

# Deploying an R80.20 SMS in Azure and an R80.10 Cluster and testing failover

**Danko Causevic**  
**Security Engineer – Central Canada**  
**December 24, 2018**

## Table of Content

Deploying an R80.20 SMS in Azure and an R80.10 Cluster and testing failover .....	1
Module 1 - Deploying an R80.20 management server in Azure .....	2
Module 2 - Deploying an R80.10 IaaS Cluster .....	5
Module 3 - Creating cluster in dashboard and establishing SIC .....	8
Module 4 - Testing cluster failover .....	10

## Module 1 - Deploying an R80.20 management server in Azure

First we will deploy a management server in Azure, then the cluster which will be management by the SMS we created.

Once logged into Azure, go to “**Create a resource**” tab on the top left, type in “**Check Point Security Management**”

Name: DankoSMS (can use any you'd like)

Password:Checkpoint@123

Subscription: leave as is

Resource group: choose the first one if using the lab (or if it's a customer environment create a new recourse group)

Location: Canada Central (can choose any you'd like, same region must be used in the cluster deployment so remember which one you choose. Note that If you choose a different region then vnet peering must be performed)

The screenshot shows the 'Basics' configuration window for a Check Point Security Management server in Azure. The window has a title bar with 'Basics' and a close button. Below the title bar, there are several fields and options:

- Name:** DankoSMS (with a green checkmark)
- Authentication type:** Password (selected) and SSH public key (available)
- Password:** Masked with dots (with a green checkmark)
- Confirm password:** Masked with dots (with a green checkmark)
- Subscription:** Checkpoint HOL - B (dropdown menu)
- Resource group:** ODL-checkpointtemplate-46738-01 (dropdown menu) with a 'Create new' link below it.
- Location:** Canada Central (dropdown menu)

At the bottom of the window is a blue 'OK' button.

After hitting OK you will be taken to the page below.

CloudGuard Version:R80.20

License: BYOL

VM size: choose a small one or leave as is

Rest leave as is

Security Management set... □ ×

Check Point CloudGuard version ⓘ  
 R80.20 ▾


License type ⓘ  
 Bring Your Own License ▾

---

\* Virtual machine size ⓘ >  
 1x Standard D3 v2

---

\* Allowed GUI clients ⓘ  
 0.0.0.0/0

Bootstrap script ⓘ  
 Select a file 


Allow download from/upload to Check Point ⓘ  
 Yes  No

Additional disk space (GB) ⓘ

**OK**

After hitting OK you will be prompted to create a new Vnet. Choose your own vnet name and subnet. After hitting ok you will be taken to the summary page where you can review your setup. This is what I have used below.

## Summary

 Validation passed

Subscription	Checkpoint HOL - B
Resource group	ODL-checkpointtemplate-46738-01
Location	Canada Central
Server Name	DankoSMS
Password	*****

**Security Management settings**

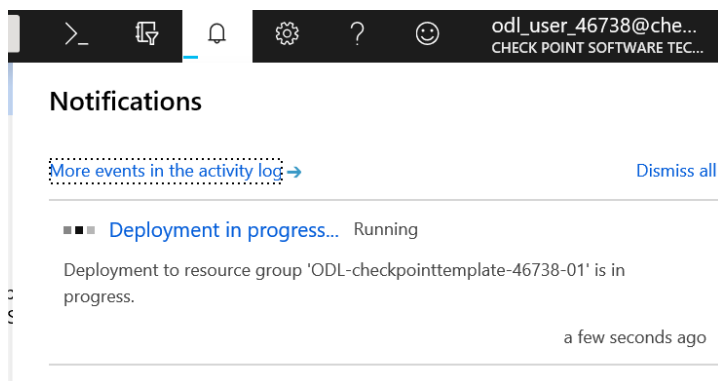
Check Point CloudGuard versi...	R80.20
License type	Bring Your Own License
Virtual machine size	Standard D3 v2
Allowed GUI clients	0.0.0.0/0
Bootstrap script	-
Allow download from/upload...	Yes
Additional disk space (GB)	0

**Network settings**

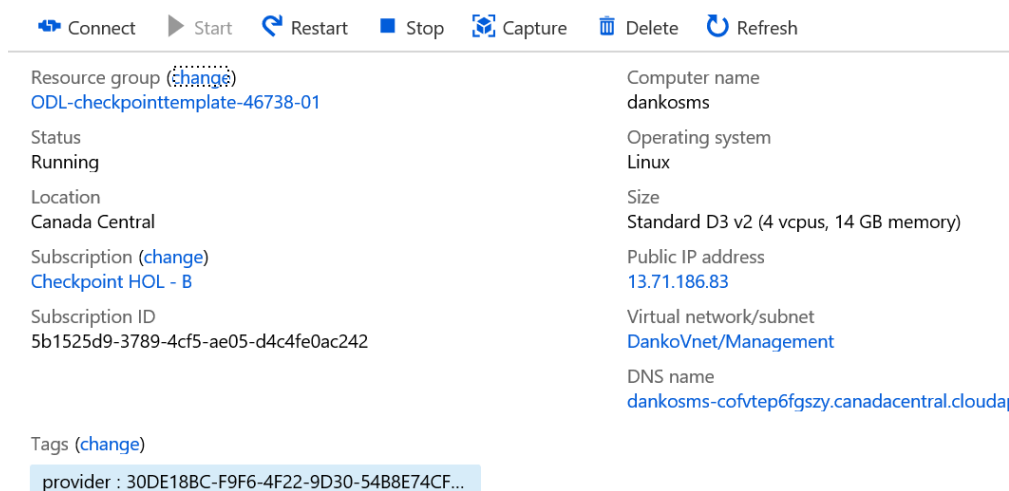
Virtual network	DankoVnet
Management subnet	Management
Management subnet address...	10.1.0.0/24

**OK** [Download template and parameters](#)

After clicking ok, you can click on **“Create”** which will spin up the VM in Azure. You can keep tabs on the progress of the VM creation in the notifications pane on the top right.



Once deployment is finished, go to “Virtual Machines” on the left pane, you will find your newly created SMS, we will click on this VM which will take you to the overview page. Make note of the Public IP (you will use this IP to connect to the VM), it is automatically created by Azure.



- Note that even though the VM creation is done (should be around 10 min) you still have to wait for the full setup to finish in the background), you will see a “system is being configured” message when you go to <https://<publicIP>> of the SMS.

Once setup is completed, make sure you can access the web GUI and the SMS using the public IP above, connect using the R80.20 Smart Console using the credentials created earlier (user:admin, pass:Checkpoint@123), make sure everything is up and running.

Login to the SMS using putty and make sure that you can ping 4.2.2.2 (NOTE: Ping is not a good test when you have an Azure Load balancer deployed, ping will not pass external to it) Once ping is successful we are ready now to create HA cluster and connect to it with the SMS.

## Module 2 - Deploying an R80.10 IaaS Cluster

Go to “Create a resource” in Azure and type in “Check Point CloudGuard IaaS Cluster”  
click on “Create” and enter the details as below.

Name: DankoCluster (can use any you’d like)

Password: Checkpoint@123

Subscription: leave as is

Resource group: Choose second on the list if using the lab or create new

Location: Canada Central, same as the one chosen for the SMS

Once done click OK

**Basics**

DankoCluster ✓

\* Authentication type  
Password SSH public key

\* Password ⓘ  
●●●●●●●●●● ✓

\* Confirm password  
●●●●●●●●●● ✓

Subscription  
Checkpoint HOL - B ▼

\* Resource group ⓘ  
ODL-checkpointtemplate-46738-02 ▼  
[Create new](#)

\* Location  
Canada Central ▼

Next enter the settings as below

License: BYOL  
SIC: Checkpoint123

Everything else leave as is.

### Cluster Object settings >

Check Point CloudGuard version ⓘ  
R80.10

License type ⓘ  
Bring Your Own License

---

\* Virtual machine size ⓘ >  
2x Standard D3 v2

---

\* SIC key ⓘ  
●●●●●●●●●● ✓


Create a System Assigned Identity ⓘ

Bootstrap script ⓘ

Allow download from/upload to Check Point ⓘ

After clicking ok you will need to create a new Vnet to be used for your cluster. Choose a unique Vnet (I chose 10.2.0.0/16) and then create the subnets (Azure will automatically create the /24 front and backend subnets that are a part of your /16 network). Click ok, the validation process will start. Once completed click on "Create" and the deployment will start. Once again, this should take some time to complete.

## Summary

 Validation passed

Location	Canada Central
Cluster Name	DankoCluster
Password	*****
<b>Cluster settings</b>	
Check Point CloudGuard versi...	R80.10
License type	Bring Your Own License
Virtual machine size	Standard B2ms
SIC key	*****
Bootstrap script	-
Allow download from/upload...	Yes
Additional disk space (GB)	0
<b>Network settings</b>	
Virtual network	DankoClusterVnet
Frontend subnet	Frontend
Frontend subnet address prefix	10.2.0.0/24
Backend subnet	Backend
Backend subnet address prefix	10.2.1.0/24

Once the deployment has been completed, log into each cluster member to the public IP (go to Virtual Machine tab as mentioned earlier to get these). Make sure you can ping out to 4.2.2.2.

## Module 3 - Creating cluster in dashboard and establishing SIC

We are now ready to create the new cluster object in smart dashboard and establish SIC to it from your management server that was created earlier.

Follow the steps below, I will be using the names that I created earlier, please substitute them with whatever you used.

1. Open up the R80.20 SmartConsole and connect to the public IP of your Management server.

2. Create a new Cluster object with the following details

- Name Danko-Cluster
- Cluster IP public address

*You can find the cluster IP address in the Azure portal when you select the resource group then click on DankoCluster Type - Public IP address (automatically created by Azure).*

3. Add each the two members to the Cluster. Use the Public IP for each of the objects. The SIC key used was **Checkpoint123**

4. Update the Cluster Topology as follows (if the interfaces are not pulled down, click on Network Management – Get interfaces with topology).

- Eth0 – Cluster + Sync

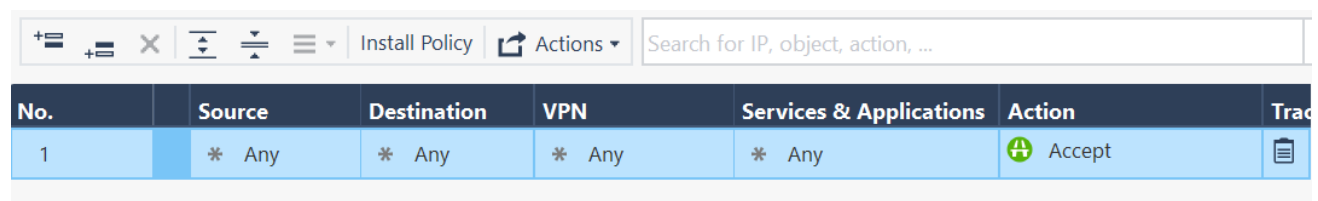
*The Private VIP address is: 10.X.X.6. (in my case its 10.2.0.6 as 10.2.0.0/24 is my front end subnet) Note - You can find the cluster private VIP address in the Azure portal when you select the Active member primary NIC > IP configuration > cluster-vip*

- Disable Anti-Spoofing

- Eth1 Sync

- Disable Anti-Spoofing

Once completed and SIC has been successfully established, we need to change the base rule to accept all traffic.



The screenshot shows the SmartConsole interface with a search bar at the top and a table of policy rules. The table has columns for No., Source, Destination, VPN, Services & Applications, Action, and Track. The first row shows a rule with source and destination set to '\* Any', VPN set to '\* Any', Services & Applications set to '\* Any', and Action set to 'Accept'.

No.	Source	Destination	VPN	Services & Applications	Action	Track
1	* Any	* Any	* Any	* Any	Accept	

Publish all changes and install the policy.

Log in to each of the members and check the HA state by typing:

```
cphaprob state
```



cphaprob -a if

```
[Expert@dankocluster1:0]# cphaprob stat
Cluster Mode:   High Availability (Active Up) with IGMP Membership

Number        Unique Address  Assigned Load   State
-----
1 (local)     10.2.0.4        0%              Standby
2             10.2.0.5        100%            Active

Local member is in current state since Mon Dec 24 18:44:06 2018

[Expert@dankocluster1:0]# cphaprob -a if

Required interfaces: 2
Required secured interfaces: 2

eth0          UP                sync(secured), unicast
eth1          UP                sync(secured), unicast

Virtual cluster interfaces: 1
eth0          10.2.0.6
```

## Module 4 - Testing cluster failover

Now if your cluster is in active/standby state you are ready to test the failover. We will be doing this by manually shutting down one of the members, alternatively the failover should happen automatically if one of the members interfaces goes down, there is an internal issue or whatever fault causes a failover.

I will be logging into cluster2 since it's currently in the "active" state and manually shutting down the clusterXL using the command:

clusterXL\_admin down (state can be brought up with the command clusterXL\_admin up)

```
Number      Unique Address  Assigned Load  State
1           10.2.0.4        0%             Standby
2 (local)   10.2.0.5        100%           Active

Local member is in current state since Mon Dec 24 18:43:57 2018

[Expert@dankocluster2:0]# clusterXL_admin down
Setting member to administratively down state ...
Member current state is Down
[Expert@dankocluster2:0]# █
```

```
[Expert@dankocluster1:0]# cphaprob stat

Cluster Mode:   High Availability (Active Up) with IGMP Membership

Number      Unique Address  Assigned Load  State
1 (local)   10.2.0.4        100%           Active
2           10.2.0.5        0%             Down

Local member is in current state since Mon Dec 24 18:58:46 2018
```

The failover was successful and only took about 1-2 seconds.

**Note:** The actual traffic failover might take up to 5 min in Azure for the internal traffic to route over to the new active cluster member (this is for the cluster deployment option), this is because there is no load balancer in place and the API calls need to install the new routes to the active member. In the High Availability IaaS Cluster deployment, this issue is solved as the load balancers are automatically deployed by Azure and traffic is failed over in seconds as the load balancer always keeps track of state and moves the routing over to the new member.