration.

To install the midonet-analytics package in the analytic node, execute the following commands as root.

- # yum install midonet-tools
- # yum install midonet-analytics

3.6.2 Quickstart

As a prerequisite, the core MidoNet components should be correctly installed and configured.

In particular, the NSDB must contain the correct values for the list of Apache ZooKeeper instances (in the zookeeper. zookeeper_hosts key). Note that this value was not required for legacy installations and may be missing or incorrectly set; in order to set it properly, you can run the following command (where nsdb1, nsdb2, and nsdb3 are the NSDB nodes containing the Apache ZooKeeper instances).

```
$ cat << EOF | mn-conf set -t default
zookeeper {
zookeeper_hosts = "nsdb1:2181,nsdb2:2181,n
sdb3:2181"
}
EOF</pre>
```

Apache Cassandra must also be configured correctly in NSDB for the Midokura Enterprise MidoNet features. In order to ensure the correct settings, you may run the following command (where cass1, cass2, and cass3 are the IP addresses of the nodes containing the Apache Cassandra instances).

```
$ cat << EOF | mn-conf set -t default
cassandra {
servers = "cass1,cass2,cass3"
cluster = "midonet"
}
EOF</pre>
```

This quickstart assumes that the midonet-analytics package has been installed in a single dedicated node (the analytics node). The minimum setup needed for running the Midokura Enterprise MidoNet features solution consists of configuring the communication endpoints for the MidoNet Agent and the Midokura Enterprise MidoNet services, as well as setting up the authentication information to make the data available to MidoNet Manager.

Before starting, it is recommended to increase the default heap size for both Logstash and Elasticsearch up to a minimum of 4 GB respectively (note that it is not recommended to set the total beyond half of the available physical RAM). These values can be set by editing the corresponding configuration files.

On Red Hat Enterprise Linux:

- Set LS_HEAP_SIZE="4g" in the /etc/sysconfig/logstash file for Logstash.
- Set ES_HEAP_SIZE="4g" in the /etc/sysconfig/ elasticsearch file or Elasticsearch.
- Restart the services.

The next step is to create a configuration file in the analytics node indicating how to locate the NSDB nodes containing the MidoNet configuration. MidoNet Analytics tries to locate this information at the following location: /etc/midonet/ midonet-analytics.conf; if the file does not exist, it searches in the following locations:

- \$HOME/.midonetrc
- /etc/midonet/midonet.conf
- /etc/midolman/midolman.conf

The following is the template for this configuration data (the value of the zookeeper_hosts key should be a commaseparated list of the IP addresses and ports of the Apache ZooKeeper instances, represented in the template by nsdb1, nsdb2, and nsdb3—the standard port for Apache ZooKeeper is 2181).

> [zookeeper] zookeeper_hosts = nsdb1:2181,nsdb2:2181,ns db3:2181

The JMXScraper service running in the compute nodes needs the same configuration file (if that file does not exist, it will use the same configuration as the Midonet Agent running in the same node).

Once the NSDB location has been set via the midonetanalytics.conf file, all the Analytics services can be configured via the MidoNet's mn-conf tool (a tool used to manage the Midonet configuration stored on NSDB). The mn-conf tool is part of the midonet-tools package, and it can be used from any MidoNet node where this package is installed.

The following is the example configuration. On a node with the mn-conf tool available, create a file according to the following template:

clio.enabled : true clio.service.udp_port : 5001 clio.service.encoding : "binary" clio.data.fields : ["cookie", "devices", "host_uuid", "in_port", "in_tenant", "out_ports", "out_tenant", "match_eth_src", "match_eth_dst", "match ethertype", "match network dst", "match_network_src", "match_network_proto", "match_src_port", "match_dst_port", "action_drop", "action_arp_sip", "action_arp_tip", "action_arp_op", "rules", "sim_result", "final_eth_src", "final_eth_ dst", "final_net_src", "final_net_dst", "final_transport_src", "final transport dst", "timestamp", "type"] calliope.enabled : true calliope.service.ws port : 18181 calliope.auth.ssl.enabled : true jmxscraper.enabled : true jmxscraper.target.udp endpoint : "analytics_ip:5000" mem_cluster.flow_tracing.enabled : true

mem_cluster.flow_tracing.service.ws_port :
8400
mem_cluster.flow_tracing.auth.ssl.enabled
: true
agent.flow_history.enabled : true
agent.flow_history.encoding : "binary"
agent.flow_history.udp_endpoint :
"analytics_ip:5001"
jmxscraper.target.udp_endpoint :
"analytic_ip:5002"
clio.target.udp_endpoint : " analytic_
ip:5002"

The template above assumes that the MidoNet Manager will use SSL connections to communicate with the Midokura Enterprise MidoNet services; if this is not necessary (for example, because the services are behind a proxy), SSL can be deactivated by setting the *.ssl.enabled properties to false (see the configuration section for more details).

The above configuration also assumes that Logstash and Elasticsearch are installed in a single analytics node, together with the midonet-analytics package; <analytics_ip> represents the IP address or host name of such analytics node.

The configuration template can be applied by creating a file named analytics_settings.conf with the placeholders from the template replaced with the proper values, and then applying these settings with.

```
$ mn-conf set -t default < analytics_
settings.conf</pre>
```

By default, the analytics node receives data via UDP to ports 5000 and 5001 from the cluster and agent nodes, and exposes the interface to the MidoNet Manager via port 8080 (websocket). The analytics node needs to access the Apache ZooKeeper ensemble (port 2181) in the MidoNet cluster nodes and also the OpenStack Identity service (port 35357) for authentication. The flow tracing data is exposed to MidoNet Manager via port 8460 (websocket) in the cluster nodes.

3.6.3 Configuration

The Midokura Enterprise MidoNet services are configured using the MidoNet mn-conf command, provided by the midonet-tools package.

The following options can be set for the analytics node:

- clio.enabled (true false). Enable or disable flow history collection service (default is false disabled).
- clio.service.udp_port (port number). The port to listen for Midonet Agent flow history reports (default is 5001). This value must be the same as the port in the agent setting agent.flow_history.udp_endpoint.
- clio.service.encoding ("binary"|"json"|"none"). The encoding of the data received from MidoNet Agents. It must match the value in agent.flow_history.encoding. The binary setting offers a more efficient encoding of the data, while json allows easier debugging.

- clio.service.fields (list of comma-separated, quoted strings). The list of flow attributes to collect. Note that some of the values in this list are required for some of the Midokura Enterprise MidoNet features and removing them may result in limited functionality. For example, removing the "devices" field from the list might result in not having this information showed in the MidoNet Manager. The default list of reported attributes per flow is:
- cookie: internal flow id.
- devices: list of devices traversed by the flow.
- host_uuid: the id of the host generating the flow.
- in_port: the id of the port originating the flow.
- in_tenant: tenant associated to the device originating the flow.
- out_ports: the ids of the target ports for the flow.
- out_tenant: tenant associated to the device receiving the flow.
- match_eth_src: source Medium Access Control (MAC) address.
- match_eth_dst: destination MAC address.
- match_ethertype: ethernet type of flow.
- match_network_src: source IP address.
- match_network_dst: destination IP address.
- match_network_proto: the protocol id.
- match_src_port: source port.
- •match_dst_port: destination port.
- action_drop: the flow was dropped.
- action_arp_sip: Source IP address (SIP) for Address Resolution Protocol (ARP) packages.
- action_arp_tip: Target IP address (TIP) for ARP packages.
- action_arp_op: ARP operation.
- rules: list of rules affecting the flow.
- sim result: Midonet simulation result for this flow.
- final_eth_src: the source MAC address after any actions taken by the flow.
- final_eth_dst: the destination MAC address after any actions taken by the flow.
- final_net_src: the source IP address after any actions taken by the flow.
- final_net_dst: the destination IP address after any actions taken by the flow.
- final_transport_src: the source port after any actions taken by the flow.
- final_transport_dst: the destination port after any actions taken by the flow.
- timestamp: time stamp for the reception of the flow information.

- type: internal data set identifier.
- clio.service.compress (list of comma-separated, quoted strings). A subset of the flow attributes listed in clio.service.fields that are to be stored in compressed format. Note that compressed fields may reduce the storage space, but the values are not searchable. No field set is compressed by default.
- calliope.enabled (true|false). Enable or disable the Analytics front-end service (default is false disabled).
- calliope.service.ws_port (port number). The port to listen for Analytics queries from the MidoNet Manager (default is 8080).
- calliope.auth.ssl.enabled (true|false). Enable or disable SSL support (default is true).

The following options can be set for the nodes running the MidoNet Agent and the jmxscraper:

- agent.flow_history.enabled (true|false). Enable or disable flow history reporting in the Agent (default is false).
- agent.flow_history.encoding ("binary"|"json"|"none"). The format of the flow history records emitted by the Midonet Agents. The value must match the setting clio.service.encoding in the analytics node; the recommended value is binary and none does not generate any data (default is none).
- agent.flow_history.udp_endpoint ("host:port"). The host name or IP address of the analytics node and the destination port. The port must match the port set for the clio.service.udp_port property in the Analytics node. No default value is provided.
- jmxscraper.enabled (true|false). Enable or disable the MidoNet Agent JMX API scraper (default is false).
- jmxscraper.interval (time spec). The time interval between consecutive JMX API polls (default is 60s). Note that due to technical reasons, intervals below 60s are not supported.
- jmxscraper.target.udp_endpoint ("host:port"). The host name or IP address of the analytics node, and the port where the storage system (Logstash) is listening (the recommended settings use port 5000). No default value is provided.

The following options can be set for the nodes containing the Cluster:

- mem_cluster.flow_tracing.enabled (true|false). Enable or disable the flow tracing feature (default is true).
- mem_cluster.flow_tracing.service.ws_port (port number). The port to listen for flow tracing queries (default is 8460).
- mem_cluster.flow_tracing.auth.ssl.enabled (true|false). Enable or disable SSL support (default is true).

Apart from the options above, the midonet-analytics package installs a cron job in the analytics node to purge old data from the storage system. The initial configuration limits the size of the stored data to 100 GB; in order to modify this value, you may edit the following file and change the threshold value.

3.6.4 Files and Directories

- /etc/midonet/midonet-analytics.conf: Bootstrap configuration with Apache ZooKeeper location.
- /etc/midonet/midonet-{calliope,clio}/logback.
 xml: Logging settings for the Midokura Enterprise Midonet components in the analytics node.
- /etc/midonet/midonet-jmxscraper/logback.xml: Logging settings for the JMX scraper component in the Agent Nodes.
- /etc/midonet-cluster/logback.xml: Logging settings for the cluster node, including the Midokura Enterprise MidoNet extensions.
- /etc/midonet/midonet-*/logback.xml: Logging settings for the different Midokura Enterprise MidoNet components.
- /etc/logstash/conf.d/midonet.conf: Configuration for the Logstash storage back-end in the analytics node.
- /etc/default/logstash: Startup options for Logstash in Debian*-based systems.
- /etc/default/elasticsearch: Startup options for Elasticsearch in Debian-based systems.
- /etc/sysconfig/logstash: Startup options for Logstash in rpm-based systems.
- /etc/sysconfig/elasticsearch: Startup options for Elasticsearch in RPM*-based systems.
- /etc/init/midonet-{analytics,calliope,clio,jmx scraper}.conf: Upstart configuration files for Analytics components.
- /usr/lib/systemd/system/midonet-{analytics,call iope,clio,jmxscraper}.service: systemd configuration files for Analytics components.
- /var/lib/midonet/analytics_host_id.properties: Contains the MidoNet host id that the mn-conf tool uses to identify the Analytics Node components and the JMX scraper in the agent nodes.
- /var/lib/logstash/data: Contains the data stored by the Analytics back-end storage system (Logstash).
- /etc/cron.d/midonet-elk-cleaner: Automated data purging script for Midokura Enterprise MidoNet storage back-end.
- /var/log/midonet/{clio,calliope,jmxscraper}.
 log: Log files for the different Analytics components in the Analytics Node and the Agent Nodes.
- /var/log/midonet-cluster/midonet-cluster.log: Log file for the cluster node components, including the Midokura Enterprise MidoNet extensions.
- /usr/share/midonet-{analytics,calliope,clio,jmx scraper}: Directories with Analytics management scripts and dependencies.

3.6.5 Usage

Once you have configured the services, you can start the Midokura Enterprise MidoNet services by executing the following commands as root.

On analytics node, execute the following commands.

#	systemctl	start	logstash
11			

systemctl start elasticsearch

```
# systemctl start midonet-analytics
```

On cluster nodes, execute the following command.

systemctl restart midonet-cluster

On agent nodes, execute the following commands.

systemctl restart midolman
systemctl start midonet-jmxscraper

3.6.6 Update the OpenStack EndPoints

This is required by the MidoNet SDN Controller API in the Open Security Controller (OSC).

Create a script file called mn_endpoint_config.sh in the Controller. Add the following content to the file:

#!/bin/bash

```
##
## Usage:
## mn endpoint config.
sh controllerIP:controllerPort
analyticsIP:analyticsPort
##
MIDOAPI="$1"
MEMAPI="$2"
if [ -z "$MIDOAPI" -0 "${MIDOAPI%:*}" =
"$MIDOAPI" ]; then
  echo invalid host:port for Midonet API
  exit 1
fi
if [ -z "$MEMAPI" -0 "${MEMAPI%:*}" =
"$MEMAPI" ]; then
  echo invalid host:port for MEM Insights
APT
  exit 1
fi
keystone service-create --name=midonet-
api --type=midonet \
  --description="Midonet REST API"
keystone endpoint-create \
  --service-id=$(keystone service-list
|awk '/ midonet-api / {print $2}') \
  --publicurl="http://$MIDOAPI/midonet-
api" \
  --internalurl="http://$MIDOAPI/midonet-
api" \
  --adminurl="http://$MIDOAPI/midonet-api"
```

region="RegionOn	ne"
regron negronor	

```
keystone service-create --name=mem-
insights --type=insights \
    --description="MEM Insights API"
```

```
keystone endpoint-create \
    --service-id=$(keystone service-list
|awk '/ mem-insights / {print $2}') \
    --publicurl="ws://$MEMAPI/analytics" \
    --internalurl="ws://$MEMAPI/analytics" \
    --adminurl="ws://$MEMAPI/analytics" \
    --region="RegionOne"
```

To run the script, execute the following command:

./mn_endpoint_config.sh
mnControllerIp:mnControllerPort
analyticsIp:analyticsPort

To get the port of analytics node, execute the following command:

mn-conf get calliope.service.ws_port

To get the port of your MidoNet controller, execute the following command:

mn-conf get cluster.rest_api.http_port

3.7 OpenStack Deployment—Create Tenants

1. Log in to the OpenStack dashboard.



2. Select Identity Section.

-	MT DITERPRISE	LINUK OPENSTREK PLATFORM Project Admin		Project + Red	Hat Acres - Help & admin
-					
Free	an Daers				
Pr	ojects				
				q +Deate	Project Grine Projects
0	Name	Description	Project @	Enabled	Actions
0	-	Tenent for the operatack services	3%2x058x11x5407%ba2x431404b4738x	Yes	Manage Members +
-	95		30c0305w702348ew03d743e7cd56e467	Yes	Manage Members +
	Tenant2		MMG2dauc75544eab1w9bcc5a7bda095	Yes	Manage Members +
0	-	admin tenant	a8854c8ab2e4841b7579518502c1e78	Yes	Manage Members +
-	Tananti		%3dad52785666666411891a71p66966	Yes	Manage Members 👻

3. Click Create Project, and then in the pop-up window, click the Create Project button.

800 8	AT ENTERPRISES		PLATFORM Project Admin	(minut)		aper of the last	tattana - naji 1	admin -
Adapter of	a start		Create Project					-
Pr	ojects		Project Information #	Despect Mamburs Quera #				
	2 2 2120128		Name 4	Tanant				
			Description			· Craste	Property Design Property	-1
	Name	Description				and .	Actions	
		Tanana					Manage Marrison	
			Enabled	v			Marage Muniters	-
				6	Courte Property		Managa Mandarra	•
		Advent in		a contraction of the	-		Manage Members	•
				#3444027804444404118914714894	•	Yes	Manage Members	-
Dayle	ang Linete							

There should be created three projects (tenants) in total:

- For security
- For client VM (attackers), called Tenant 2
- For Web-Servers, called Tenant 1



Security Tenant should look similar to the following figure:







Installation Guide | Security Solution Implementation Installation Guide

Tenant 1:



3.8 Creating and Testing a Web Server

This section describes how to create and test the web server that supports a variety of features, many of which are implemented as compiled modules that extend core functionality. To create and test a web server, perform the following steps.

- 1. Create a web server instance with DataCache and the Management network.
- 2. In the Fedora* terminal of the Web server, run the following in the order shown:

sudo —i # ifconfig

Make a note of the interface private IP address.

3. Edit the /etc/httpd/conf/httpd.conf file. Change the IP address for <listen> to have the machine's eth2 IP. Start the HTTP service.

service httpd start

4. Edit the /etc/ssh/sshd_config file. Uncomment PasswordAuthentication = yes, (leave the rest as it is), PermitRootLogin=yes [Password to ssh:Account6All]. Start the SSH service.

service sshd start

- 5. Test whether the web server page opens up on the browser for the web server instance.
- 6. Allocate and assign a floating IP address for the private instance of the web server.

- 7. Check whether the web server is functioning from the external browser by pinging a floating IP.
- 8. Repeat steps 1 through 7 to create another web server.

3.9 Windows* VM Configuration

1. Set the Domain Name System (DNS) servers.



Installation Guide | Security Solution Implementation Installation Guide



23

3.10 Network Security Manager Installation

1. Launch a Microsoft Windows Server* 2012 r2 instance on the Security Tenant.

vervi	ew Instances Volumes	Images Acces	is & Security					
					# Project (8)	C Shared with Me (0)	Public (15)	Create Image Delete Image
	Image Name	Туре	Status	Public	Protecte	d Format	size	Actions
	Ubuntu_Webserver	Image	Active	Yes	No	QCOW2	1.7 GB	Launch Instance
	Windows2012r2	Image	Active	Yes	No	QCOW2	2 10.3 GB	Launch Instance
	BIGIP-12.0.0.0.606	Image	Active	Yes	No	QCOW2	2.9 GB	Launch Instance
0	Windows-NSM	Image	Active	Yes	No	QCOW2	16.0 GB	Launch Instance
	Webserver3	Image	Active	Yes	No	QCOW2	2 7.1 GB	Launch Instance
0	Webserver2	Image	Active	Yes	No	QCOW2	2. 7.1 GB	Launch Instance
	Webserver1	Image	Active	Yes	No	QCOW2	7.1 GB	Launch Instance
_		Image	Active	Yes	No	OCOW2	12.7 M	B Launch Instance

Launch Instance

Project & User * Details * Access & Security	Networking * P	ost-Creation
Advanced Options		
Availability Zone	Specify the details for	launching an instance.
Compute2	The chart below show	s the resources used by this
Instance Name *	Flavor Details	die project's quotas.
NSM	Name	m1.large
Flavor * 🛛	VCPUs	4
m1.large •	Root Disk	80 GB
Instance Count * 🛛	Ephemeral Disk	0 GB
1	Total Disk	80 GB
Instance Boot Source * 9	RAM	8,192 MB
Boot from image •	Project Limits	
Image Name *	Number of Instances	
Windows2012r2 (10.3 GB)		
	Number of VCPUs	
	Total RAM	

Cancel

2. Copy the McAfee Network Security Manager executable inside the Windows VM, and run the file; in the wizard, click Next.

		Application Tools	Downloads	5	- 0
file Home Sh	are View	Manage			````
) - † 🍺 ·	This PC + Dov	wnloads	~ (Search Down	loads
Favorites	Name	*	Date modified	Туре	Size
Desktop	🕷 npp.6.	9.Installer.exe	3/1/2016 11:46 PM	Application	4,106 KB
L Downloads	💟 setup.	exe	2/25/2016 1:14 AM	Application	670,126 KB
		Insta	allAnywhere		
	V	Instal InstalAnywhere is prepa	allAnywhere		
	۵	Instal InstalAnywhere is prepu	allAnywhere aring to rutal 81		
	۵	Instal Instal Anywhere is prepu	allAnywhere aring to install. 8%	Cancel	



3. Accept the terms and conditions, and then click Next.



4. Select the Manager type: Network Security Manager, and then click Next.

	www.mcafee.com/support
 Manager 8.2.7.73.3 License Agreement Choose Install Type 	Upgrading existing Network Security Manager installation.
Choose Install Folder Choose Shortcut Folder Customize Installation Pre-Installation Summary Installing Installing	Manager Type Network Security Manager V
	The Network Security Manager is the traditional Manager for Network Security Platform. It is required to manage Network Security Sensors.

5. Select the folder location, and click Next.

Where Would You Like to Install the Manager?			
C:\Program Files\McAfee\Network Security Manager\App			
Restore Default Folder Choose			

6. Select where NSM will create product icons.

McAfee An amail Company	www.mcafee.com/support
Manager 8.2.7.73.3 License Agreement Choose Install Type Choose Install Folder Costomize Installation Pre-Installation Summary Installing Install Complete	Where would you like to create product icons? C On the Start Menu On the Desktop On the Quick Launch Bar
	Create Icons for All Users (Applicable to the Start Menu and Desidop only)
InstallAnywhere Cancel	Previous Next

- 7. Select the type of database and credentials and click Next.
- 8. Set a password for the root user and click Next.

Q	Manager Installation Wizard
McAfee	www.mcafee.com/support
Manager 8.2.7.73.3 License Agreement Choose Install Type Choose Install Folder Choose Shortcut Folder	Database Connection Information. Note: This one time information is used by the Manager to read from and write to its database.
Customize Installation Pre-Installation Summary Installing Install Complete	Database Type MySQL v Database Name If Database User root Database Password ******* Retype Password ******** MySQL Instalation Directory
InstallAnywhere	C: Program Files WcAree Wetwork Security Manager Wr/SQL Previous Next



9. Select the folder for Apache Solr* installation, and then click Next.



10. Set the size of RAM memory to be used by McAfee Network Security Manager.



11. Set the amount of concurrent connection.

www.mcafee.com/support
Optionally Specify Maximum DB Connections Note: The recommended (default) value for the maximum quantity of database connections the Manager application will simultaneously open depends on the number of Sensors it will manage.
Number of Sensors 1-5 v Recommended Maximum DB Connections 40 Actual Maximum DB Connections 40 [40-60]

- 12. Click Install. A summary will be presented. Continue with the installation.
- 13. For the McAfee Network Security Manager 8.3 installation, uninstall the 8.2 version, and execute the fresh installation.
- 14. After you have finished, open a command prompt and log in to MySQL.

../Mcafee/Network Security Manager/MySQL/ bin>mysql —uroot —padmin123 ../Mcafee/Network Security Manager/MySQL/ bin>use lf; ../Mcafee/Network Security Manager/MySQL/ bin>ALTER TABLE iv_alert ADD COLUMN sourceVMIP CHAR(32) DEFAULT NULL; ../Mcafee/Network Security Manager/MySQL/ bin>ALTER TABLE iv_alert ADD COLUMN

- targetVMIP CHAR(32) DEFAULT NULL;15. Go to the ../Mcafee/Network Security Manager/ App/config/ directory and open the ems.properties file.
- 16. Turn off the AKKC settings.

iv.core.akka.enableakka=0

17. Restart the McAfee Network Security Manager VM.

3.11 Open Security Controller (OSC) Installation

1. Add the image in the OpenStack setup (in case the OSC will run inside of the same setup).

RED H	AT' ENTERPRISE LINUX OPENSTA	CK PLATFORM Project							
Vervi	ew Instances Volumes	Images Access	s & Security						
					# Project (5) 🐮 Shar	red with Me (0)	Public (15)	Create Image Delet	te Images
	Image Name	Туре	Status	Public	Protected	Format	Size	Actions	
	Perf-Server-RHEL7.1	Snapshot	Active	No	No	QCOW2	1.6 GB	Launch Inst	ance •
	RHEL 7.1	Image	Active	Yes	No	QCOW2	408.4 MB	Launch Inst	ance -
	ISC-build3589	Image	Active	Yes	No	VMDK	203.1 MB	Launch Inst	ance +
	Perf-CentOS	Snapshot	Active	Yes	No	QCOW2	7.1 GB	Launch Inst	ance +
	ISC-2.01_Build3449	Image	Active	Yes	No	VMDK	199.7 MB	Launch Inst	ance v

2. Launch the OSC instance from the previous image in the OpenStack Image Service*.

L <mark>a</mark> unch Instance		
Project & User * Details * Access & Security	Networking * P	ost-Creation
Advanced Options		
Availability Zone	Specify the details for	r launching an instance.
Compute2 •	The chart below show	vs the resources used by this
Instance Name *	project in relation to	the project's quotas.
	Flavor Details	
ISC-Instance	Name	m1.large
Flavor * 🛛	VCPUs	4
m1.large •	Root Disk	80 GB
Instance Count * 🖗	Enhomoral Dick	0 GB
1	Ephemeral Disk	80 GB
	Total Disk	8 192 MR
Instance Boot Source * 9	RAM	0,152 MD
Boot from image •	Project Limits	
Image Name *	Number of Instances	
ISC-build3589 (203.1 MB)	Number of instances	
13C-54113355 (253.7 mb)	Number of VCPUs	
	Total RAM	36364 of 81 200 MB Use
		Cancel Launch

- 3. Assign a floating IP address to the OSC instance.
- Access the OSC dashboard using the floating IP: https://<OSC-floatingIP>/ Default credentials: admin/ admin123.



- 5. Add a sensor image in the OSC deployment.
 - In the menu, select Setup/Service Function Catalog
 - Click Auto Import.
 - Browse the sensor zip file, and then click OK.

St Date 2 Aut			
Model			
151012115			
	Auto Import Ap	pliance Software Version	
	Upload Appliance Image File (zip)	Browse No file selected.	
SoftwareVersion		Canoel OK	
BE Delete			
Schwara			
91221			





versio	n: 2.5 (Build:3589, 20160325-12:	30)				
∐ Status	Model				2	C
Setup	3€ Delete 🐑	Auto Import				
Virtualization Connectors	Model	Manager Type	Manager Software Versio	in		
Manager Connectors	IPS-VM100-VSS	NSM	8.2			
Service Function Catalog						
Distributed Appliance						
Distributed Appliance						
Distributed Appliance Manage	Software Version					
Distributed Appliance	Software Version		_			
Distributed Appliance	Software Version 30 Delete Software	Virtualization Type	Image Name			C

- 6. Set the DNS servers to OSC setup (this is required for the Network Time Protocol configuration).
- Select Manage/Server/Network.
- Select static IP Details, and then add the DNS servers.

Status	Summary Network Email Maintenance Archive Support	
Setup	Network Settings	2
Jana Manage	IP Details	
Users	DHCP	
Alarms	• Static	
	IPv4 Address:	172.16.36.45
Plugins	Netmask:	255.255.255.0
	Default Gateway:	172.16.36.1
	Primary DNS Server:	4.4.2.2
	Secondary DNS Server:	4.2.2.1
	NAT Details	
	Edit	
	Dublic ID-d Address	173 16 26 46

7. Add the SDN Controller.

- In the menu, select Manage/Plugin.
- Browse for the zip file.
- Click Upload.

(intel) Security Ver	tel Security Controller sion: 25 (Build:3589, 20160325-1230)	User: admin Logout ?
Q. Status	SDN Controller Plugns Manager Plugns	
da setup	SDN Controller Plugins	
2 ^{HD} Manage	upload	
Users	Remove the file extended United	
Alarms	LIGHTER IN THE REPORTED.	
Plugins	Plugins	
Sener	Norma Verson jar file MDOUT 135 p.11 mitore do puppur Dees MDOUT 135 p.11 mitore do puppur Dees Socie Deensul 255 Consoler Pupp 251	

- 8. Add a manager connector.
- In the menu, select Setup/Manager Connectors.
- Click Add.
- Set the name of the manager connector.
- Set the IP address of the Network Security Manager.
- Set the credentials to connect to the Network Security Manager.





9. Add the Virtualization Connector.

- In the menu, select Setup/Virtualization Connector
- Click Add.
- Set a name to the virtualization connector.
- Select type: OpenStack.
- Select SDN Controller: Midonet.
- Add OpenStack Identity credentials.

(Babe	Minturdination Comments								
50410	Virtualization Connector								Ľ
stup	Add / Est	20 Deite		Controlar I2			Dravidar ID		
Virtualization Connectors		1994							
Manager Connectors									
Service Function Catalog									
Distributed Applance									
Manage									
									_
	Security Group								2
	+ 455 / Esc								
	Name	renant	метюе	8	services	Deleted	v	50003	
Tal Canvoluter Intel Se	ourity Controller							(har lefter	- Land
tel Security • Intel Se	controller							User: Jahre	Lapur
Security o Intel Security o	ng Controller Management Controller Vertaalisation Controller					_	_	User: John	toput
Security a Intel Se mana 3 Sety	Vrtafiation Culture	1.04						Uw: John	taput 2
Security Contract Security	tor by Controller	al Down		Add Virtualization	Connector		Previder (P	User Lifes	taput
Reter Security C Free Security C Transition	South Controller South States States 1230 States States Control Control States States Control Control North States St	Types	Name*	Add Virtualization I	Connector		i Previder IP	Use: admir	Eggest 2
Executivy to tested So Security to tested So Name water Source So	nety Controller Sector 2010 (1990) Internet (1990) Maria	a Dear	Name * Type *	Add Virtuslization i Gene-Operator OPENTACK v	Connector	ī	Provider ()	Use: advis	Lagout
Texas Decurity of Texas Decuri	Sy Contrailer Seg Contrailer	a bear	Name * Type *	Add Virtualization (Cm=0pmface OPDISTRC ~ ~	Connector	ī	Provider (D	User adver	Eagout (2)
Security Control Security Control Security Control Security Control Security Control Security	V Controller Sensitiv and the sense references and the sense the sense converse A sense Name	Total Types	Name * Type *	Add Virtuslization i Cene-Confuse OfBuStock v SDN Costroller	Connector	ī	Provider IP	Uner Lefter	Esperi E
Security of Intel Security of	norty Controller New York Controller March 2 (1997) New York Controller New York Controller New York Controller	1 (200) 1 (200)	Name * Type *	Add Virtualization Cene-Opmbas OPB030cc v SDN Controller Type NONE	Connector v	Ī	Provider D	Decision	· Lapor
Security V Intel Securi	Ny Controller Marcale at Heart Hallin Andread Andread Constant Andread Andread Constant Name	n Den	Name * Type *	Add Virtualization i Cene-OpenSex OPENSIXC. V SDN Controller Type NONE IP	Connector U	Ī	Provider ID	Over-Lefrer	taput
Annual Security of Lense Jacobie Security of Lense Jacobie Security of Lense Jacobie Security Jacobie Securi	And a statute state	N. SHE	Name * Type *	Add VirtusRizzelon i Cene-OperSust OPENSION v SDN Controller Type MONE p User Name	Connector	Ī	Prode 0	Gue serve	2 Lagour
Becarity Control States		n, inner Teen	Name * Type *	Add Virrussization Gene-Operació Setto Costroller Type none pr User Name Passuerd	Connector		Pender P	Ourstation	2
Security of Security and Security of Secur	Annual Annua	Ter .	Name* Type*	Add Vinustation Generates of Striktor v Stock Container P Deer Name Passeord Fasseord	Connector u	Ì	Provider (7	User Jahre	Caput T
Security Intel Security Manual Manu		10 June 1	Name * Type *	Add Vimultation Gene Spellas ontypick v SDL Cotentier Pge Daer laare Pessood Keystore	Sonedar U	Ī	Prodect II		2
Sourceity of test of t	Contract of the second se		Name * Type *	Add Vinualization Gree deetlos onstatos v SRA Generaliz p Deer Isane Pessond Keystone p+	Connector v		Provider D	Own Jeffer	2
Security a Media Security Security and Security Security Manager Canadata Manager Canadata Manager Canadata Manager Canadata Manager	Control monotone control control monotone control monotone Control monotone control monoto	n Door	Name ¹ Type *	Add Vinuezziten Grei danka u Oddh Cotester 7 pe Mole Pessool Keystor P	Consector 		Provide IP		• Caput (2) (2) (2)
Becarity Constrained Sectors	Controller C	2. (m) 2. (m) 2. (m) 3. (m) 3. (m)	Name * Type *	Add Vinualization Gene Quellus Official Control SPR Control P Duer Name P Restord P R Admin Trater tame *	Conector			Over Jahre	2 2 2 2
Security V Med Sec New Workshow Wanger (Innews) Manger (Innews) Manger (Innews) Manger (Innews) Manger (Innews) Manger		7 (mm) 799 799 799 799 799 799 799 799 799 79	Name * Type *	Add Vinueszeren Grenisyskik – Sóli Consulter Sóli Consulter Passod Dar taare Pi Sóli – Krytsne Pi Admo Traart Name * Dar Name *	Unnector (1231-111-12) (1231-12)		Provide D	Une select	 Spuring 2 2 3 4 4<

3. Status	Virtualization Conr						
setup	🔶 Add 🎤 Ed	c 30 Delete					_
Virtualization Connectors	Name		Type	Controller	10	Provider IP	
Manager Connectors	Cemer-OpenStack		OPENSTACK			10.250.101.10	
Service Punction Catalog							
Distributed Appliance							
Manage							
	Security Group						
	🔶 Add 🕢 2 Ed	t 30 Delete Bro					
	Name	Tenant	Members	Services	Deleted	Last job Status	

- 10. Deploy the distributed appliances.
- Select Setup/Distributed Appliance.
- Click Add.
- Set a name for the distributed appliance.
- Select the Manager Connector (the Network Security Manager setup).
- Select the Service Function Definition.

Status	Distributed Appliance							
Setup	- + Add → 550							
Virtualization Connectors	Name	Manager	Model	Version	Last Job Status		Deleted	
Manager Connectors								
Service Function Catalog								
Distributed Appliance								
Manage								
	Virtual Systems							
	Virtual Systems	ný: Tatls Polsy Masongs	K Deex					
	Virtual Systems eiji: Deskymens VSS Name	w∳ Tatfe Poley Vapongs Vrtualization Connects	12 Devre	Vrualizatio	n Type	Damain	Deleted	



- 11. Deploy the vIPS appliances.
- In the menu, select Setup/Distributed Appliance.
- Click Deployment.
- Click Add.
- Set the name for the deployment specification.
- Select the tenant for the security deployment.
- Select the region (that is, RegionOne).
- Select the hosts that should launch vIPS appliances.
- Select the management network.
- Select the inspection network.
- Set the amount of appliances per host.
- Click OK.

Setup							2	2
Virtualization Connectors	🔶 Add 🥒 Edit	36 Delete 23 Sync						
***************************************	Name	Manager	Model	Version	Last Job Status		Deleted	
Manager Connectors	Cemero#S	mm-NSM	IPS-VM100-VSS	8.1.7.27	PASSED (job ld: 2)		* taba	
Service Function Catalog								
Distributed Appliance								
	1							
lanage								
	1							
	-							-
								_
	Virtual Systems							
	elp Deployments	up name rowy wappings -						
	wije Deployments VSS Name	Virtualization Conr	a poss-	Virtualization Type	D	omain	Deleted	
	wijk Deployments VSS Name	Virtualization Conr	R Deco	Virtualization Type	Di V	main	Deleted	





(intel) Security Version	ecurity Controller 2.5 (Build:3589, 20160325-1230)					User: admin Logout	?	(intel) Security 🐨 Intel S	Security Controller 2.5 (Build:3589, 20160325	1230)				User:ad	dmin Logout	?
Q. Status	Distributed Appliances					?	C	O. Ratus	Virtualization Con	nector					2	C
🏟 Setup	🔶 Add 🍡 Edit 🔅	g Delete 🖉 Sync						i Setup	🔶 Add 🖉 B	it 36 Delete						
Virtualization Connectors	Name	Manager	Model	Version	Last, lob Status	Deleted		Virtualization Connectors	Name		Type	Controller IP		Provider IP		
Manager Connectors	CemeraPS	mis-NSM	IPS-VM100-VSS	8.1.7.27	PASSED (Job Id: 2)	filter		Manager Connectors	Certer-OpenStack		OPENSTACK			10.250.101.10		
Service Function Catalog								Service Function Catalog								
Distributed Appliance								Distributed Appliance								
2 ⁸⁰ Manage								200 Manage								
	California Cae Galace Television (Cae Cae Cae Name K Caelopme	s for Victual System - Cer ≱ Ede ¥ Delen ⊊ Transit S<	en vi95 (Nortual Connector V 2 Sprc) Retrors anti-generati	Arts Crand	Devised V Site	(1400) Store W MODION IN R	2 2		Security Group	IC 26 Delete 5 Tenant Scillent	nd 🗍 🐼 Synt.) Monitoris ME 5, Narrows 1	Serves	Deleted Salue	Lant2xib Status V PROCE but let 77	7	¢

- 12. Create the security group.
- In the menu, click Setup/Virtualization Connector.
- Click Add.
- Set a name for the security group.
- Select tenant.
- Select region.
- Select type of security: Network/Sub-Network/VM
- Add the instance into the security group.
- Click OK.





- 13. Bind a security Group.
- In the menu, select Setup/Virtualization Connections.
- Select the security group.
- Click Bind.
- Check the Enabled box.
- Click OK.



Status	Virtualization Connec								
Setup	🔶 Add 🏒 Edit	36 Delete							
virtualization Connectors	Name		Type	Co	ntroller IP		Provider IP		
Manager Connectors	Cerner-OpenStack		OPENSTROK	~			10.250.101.10		
Service Function Catalog									
Distributed Appliance									
Manare									
Manage									
Manage									
Manage									
Manage									
⁸ Manage									
Manage									
Manage	Security Group							2	
Manage	Security Group							2	
Manage	Security Group	36 Delete	Bind J Sync					?	
Manage	Security Group	36 Delete	Bod [25 Sprc] Members		Services	Deired	Lation Status	2	
Noragi	Security Group	32 Delete	Bind 🖉 Sync] Members	-	Services	Deleted	Last Job Status	?	
Manage	Security Group	36 Delete	End 2 Sec. Menters With Server 1 Gener 2	-	Services	Deleted	Lastjob Status	?	
Manap	Security Group	38 Delete	Ind Sign: Members Mit Shence (School 2)		Services Center-viPS	Deleted	Lastjob Status	?	

3.12 F5 Load Balancer Installation

This section describes how to create and configure an F5 BIG-IP* instance. The F5 BIG-IP performs a variety of functions that drive application availability, optimization, and security. To create a F5 BIG-IP instance, perform the following steps.

- 1. Copy release.fedora, release.redhat.
- 2. On the terminal (on both compute nodes), run the following commands:
 - # cd /etc/nova
 - # cp release release.fedora
 - # cp /home/../release.redhat release
 - # service openstack-nova-compute restart
- 3. Launch a F5 BIG-IP instance with the networks in the following order:
 - Management
 - DataCache
 - Client
 - Data
- 4. Make sure there is no error in the instance. Log in: root, password: default.
- 5. Get the management address of the instance from OpenStack.
- 6. On the browser https://<managementIP>/tmu/login.jsp, log in: admin, password: admin.
- 7. Download the dossier.do file, and then save it locally.
- 8. Activate the license: https:/activate.f5.com.
- 9. Select the appropriate "Activate" option for the version of F5 BIG-IP you are using.
- 10. If activating behind a proxy, manually add a dossier file as follows:
- Select the dossier file downloaded in step 7 to activate, and then click Next.



• Download the license.txt file.



- Upload the license.txt file on the https://<managementIP> portal under the License tab.
- 11. If not activating behind a proxy, upload the license file directly via the Internet.
- 12. After activating, do the following in the F5 BIG-IP portal:
- From the Setup Utility navigation menu, select Resource Provisioning, and then check. Nominal from Local Traffic (LTM) and Advanced Firewall (AFM) drop-down menus.

https://192.168.8.204/xui/					✓ C ^e Soogle	٩	合自 🕹	Ĥ
						Parmore Comm	58 Y	Logiout
ONLINE (ACTIVE) Standalore Hep Ablue	The chart is now al Click Revert to again Setup Utility — Resource Pr	towing the minist show the current ovisioning	num resources required resource a location	for the select	ed nodules			
tup Utility								
Introduction	Modified Resource Allocation	(prior to redist	(buildin)					_
Licerse	CPU	MGMT	(188/89%)					
Resource Provisioning	Disk (44GB)	AFM			Unallocated			
Device Certificates	Memory (15.7GB)	MGMT	TMM		Unallocated			
Platorn	Module		Provisioning		Licerse Status	Required Disk (GB)	Required Memor	ry (MB)
Notwork	Marganemerr (MSMT)		Small		NPA	0	1564	
Recurcancy			Deabled	-	l inersed	0	0	
VLANS	Camer Grade NAT (CC)	eAT)	- Company			-	1	
ConfigSync	Local Traffic (LTM)		Nominal Nominal	-	Licensed	0	848	
Fallover	Application Security (ASI	01	C None		Licensed	12	808	
Minoring	Gibbel Letter (CTM)		None		Licensed	0	148	
Active/Standby Pair			O • • • •		E. Delemand		140	
Discover Peer	Link Controller (LC)		None		E Outenau		140	
	Access Policy (APM)		None		Limited mode available without a license	12	494	
	Application Visibility and	Reporting (AVR)	None		Not the second s	16	448	
	Policy Enforcement (PEM	0	None		E Unicensed	16	760	
	Advanced Firewall (AFM		Nomina.	-	Licensed	16	756	
	Application Acceleration	Nonagar (AAN)	C None		tioned	32	2050	
	-		None		Evaluation expires after: Nov 14, 2014	24	4095	

- Click Next to reboot the system, and then configure the list items below.
- Enter the hostname: xxx.xxx.com
- Root account: default
- Password: default
- Admin password
- Log in again with a new admin password
- SSH: Checked
- 14. In Advanced Options, click Finished.

- 15. From the Network navigation menu, select VLANS, and then create the following new VLANs as shown in the screenshots below:
- Apache VLAN : : Interfaces Untagged: 1.1, Available: 1.2, 1.3
- Client VLAN : : Interfaces Untagged: 1.2, Available: 1.1, 1.3
- Data VLAN : : Interfaces Untagged: 1.3, Available: 1.1, 1.2

		❤ ੴ <mark></mark> \ 🛃 ❤ Goo
Hostrame: host-192-168-8-204 open stacklos IP Address: 192.158.8.204	al Date: Sep 29, 2014 Time: 7:43 AM (PDT)	User, admin Role: Administrator
Main Help About	Network » VLANS: VL	AN LISE >> New VLAN
Statistics	General Properties	
IADDS	Name	DataVLAN
😚 dns	Description	
fin Local Traffic	тад	
	Resources	
Device Management	Interlaces	Urtzgged Avaitable Tagged
Security		
Network	Configuration: Basic	<u>_</u>
Interfaces	Source Check	0
Routes 🕘	MTU	1500
Self IPs 📀	s F low	
Packet Filters	Polling Interval	Dofault Default Value: 10 seconds
T runks >	Sampling Rate	Default Value: 2018 seconds
T unnels >		
Route Domains 🕘	Cancel Repeat	Finished
VLANs >		
Class of Service		
ARP		
IPsec >		
WCCP 💿		
DNS Resolvers		
System		



- 16. From the Network navigation menu, create and configure self IP addresses for the following networks.
- ApacheNetwork
 - IP address: ApacheNetwork IP address of F5 BIG-IP instance from OpenStack
 - Netmask: 255.255.255.0
 - Port Lockdown: Allow All
- ClientNetwork
 - IP address: ClientNetwork IP address of F5 BIG-IP instance from OpenStack
 - Netmask: 255.255.255.255
 - Port Lockdown: Allow All

- DataNetwork
 - IP address: DataNetwork IP address of F5 BIG-IP instance from OpenStack.
 - Netmask: 255.255.255.0
 - Port Lockdown: Allow All

♦ A https://192.168.8.204/xui/			× €		
Hostname: host-192-168-8-204.openstackiocal IP Address: 192-168.8.204	Date: Sep 29, 2014 Use Time: 9:27 AM (PDT) Rok	r: admin e: Administrator			
CNL NE (ACTIVE) Standalone					
Main Help About	Network » Self IPs » Apache	Network			
Statistics	🔅 🗸 Properties Secu	rity			
IApps	Configuration				
S DNS	Nane	ApacheNetwork			
~ ~~	Partition / Path	Common			
Local Traffic	IP Address	198.24.0.6			
Acceleration	Netmask	255.255.255.0			
Device Management	VLAN / Tunnel	ApacheVLAN 📩			
~	Port Lockdown	Allow All			
Security	Traffic Group	Inherit traffic group from current partition / path	-		
Network	Thank choup	traffic-group-local-only (non-floating)	•		
Interfaces	Update Cancel Delete				
Routes 🕒					
Self IPs 📀					
Packet Filters					
Trunks					
Tunnels					
Route Domains 🕙					
VLANs >					
Class of Service					
ARP					
IPsec >					
WCCP 💿					
DNS Resolvers					
System					

♠ https://192.168.8.204/xu/				× €	S v Google		Q 🕁	ė	4 +	=
Ficetromer. Acut-192-109-8-234.openatic Mocial IP Ackinese. 192.198.8.204	Date: Sep 29, 2014 Time: 9:28 AM (POT)	User: adeia Rola: Administrator				Par	tion Common	~	log	BUT!
Starchiksen										
Main Help About	Network Self IPs									
Statistics	🗢 👻 GelliP List									
Apps									Creat	
S DNS	🔽 = Name		· Application		· Nethask	· VLAN / Tunnel	· Traffic Group		Parton	Path
255 Local Testla	ApacheNetwork			198.24.0.6	255.255.255.0	ApacheVLAN	traffic-group-local	oniy (Common	
ED recei (rane	ClientNetwork			198.58.0.2	255.255.255.255	ClenVLAN	traffic-group-local	oriy (Common	
Acceleration	DomNetwork			198.43.0.4	255.255.255.0	DBBVLAN	traffic-group-local	aniy (Common	
Device Management	Dekte									
Security										
Network										
Interfaces										
Routes										

- 17. From the Local Traffic navigation menu, select Pools, and then configure as follows.
- Name (ServerPool Nodename): Apacheservers1
- Health Monitors: http
- Address: Get IP address from the OpenStack.
- New Members: Servers 1 and 2.

/	L Dute: Dec 20 2014	In the second	
osname: host 192-168/6-204.openstac.koca ^o Address: 192.168/8.204	Time: 7:55 AM (PDT)	∪ser:acmin Role: Administrator	
ONLINE (ACTIVE) Stasdalons	Local Traffic 1/ Pools - Pool	Liter on Many Produ	
Substice	Local Hand w Foots (Foot		
	Configuration: Basic -		
IApps	Name	Apacheservers1	
DNS	Description		
Local Traffic		Active Available	
Network Map Vinual Servers	Health Monitors	http	
Policies	-		
Profiles	He sources	Davad Dakin al	
Deale	Dringite Carrier Antenntian		
Notes -	Frionty cricup Activation		
Monitors		Address: 198.24.0.2	ional)
Traffic Class		Service Port: Select	
Address Translation	New Monhore	Add	
Acceleration			
Device Management		Edit Delete	
Security	Cancel Repeat Finis	ihed	
Network			
System			

18. Repeat step 16 for Apache Server 2.

19. From the Local Traffic navigation menu, select Virtual Servers. In the Destination field, enter the Client Network IP address of the F5 BIG-IP instance from OpenStack.

https://192.168.8.204/xui/		V C 🔣 V Google		
Main Help About	Local Traffic + Vinual Servers	:: Vintual Server List New Vintual Server		
Statistics				
-	General Properties			
Apps	Name	Apacho virtual server		
DNS	Description			
Cocal Traffic	Тура	Stardaid		
Abstract Max	Source			
Vidual Separat	Device ten	Type: Host O Network		
Policies	LASOFEDOR	Address: 198.58.0.2		
Profiles	Service Port	00 HTTP -		
iBules -	Notify Status to Virtual Address	V		
Pools >	Gtate	Enabled .		
Nodes >	Configuration: Basic 1			
Monitors	Protocol	TCP		
Traffic Class 💿	Protocol Profile (Client)	кр		
Address Translation	Protocol Profile (Server)	Use Client Profile)		
Acceleration	HTTP Profile	None		
ACCONTRIAN	FTP Padle	None v		
Device Management	DTCD Durfile			
) Security	n for riune	None •		
a) Manuali	SMTPS Profile	None -		
Network		Selected Available		
System	SSL Profile (Client)	diertssl diertssl-insecure-compatible wom-default-dientssl		
	SSL Profile (Server)	Selected Analobie Comment accords ac		

- 20. From the Local Traffic navigation menu, select Address Translation and configure as follows:
- Name: SNAT List
- Translation: Automap
- Origin: All IPv4 Addresses
- VLAN/Tunnel Traffic: * All
- Auto Last Hop: Default

21. Click Finished.

Datame: 10 Del No 106 20 2009 Into Local T Tendelson: 10 Del No 106 20 2009 Into Local T Tendelson: Del No 10 Del No 106 20 2009 Into Local T Statistic s Del S Local Traffic Nature Nature Nature Del S Local Traffic Nature Nat	r sep 23, 2014 e 8:15 AM (PDT) rattic + Address Tr Propenies tion auton	Uder: adams Rake: Administrator framskubm: SNAT List + New ShAT SNAT List Automap	
OHLINE (ACTIVE) Standakow Malin Help About Local T Standakow	raffic +> Address Tr Propenies Idon ration Iaton	franslation : SNAT Lin: >> New SNAT	
Standalow Main Pelp About Local T Statestics Coneral Rape Name DHS Description Local Traffic Configure Virtual Servers Origin	raffic +> Address Tr Propenies Idon ration Iaton	franskuba : SNAT List >: New SKAT	
Main Help About Local T Statistics Canenal Apps DNS Decong Local Traffic Contigue Virtual Servers (Origin	ratfic » Address Tr Properies dion auton	framkaton : SNAT Lint >= New SHAT	
Main Pelp About Local T Statistics Control Name DNS Descript Network Map Untuit Servers (Origin	ratific >> Address Tr Properties tion ration	Familyaruban : SNAT Likt >> New SHAT	
Statistics Apps DNS Local Traffic Network Map Virtual Servers Origin	Properties tion ration	SNAT LIN	
Apps Coveral Name Description Coveral Name Description Coveral Name Description Coverage Name Name Name Name Name Name Name Nam	Properties tion ration	Ausmap	_
Diss Descrip Diss Descrip Local Traffic Configure Network Map Transit Vintual Servers Origin	ition iation	SIVAT LIst	_
DHS Descrip Local Traffic Configur Network Map Trans ViriLail Servers , Origin	nation lation	Aubmap 💌	_
Local Traffic Configure Network Map Trans Vinual Servers Drigin	nation lation	Automap 💌	
Network Map Transl Virtual Servers , Origin	lation	Automap	
Vinual Servers , Origin			
		All IPv4 Addresses 💌	
Policios > VLAN /	Turnel Traffic	TAIL I	
Profiles > Auto La	ist Hop	Default	
IRules > Como	Report	nie herd	
Pools >	(nopon) (nin		
Nodes >			
Monitors 🕞			
Traffic Class 🕤			
Address Translation			
Acceleration			
Device Management			
) Security			
Network			
System			

- 22. Create a SNAT pool list.
- Name: Apache SNAT List
- IP address: Apache IP address

 https://192.168.8. 	.204/xui/	
Hostname: host-192-168-8-201, P Address: 192.168.8.204	openstacklocal Date: Se Timo: 8:1	p.29,2014 User:admin. 8 ANI (PDT) Rob:Administrator
Main Help) About Local Traifi	c » Address Translation : SNAT Pool List » Hew SNAT Pool
Statistics	General Pro	perties
Mpps	Name	ApacheSNATLIst
DNS	Configuratio	n
E Local Traffic		IP Address: 198.24.0.6
Network Map		Add
Virtual Servers	, Member Li	st
Policies		
Profiles		Edit Delete
iRules	Camel	Papat Einichari
Pools	Cathor	Ropeal Pittshou
Nodes	•	
Monitors	 Image: Image: Ima	
Traffic Class		
Address Translation	÷.	
Acceleration		
Device Management		
J Security		
Network		

23. Click Finished.

- 24. Assign a floating IP address to the client and data network of a F5 BIG-IP instance and a secondary management network to a Steelhead instance.
- 25. Check the web browser: http://<floatingIP_of_client_ network_IP_of_BIG-IP_Instance>/Pictures
- 26.Copy back:cp /etc/nova/release.fedora /etc/ nova/release.

The network topology after configuration is shown below.

4.0 Demo Setup: Cross-Tenant Cross-Machine Attack

Tenants in OpenStack are different projects that represent different customers of Cerner. The idea of the setup is to simulate two different customers inside the cloud, and perform the attack from one project to another.

The demo shows the interaction of VMs in a multi-tenant environment, where one VM represents the attacker (in Tenant 2) and the other VM is the destination of the attack (in Tenant 1). The MidoNet SDN controller redirects the traffic for inspection to the Security Tenant (Intel ISC Tenant), containing security functions, that is, OSC, McAfee Network Security Manager and vIPS. The vIPS performs analysis of the packets. If packets correspond to the malicious activity, these will be blocked; otherwise, packets will continue the normal data path.



Demo Setup

Scenario #1

- a) Protect Load Balancer only (on controller)b) Access LB (with & without attack)
- c) View results in Real Time Threat Analyzer

Scenario #2

- a) Protect Web3 only (on compute)
- b) Access LB (with & without attack)
- c) When LB uses Web3, it is protected





To set up the demo, perform the following steps.

1. Set a floating IP address to the Network Security Manager Windows VM and OSC VM.

ED HA	T'ENTERPRISE LINUX OPENSTACE	K PLATFORM Project Admin Identity			
Vervie	w Instances Volumes	Images Access & Security			
Secur	rity Groups Key Pairs Float	ong IPs API Access			
		k		%Alocate IP To Project	Chelesse Fouring Ps
	IP Address	Mapped Fixed IP Address	Pool	Status	Actions
	10,250,101.135	ISC-latest-version 172.16.36.45	Public	Active	Disassociate
-		NUMBER OF STREET, STRE	Public.	Latera .	The second s

2. Using the floating IP address of the OSC, access the OSC dashboard and verify whether the network "client" from Tenant 1 is bind enabled.

Solution Image Solution Value Type Controlor 3P Boder 3P Solution Control 2P Solution 2P Solution 2P Solution 2P Solution Control 2P Solution 2P Solution 2P Solution 2P Solution Control 2P Solution 2P Solution 2P Solution 2P Solution Control 2P Solution 2P Solution 2P Solution 2P Solution Control 2P Solution 2P Solution 2P Solution 2P Solution Control 2P Solution 2P Solution 2P Solution 2P Solution Control 2P Solution 2P Solution 2P Solution 2P	Status	Virtualization Connector						
Annuel Consider # Annuel * Type Consider # Provider # Wanger Constants Consider # Provider # Provider # Provider # Some Andern College Consider # OpenCollege Provider # Provider # Wanger Some Andern College Consider # OpenCollege Provider # Wanger Some Andern College Consider # Some Andern College Provider # Wanger Some Andern College Consider # Some Andern College Provider # Wanger Some Andern College Consider # Some Andern College Provider # Wanger Some Andern College Consider # Some Andern College Provider #	Setup	💠 Add 🍃 Edit 🛛 Sit Delete						
Marger Conversion Severa Ancoin Cassing Dember of Agencia/S Marger	Virtualization Connectors	Name	Type	Controller IP		Provider IP		
Sever Anction Cadeling Derivation Registeries Severage Several Market Several Services Derived Lastrido Services Name Technik Wenteries Services Derived Lastrido Services	Manager Connectors	Cemer-OpenStack	OPENSTACK	*		10.250.101.10		
Strikul Agelann Mange Senerge Snage ▲ Art _ Arts _ Market _ Banet _ Or Spec Name Taneet _ Monters _ Servers Desked Larbö Strat	Service Function Catalog							
teory beag Security beag ■ 4.44 (> 100 (> 100 (> 000)) New Touck Meders Serves Daved Larbb Stars	Distributed Appliance							
Society Servey → Aut Mark Mark Bear Server None Reset Monteyn Servers Deleved Ladde Social →								
Security Strange 	Manage							
Scority Group Scority Group (a) Air (a) (b) (b) (b) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c	danage							
Saturity Servey	danage							
(lange							
Name Tinant Members Services Deleted Latitod Status	danage	Security Group		-			2	
	lang	Security droup	Text of Sec	_			?	
	lange	security droup ↓ Ad / ≠ fdt 34 Dates Name Tenant	Ind 25pc	Servoes	Deleted	Last Job Status	?	
CREMENT RELATED RELATED CREMENTS TASE PROSECUES RELATED	Marage	Security Orolop @Add // Edr. 3g Deen Name Tinant	Red 2 Syrc. Members	Services	Deleted	Last Job Status	1	2

- 3. Access any Microsoft Windows machine in Tenant 2.
- 4. Access the dashboard of the Network Security Manager using the floating IP address of the Network Security Manager. Log in with the Network Security Manager credentials.





5. Click Analysis.

McAfee Network Se Version: 8.2.7.	curity Manag .73.3	er P Dashboard	Arady six	olicy	Devices	Aanage	5
Threat Explorer Malware Detections	Filter:	npany > Threat Explor	rer		Top: 5 ¥	Any direction	Last 14 days 💌
Active Botnets High-Risk Endpoints Network Forensics Endpoint Executables	Төр	Attacks				Attack Name	*
Quarantine Threat Analyzer		Attack Name	Attack Category	Att	ack Subcategory	Attack Severity	Attack Count
Real-Time Historical # Event Reporting	1	HTTP: IIS root.exe	Exploit Exploit	pris pris	illeged-access illeged-access	HighHigh	11
Next Generation Reports Traditional Reports	Tep	Attackers					~
						Attacker IP A	ddress 👻
		ttacker IP Address	Attacker	DNS N	Attacker Country	Attacker User	Attack Count
	1 1	0.250.101.141				Unknown	18
De .	Top	Targets					*
						Target IP Add	Iress 👻
		arget IP Address	Target DI	15 Na	Target Country	Target User	Attack Count
	1 1	72.16.58.4				Unknown	18
	Top	Attack Applications					~

- 6. In the Thread Analyzer menu, select Real-Time.
- 7. Download the JNLP file to start the Real-Time Threat Analyzer.
 - Click in the link Start the Real-Time Threat Analyzer.
 - Go to downloads and start the file with JAVA Web Start Launcher.

a	McAfee Network Security Manager - 10.250.101.136 - Internet Explorer	
CMT-07:00 /My Company Administrator	1 Login History	Log.Out 🛠 ?
W McAfee Network Securi Version: 8.2.7.73.3	ty Manager Relation of the second secon	±0
Domain: //My Company	/Hy Company > Threat Analyzer > Real-Time	?
Trans Explorer Halanes Extensions Active Bords High-Ball Engones Interacti Forensios Engolinis Executables Quarantine Real-Time Natornal Autornal Autornal Autornal Autornal Nett Concention Reports Traditional Reports	Los the Real-Sine Threat Analyse to analyse security events as they occur. Real-Time • Start the Real-Time Threat Analyze	

🛣 l 🔁 🌆 = 1	Do	wnloads		- 🗆 X
File Home Sha	re View			~ 6
🐑 - + 🚺 + 1	This PC + Downloads	~ C	Search Down	loads P
Favorites	Name	Date modified	Туре	Size
E Desktop	🖾 setup	2/25/2016 1:04 AM	Application	670,126 KB
🗼 Downloads	ThreatAnalyzer (1)	3/1/2016 6:13 PM	JNLP File	4 KB
Secent places	🚠 ThreatAnalyzer (2)	3/2/2016 12:01 AM	JINLP File	4 KB
	i ThreatAnalyzer (3)	3/3/2016 10:55 PM	JNLP File	4 KB
1 This PC	freatAnalyzer (4)	3/9/2016 4:13 PM	JINLP File	4 KB
	🚔 ThreatAnalyzer (5)	3/9/2016 4:15 PM	JINLP File	4 KB
Network.	i ThreatAnalyzer (6)	3/9/2016 4:17 PM	JNLP File	4 KB
	ThreatAnalyzer (7)	3/9/2016 4:19 PM	JINLP File	4 KB
	in ThreatAnalyzer (8)	3/21/2016 4:23 PM	JINLP File	4 KB
	i ThreatAnalyzer (9)	3/21/2016 4:33 PM	JNLP File	4 KB
	🚠 ThreatAnalyzer (10)	3/21/2016 4:34 PM	JNLP File	4 KB
	🖆 ThreatAnalyzer (11)	3/28/2016 1:54 PM	JINLP File	4 KB
	ThreatAnalyzer (12)	4/6/2016 3:33 PM	JINLP File	4 KB
	🚠 ThreatAnalyzer (13)	4/6/2016 3:35 PM	JNLP File	4 KB
	ThreatAnalyzer (14)	4/25/2016 10:44 PM	JINLP File	4 KB
	in ThreatAnalyzer (15)	4/26/2016 9:31 AM	JINLP File	4 KB
	🚠 ThreatAnalyzer	2/25/2016 11:10 PM	JINLP File	4 KB

- 🔊 🖓	Downl	oads	
e Hom	e Share View		
	👔 🕨 This PC 🕨 Downloads	v (Search Downlo
Favorites	Name	Date modified	Туре
Deskt		25/2016 1:04 AM	Application
😹 Down	lieu de concepte en en this 61-2	1/2016 6:13 PM	JNLP File
Recen	How do you want to open this file?	2/2016 12:01 AM	JINLP File
	I lice this and for all join flas	3/2016 10:55 PM	JNLP File
This PC	Solution and the second	9/2016 4:13 PM	JNLP File
-		9/2016 4:15 PM	JINLP File
Networ	Keep using Java(TM) Web Start	9/2016 4:17 PM	JNLP File
	Launcher	9/2016 4:19 PM	JNLP File
		21/2016 4:23 PM	JINLP File
		21/2016 4:33 PM	JINLP File
	More options	21/2016 4:34 PM	JINLP File
L		28/2016 1:54 PM	JNLP File
	🖾 ThreatAnalyzer (12)	4/6/2016 3:33 PM	JINLP File

• In the Security Warning dialog, click Continue.



8. Click Alert to see the real-time attacks.



- 9. Open Internet Explorer in any Microsoft Windows machine on Tenant 2.
- 10. Navigate to the web servers passing the floating IP address of the load balancer, which is connected to the client network (the network that is bind enabled in OSC). To navigate, use: http://10.250.101.137/HelloWorld.php.

🚖 🕘 root 🧃 cmd 🧃 HelloWorld		0.0010000000000000000000000000000000000
Hello World Machine WebServer 2		

- 11. Execute and attack requesting cmd.exe from the web servers: http://10.250.101.137/cmd.exe
- Because the file is not allowed, it should be blocked and the browser should show an error failing to get the file by timeout.



12. In the Real-Time Threat Analyzer windows, the attack should show up.

A 🗼		R	eal-time Threa	t Analyz	ter			×
Server Name: 10.250	0.101.136 User Name: Adminis	trator Domain: /M	y Company	-				?
	Network Security Manag Threat Analyzer	per P Dashboard	Alerts	Endpol	ints Forer	Preferences		
All Alerts								bisplay Filtering *
II / <u>All Alerts</u>					Detai	I View O Group By	Admin Domain	
1 Time	Attack Name	Sec IP	Src VM Name		DestIP	Dest VM Na	Dest P	Attack Count
XX	×	×		×	X	×	×	
04/28 12:45:11	HTTP: IIS cmd.exe Execution	10.250.101.141	Attacker-3		172.16.58.4	Big1P_LoadBalancer	80	1
1	H.							•
Total Rows 1								Options

13. There is another kind of attack that should pass to the user by sending a notification to Real Time Threat Analyzer. For this kind of attack we use: http://10.250.101.137/root.exe.

Image: 10220 107137/root exe P - C Image: 10220 107137/root exe N<	· · · · · ·								×
Content in the set of the se	(+) A http://1	0.250.101.137/root.exe		0-0	10.250.101.	137	×		
Real-time Thread Analyzer Image: Thread Analyzer Process Real-time Thread Analyzer Process Process	🐅 🕘 root 🕘 cmd 🤅	HelloWorld							
Image: Include the second advectation of Contract for Company Image: Include the second advectation of Contract for Company Image: Include the second advectation of Contract for Company Image:	hello world root	test webserver3							
Image Attack Rames En Image									
All Advers Control 1/02 Control 1/02 Company Control 1/02 Company Company <thcompany< th=""> <thcompany< th=""> Company</thcompany<></thcompany<>	<u>ه</u> ا		R	eal-time Thr	reat Analyzer				
Network Network Security Manager Dread Security Manager Main Security Main Display Filtering * 1 Attack Resex X X X Note Note </td <td>Serve ame: 10.250.101.</td> <td>136 User Name: Adminis</td> <td>trator Domain: /M</td> <td>y Company</td> <td></td> <td></td> <td></td> <td>1</td> <td></td>	Serve ame: 10.250.101.	136 User Name: Adminis	trator Domain: /M	y Company				1	
Interest Analyzer Databased Average Subdacts Produces Databased Average Subdacts Databased Databased Average Subdacts Databased Databased Subdacts Databased Databased Subdacts Databased Databased <thdatabased< th=""> Databased Dat</thdatabased<>						EC.			
At Aders Deploy Effering 2 1) Attack Name Sec 1P Sec VVR Name Dect SP Geno By Attack Count Image: Count Address Image: Count	W McAfee N	etwork Security Manag	per and						
Image: Image:<	McAfee T	etwork Security Manag hreat Analyzer	Dashboard	Alers	Endpoints	Forer	sics Preferences		
Time: Attack Name Set IP Set VIR Name Deat VIR Name Owat P Attack Conet A/218 11:06:01 HTTP: III rest.eve Ibecn.1 10:29:01:14.14 Attacker.3 1772:16:86.4 BigPL_coddbalancer 80 1 GA/28 12:04:01:11 HTTP: III rest.eve Ibecn.1 10:29:01:01:141 Attacker.3 1772:16:86.4 BigPL_coddbalancer 80 1 GA/28 12:04:01:11 HTTP: III rest.eve Ibecn.1 10:29:01:01:141 Attacker.3 1772:16:86.4 BigPL_coddbalancer 80 1 GA/28 12:04:01:11 HTTP: III rest.eve Ibecn.1 10:29:01:01:141 Attacker.3 1772:16:86.4 BigPL_coddbalancer 80 1	All Alerts	etwork Security Manag hreat Analyzer	Dashboard	Alers	Endpoints	Forer	sics Preferences	-	Display Filtering
M Machine M </th <th>All Alerts</th> <th>etwork Security Manag hreat Analyzer</th> <th>Dashboard</th> <th>Alerts</th> <th>Endpoints</th> <th>Forer</th> <th>Sics Preferences</th> <th>Admin Domain</th> <th>Display Filtering</th>	All Alerts	etwork Security Manag hreat Analyzer	Dashboard	Alerts	Endpoints	Forer	Sics Preferences	Admin Domain	Display Filtering
04/28 12/50 1 #TTP: IIS restore banch 10.230.101.141 48nder-3 17.214.584 Big/P_LoadBiblecer 80 1 04/28 12/4511 #TTP: IIS restore banch 10.230.101.141 48nder-3 17.214.584 Big/P_LoadBiblecer 80 1 04/28 12/4511 #TTP: IIS restore banch 10.230.101.141 48nder-3 17.214.584 Big/P_LoadBiblecer 80 1 04/28 12/4511 #TTP: IIS restore banch 10.230.101.141 48nder-3 17.214.584 Big/P_LoadBiblecer 80 1 04/28 12/4511 #TTP: IIS restore banch 10.230.101.141 48nder-3 17.214.584 Big/P_LoadBiblecer 80 1 04/28 12/4511 #TTP: IIS restore banch 10.230.101.141 48nder-3 17.145.84 Big/P_LoadBiblecer 80 1	All Alerts	etwork Security Manag hreat Analyzer	Dashboard	Alerts	Endpoints	Forer	sics Preferences	Admin Domain	Display Filtering
04/28 12/45:1) VTTP: IIS ond-exe becades 10.350.101.141 Attacker-3 172.16.58.4 Bg/P_LoadBabacar 80 1	All Alerts 1 Time =	etwork Security Manag hreat Analyzer Attack Name	Dashboard Sec IP	Alerts	Endpoints te Des	Detai	sics Preferences	Admin Domain Dest P	Display Filtering
Taba Rows 2 Options	Million Million <t< td=""><td>etwork Security Manag hreat Analyzer Attack Name X I IS root.exe Execut</td><td>Sec IP X 10.250.101.141</td><td>Alerts</td><td>Endpoints Te Des¹ X -3 172.</td><td>Detail EIP X 16.58.4</td><td>sics Preferences I View O Group By Dest VH Na Big1P_LoadBalancer</td><td>Admin Domain Dest P</td><td>Display Filtering</td></t<>	etwork Security Manag hreat Analyzer Attack Name X I IS root.exe Execut	Sec IP X 10.250.101.141	Alerts	Endpoints Te Des ¹ X -3 172.	Detail EIP X 16.58.4	sics Preferences I View O Group By Dest VH Na Big1P_LoadBalancer	Admin Domain Dest P	Display Filtering
Total Rows 2 Options	All Alerts 1 /All Alerts 04/28 12:45:11 HTTP	Attack Name Attack Name Its root.exe Execut Its cont.exe Execut	Sec IP X 10.250.101.141 10.250.101.141	Alers Sec VM Nam Attacker Attacker	Endpoints Endpoints ** ** ** ** ** ** ** ** ** *	• Detai • Detai t IP X 16.58.4 16.58.4	sics Preferences View O Group By Dest VH Na BigIP_LoadBalancer BigIP_LoadBalancer	Admin Domain Dest P 80 80	Display Filtering Attack Count I I I
	Mathematica T All Alleris I Alleris	etronf. Security Management Analyzer Attack Rame X Hitack Rame X IIIS root are (secil IIIS ond are (secil IIIS ond are (secil IIIS ond are (secil)	Cashboard Cashboard	Sec VH Naw Attacker Attacker	ie Dest X -3 172.	© Detail * Detail * LIP X 16.58.4	A Provinces	Admin Domai Desit Pr., 80 80	Display Filtering

Appendix A: The PackStack Answer File

[general]
CONFIG SSH KEY=/root/.ssh/id rsa.pub
CONFIG DEFAULT PASSWORD= <set td="" your<=""></set>
password>
CONFIG_MARIADB_INSTALL=y
CONFIG_GLANCE_INSTALL=y
CONFIG_CINDER_INSTALL=y
CONFIG_MANILA_INSTALL=n
CONFIG_NOVA_INSTALL=y
CONFIG_NEUTRON_INSTALL=y
CONFIG_HORIZON_INSTALL=y
CONFIG_SWIFT_INSTALL=y
CONFIG_CEILOMETER_INSTALL=y
CONFIG_HEAT_INSTALL=n
CONFIG_SAHARA_INSTALL=n
CONFIG_TROVE_INSTALL=n
CONFIG_IRONIC_INSTALL=n
CONFIG_CLIENT_INSTALL=y
CONFIG_NTP_SERVERS=
CONFIG_NAGIOS_INSTALL=n
EXCLUDE_SERVERS=
CONFIG_DEBUG_MODE=n
CONFIG_CONTROLLER_HOST=10.250.101.10
CONFIG_COMPUTE_HOS
TS=10.250.101.12,10.250.101.14
CONFIG_NETWORK_HOSTS=10.250.101.10
CONFIG_VMWARE_BACKEND=n
CONFIG_UNSUPPORTED=n
CONFIG_USE_SUBNETS=II
CONFIG_VCENIER_HOSI-
CONFIG_VENIER_USER-
CONFIG_VCENTER_FASSWORD-
CONFIG_VEENIEK_CHOSTEK_NAME
CONFIG_SIGKAGE_HOST=10.250.101.10
CONFIG USE EPEL=n
CONFIG REPO=
CONFIG ENABLE RDO TESTING=n
CONFIG_BH_USER=
CONFIG_SATELLITE_URL=
CONFIG RH PW=
CONFIG BH OPTIONAL=V
CONFIG BH PROXY=
CONFIG BH PROXY PORT=
CONFIG_RH_PROXY_USER=
CONFIG RH PROXY PW=
CONFIG_SATELLITE_USER=
CONFIG_SATELLITE_PW=
CONFIG SATELLITE AKEY=
CONFIG SATELLITE CACERT=
CONFIG SATELLITE PROFILE=
CONFIG SATELLITE FLAGS=
CONFIG SATELLITE PROXY=
CONFIG SATELLITE PROXY USER=
CONFIG SATELLITE PROXY PW=
CONFIG SSL CACERT FILE=/etc/pki/tls/
certs/selfcert.crt
CONFIG_SSL_CACERT KEY FILE=/etc/pki/
tls/private/selfkey.key
CONFIG_SSL_CERT_DIR=~/packstackca/

CONFIG SSL CACERT SELFSIGN=y CONFIG SELFSIGN CACERT SUBJECT C=--CONFIG SELFSIGN CACERT SUBJECT ST=State CONFIG SELFSIGN CACERT SUBJECT L=City CONFIG SELFSIGN CACERT SUBJECT 0=openstack CONFIG SELFSIGN CACERT SUBJECT OU=packstack CONFIG SELFSIGN CACERT SUBJECT CN=securitypoc CONFIG SELFSIGN CACERT SUBJECT MAIL=admin@securitypoc CONFIG AMOP BACKEND=rabbitmg CONFIG AMOP HOST=10.250.101.10 CONFIG AMQP ENABLE SSL=n CONFIG AMQP ENABLE AUTH=n CONFIG AMQP NSS CERTDB PW=<set your CONFIG_AMQP_AUTH_USER=amqp_ password> user CONFIG AMOP AUTH PASSWORD=<set your password> CONFIG MARIADB HOST=10.250.101.10 CONFIG MARIADB USER=root CONFIG MARIADB PW=intel CONFIG KEYSTONE DB PW=intel CONFIG KEYSTONE REGION=RegionOne CONFIG KEYSTONE ADMIN TOKEN=intel CONFIG KEYSTONE ADMIN EMAIL=root@ localhost CONFIG KEYSTONE ADMIN USERNAME=admin CONFIG KEYSTONE ADMIN PW=intel CONFIG KEYSTONE DEMO PW=intel CONFIG KEYSTONE API VERSION=v2.0 CONFIG KEYSTONE TOKEN FORMAT=UUID CONFIG KEYSTONE SERVICE NAME=keystone CONFIG KEYSTONE IDENTITY BACKEND=sql CONFIG KEYSTONE LDAP URL=ldap://10.250.101.10 CONFIG KEYSTONE LDAP USER DN= CONFIG KEYSTONE LDAP USER PASSWORD= CONFIG_KEYSTONE_LDAP_SUFFIX= CONFIG KEYSTONE LDAP QUERY SCOPE=one CONFIG KEYSTONE LDAP PAGE SIZE=-1 CONFIG KEYSTONE LDAP USER SUBTREE= CONFIG KEYSTONE LDAP USER FILTER= CONFIG KEYSTONE LDAP USER OBJECTCLASS= CONFIG_KEYSTONE_LDAP_USER_ID_ ATTRIBUTE= CONFIG_KEYSTONE_LDAP_USER_NAME_ ATTRIBUTE= CONFIG_KEYSTONE_LDAP_USER_MAIL_ ATTRIBUTE= CONFIG_KEYSTONE_LDAP_USER_ENABLED_ ATTRIBUTE= CONFIG KEYSTONE LDAP USER ENABLED MASK = -1CONFIG KEYSTONE LDAP USER ENABLED DEFAULT=TRUE CONFIG KEYSTONE LDAP USER ENABLED INVERT=n

CONFIG KEYSTONE LDAP USER ATTRIBUTE IGNORE= CONFIG KEYSTONE LDAP USER DEFAULT PROJECT_ID_ATTRIBUTE= CONFIG KEYSTONE LDAP USER ALLOW CREATE=n CONFIG KEYSTONE LDAP USER ALLOW UPDATE=n CONFIG_KEYSTONE_LDAP_USER_ALLOW_ DELETE=n CONFIG_KEYSTONE_LDAP_USER_PASS_ ATTRIBUTE= CONFIG KEYSTONE LDAP USER ENABLED EMULATION DN= CONFIG KEYSTONE LDAP USER ADDITIONAL ATTRIBUTE MAPPING= CONFIG KEYSTONE LDAP GROUP SUBTREE= CONFIG_KEYSTONE_LDAP_GROUP FILTER= CONFIG KEYSTONE LDAP GROUP OBJECTCLASS= CONFIG_KEYSTONE_LDAP_GROUP_ID_ ATTRIBUTE= CONFIG_KEYSTONE_LDAP_GROUP_NAME_ ATTRIBUTE= CONFIG_KEYSTONE_LDAP_GROUP_MEMBER_ ATTRIBUTE= CONFIG KEYSTONE LDAP GROUP DESC ATTRIBUTE= CONFIG KEYSTONE LDAP GROUP ATTRIBUTE_IGNORE= CONFIG_KEYSTONE_LDAP_GROUP_ALLOW_ CREATE=n CONFIG KEYSTONE LDAP GROUP ALLOW UPDATE=n CONFIG KEYSTONE LDAP GROUP ALLOW DELETE=n CONFIG KEYSTONE LDAP GROUP ADDITIONAL_ATTRIBUTE MAPPING= CONFIG KEYSTONE LDAP USE TLS=n CONFIG KEYSTONE LDAP TLS CACERTDIR= CONFIG KEYSTONE LDAP TLS CACERTFILE= CONFIG KEYSTONE LDAP TLS REQ CERT=demand CONFIG GLANCE DB PW=intel CONFIG GLANCE KS PW=intel CONFIG GLANCE BACKEND=file CONFIG CINDER DB PW=intel CONFIG CINDER KS PW=intel CONFIG CINDER BACKEND=lvm CONFIG CINDER VOLUMES CREATE=y CONFIG CINDER VOLUMES SIZE=20G CONFIG CINDER GLUSTER MOUNTS= CONFIG CINDER NFS MOUNTS= CONFIG CINDER NETAPP LOGIN= CONFIG CINDER NETAPP PASSWORD= CONFIG_CINDER_NETAPP_HOSTNAME= CONFIG CINDER NETAPP SERVER PORT=80 CONFIG CINDER NETAPP STORAGE FAMILY=ontap_cluster CONFIG CINDER NETAPP TRANSPORT TYPE=http CONFIG CINDER_NETAPP_STORAGE_ PROTOCOL=nfs CONFIG CINDER NETAPP SIZE

MULTIPLIER=1.0 CONFIG CINDER NETAPP EXPIRY THRES MINUTES=720 CONFIG CINDER NETAPP THRES AVL SIZE PERC_START=20 CONFIG CINDER NETAPP THRES AVL SIZE PERC_STOP=60 CONFIG CINDER NETAPP NFS SHARES= CONFIG CINDER NETAPP NFS SHARES CONFIG=/ etc/cinder/shares.conf CONFIG CINDER NETAPP VOLUME LIST= CONFIG CINDER NETAPP VFILER= CONFIG CINDER NETAPP PARTNER BACKEND NAME= CONFIG CINDER NETAPP VSERVER= CONFIG CINDER NETAPP CONTROLLER IPS= CONFIG CINDER NETAPP SA PASSWORD= CONFIG CINDER NETAPP ESERIES HOST TYPE=linux_dm_mp CONFIG CINDER NETAPP WEBSERVICE PATH=/devmgr/v2 CONFIG CINDER NETAPP STORAGE POOLS= CONFIG_MANILA_DB_PW=intel CONFIG_MANILA_KS_PW=intel CONFIG MANILA BACKEND=generic CONFIG MANILA NETAPP DRV HANDLES SHARE SERVERS=false CONFIG MANILA NETAPP TRANSPORT TYPE=https CONFIG MANILA NETAPP LOGIN=admin CONFIG MANILA NETAPP PASSWORD= CONFIG MANILA NETAPP SERVER HOSTNAME= CONFIG MANILA NETAPP STORAGE FAMILY=ontap_cluster CONFIG MANILA NETAPP SERVER PORT=443 CONFIG MANILA NETAPP AGGREGATE NAME SEARCH PATTERN=(.*) CONFIG_MANILA_NETAPP_ROOT_VOLUME_ AGGREGATE= CONFIG MANILA NETAPP ROOT VOLUME NAME=root CONFIG MANILA NETAPP VSERVER= CONFIG MANILA GENERIC DRV HANDLES SHARE SERVERS=true CONFIG MANILA GENERIC VOLUME NAME TEMPLATE=manila-share-%s CONFIG MANILA GENERIC SHARE MOUNT PATH=/shares CONFIG MANILA SERVICE IMAGE LOCATION=https://www.dropbox.com/s/ vi5oeh10q1qkckh/ubuntu 1204 nfs cifs. acow2 CONFIG MANILA SERVICE INSTANCE USER=ubuntu CONFIG MANILA SERVICE INSTANCE PASSWORD= CONFIG_MANILA_NETWORK_TYPE=neutron CONFIG_MANILA_NETWORK_STANDALONE GATEWAY= CONFIG_MANILA_NETWORK_STANDALONE_ NETMASK= CONFIG_MANILA_NETWORK_STANDALONE_ SEG ID=

CONFIG MANILA NETWORK STANDALONE IP RANGE= CONFIG MANILA NETWORK STANDALONE IP VERSION=4 CONFIG IRONIC DB PW=intel CONFIG IRONIC KS PW=intel CONFIG NOVA DB PW=intel CONFIG NOVA KS PW=intel CONFIG NOVA SCHED CPU ALLOC RATIO=16.0 CONFIG NOVA_SCHED_RAM_ALLOC_ RATIO=1.5 CONFIG NOVA COMPUTE MIGRATE PROTOCOL=tcp CONFIG NOVA COMPUTE MANAGER=nova. compute.manager.ComputeManager CONFIG VNC SSL CERT= CONFIG VNC SSL KEY= CONFIG NOVA COMPUTE PRIVIF=ens20f1 CONFIG NOVA NETWORK MANAGER=nova. network.manager.FlatDHCPManager CONFIG NOVA NETWORK PUBIF=ens20f0 CONFIG_NOVA_NETWORK_PRIVIF=ens20f1 CONFIG_NOVA_NETWORK_ FIXEDRANGE=192.168.32.0/22 CONFIG NOVA NETWORK FLOATRANGE=10.3.4.0/22 CONFIG NOVA NETWORK AUTOASSIGNFLOATINGIP=n CONFIG NOVA NETWORK VLAN START=100 CONFIG NOVA NETWORK NUMBER=1 CONFIG NOVA NETWORK SIZE=255 CONFIG NEUTRON KS PW=intel CONFIG NEUTRON DB PW=intel CONFIG NEUTRON L3 EXT BRIDGE= CONFIG NEUTRON METADATA PW=intel CONFIG LBAAS INSTALL=n CONFIG NEUTRON METERING AGENT INSTALL=n CONFIG NEUTRON FWAAS=n CONFIG NEUTRON ML2 TYPE DRIVERS=vxlan CONFIG NEUTRON ML2 TENANT NETWORK TYPES=vxlan CONFIG NEUTRON ML2 MECHANISM DRIVERS=openvswitch CONFIG NEUTRON ML2 FLAT NETWORKS=* CONFIG NEUTRON ML2 VLAN RANGES=physnet1,physnet2 CONFIG NEUTRON ML2 TUNNEL ID RANGES= CONFIG NEUTRON ML2 VXLAN GROUP=239.1.1.100 CONFIG NEUTRON ML2 VNI RANGES=1001:2000 CONFIG_NEUTRON_L2_AGENT=openvswitch CONFIG NEUTRON LB INTERFACE MAPPINGS= CONFIG_NEUTRON_OVS_BRIDGE_MAPPINGS= CONFIG_NEUTRON_OVS_BRIDGE IFACES= CONFIG NEUTRON OVS TUNNEL IF= CONFIG NEUTRON OVS VXLAN UDP PORT=4789 CONFIG HORIZON SSL=n

CONFIG HORIZON SECRET KEY=dd5a2abbce f747f7a7bafede42947d71 CONFIG HORIZON SSL CERT= CONFIG HORIZON SSL KEY= CONFIG HORIZON SSL CACERT= CONFIG_SWIFT_KS_PW=intel CONFIG SWIFT STORAGES= CONFIG SWIFT STORAGE ZONES=1 CONFIG SWIFT STORAGE REPLICAS=1 CONFIG SWIFT STORAGE FSTYPE=ext4 CONFIG SWIFT HASH=c2a8ece9563b4666 CONFIG SWIFT STORAGE SIZE=2G CONFIG HEAT DB PW=intel CONFIG HEAT AUTH ENC KEY=eb12297f095c4958 CONFIG_HEAT_KS_PW=intel CONFIG_HEAT_CLOUDWATCH_INSTALL=n CONFIG_HEAT_CFN_INSTALL=n CONFIG HEAT DOMAIN=heat CONFIG_HEAT_DOMAIN_ADMIN=heat_admin CONFIG HEAT DOMAIN PASSWORD=<set your password> CONFIG PROVISION DEMO=n CONFIG PROVISION TEMPEST=n CONFIG PROVISION DEMO FLOATRANGE=172.24.4.224/28 CONFIG PROVISION IMAGE NAME=cirros CONFIG PROVISION IMAGE URL=http:// download.cirros-cloud.net/0.3.3/cirros-0.3.3-x86_64-disk.img CONFIG PROVISION IMAGE FORMAT=qcow2 CONFIG PROVISION_IMAGE_SSH_ USER=cirros CONFIG_PROVISION_TEMPEST_USER= CONFIG PROVISION TEMPEST USER PW=intel CONFIG PROVISION TEMPEST FLOATRANGE=172.24.4.224/28 CONFIG PROVISION TEMPEST REPO URI=https://github.com/openstack/tempest. ait CONFIG PROVISION TEMPEST REPO REVISION=master CONFIG PROVISION ALL IN ONE OVS BRIDGE=n CONFIG CEILOMETER SECRET=54188c6a86154776 CONFIG CEILOMETER KS PW=intel CONFIG CEILOMETER COORDINATION BACKEND=redis CONFIG MONGODB HOST=10.250.101.10 CONFIG REDIS MASTER HOST=10.250.101.10 CONFIG REDIS PORT=6379 CONFIG REDIS HA=n CONFIG_REDIS_SLAVE_HOSTS= CONFIG REDIS SENTINEL HOSTS= CONFIG REDIS SENTINEL CONTACT HOST= CONFIG REDIS SENTINEL PORT=26379 CONFIG REDIS SENTINEL QUORUM=2 CONFIG REDIS MASTER NAME=mymaster CONFIG SAHARA DB PW=intel CONFIG SAHARA KS PW=intel CONFIG_TROVE_DB_PW=intel

CONFIG_TROVE_KS_PW=intel	
CONFIG_TROVE_NOVA_USER=trove	
CONFIG_TROVE_NOVA_TENANT=servic	es
CONFIG_TROVE_NOVA_PW=intel	
CONFIG_NAGIOS_PW=intel	

Appendix B: Updating the vIPS Sensor Image (Upgrade Version)

- 1. Log in to the OSC dashboard.
- 2. On the menu, select Setup, Service Function Catalog.
- 3. Click Auto Import.
- 4. Select the zip file with the new vIPS sensor.
- 5. Click OK.
- 6. On the menu, select Setup, Distributed Appliance.
- 7. Select the current distributed appliance.
- 8. Click Edit.
- 9. On the menu Service Function Definition, select the new sensor.

Vame *						
Manager C	onnector*					
ervice Fun	ction Definition *	IPS-V	/M100-VSS-8.1.	7.37		
Virtualiza	tion System:	IPS-	VM100-VS5-8.1 VM100-VS5-8.1	7.37 7.27		
Enabled	Virtualization Conn	ector	Туре	Manager Domain	Encapsulation Ty	pe
-	Cerner-OpenStack		OPENSTACK	/Wy Company 🚽 😔	VLAN	

- 10. Click OK.
- 11. Wait until the job is complete.
- 12. Check whether vIPS has a new image in the OpenStack dashboard.

Appendix C: References

NAME	REFERENCE
Elasticsearch (v1.7.3)	https://www.elastic.co/guide/en/elasticsearch/reference/1.7/setup-repositories.html
F5 BIG-IP	https://www.f5.com/pdf/products/big-ip-local-traffic-manager-ds.pdf
Installing MidoNet for OSC	https://docs.google.com/a/intel.com/document/d/107nBgYS9dFd3qqLDAKdNMC_ pVsBko5zQqGcJrctqQuM/edit?usp=sharing_eid
Open Security Controller	http://www.intel.com/content/dam/www/public/us/en/documents/datasheets/open- security-controller-datasheet.pdf
Logstash (v1.5.4)	https://www.elastic.co/guide/en/logstash/1.5/package-repositories.html
McAfee® Network Security Manager	http://www.mcafee.com/sg/resources/data-sheets/ds-network-security-manager.pdf
McAfee® Network Security Platform virtual sensor	http://www.mcafee.com/us/resources/data-sheets/ds-virtual-network-security- platform.pdf
Midokura Enterprise Midonet	http://www.midokura.com/midonet-enterprise/
Midokura Enterprise MidoNet (MEM) Quick Start Guide for Red Hat Enterprse Linux 7 / Kilo	http://docs.midokura.com/docs/latest-en/quick-start-guide/rhel-7_kilo-osp/content/ index.html
Midokura page on GitHub*	https://github.com/midokura
Red Hat Enterprise Linux 7	https://www.redhat.com/en/resources/red-hat-enterprise-linux-server
Red Hat OpenStack Platform 7	https://access.redhat.com/documentation/en/red-hat-openstack- platform?version=7/

Appendix D: Abbreviations

ABBREVIATION	DESCRIPTION	ABBREVIATION	DESCRIPTION
ARP	Address Resolution Protocol	NSM	McAfee Network Security Manager
CLI	Command Line Interface	OSC	Open Security Controller
DNS	Domain Name System	RAM	Random Access Memory
GRE	Generic Routing Encapsulation	SDN	Software-Defined Networking
IDS	Intrusion Detection System	SHVS	Standard High Volume Servers
IP	Internet Protocol	UDP	User Datagram Protocol
IPS	Intrusion Prevention System	vIPS	Virtual IPS
JVM	Java Virtual Machine	VLAN	Virtual LAN
LAN	Local Area Network	VM	Virtual Machine
MAC	Medium Access Control	VxLAN	Virtual eXtensible LAN
NFV	Network Functions Virtualization		

Installation Guide | Security Solution Implementation Installation Guide



By using this document, in addition to any agreements you have with Intel, you accept the terms set forth below.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a nonexclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRIGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Intel technologies may require enabled hardware, specific software, or services activation. Check with your system manufacturer or retailer. Tests document performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. Consult other sources of information to evaluate performance as you consider your purchase. For more complete information about performance and benchmark results, visit http://www.intel.com/performance.

All products, computer systems, dates and figures specified are preliminary based on current expectations, and are subject to change without notice. Results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at intel.com, or from the OEM or retailer. No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Intel does not control or audit third-party websites, software, data or other information referenced in this document. You should contact such third parties to confirm whether the referenced data is accurate.

No endorsement, sponsorship by, or association between, Intel and any third parties is expressed nor should be inferred from references to third parties and their products and services in this document.

Intel Corporation may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights that relate to the presented subject matter. The furnishing of documents and other materials and information does not provide any license, express or implied, by estoppel or otherwise, to any such patents, trademarks, copyrights, or other intellectual property rights.

Intel, the Intel logo, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries. *Other names and brands may be claimed as the property of others. © 2016 Intel Corporation. 1216/MH/MESH/PDF 335218-001US