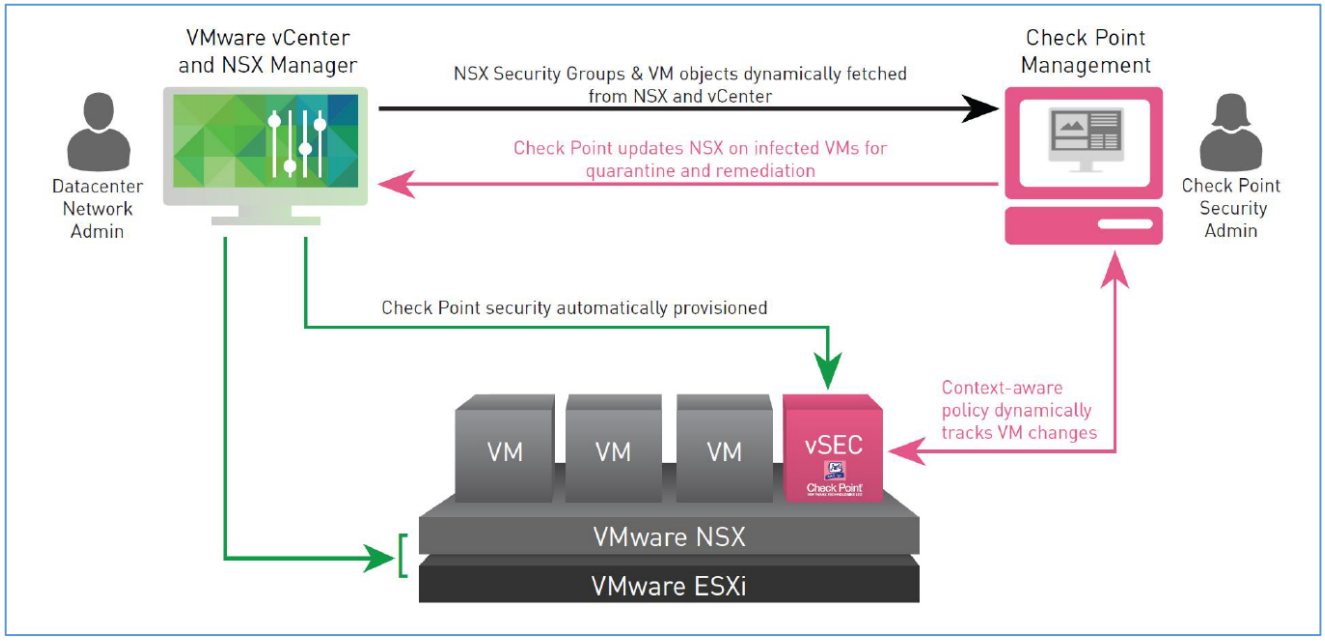
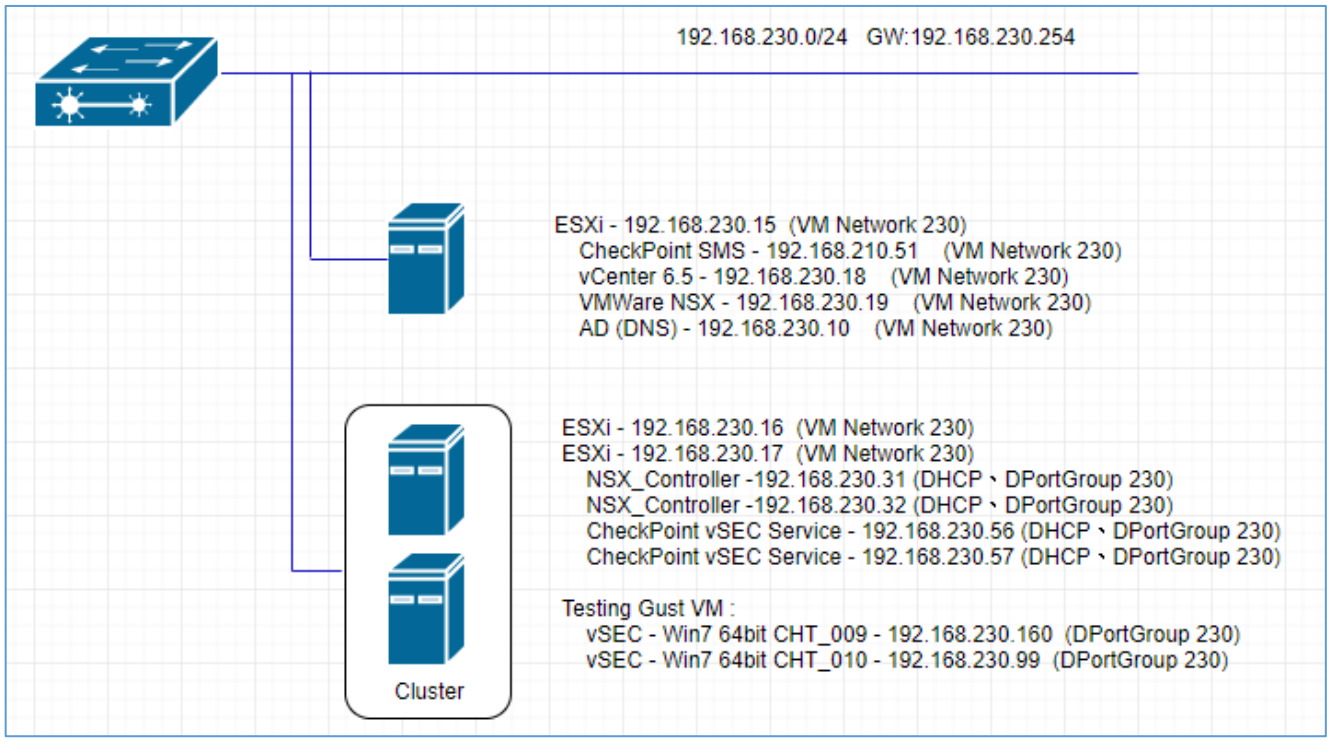
目錄：

一、 架構圖 & Lab 架設步驟：.....2
二、 Enviroment and Prepare：.....3
三、 Depoly one AD Server。.....3
四、 安裝 vCenter 6.5 版本：.....4
略.....4
五、 建立 Datacenter、Cluster、virtual Distributed Switch。.....4
略.....4
六、 Deploy one NSX Manager。.....4
七、 CheckPoint：.....11
八、 設定 vCenter 新增 Service。.....14
九、 Configuring NSX redirect traffic to the Security Gateway Virual Edition：.....18
十、 驗證：.....23

一、架構圖 & Lab 架設步驟：





LAB 架設流程：

1. 準備 AD Windows2012 並設定好各主機 DSN 解析。
2. 安裝設定兩台 ESXi 5.5 版本以上。
3. 安裝設定 vCenter 6.5 版本。
4. vCenter 納管兩台 ESXi。
5. 設定 Distribution Switch。
6. 設定 iSCSI Storage 主機，並設定 vCenter 的兩台 ESXI 共用 iSCSI Storage。
7. 安裝設定 NSX 6.3 版本，整合 vCenter & NSX。
8. 發布 NSX Controller、設定 NSX Host Preparation、Logical Network Preparation。
9. 安裝 CHP SMS，install 最新 jumbo hotfix、Check_Point_R80.10_vSEC_Service_Hotfix4_FULL。
10. 啟動 vsec。

11. 連線 SmartConsole 新增 DataCenter 物件 – vCenter、NSX。
12. 透過 ssh 連到 SMS 設定 vsec_config 的 nsx 參數，在 vCenter 設定 NSX 的 Service Deploymemts。
13. 等待 vSEC Service deployment(vSEC Firewall)佈署完成，登入 SMS 調整 Cluster 物件。
14. 修改 policy 後 install policy。
15. 回到 vCenter 設定 Service Composer。
16. 打開 Client 測試連線。

二、Enviroment and Prepare：

1. AD Windows 2012。
2. VMWare vCenter (version 6.5.0.12000 Appliance)。
   File : VMware-VCSA-all-6.5.0-7119157.iso。
3. VMWare NSX Manager (version 6.3.5-7119875 Appliacne)。
   File : upgrae from 6.2.2 version , VMware-NSX-Manager-upgrade-bundle-6.3.5-7119875.tar.gz。
4. ESXi (version 5.5 u3) and 2 appliance with cluster。
5. CheckPoint SMS R80.10，Recommand RAM 16GB。
   File :
   (i) Check_Point_R80.10_T421_Gaia.iso。
   (ii) Check_Point_R80.10_vSEC_Service_Hotfix4_FULL.tgz。(vSEC patch)
   (iii) Check_Point_Security_Gateway_R77_30_vSEC_for_NSX_v4_OVF.tgz。(vSEC Firewall)

Network	VLAN	Network / Mask	Gateway	Related Network Interfaces
Management Network / vMotion Network / VXLAN Network	230	192.168.230.0/24	192.168.230.254	Mgmt Cluster Host Management Kernel / VC / NSX Manager / Controllers / VM or Physical Machines on Physical Network

Component	Hostname	IP Address	Gateway	Note
AD/DNS	ad.9fdemolab.com	192.168.230.10	192.168.230.254	
vCenter	vc65.9fdemolab.com	192.168.230.18	192.168.230.254	
NSX Manager IP	nsx.9fdemolab.com	192.168.230.19	192.168.230.254	
NSX Controller IP	-	192.168.230.31-40	192.168.230.254	
CheckPoint vSEC Service		192.168.230.56-60	192.168.230.254	
ChecPoint SMS		192.168.230.51	192.168.230.254	R80.10
ESXi-16	esxi-16.9fdemolab.com	192.168.230.16	192.168.230.254	
	esxi-17.9fdemolab.com	192.168.230.17	192.168.230.254	
ESXi		192.168.230.15	192.168.230.254	include AD、vCenter、NSX、CHP SMS

三、Depoly one AD Server。

略

四、安裝 vCenter 6.5 版本：

略

五、建立 Datacenter、Cluster、virtual Distributed Switch。

略

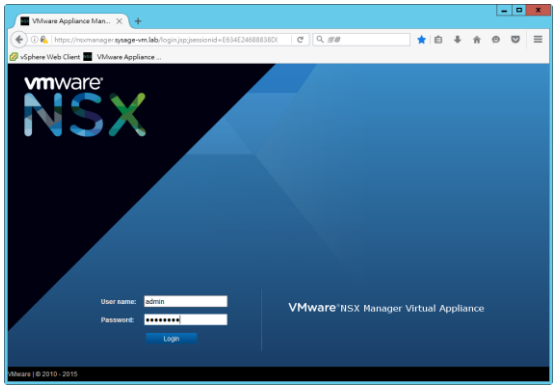
六、Deploy one NSX Manager。

1. NSX Deployment。

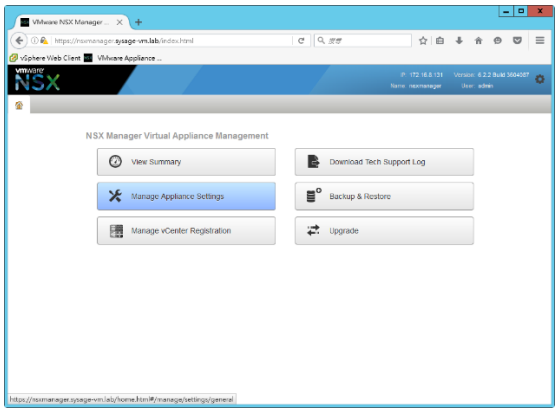
   略

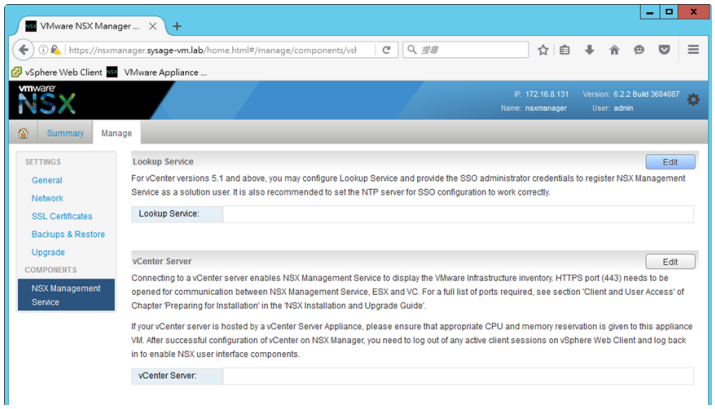
2. 設定 NSX Manager。

   a. 開啟瀏覽器 https://<NSX manager IP> or https://nsx.9fdemolab.com，帳號：admin，密碼：P@ssw0rd。

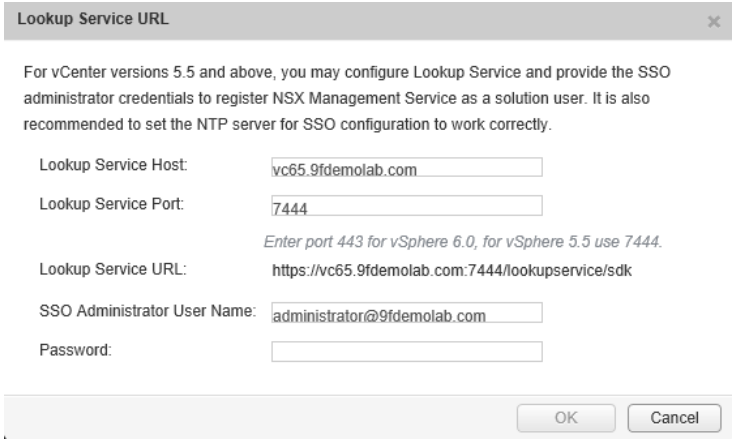


   b. 點擊『Manage Appliance Settings』，點選『NSX Management Service』，於 Lookup Service，點擊『Edit』。

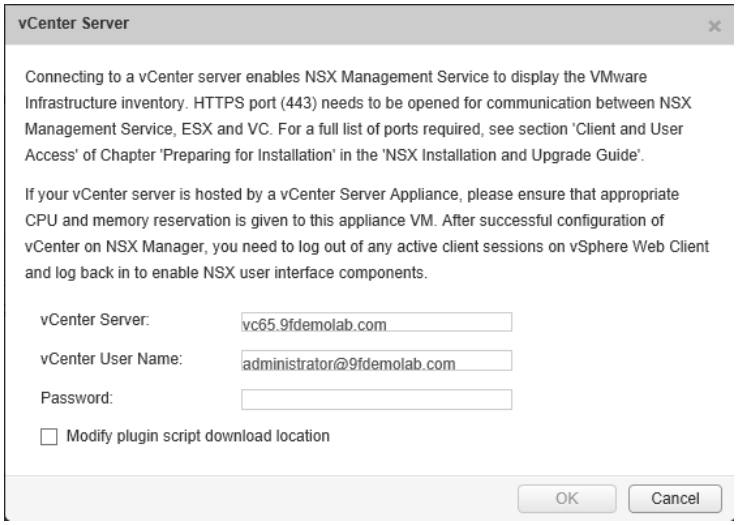




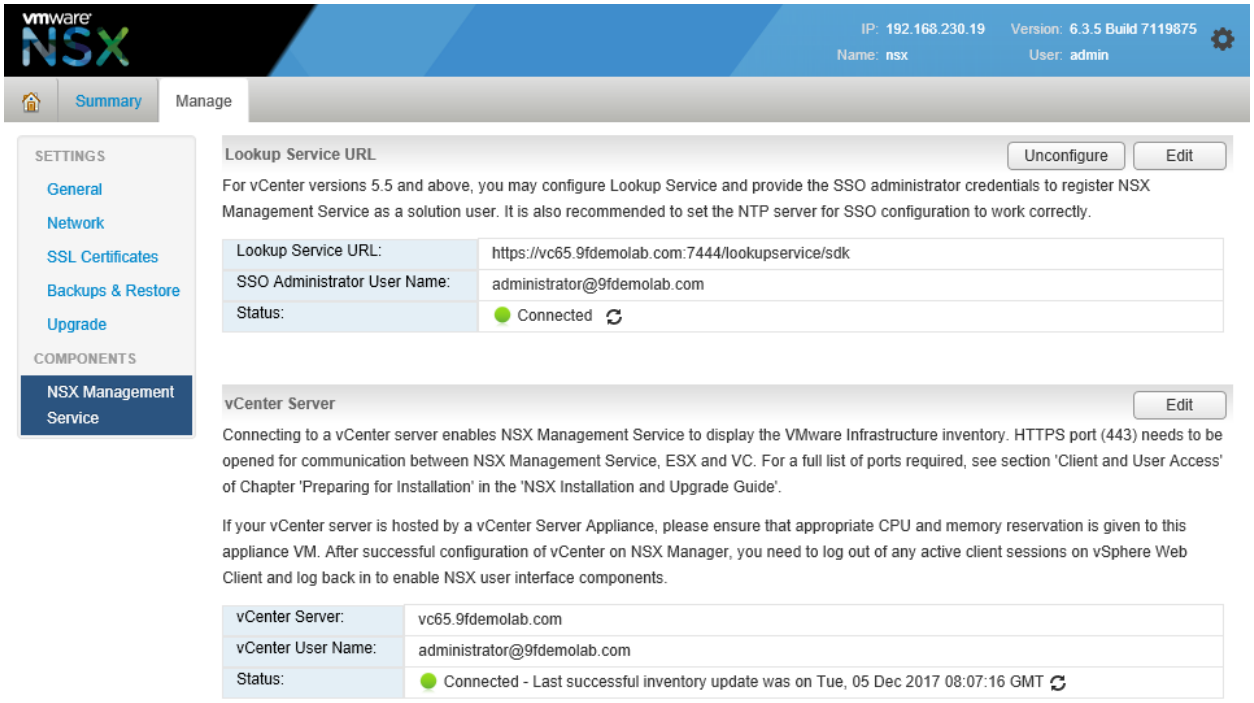
   c. NSX Manager 連結 vCenter PSC(SSO) : Lookup Service IP：192.168.230.18 or vc65.9fdemolab.com，Lookup Service Port：7444，帳號：administrator@9fdemolab.com，密碼：P@ssw0rd，點擊『Yes』。



d. Lookup Service 設定完成，於 vCenter Server 點擊『Edit』，NSX Manager 連結 vCenter Server : vCenter Server：192.168.230.18 or vc65.9fdemolab.com，vCenter User Name：administrator@9fdemolab.com，Password：P@ssw0rd，點擊『Yes』。

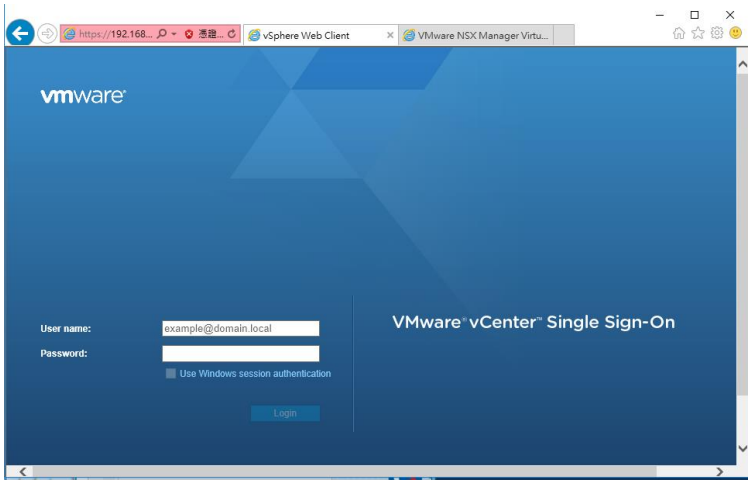


e. 設定完成。

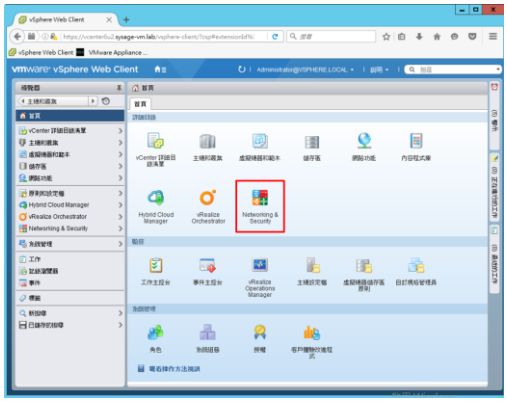


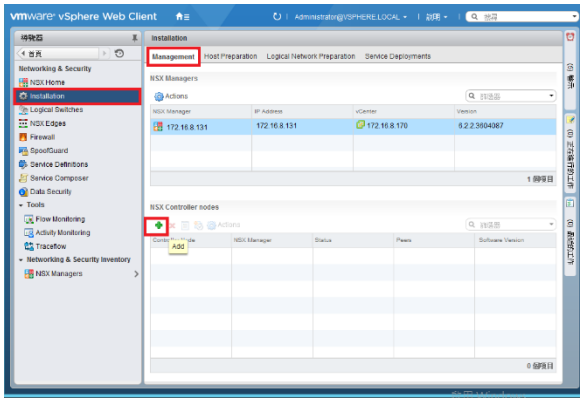
f. 匯入 NSX License。
從 Home > administration > Licensing > Licenses 中匯入。

3. 發佈 NSX Controller。
a. 採用 vSphere Web Client，登入 vCenter。https://vc65.9fdemolab.com/vsphere-client or https://192.168.230.18/vsphere-client，帳號：administrator@9fdemolab.com 密碼：P@ssw0rd。

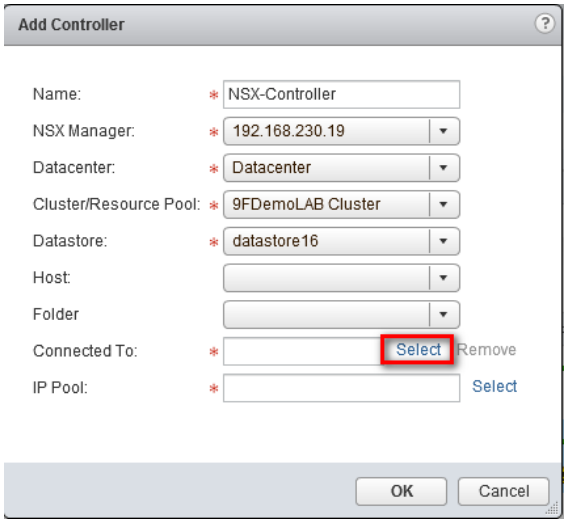


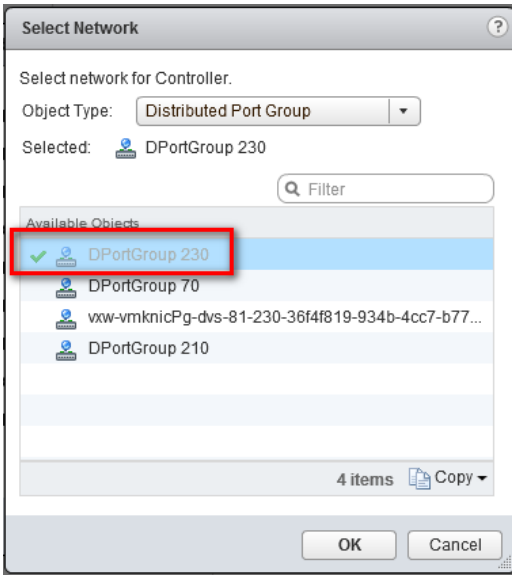
b. 點選『Networking & Security』，新增 Controller(將 Controller 部署在 Management Cluster 下的 ESXi)。



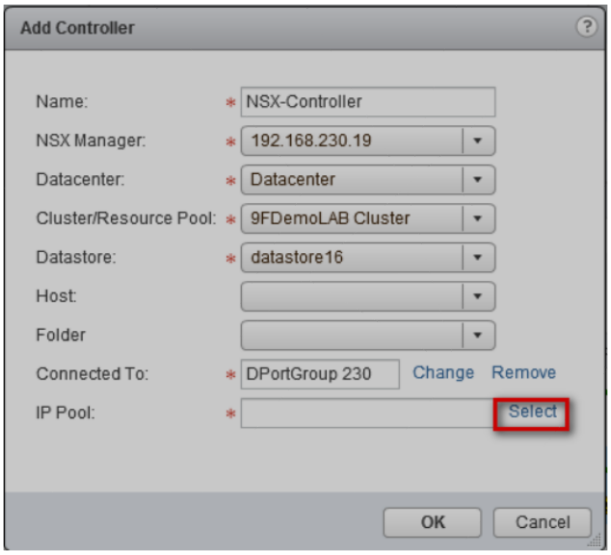


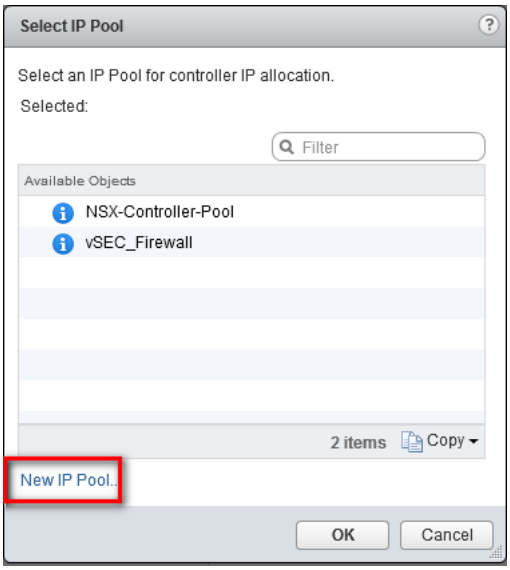
c. 選擇要部署的 ESXi，及其網路和 datastore，Connected To：點選 Select，點選 DPoortGroup230。



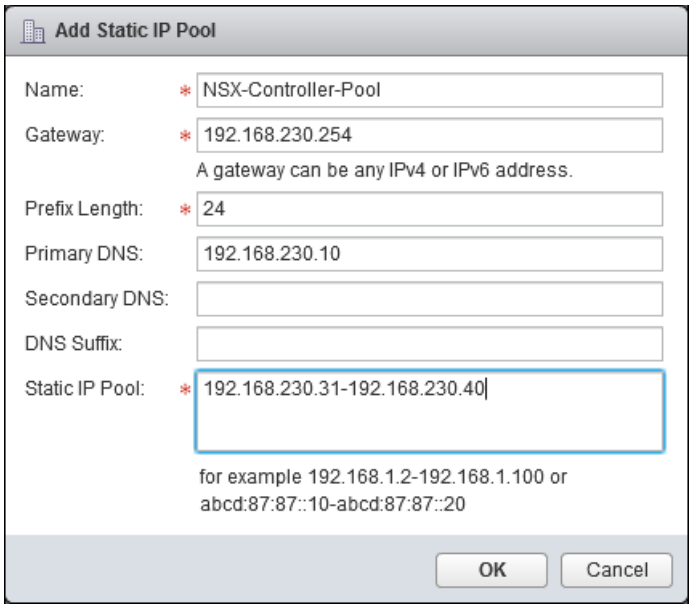


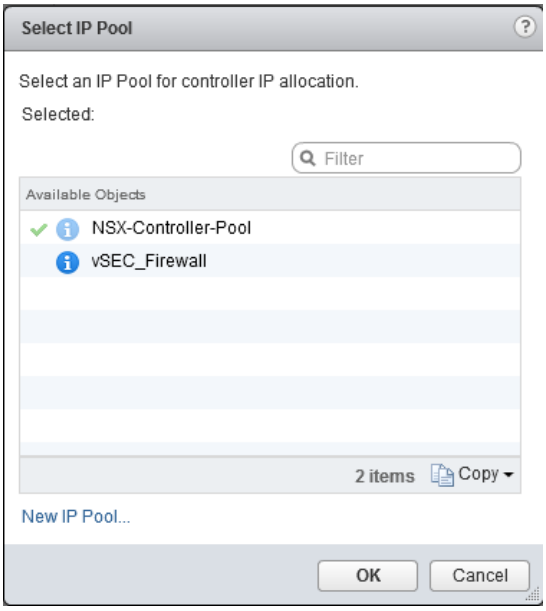
d. Connected To：Mgmt Management Network，IP Pool：點選 Select，新增 IP Pool 提供 Controller 所需 IP 位址範圍，點選 New IP Pool...。



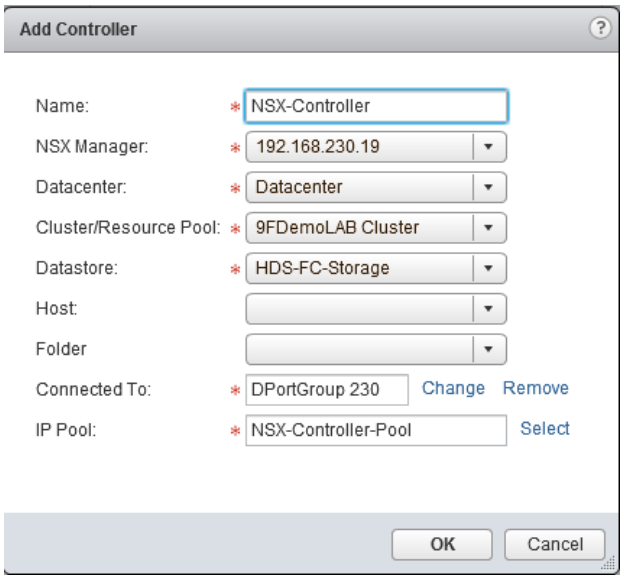


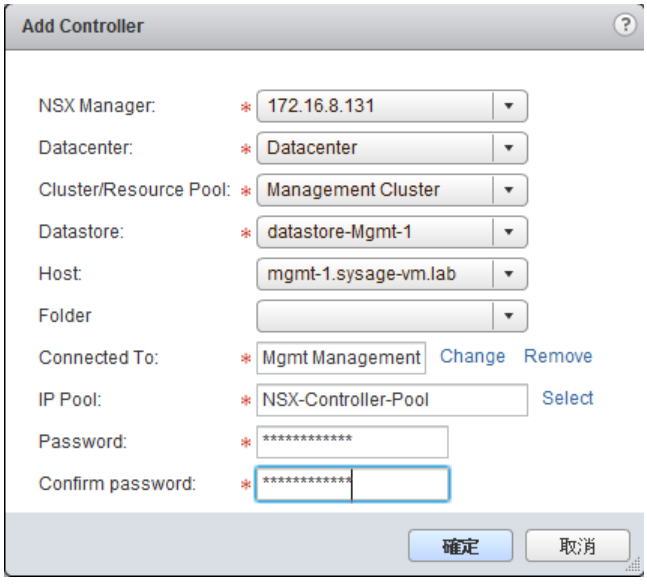
e. 新增 IP Pool 並輸入 Controller IP 資訊，點選該 IP Pool。



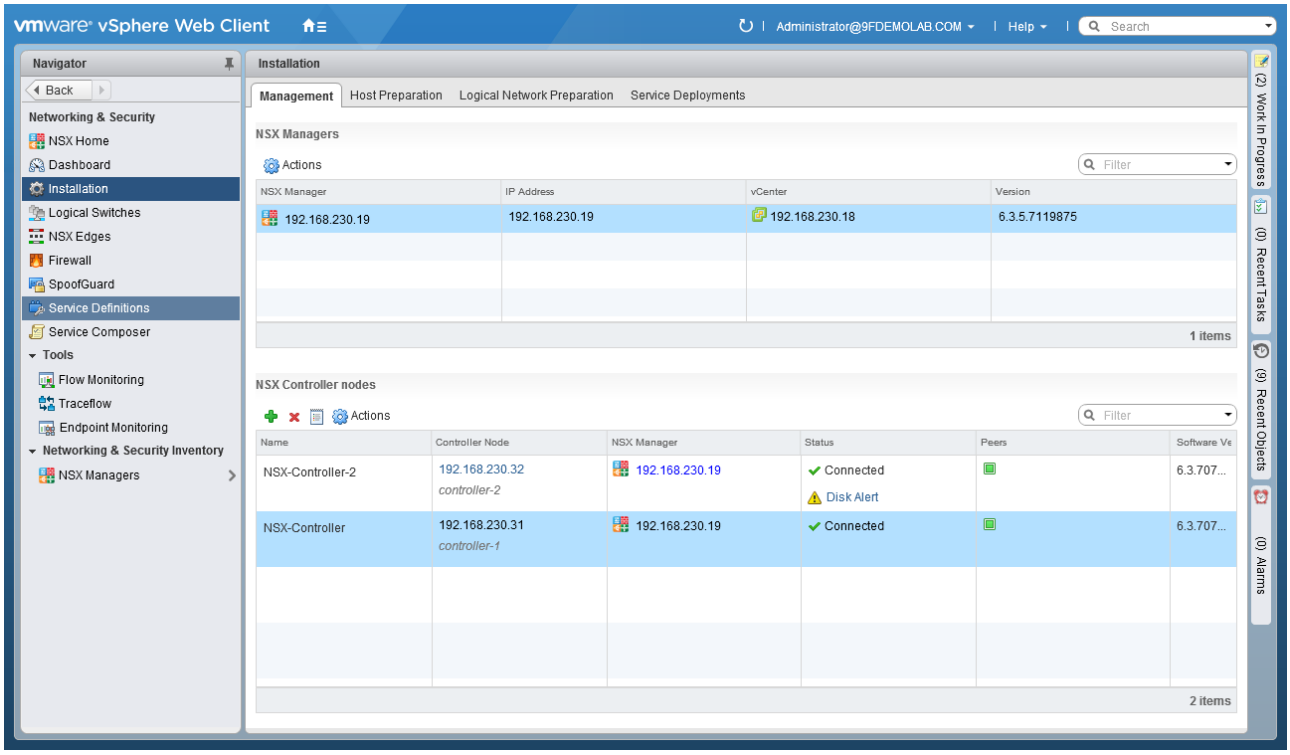


f. 密碼：PAssw0rd123!

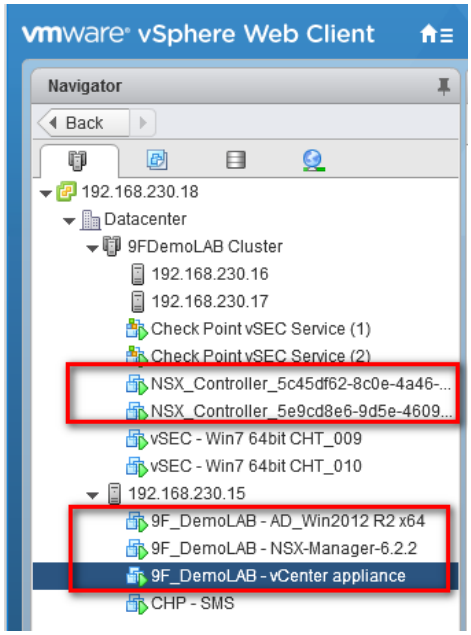




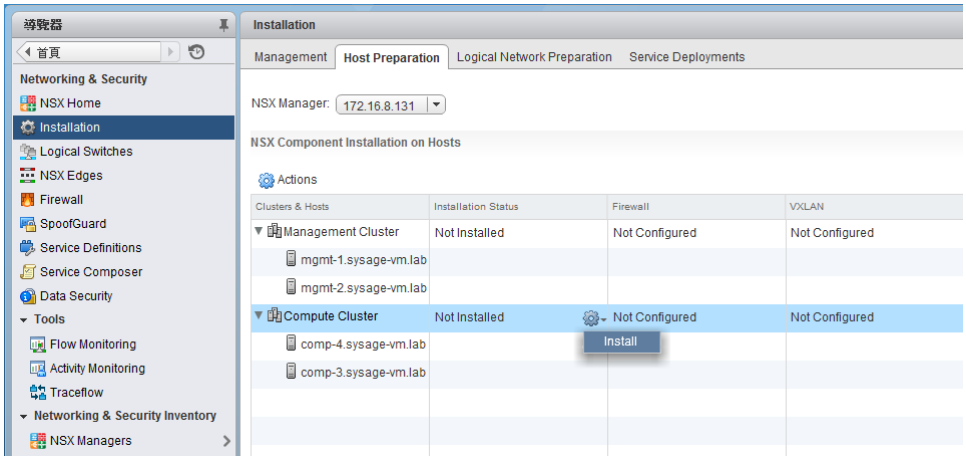
g. 依照 b ~ f 步驟建立第 2 個 NSX Controller。



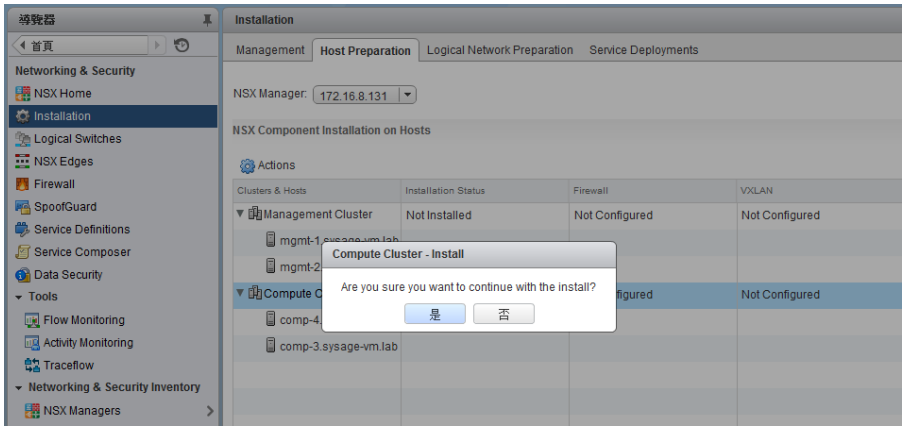
h. 安裝至此 vCenter 中會有 1 台 AD、1 台 vCenter、1 台 NSX Manager、2 台 NSX Controller。



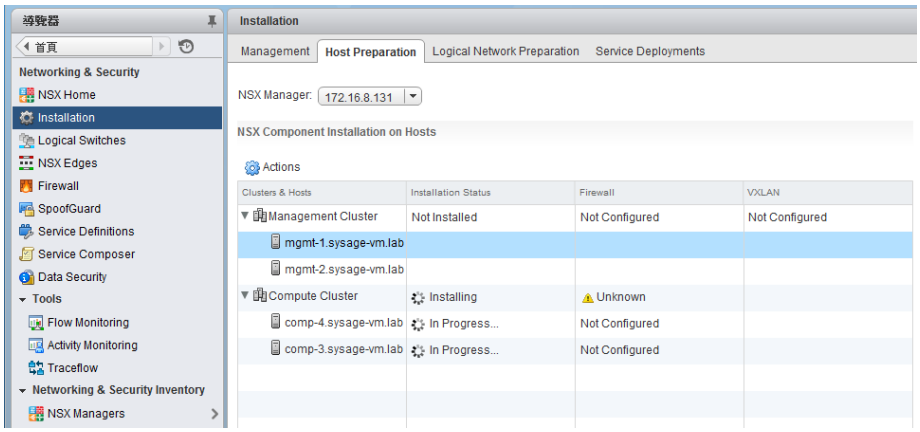
4. Host Preparation :
   a. 於 Cluster (9FDemoLAB Cluster) 中點擊安裝。備註：NSX Manger/vCenter/ESXi 間的名稱解析(正反解)及校時，都需正常。(此部分抓圖不是本次 LAB 的圖)(**NSX License 需先匯入**)

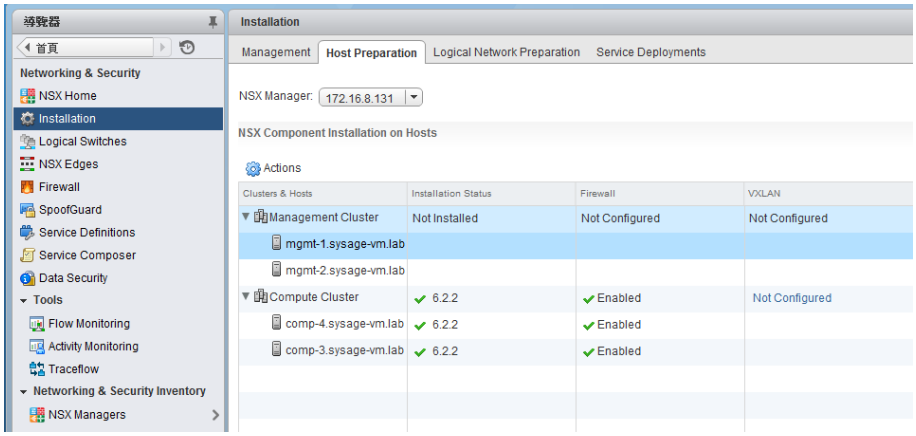


b. 點擊『是』。

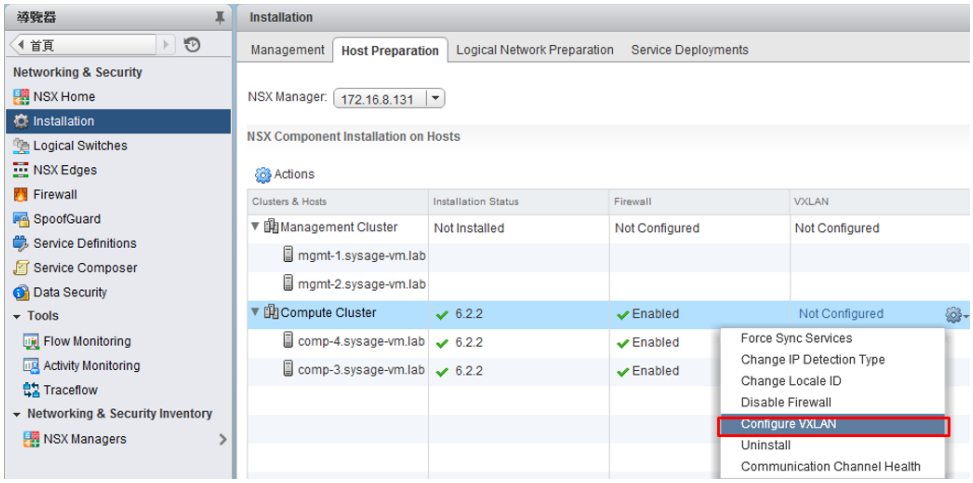


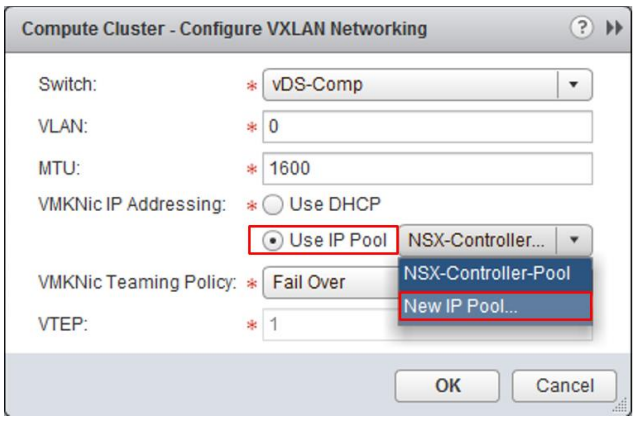
c. 等待安裝完成。





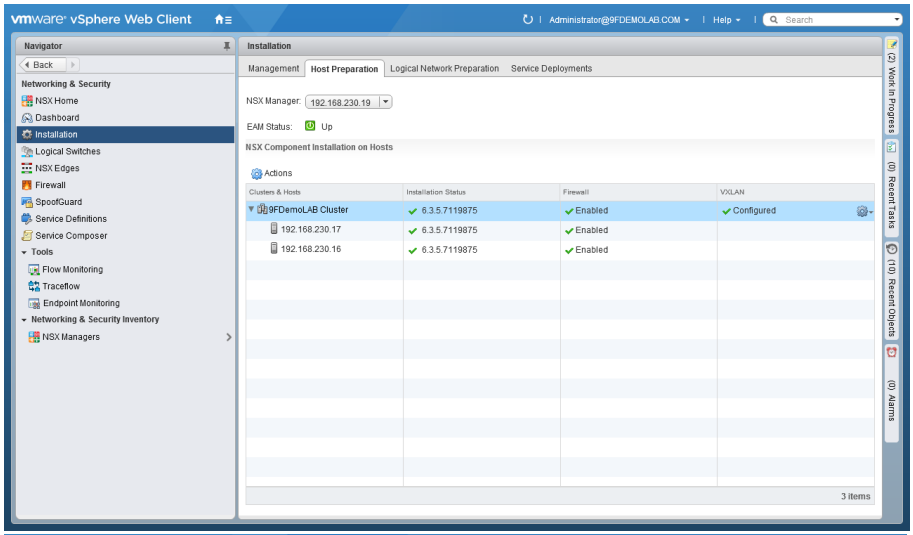
d. 點擊『Configure VXLAN』，點選 Use IP Pool，並點擊 New IP Pool，點擊 OK。

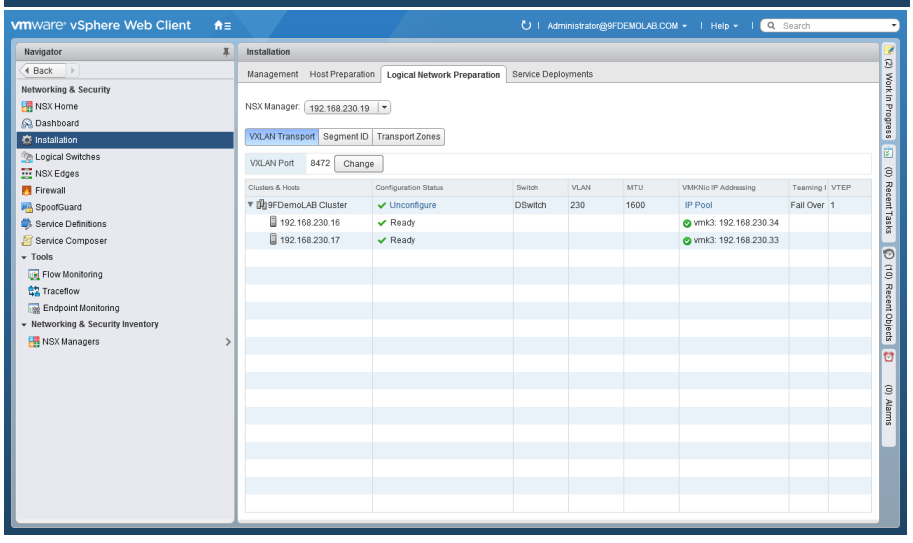




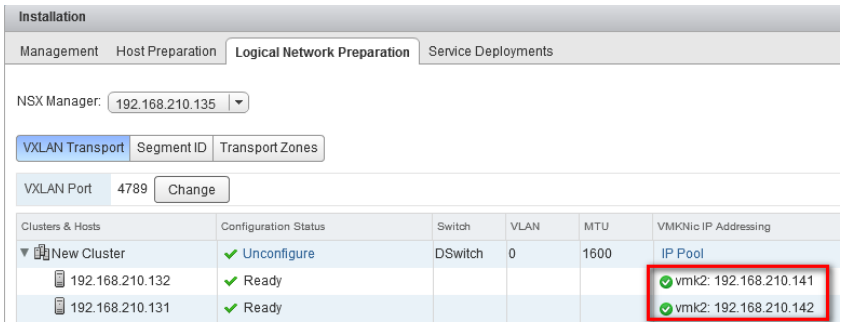
此部分我選擇前面步驟設定好的 NSX-Controller-Pool

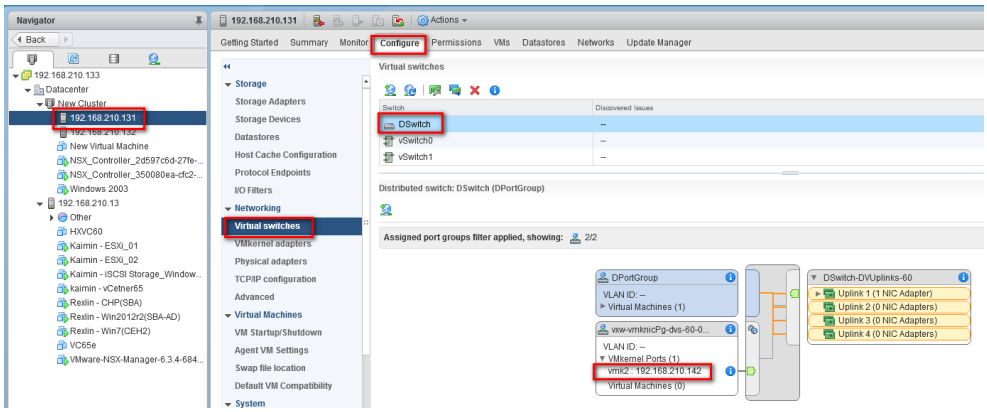
e. 完成。





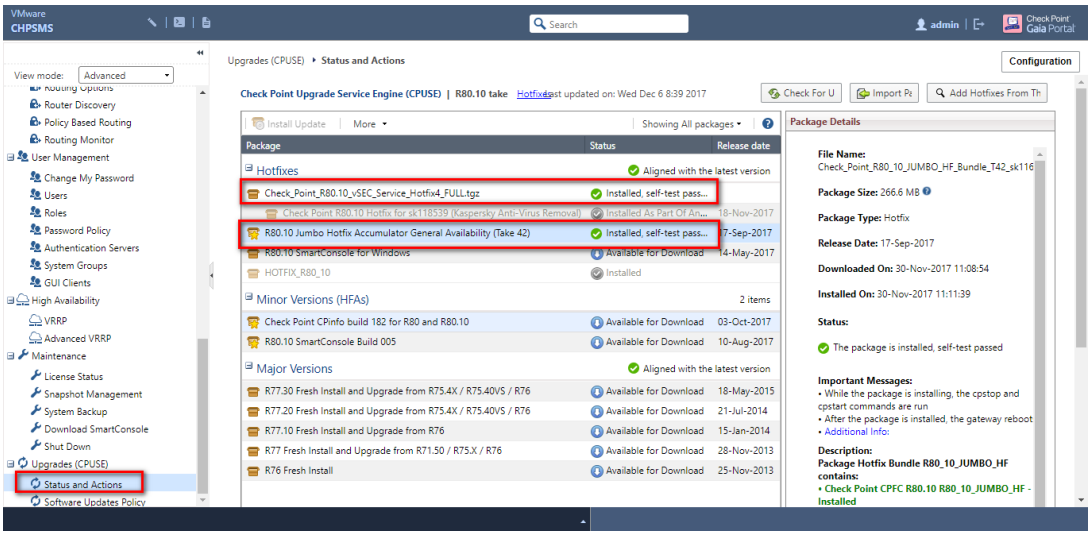
5. 設定 Logical Network Preparation：
   a. 切換到 Logical Network Preparation，可看到第 4 步驟設定的 VXLAN IP，此 VXLAN IP 其實是 VMKernl Port。



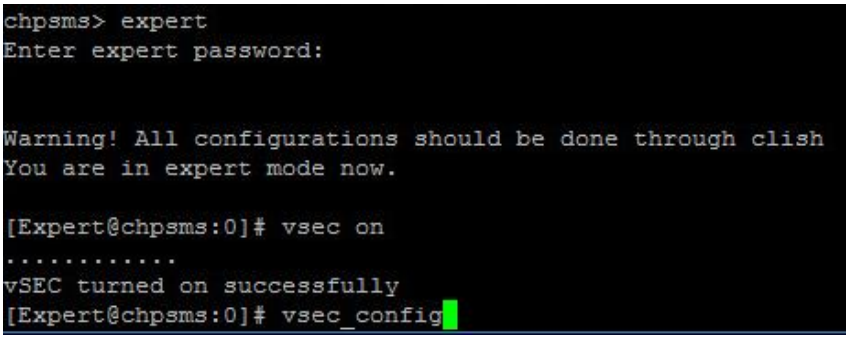


七、CheckPoint：

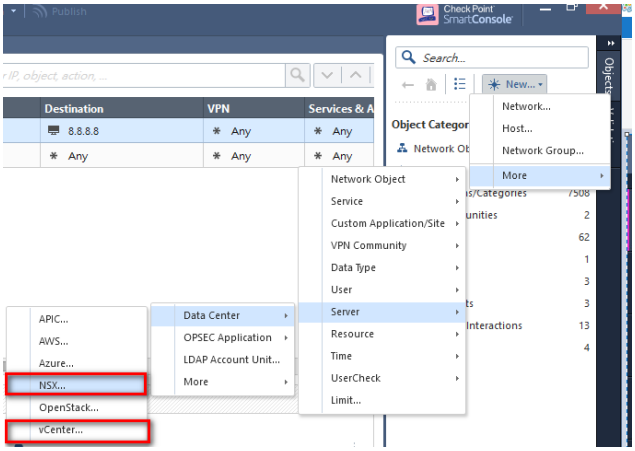
1. 登入 CHP SMS 的 WebUI(安裝省略)，透過 CPUSE 安裝最新的 jumbo hotfix 和 Check_Point_R80.10_vSEC_Service_Hotfix4_FULL.tgz。(**License & Contract 請先申請並匯入**)

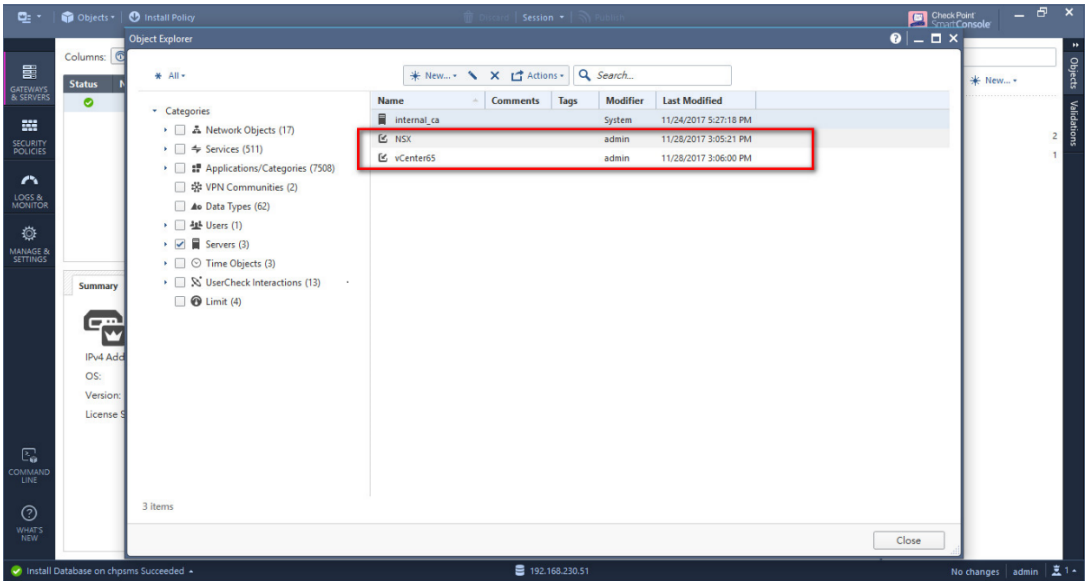


2. 使用 ssh 或 console 登入 SMS，並進入 expert mode，輸入指令 vsec on 啟動 vsec 功能。



3. 登入 CHP SMS 的 SmartConsole，新增物件 Data Center > NSX 和 vCenter。





4. 把檔案 Check_Point_Security_Gateway_R77_30_vSEC_for_NSX_v4_OVF.tgz 解壓縮後的所有檔案，傳送到 SMS 的$FWDIR/VE/jetty/ve 中。

```
[Expert@CHPSMS:0]# cd $FWDIR/VE/jetty/ve/
[Expert@CHPSMS:0]# pwd
/opt/CPsuite-R80/fw1/VE/jetty/ve
[Expert@CHPSMS:0]# ls -l
total 4127528
-rw-r----- 1 admin users 4222437888 Jun 29 22:35 Security_Gateway_R77_30VSEC-dis
k1.vmdk
-rw-r----- 1 admin users        169 Jun 29 22:35 Security_Gateway_R77_30VSEC.mf
-rw-r----- 1 admin users      13513 Jun 29 22:35 Security_Gateway_R77_30VSEC.ovf
[Expert@CHPSMS:0]#
```

5. 接著輸入指令 vsec_config，選擇 1.VMware Configuratin，確認 Service Manager IP 是 SMS IP，請 URL 中的 ovf 檔名，與上一步驟傳送的檔名一致，輸入 y 並按 Enter。

```
[Expert@CHPSMS:0]#
[Expert@CHPSMS:0]# vsec_config

=======================================
|     vSEC Service Manager Menu
=======================================
   1.   VMware Configuration
   2.   Cisco ACI Configuration
   3.   Exit
Selected option: 1

Please wait while loading...

Below are the defaults that will be used for this vSEC Manager Server:
   Service Manager IP Address: 192.168.230.51
   URL of OVF: https://192.168.230.51:443/ve/Security_Gateway_R77_30VSEC.ovf

Do you accept the default values? (y/n: y to accept, n to change) [y]:
```

6. 輸入 y 確定要 register a new service，並選擇 1.nsx。

```
Below are the defaults that will be used for this vSEC Manager Server:
   Service Manager IP Address: 192.168.230.51
   URL of OVF: https://192.168.230.51:443/ve/Security_Gateway_R77_30VSEC.ovf

Do you accept the default values? (y/n: y to accept, n to change) [y]:
Service Manager thumbprint has been updated for nsx.
Would you want to register a new service now?
(y/n) [y]:
The following NSX Managers are configured in SmartConsole. Select NSX manager:
   1.   nsx
   2.   Back
Selected option: 1
```

7. 選擇 1.admin，並輸入 SMS 所屬 admin 密碼。

```
Please Choose an administrator from the list below.
This administrator will be used by the NSX for authentication
   1.   admin
   2.   Back
Selected option: 1

Please enter the password of the administrator you chose
Password:
Creating new Service: Check Point vSEC Service
```

```
Creating new Service: Check Point vSEC Service
Updating Service Profile Failure Policy for service: Check Point vSEC Service

****************************
Service registration completed successfully.
Service deployment is now available via vSphere Web Client under Networking & Se
curity -> Installation -> Service Deployments.
****************************



=====================================
|     vSEC VMware Service Manager Menu
=====================================
   1.   Change Global Configuration
   2.   Licensing
   3.   Register Service
   4.   Manage Registered Services
   5.   Reload Data Center Servers list
   6.   Check Connection
   7.   Back
Selected option:
```

8. 設定完畢後，可檢視設定，選擇 4.Manager Registered Services > 1.Show Services > 1.nsx。

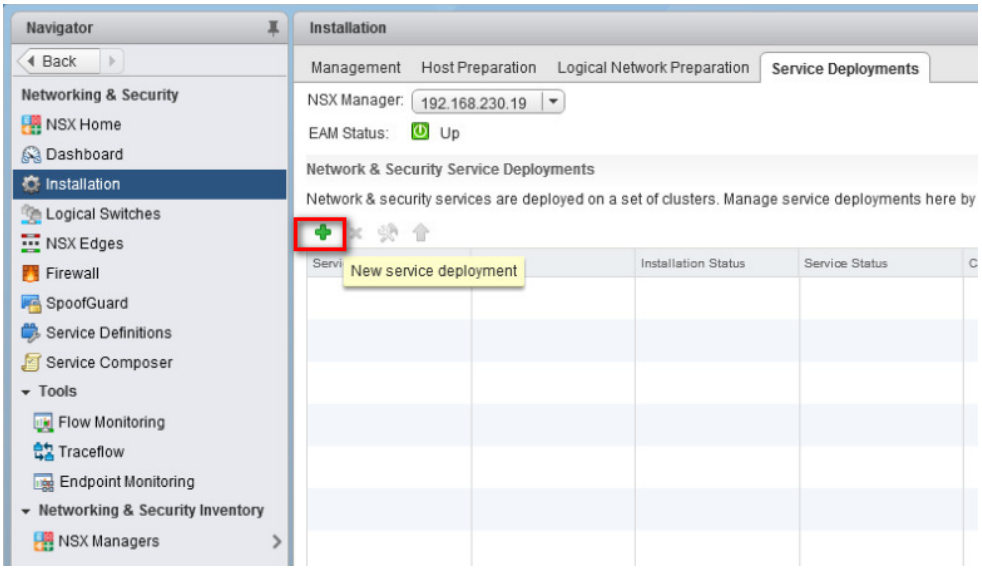
```
=====================================
|     vSEC VMware Service Manager Menu
=====================================
   1.   Change Global Configuration
   2.   Licensing
   3.   Register Service
   4.   Manage Registered Services
   5.   Reload Data Center Servers list
   6.   Check Connection
   7.   Back
Selected option: 4


=====================================
|     Registered Services Management Menu
=====================================
   1.   Show Services
   2.   Remove Service
   3.   Change Failure Policy
   4.   Back
Selected option: 1
```

```
The following NSX Managers are configured in SmartConsole. Select NSX manager:
   1.   nsx
   2.   Back
Selected option: 1

1. Service Name: Check Point vSEC Service
        Service Operation Mode: Inspection
        IPV6 support: OFF
        Profile: Check Point vSEC Service_Template_of_NSX
        Automatic Provisioning: On
        Failure Policy: Fail close
        Redirection Status: : Redirection rules applied
        Service Deployments:
        9FDemoLAB Cluster     (Status: UP)


=====================================
|     Registered Services Management Menu
=====================================
   1.   Show Services
   2.   Remove Service
```

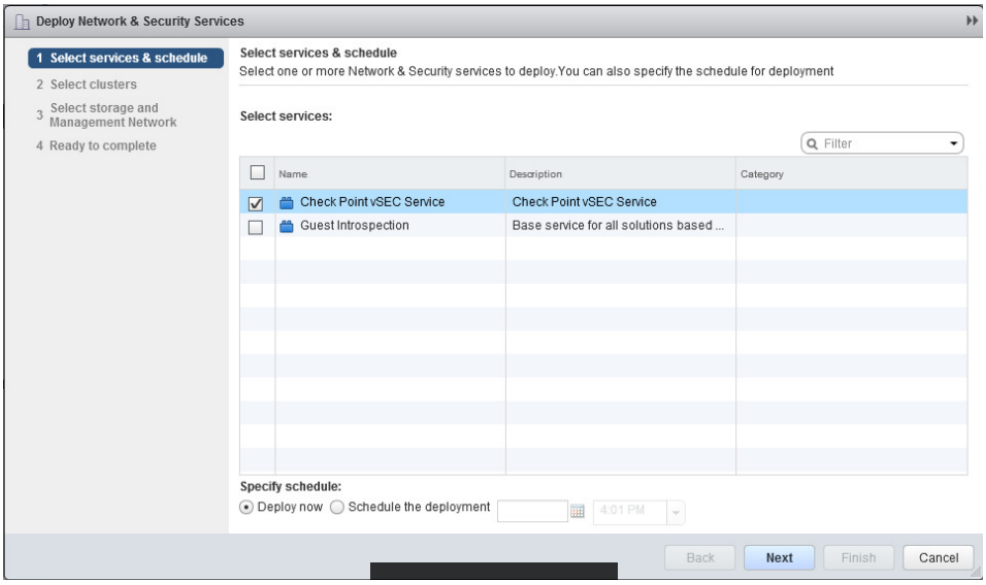
9. 設定完畢跳出 vsec_config 設定。

八、設定 vCenter 新增 Service。

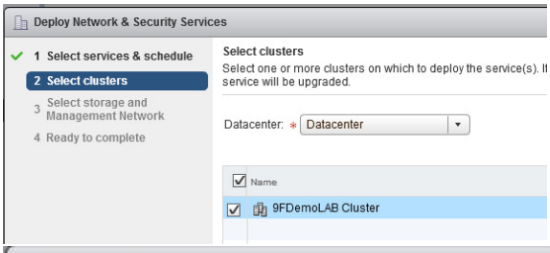
1. 登入 vCenter，切換到 Networking & Security > Installtion > Service Deployments 中，新增一 Service。



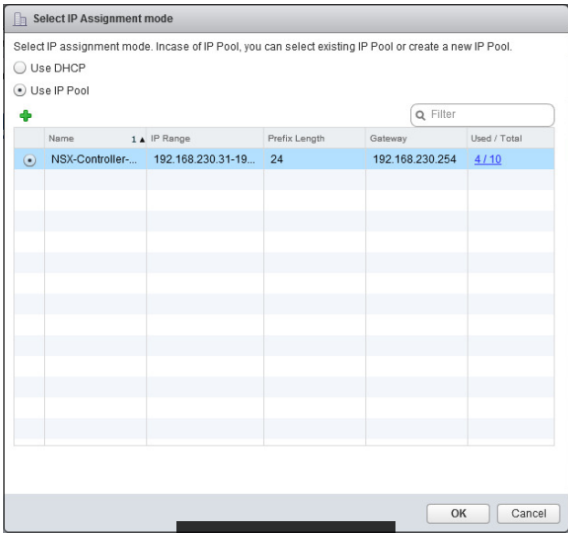
2. 可在選項中看到第七步驟完成後產生的 Servce “ CheckPoint vSEC Service”，勾選後點選 Next。



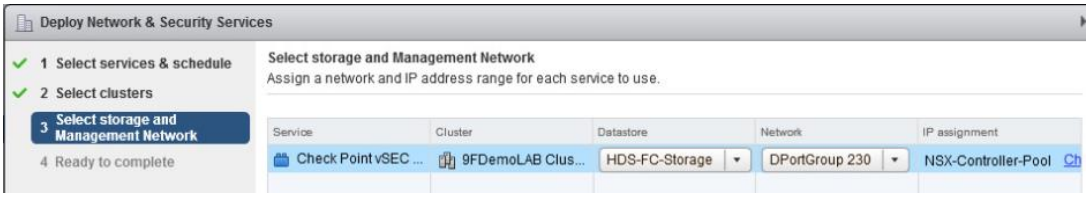
3. 選擇要套用的 Cluster 後點選 Next，接者選擇要使用的 share storage “HDS-FC-Storage”，以及要使用的 Network “ DPortGroup 230”，IP assignment 點選 change。



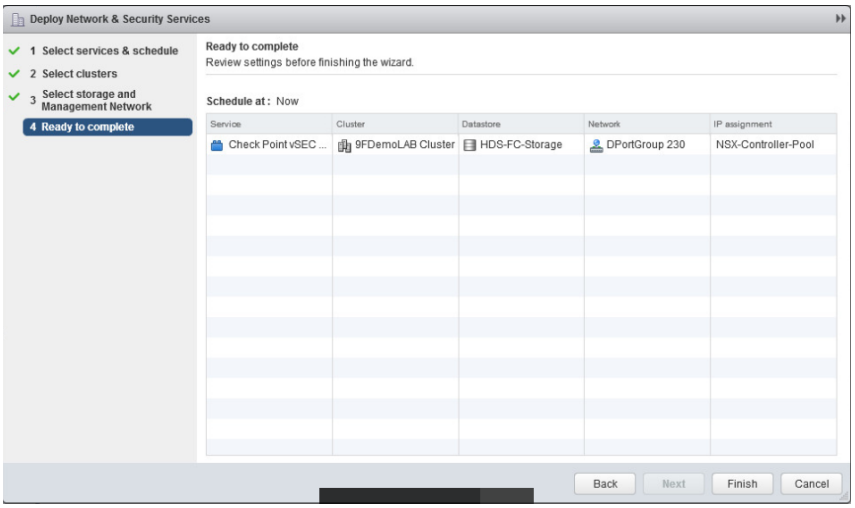
4. 此部分可以新增一組 DHCP pool，本範例選擇之前建立的 NSX-Controller-Pool，點選 OK。



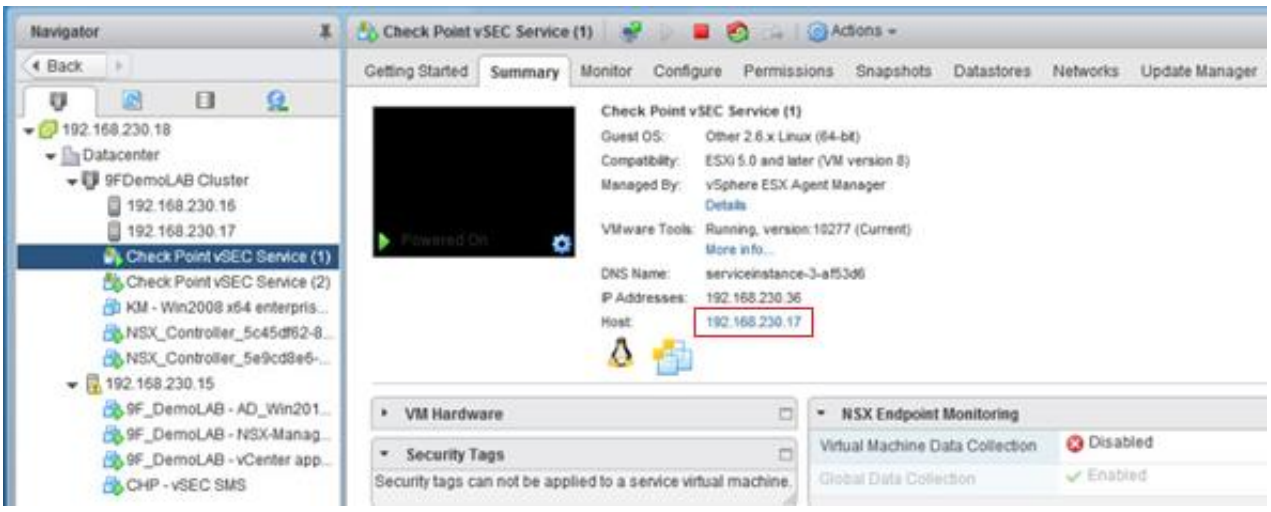
5. 設定完畢後點選 Next。

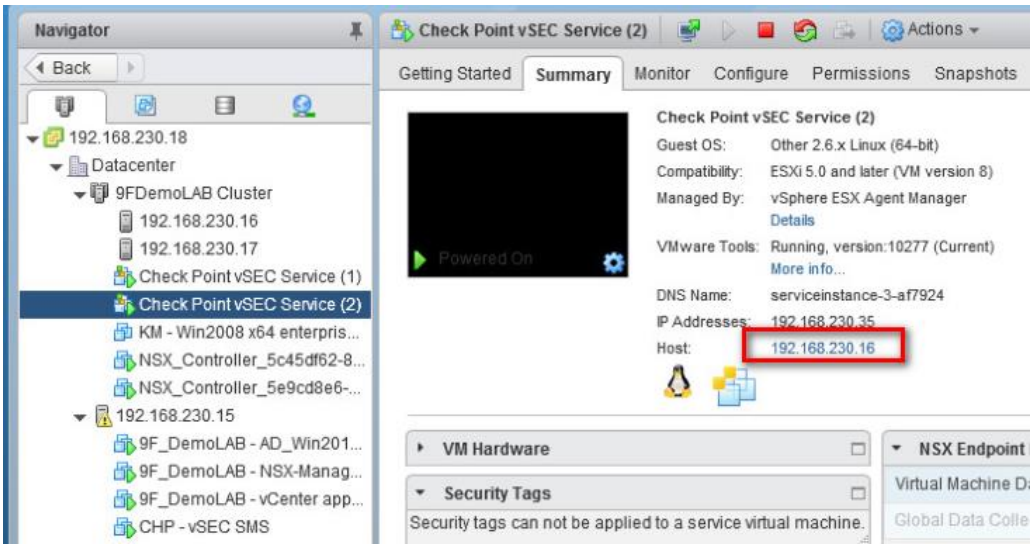


6. 確認設定參數都沒有問題後，點選 Finish。

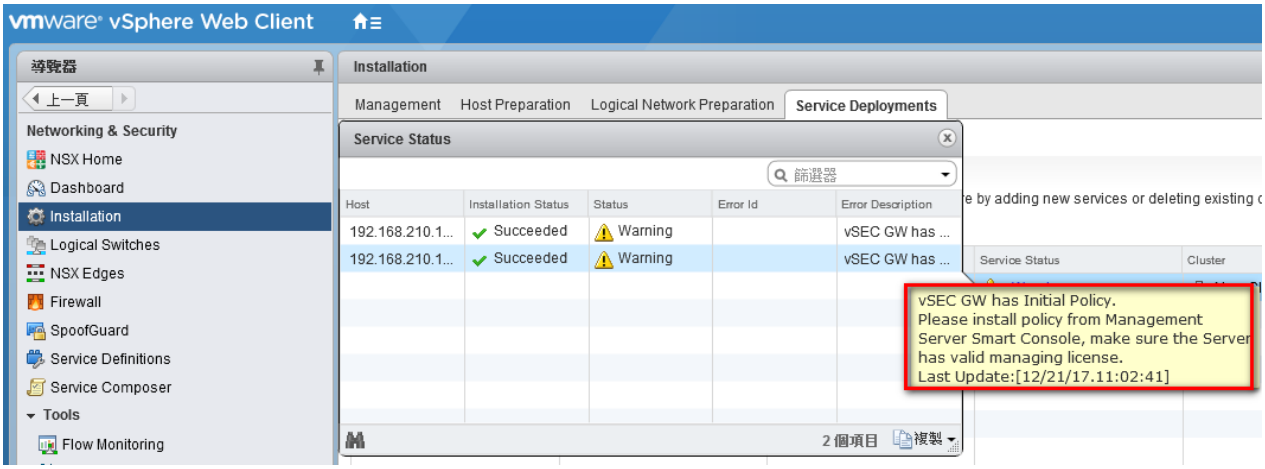


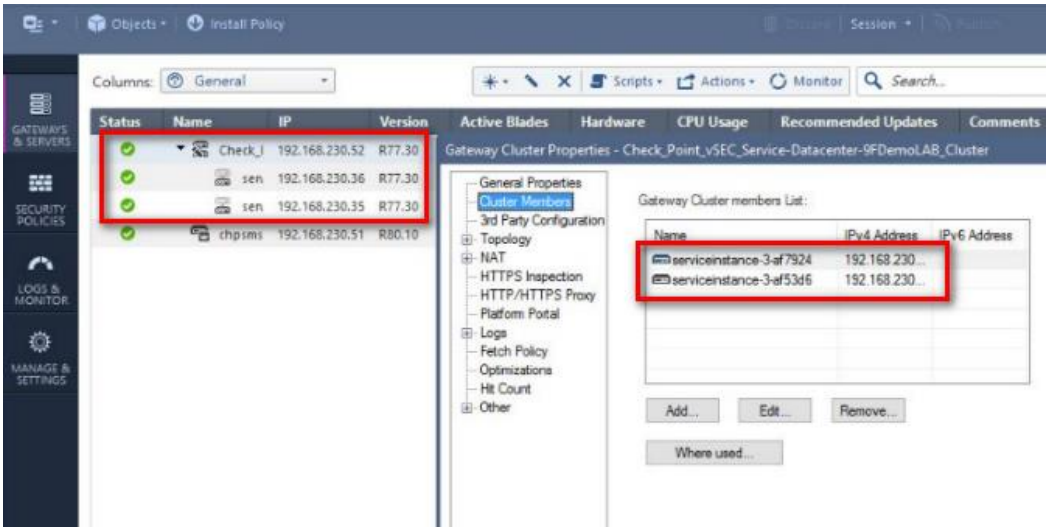
7. 當 vCenter 和 NSX 開始連線到 CHP SMS 讀取 ovf 檔，並開始佈署 vSEC Service 時，請關閉 SmartConsole，避免影響運作，此時可從 vCenter 上看到每台 ESXi 都會佈建一台 Check Point vSEC Service。**此步驟需要花費超過 30 分鐘以上。**



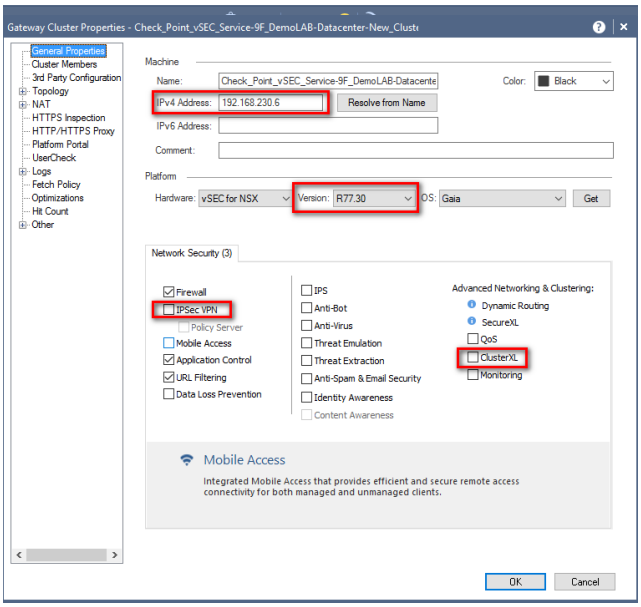
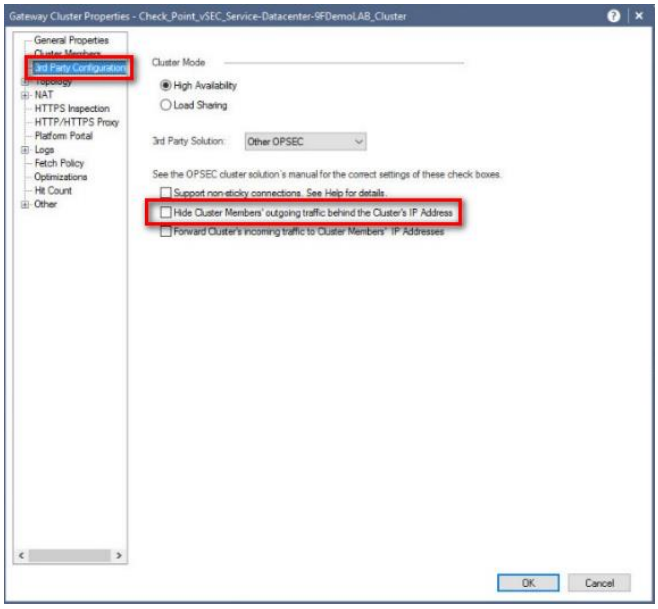


8. 等到 Service Deploy,ents 中佈建狀態顯示成功，但 status 顯示 Down，且 Error Description 顯示 vSEC GW didn't run First Time Wizard。打開 SmartConsole，可看到新的 Clueter 物件與對應的 Firewall。

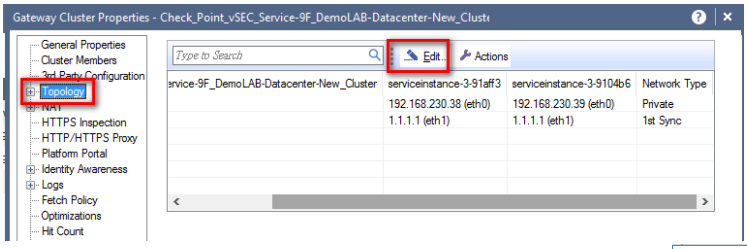
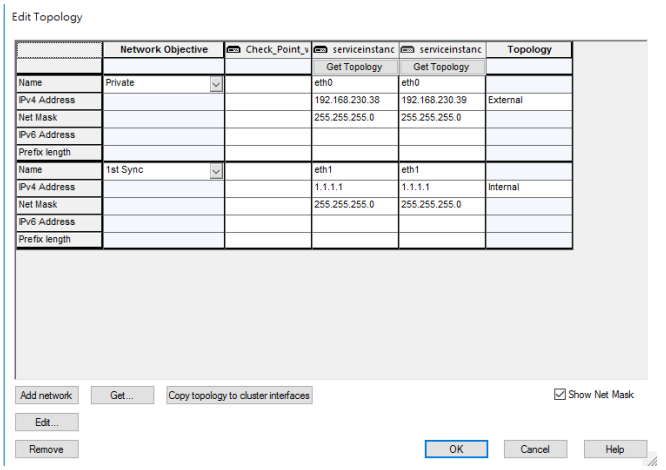
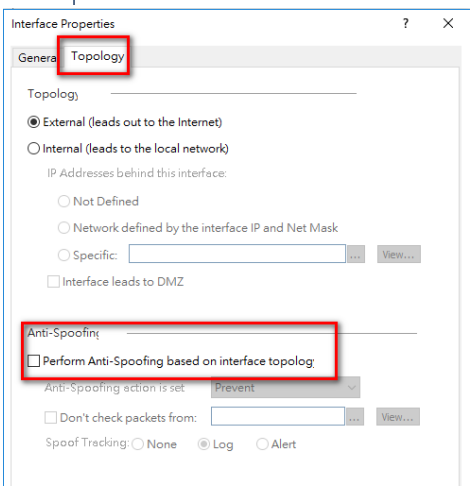
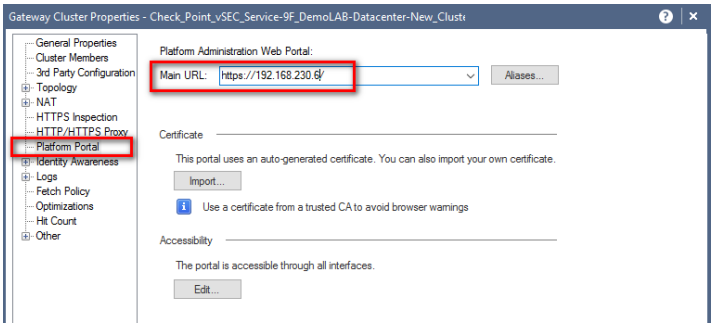




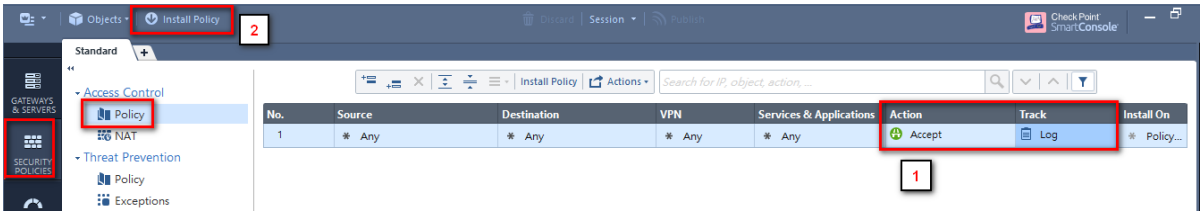
9. 確認 cluster member 是否和 SMS sync 正常，Cluster 物件的 General Properties 中，修改 Cluster 物件 IP、Version 版本、取消勾選 IPSecVPN、ClusterXL，在 3rd Party Configuration 中取消勾選 Hide Cluster Member's outgoing traffic behind the Cluster's IP Address。

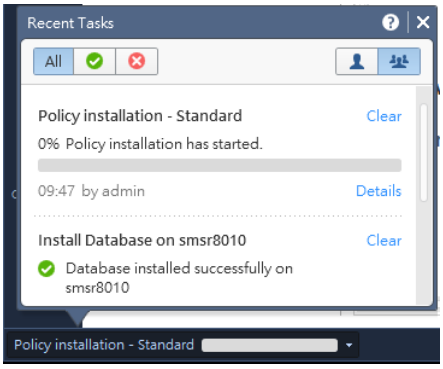



10. 到 Topology，關閉每個介面中 Topology 的 Anti-Spoofing，到 Platform Portal 修改 Main URL。

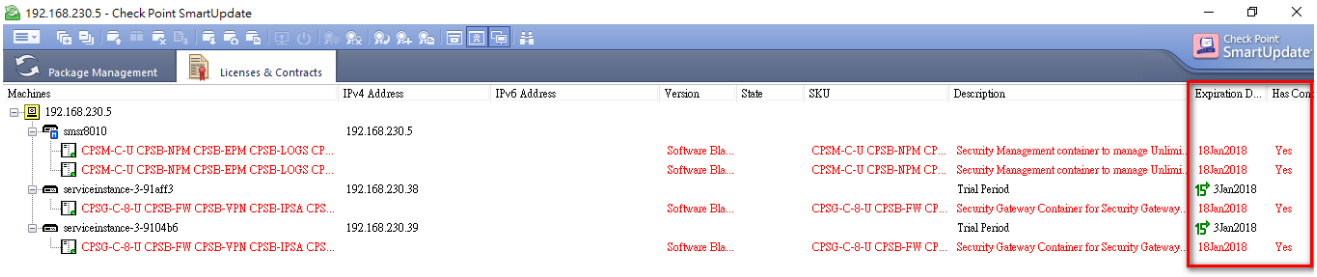





11. 到 SECURITY POLICIES > Access Control > Policy 中，修改預設 policy Action 為 Accept、Tack 為 log，然後 Install policy，等待 install policy 完成。

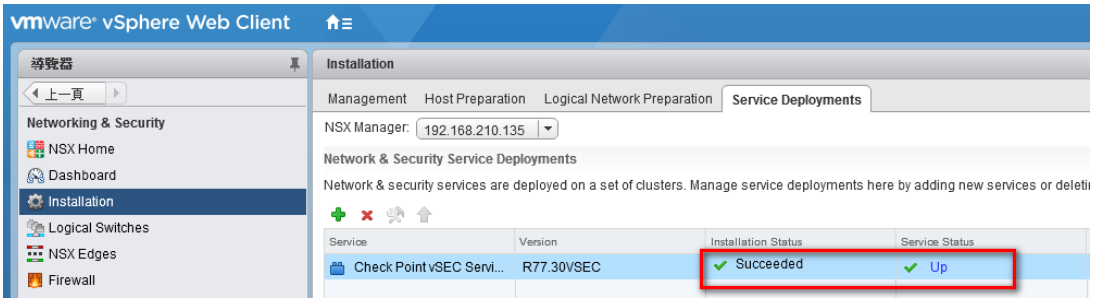




12. 匯入 gateway license & contract。

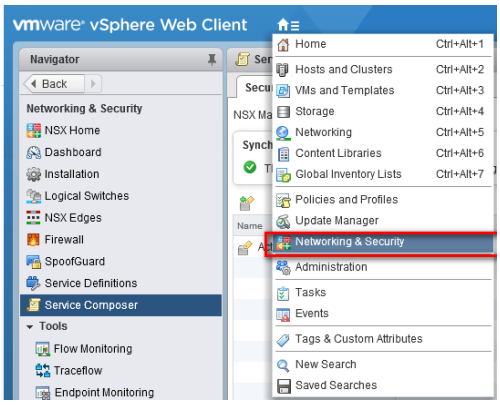


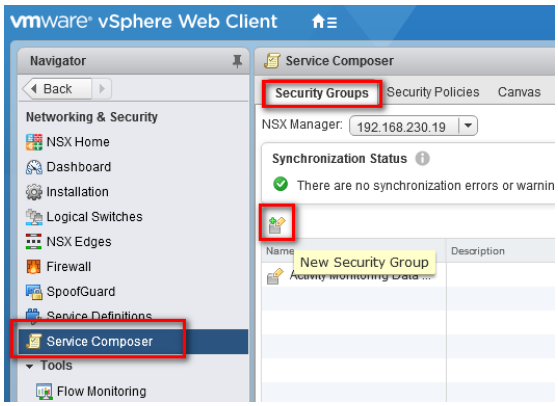
13. 回到 vCenter 檢查 NSX 佈署的 service deployment 可以看到都變成 OK。



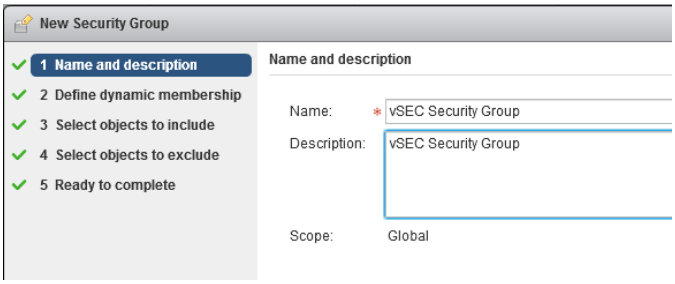
九、Configuring NSX redirect traffic to the Security Gateway Virual Edition：

1. 回到 vCenter Web Client，到 Home > Networking $ Security > Service Composer > Security Groups，點選 New Security Group。

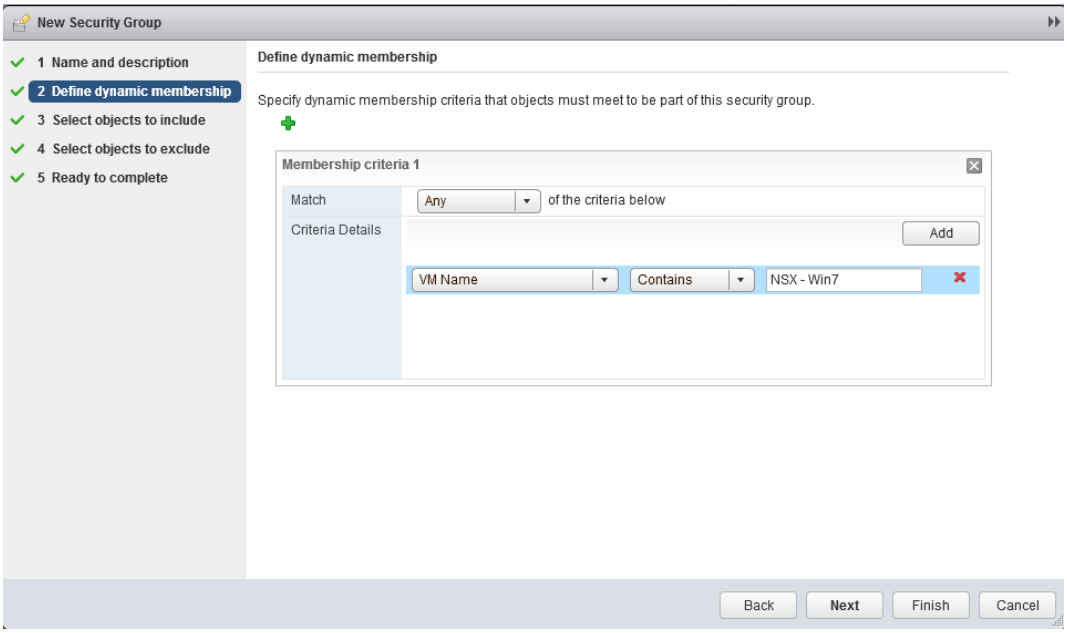




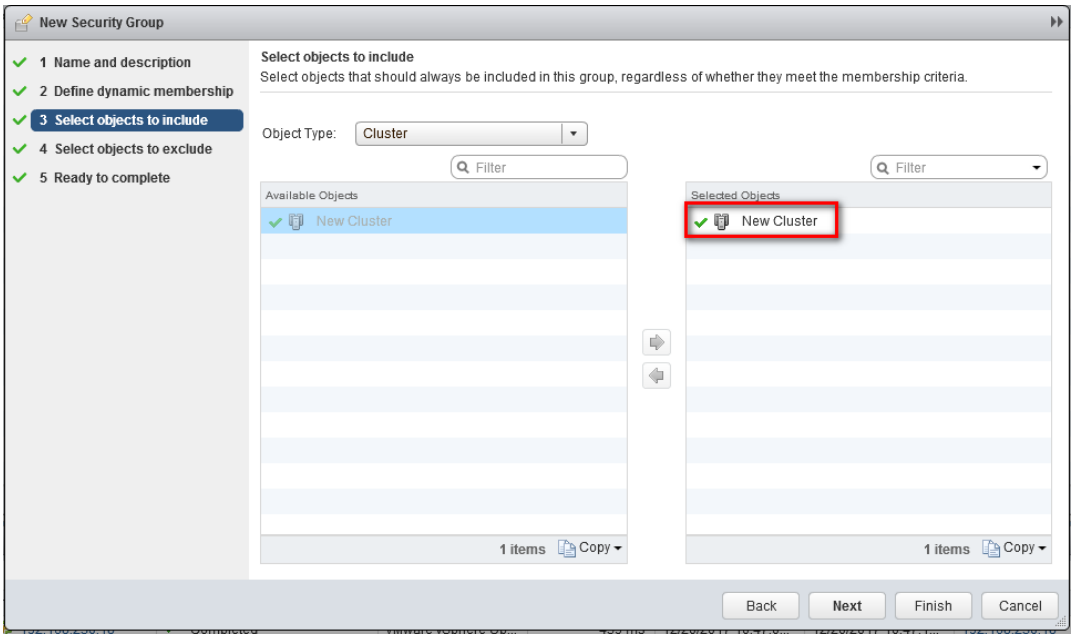
2. 設定 name

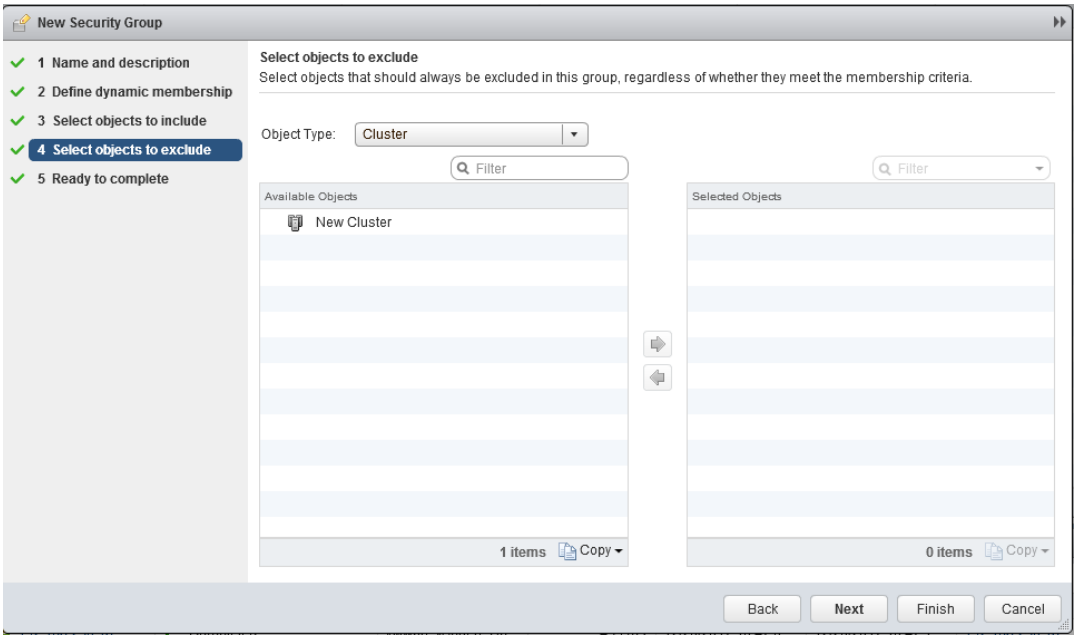


3. 設定套用的 membership 條件。

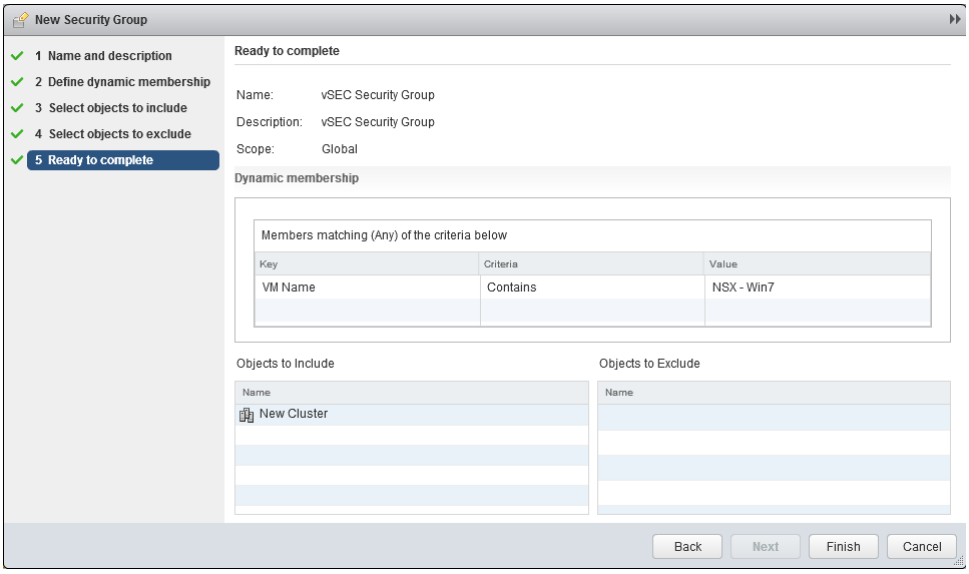


4. Select objects to include 選擇所要保護的 cluster，Select objects to exclude 不選擇，直接點 Next。

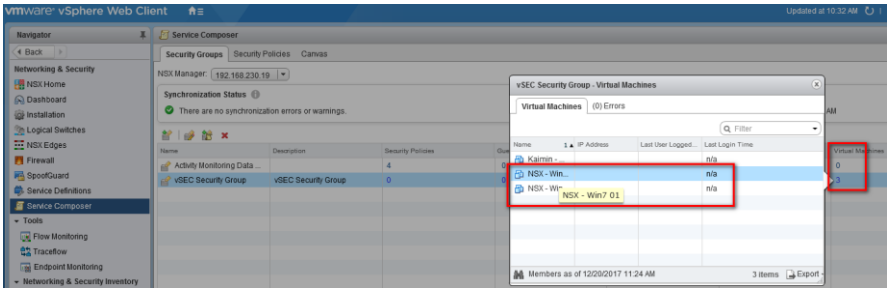




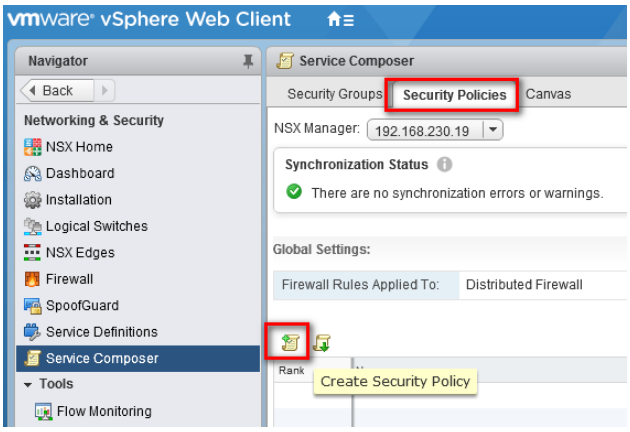
5. 確認設定資訊無誤後點 Finish。



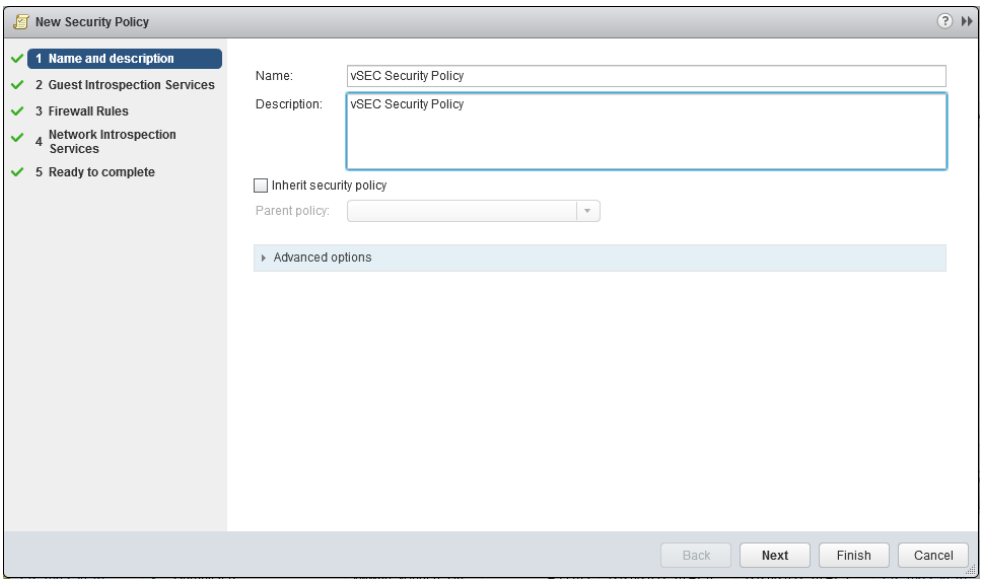
6. 確認要測試的主機在此 Security Group 中。



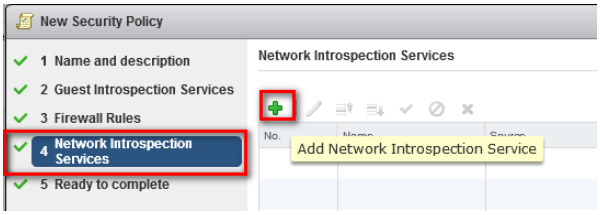
7. 切換到 Security Policied，點選 Create Security Policy。



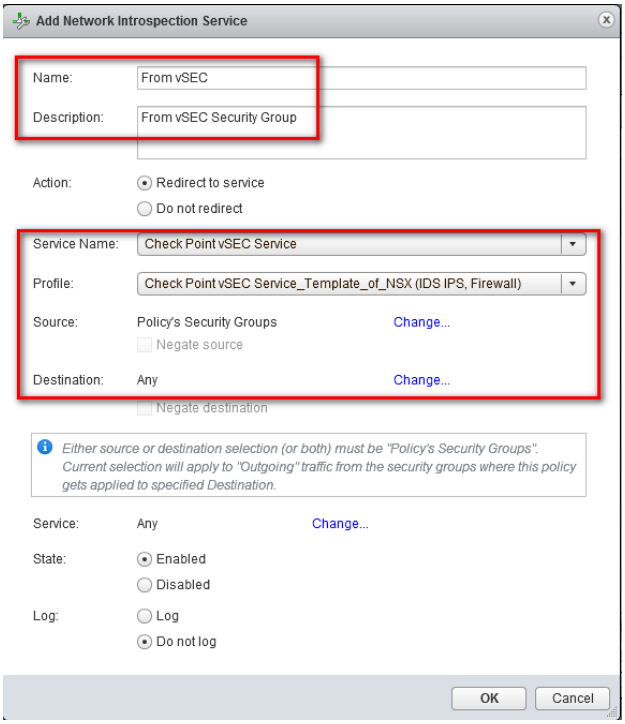
8. 設定 Security Policy Name。



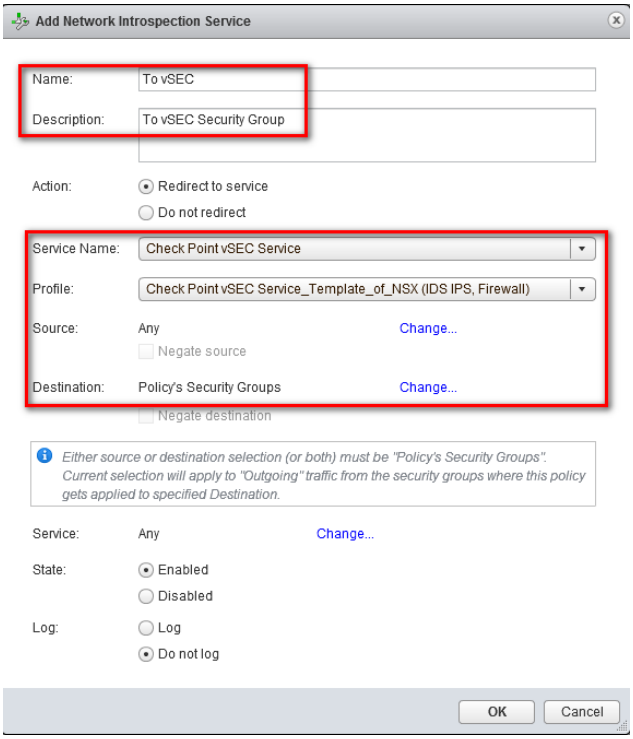
9. 接著直接跳到 Network Introspection Serevices，點選 Add Network Introspection Service。



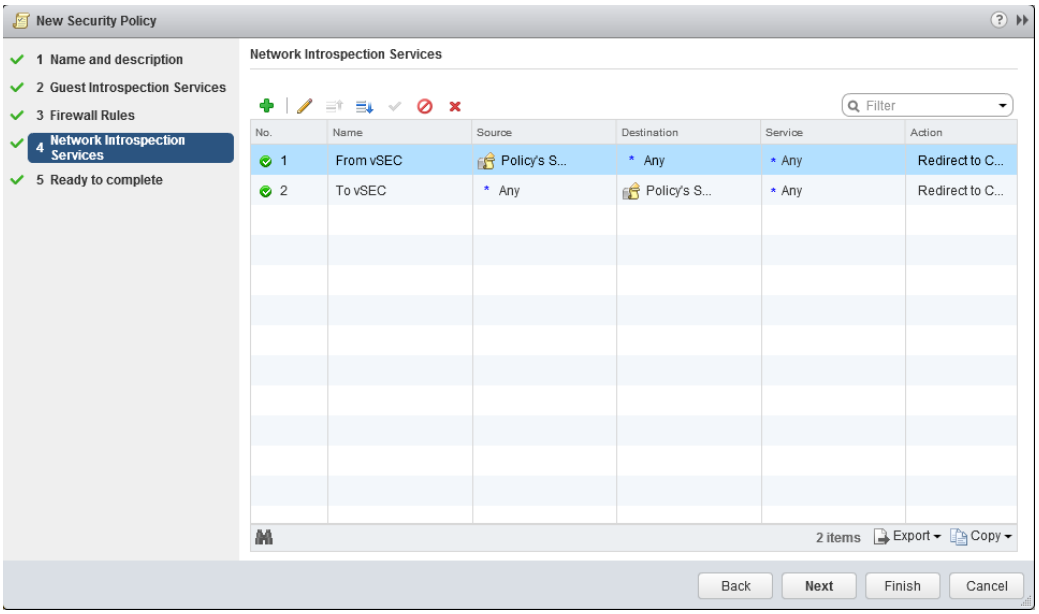
10. 新增第 1 條 Service，檢查從虛擬機對外的 traffic，設定 Name、Description，Service Name 選擇前面設定 for CheckPoint vSEC 的 Serice，Profile 選擇前面設定的 vSEC Profile， Sourcec 為 Policy's Security Group，Destination 確定為 any，點選 OK。



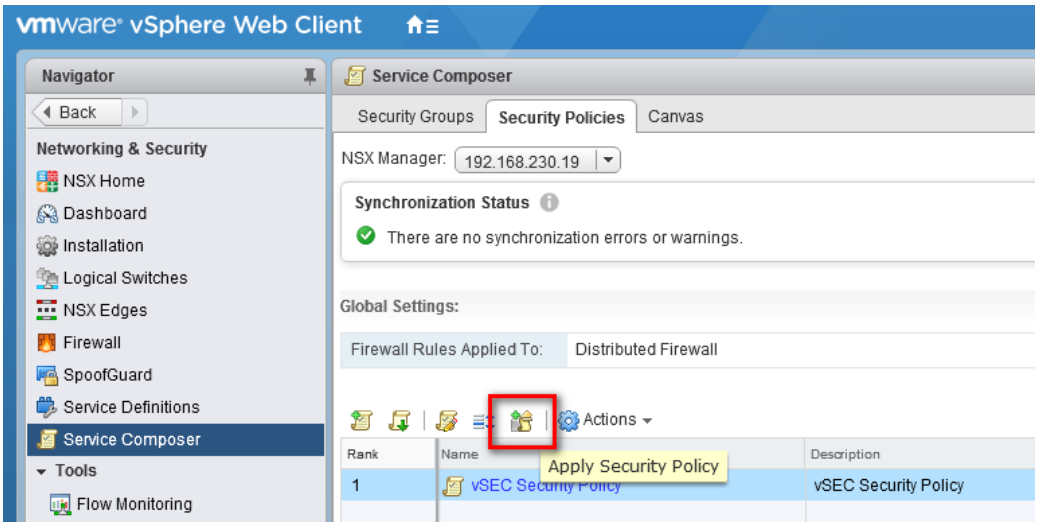
11. 新增第 2 條 Service 檢查外部 traffic 到虛擬機，設定 Name、Description，Service Name 選擇前面設定 for CheckPoint vSEC 的 Serice，Profile 選擇前面設定的 vSEC Profile， Sourcec 為 any，Destination 確定為 Policy's Security Group，點選 OK。

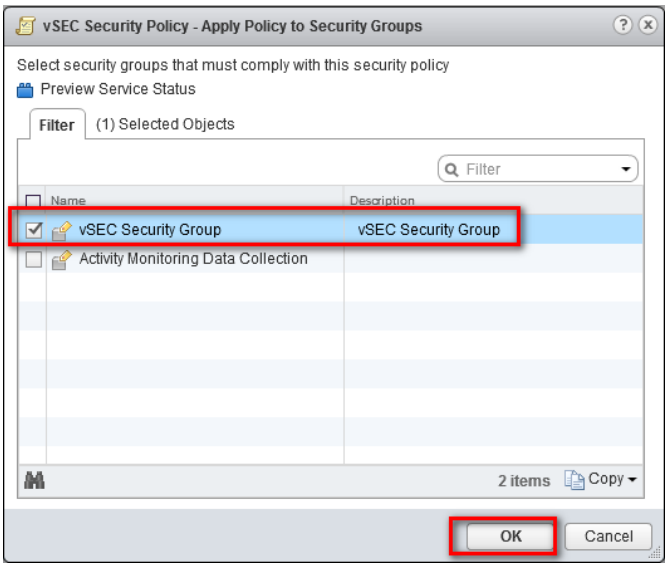


12. 確認 Service 是否正確，點 Finish。

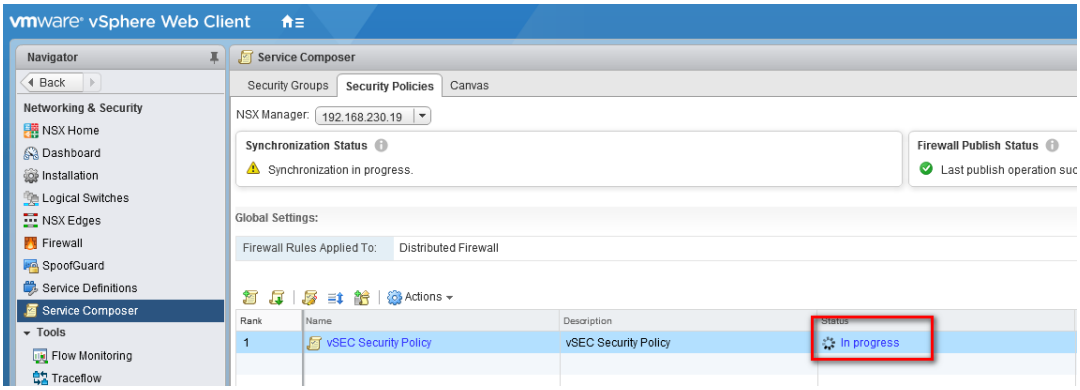


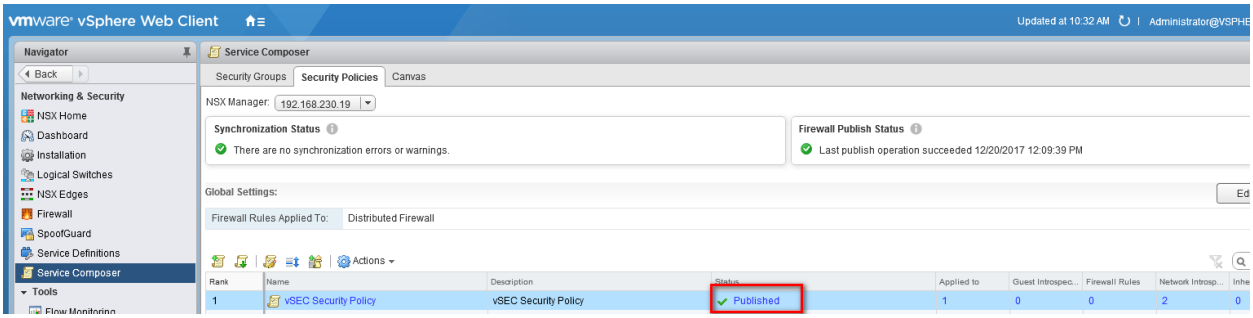
13. 點選剛剛新增的 Security Policy 再點選 Apply Security Policy，勾選要套用的 vSEC Security Group，點選 OK。





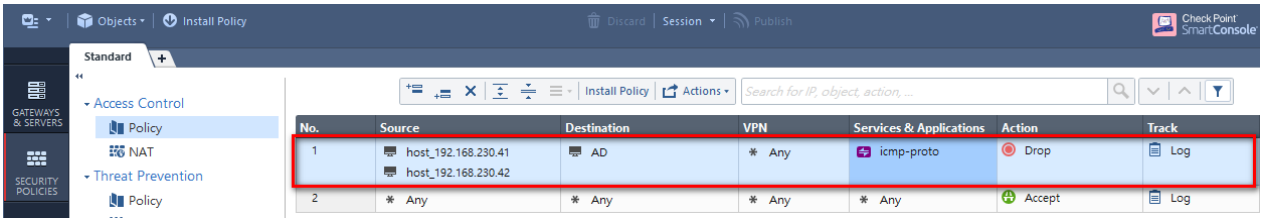
14. 等待套用完成。



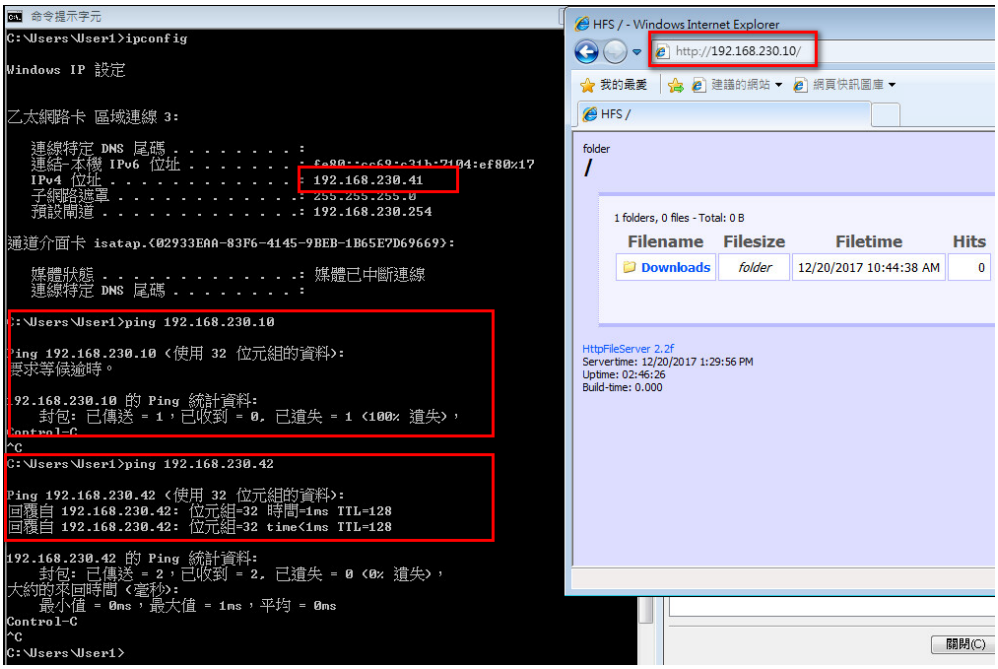


十、驗證：

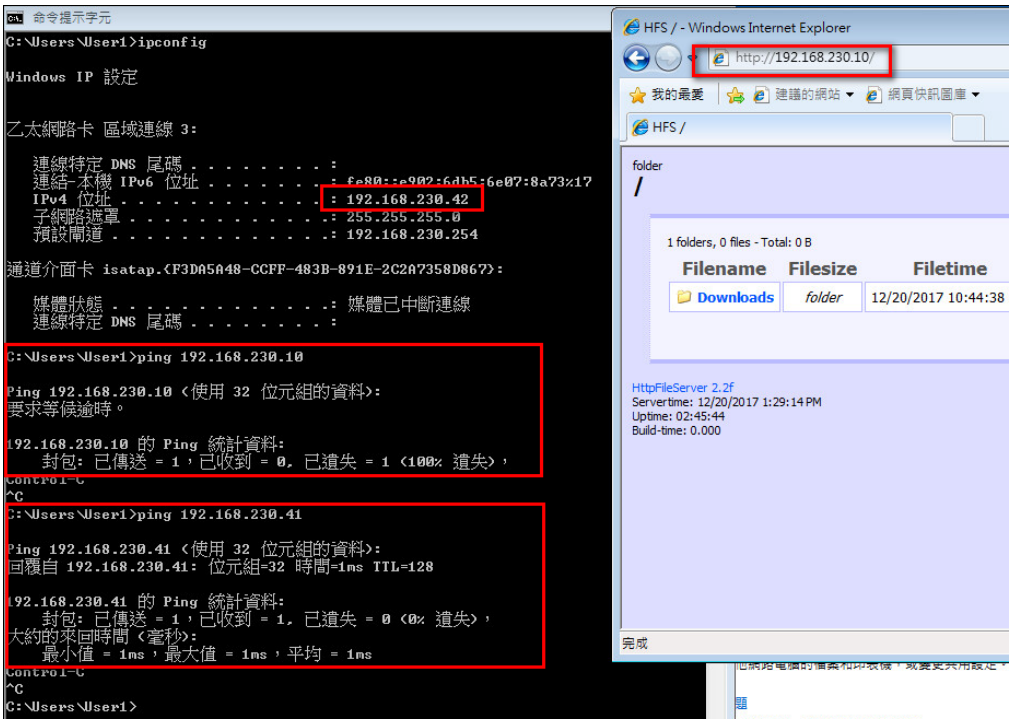
1. 設定 Policy 不允許第 1、2 台 Win7 不能 ping AD，但能存取其他資源。



2. 從 Win 7(192.168.230.41)不可 ping AD(192.168.230.10)，但能存取 AD 的 http，且能 ping 到 Win7(192.168.230.42)。



3. 從 Win 7(192.168.230.42)不可 ping AD(192.168.230.10)，但能存取 AD 的 http，且能 ping 到 Win7(192.168.230.41)。



4. 啟動 Application Control & URL Filter Blades，並設定阻擋 facebook，驗證是否能阻擋成功 。