UCSE- vWAAS Installation and Configuration Guide

Contents

Overview 2

Requirements 2

Preparing to installing ESXi & vWAAS 4

Router configuration -- ISR G2 4

Router configuration -- ISR 4K 6

VMware Installation on UCS-E Series 8

Configuration of ESXi IP address using CIMC GUI 10

VMware vSphere Client 12

ESXi Network Configuration: 13

vWAAS Installation: 16

ISR-G2 WCCP Configuration 19

WAAS Configuration: 20

# Overview

Virtual WAAS (vWAAS) software can be installed on VMware ESXi 4.1 and later. It provides various benefits like elasticity, ease of maintenance, and a reduction of branch office and data center footprint.

vWAAS can be deployed at the traditional WAN-edge, in both the branch office and data center. In this document we will focus on the branch office deployment with UCS-E series server and ISR-G2 and ISR-4K.

# Requirements

The requirements of vWAAS with UCS-E include the following

* VMware ESXi 5.1 or 5.5 image (This is a cisco supported image and can be downloaded from VMware directly [here](https://my.vmware.com/web/vmware/details?downloadGroup=CISCO-ESXI-5.1.0U3&productId=285) and [here](https://my.vmware.com/web/vmware/info/slug/datacenter_cloud_infrastructure/vmware_vsphere/5_5#custom_iso)
  + Depending which UCS-E module and which ESXi version your organization has standardized on will determine which of the above links you use. For example the UCS-E 120S has only had 5.5 validated.
* VMware vsphere [client](http://vsphereclient.vmware.com/vsphereclient/1/8/8/0/9/0/6/VMware-viclient-all-5.1.0-1880906.exe)
* vWAAS OVA file which should have been provided via DVD otherwise can be downloaded from [CCO](https://software.cisco.com/download/release.html?mdfid=280484571&flowid=&softwareid=280836712&release=5.5.1&relind=AVAILABLE&rellifecycle=&reltype=latest) 
  + vWAAS comes in 6 sizes that are supported on the UCS-E which are detailed in table 1.
  + Likely if you purchased WAAS as part of an AX bundle with your router or the App license for a UCS-E spare you will be deploying the vWAAS-1300 or vWAAS-2500 OVA file.
    - **Example** filenames on CCO:
      * Cisco-vWAAS-1300-5.5.1-b12.ova
      * Cisco-vWAAS-2500-5.5.1-b12.ova

Table 1. vWAAS model requirements, UCS-E support, Router Support

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | vWAAS-200 | vWAAS-750 | vWAAS-1300 | vWAAS-2500 | vWAAS-6000 |
| UCSEN-120S-M2 | Yes | Yes | Yes | No | No |
| UCS E-140S-M1/M2 | Yes | Yes | Yes | Yes | Yes |
| UCS E-140D | Yes | Yes | Yes | Yes | Yes |
| UCS E-160D-M1/M2 | Yes (M1 only on 39xx) | Yes (M1 only on 39xx) | Yes (M1 only on 39xx) | Yes (M1 only on 39xx) | Yes (M1 only on 39xx) |
| UCS E-180D-M2 | Yes | Yes | Yes | Yes | Yes |
| Router supported | 2911, 2921, 2951,  3925, 3945, 3925E, 3945E, 4331, 4351, 4451 | 2911, 2921, 2951,  3925, 3945, 3925E, 3945E, 4331, 4351, 4451 | 2911, 2921, 2951,  3925, 3945, 3925E, 3945E, 4331, 4351, 4451 | 2911, 2921, 2951,  3925, 3945, 3925E, 3945E, 4331, 4351, 4451 | 2911, 2921, 2951,  3925, 3945, 3925E, 3945E, 4331, 4351, 4451 |
| vCPU | 1 | 2 | 2 | 4 | 4 |
| Virtual Memory-GB | 3 | 4 | 6 | 8 | 11 |
| Virtual disk size-GB | 260 | 500 | 600 | 750 | 900 |

* Your max achievable throughput may be lower if other virtual machines are running at the same time assigned to the same cores as vWAAS. This includes running a vWAAS on a system with not enough physical CPU cores as indicated above.
* virtual memory is reserved for vWAAS
* virtual disk is thick provisioned
* vWAAS-6000 requires 10K SAS HD to achieve maximum throughput
* Router performance is impacted due to additional router services/features and packet processing. When deploying WAAS on WAVE appliances, UCS-E Router blades, or SRE module while using WCCP or AppNav-XE to the router, please verify the total throughput of processing the traffic, including packets to and from the WAAS engine, is not greater than the router's rated capacity with the services you plan to run.
* Support for UCS-E blades assumes that the UCS-E blade has sufficient memory/disk installed, and available CPU cores that can be assigned to the Virtual WAAS instance. vWAAS-1300, vWAAS-2500, and vWAAS-6000 all require 6GB or more memory. As such, your UCS-E must have more than the default 8GB memory installed to install and run these vWAAS models.

# Preparing to installing ESXi & vWAAS

## Router configuration -- ISR G2

UCSE port description:

|  |  |
| --- | --- |
| UCSE Ports | Description |
| M | Dedicated CIMC port |
| Console | backplane PCIe interface (Router Internal –ucse x/0) |
| GE1 | Backplane MGF interface (Router Internal- ucse x/1) |
| GE2 | external GE2 port |
| GE3 | external GE3 port (DW only) |

Host Router

E-Series Server

GE2 GE3

Router CPU

PCIe

MGF

ucse x/0

BMC



CIMC GUI

G0/0

GE0

GE1

ucse x/1

! (**Configuration to access the CIMC web GUI interface)**

interface GigabitEthernet0/1

description LAN

ip address 192.168.3.1 255.255.255.0

interface ucse2/0

ip unnumbered GigabitEthernet0/1

imc ip address 192.168.3.10 255.255.255.0 default-gateway 192.168.3.1

imc access-port shared-lom console

no shutdown

!(**Static route to CIMC)**

ip route 192.168.3.10 255.255.255.255 ucse2/0

! (**Static route to VMware ESXi)**

ip route 192.168.3.11 255.255.255.255 ucse2/0

**(Configure trunk mode on UCSE x/1-MGF Interface)**

interface ucse2/1

description Internal switch interface connected to Service Module

switchport mode trunk

no ip address

no shutdown

end

**(Create a VLAN Interface and configure an IP, this will be used by the router for communication with WAAS)**

router(config)#vlan 1

router(config-vlan)#name waas

interface Vlan1

ip address 172.25.60.1 255.255.255.0

no shutdown

**(Verify ucse x/1 is in trunking mode and VLAN 1 is included after ESXi is installed)**

2951-Branch#sh int ucse 2/1 trunk

Port Mode Encapsulation Status Native vlan

uc2/1 on 802.1q trunking 1

Port Vlans allowed on trunk

uc2/1 1-4094

Port Vlans allowed and active in management domain

uc2/1 1-4

Port Vlans in spanning tree forwarding state and not pruned

uc2/1 1-4

## 

## Router configuration -- ISR 4K

UCSE port description:

|  |  |
| --- | --- |
| UCSE Ports | Description |
| M | Dedicated CIMC port |
| Console | backplane MGF interface (Router Internal –ucse x/0) |
| GE1 | Backplane MGF interface (Router Internal- ucse x/1) |
| GE2 | external GE2 port |
| GE3 | external GE3 port (DW only) |

Host Router

E-Series Server

GE2 GE3

Router CPU

MGF

MGF

ucse x/0/0

BMC



CIMC GUI

G0/0/0

GE0

GE1

ucse x/0/1

! (**Configuration to access the CIMC web GUI interface)**

ucse subslot 1/0

imc access-port shared-lom console

imc ip address 10.105.1.10 255.255.255.0 default-gateway 10.105.1.1

interface GigabitEthernet0/0/0

ip address 10.105.1.1 255.255.255.0

!

interface ucse 1/0/0

ip unnumbered GigabitEthernet 0/0/0

no shutdown

!(**Static route to CIMC)**

ip route 10.105.1.10 255.255.255.255 ucse 1/0/0

!

! (**Static route to VMware ESXi)**

ip route 10.105.1.11 255.255.255.255 ucse 1/0/0

**!(Configure trunk mode on UCSE x/1-MGF Interface and bridge domain to BDI for communication between router and WAAS)**

interface ucse 1/0/1

switchport mode trunk

service instance 2 ethernet

encapsulation untagged

bridge-domain 2

no shutdown

end

interface BDI 2

description WAAS Subnet

ip address 11.0.0.1 255.255.255.0

no shutdown

**!(Create WAAS VLAN)**

router(config)#vlan 1

router(config-vlan)#name waas

**(Verify ucse x/1 is in trunking mode and VLAN 1 is included after ESXi is installed)**

router#show interface ucse x/1 trunk

Port Mode Encapsulation Status Native vlan

SM1/1 on 802.1q trunking 1

Port Vlans allowed on trunk

SM1/1 1-4094

Port Vlans allowed and active in management domain

SM1/1 1

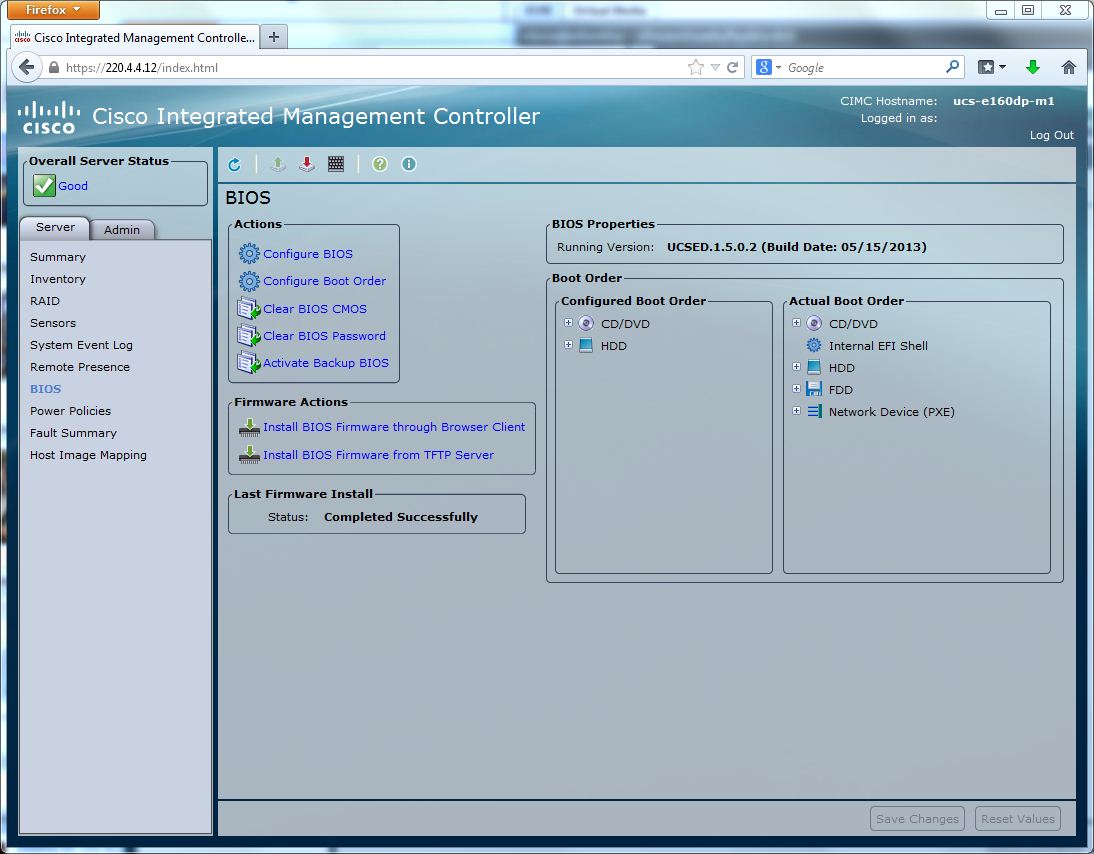
Port Vlans in spanning tree forwarding state and not pruned

SM1/1 1

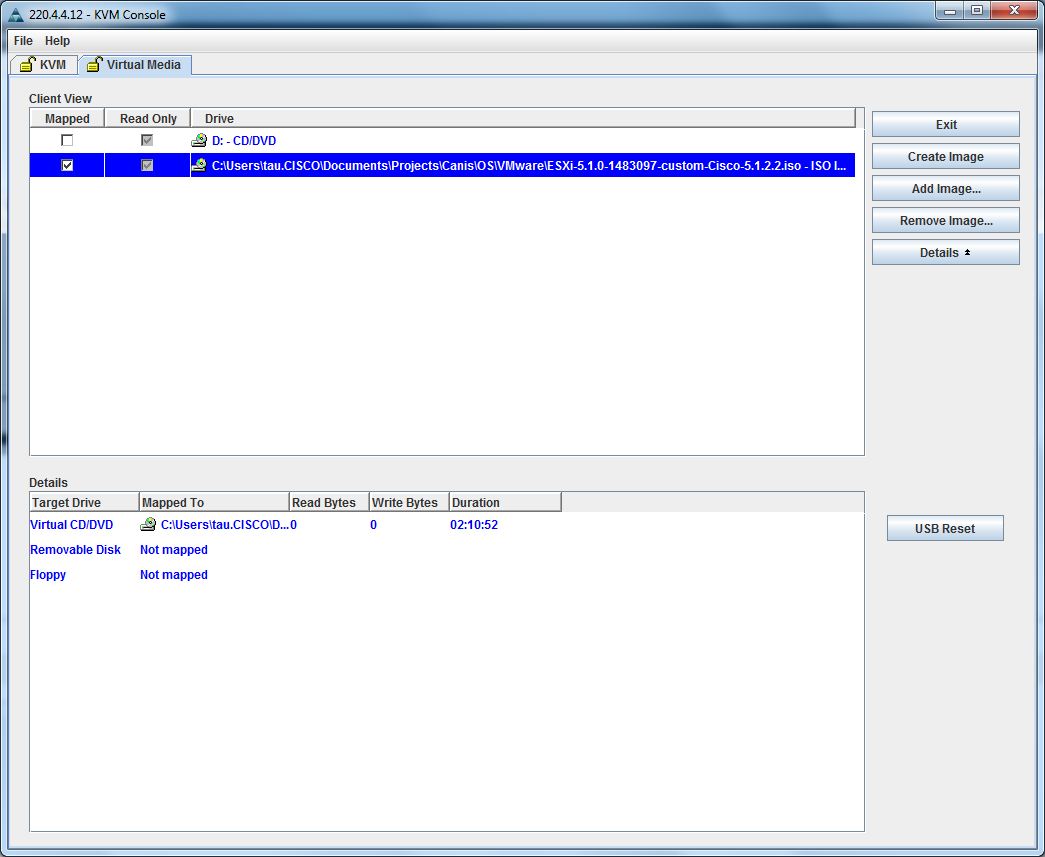
# VMware Installation on UCS-E Series

For reference follow the [UCSE quick start guide](http://www.cisco.com/en/US/docs/unified_computing/ucs/e/1.0/gs/guide/b_Getting_Started_Guide_chapter_0111.html) for installing the VMware ESXi on UCSE

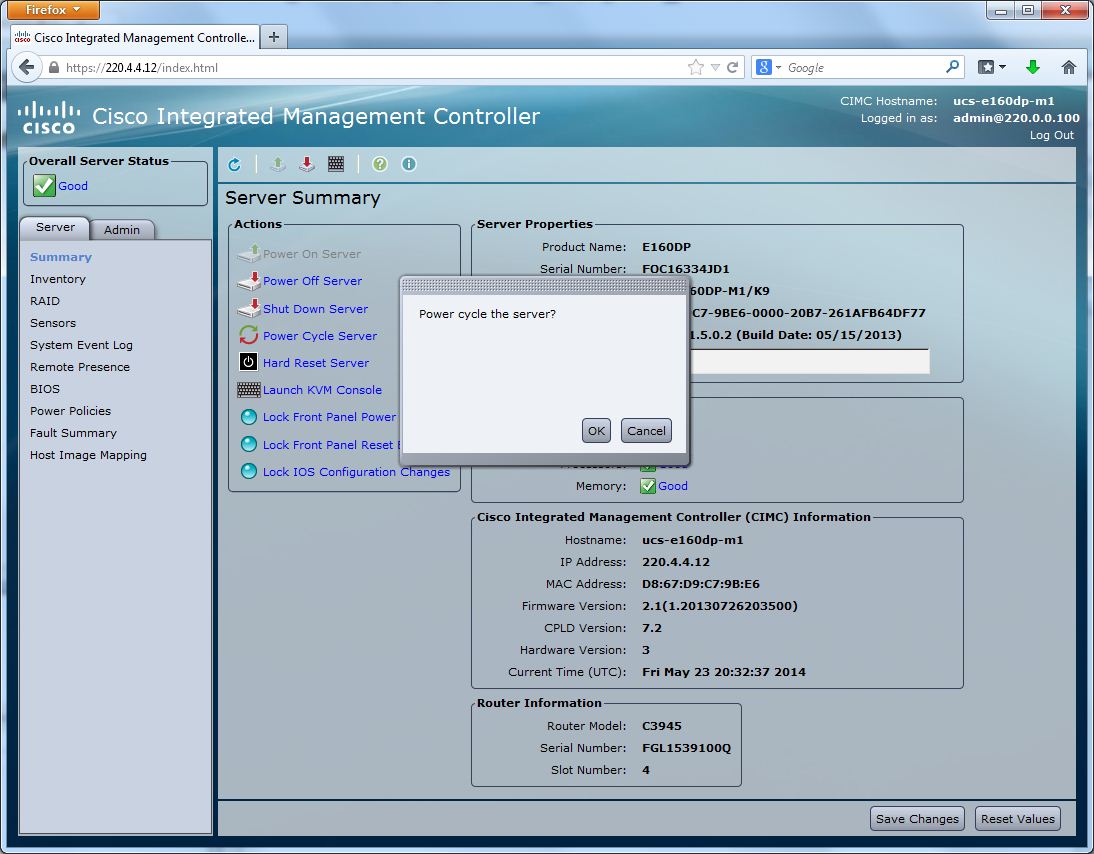
1) Configure Boot Order - CD/DVD, HDD



2) Launch vKVM, Go to Virtual Media tab, and add image (ISO)



3) Power Cycle Server

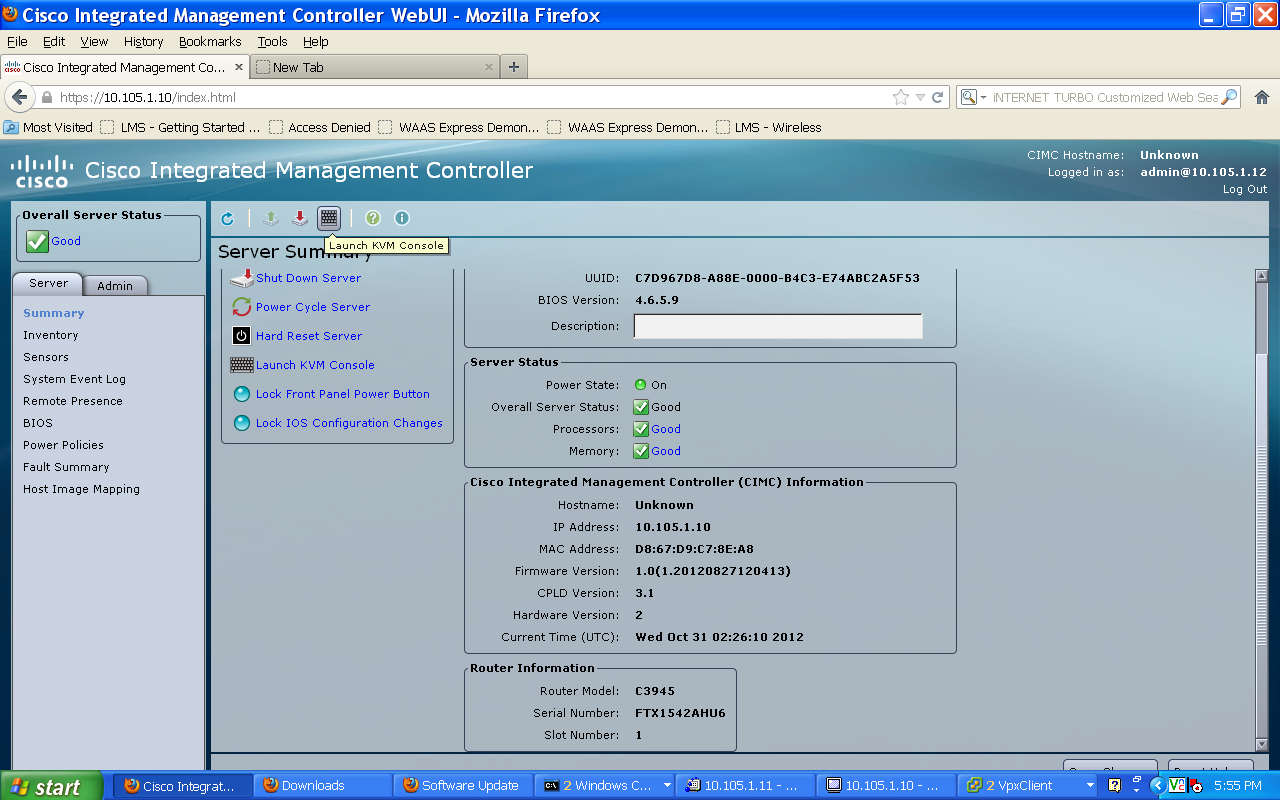


4) Check vKVM for OS installation

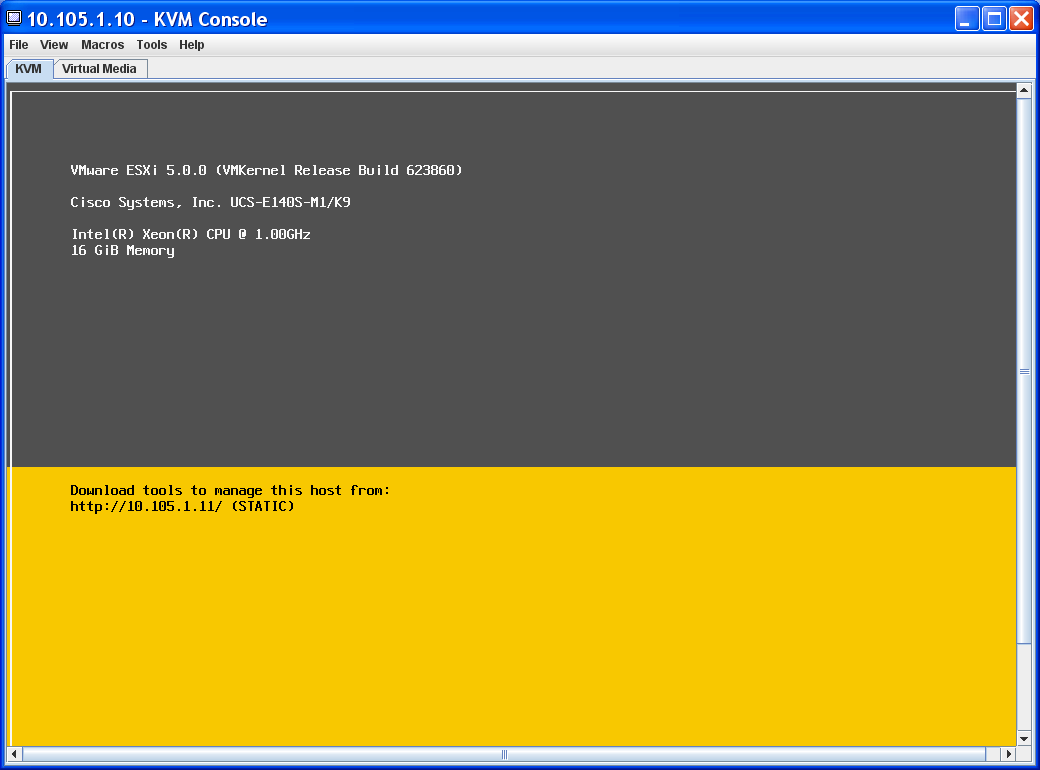
# http://wikicentral.cisco.com/download/attachments/265004138/OS_install.JPG?version=1&modificationDate=1400877864000

# Configuration of ESXi IP address using CIMC GUI

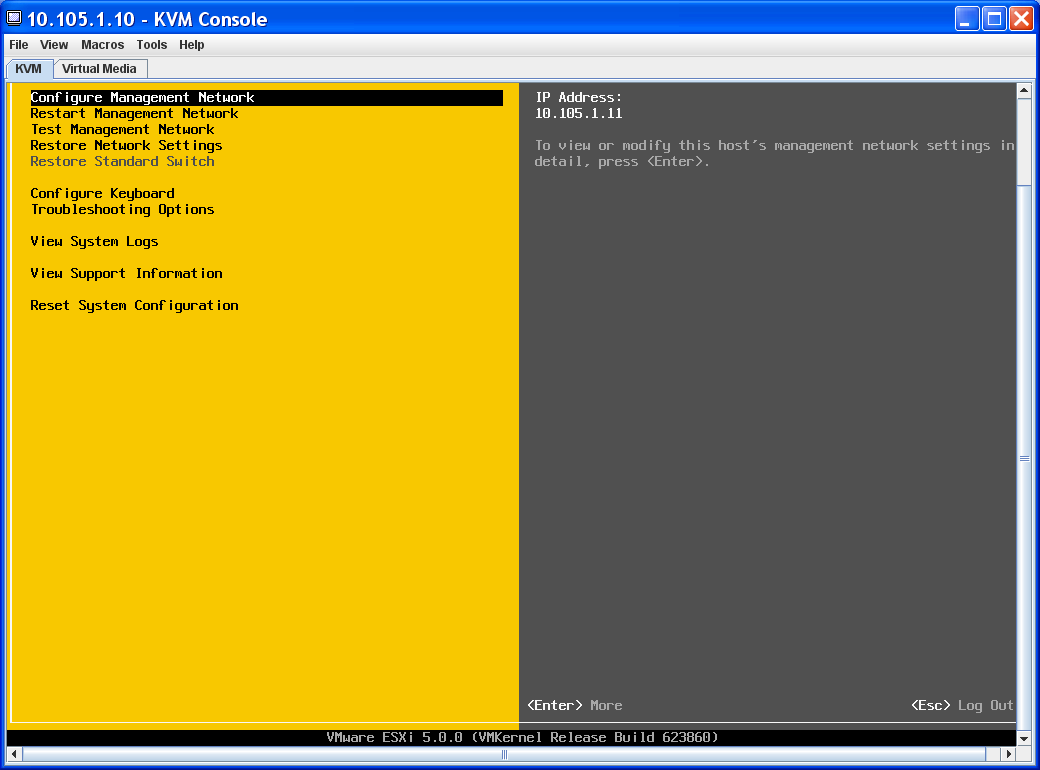
1) Access the IMC web interface (<http://10.105.1.10>) , login with default (admin/password) and click on “Launch KVM Console”



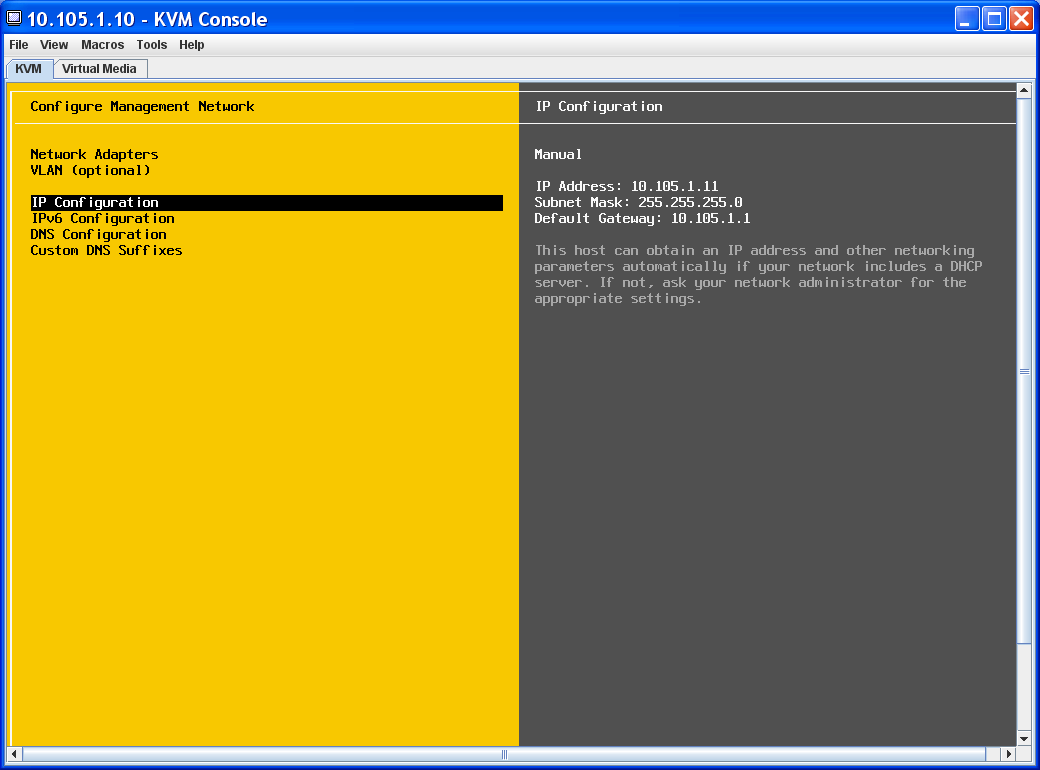
2) Install the Java Plugin if prompted and press F2



3) Press F2 again and login to the ESXi console default is (root/password), select “Configure Management Network”



4) Select IP configuration and enter the IP information



# VMware vSphere Client

1) Install vSphere client version on the PC

2) Launch vSphere client and access the ESXi Hypervisor

IP Address 🡪10.105.1.11

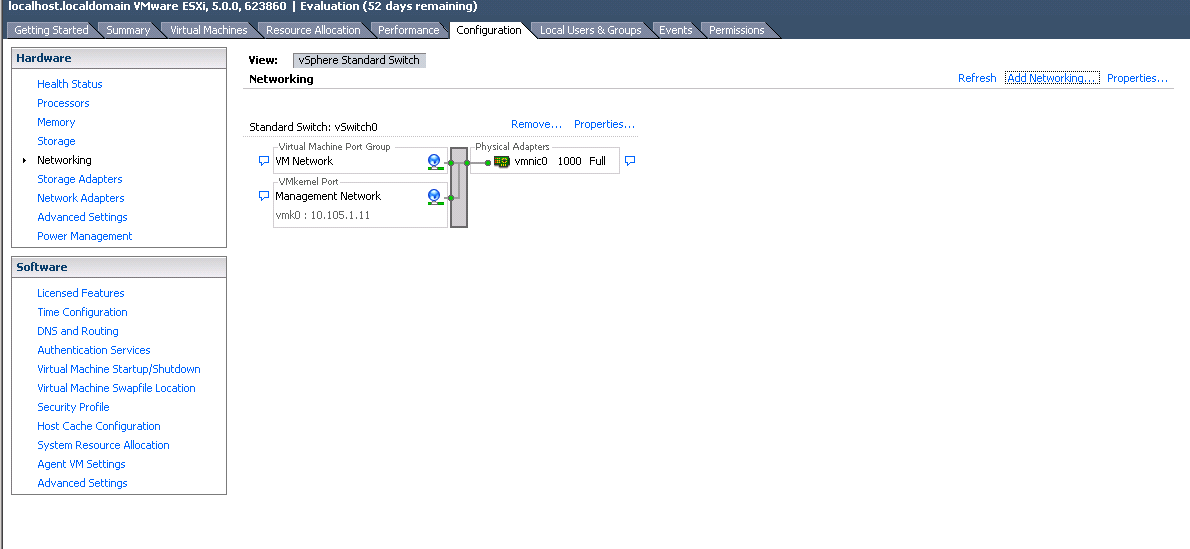
User 🡪 root /<password>

UCS-E Network Interfaces

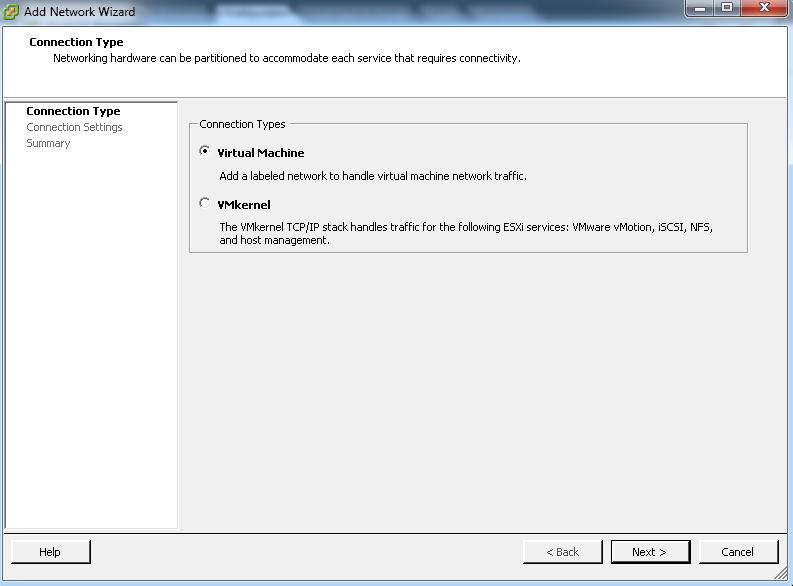
|  |  |  |
| --- | --- | --- |
| UCSE Ports | VMware ESXi | Description |
| M |  | Dedicated CIMC port |
| Console | vmnic0 | backplane PCIe interface/ MGF interface (Router Internal) |
| GE1 | vmnic1 | Backplane MGF interface (Router Internal) |
| GE2 | vmnic2 | external GE2 port |
| GE3 | vmnic3 | external GE3 port (Double Wide only) |

## ESXi Network Configuration:

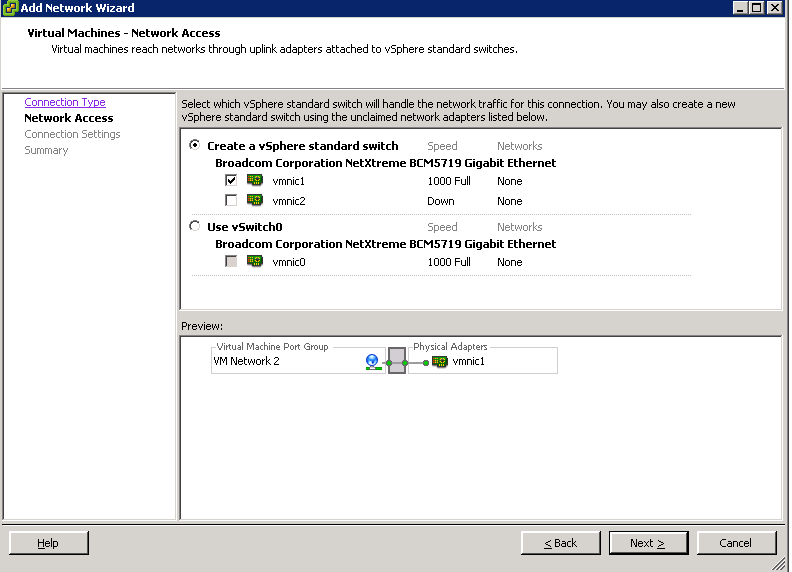
1) Click on the Configuration🡪Networking and Add Networking



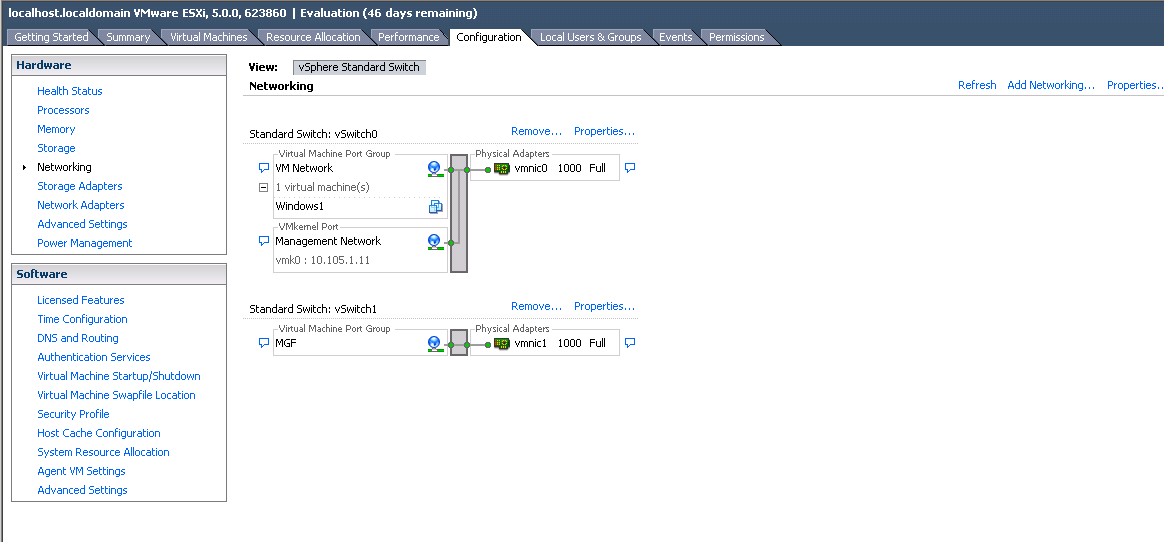
Select “Virtual Machine”



Select “vmnic1” to use GE1(MGF) interface



Configure a label for the network and click “Next” and “Finish”

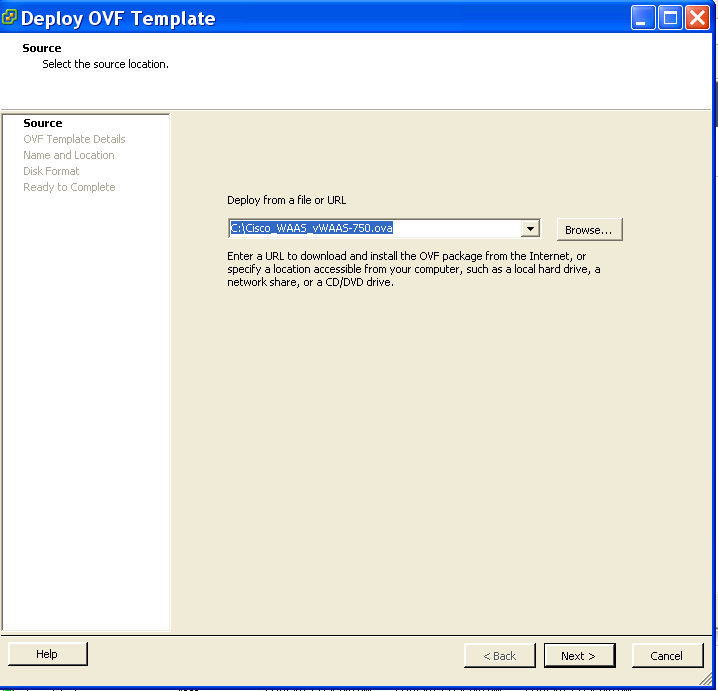


# vWAAS Installation:

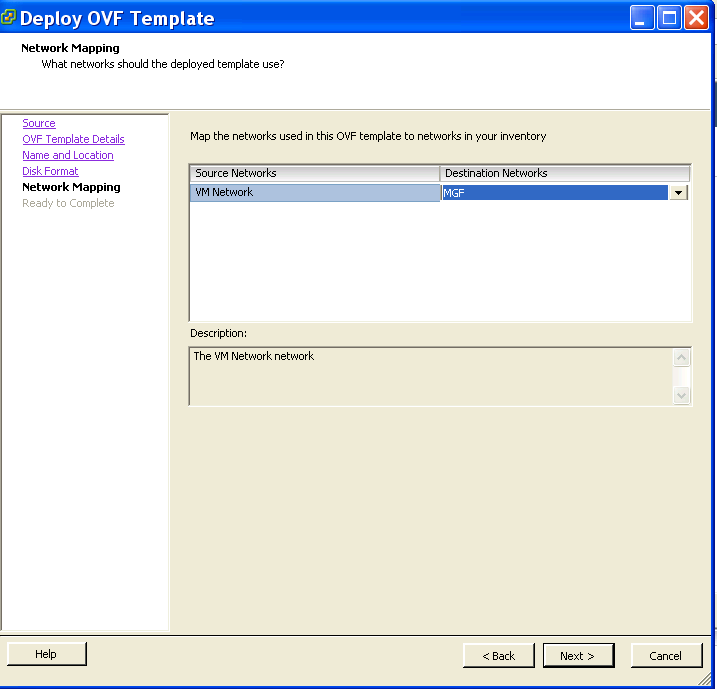
Download vWAAS OVA file from CCO or pull it off the DVD and copy it to the PC with vSphere client.

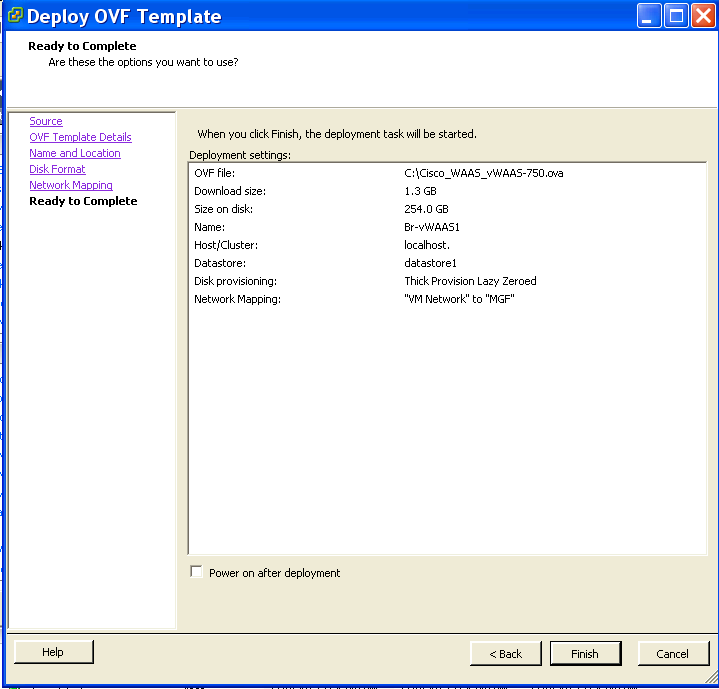
Install Steps:

1) Click on File🡪 Deploy OVF Template on the vSphere Client



2) Select “Thick provisioned format” and configure the networks (vWAAS should be mapped to the “MGF” profile)





# 

# ISR-G2 or ISR-4K WCCP Configuration

#Enable WCCP globally

!

ip wccp 61

ip wccp 62

**!(Enable WCCP 61 redirect in on the LAN interface)**

interface GigabitEthernet0/1

description LAN

ip address 192.168.3.1 255.255.255.0

ip wccp 61 redirect in

**!(Enable WCCP 62 redirect in on the WAN interface)**

interface GigabitEthernet0/0

description WAN

ip address 10.104.81.10 255.255.255.252

ip wccp 62 redirect in

# WAAS Configuration for WCCP:

If the ISR-G2 will be configured with other IWAN services, specifically IOS Zone Based Firewall, and Pfr, you must configure WAAS for L3 based WCCP (WCCP-GRE redirect).

Also note that L2 redirect is not supported with “ip unnumbered” configured in the “vlan 1” interface used.

If neither, ZBFW or Pfr are going to be used, then L2-redirect should be leveraged (default WAAS config for WCCP). For L2-redirect the vlan interface should be configured with an IP address, example was given at the beginning of the document.

!WAAS configuration

interception-method wccp

interface virtual 1/0

ip address 172.25.60.12 255.255.255.0

ip default-gateway 172.25.60.1

wccp router-list 1 172.25.60.1

**!L2 redirection configuration option**

wccp tcp-promiscuous service-pair 61 62

router-list-num 1

enable

**!L3 / GRE redirection configuration option**

wccp tcp-promiscuous service-pair 61 62

router-list-num 1

redirect-method gre

egress-method ip-forwarding

enable

# ISR-4K AppNav-XE Configuration

An option you have with the ISR-4K is to leverage AppNav-XE, which is actually the preferred redirection mechanism especially in the context of an IWAN deployment. You have 2 options to configure AppNav-XE on the 4K; via the CLI, or register the 4K to the WAAS Central Manager (WCM) and configure it via the AppNav Wizard. Both have advantages and disadvantages.

The CLI based method doesn’t consume resources on the WCM. However, will require CLI based administration if changes are required. The GUI based method consumes extra device resources on the WCM so careful planning is needed to make sure you are within the limits of your specific WCM. However, the administration and monitoring of the health of traffic redirection and optimization is now in place instead of being split between the CLI and GUI.

Below shows you the default AppNav configuration that would happen after you use the WCM AppNav wizard, which could be cut and pasted into the CLI (remember to change your IP’s).

**!Default ACLs & Class Maps**

ip access-list extended AUTOWAAS

permit tcp any any

ip access-list extended CIFS

permit tcp any any eq 139

permit tcp any any eq 445

ip access-list extended Citrix-CGP

permit tcp any any eq 2598

ip access-list extended Citrix-ICA

permit tcp any any eq 1494

ip access-list extended EPMAP

permit tcp any any eq msrpc

ip access-list extended HTTP

permit tcp any any eq www

permit tcp any any eq 3218

permit tcp any any eq 8000

permit tcp any any eq 8080

permit tcp any any eq 8088

ip access-list extended HTTPS

permit tcp any any eq 443

ip access-list extended NFS

permit tcp any any eq 2049

ip access-list extended RTSP

permit tcp any any eq 554

permit tcp any any eq 8554

ip access-list extended SN\_OR\_WCM

permit tcp host 172.16.10.10 any

permit tcp any host 172.16.10.10

permit tcp host 192.168.2.10 any

permit tcp any host 192.168.2.10

class-map type appnav match-any RTSP

match access-group name RTSP

class-map type appnav match-any AUTOWAAS

match access-group name AUTOWAAS

class-map type appnav match-any MAPI

match protocol mapi

class-map type appnav match-any HTTP

match access-group name HTTP

class-map type appnav match-any CIFS

match access-group name CIFS

class-map type appnav match-any Citrix-CGP

match access-group name Citrix-CGP

class-map type appnav match-any EPMAP

match access-group name EPMAP

class-map type appnav match-any HTTPS

match access-group name HTTPS

class-map type appnav match-any SN\_OR\_WCM

match access-group name SN\_OR\_WCM

class-map type appnav match-any NFS

match access-group name NFS

class-map type appnav match-any Citrix-ICA

match access-group name Citrix-ICA

! Default AppNav Policy

policy-map type appnav AUTOWAAS

description AUTOWAAS global policy

class SN\_OR\_WCM

pass-through

class HTTP

distribute service-node-group AUTOWAAS-SNG

monitor-load http

class MAPI

distribute service-node-group AUTOWAAS-SNG

monitor-load mapi

class HTTPS

distribute service-node-group AUTOWAAS-SNG

monitor-load ssl

class CIFS

distribute service-node-group AUTOWAAS-SNG

monitor-load cifs

class Citrix-ICA

distribute service-node-group AUTOWAAS-SNG

monitor-load ica

class Citrix-CGP

distribute service-node-group AUTOWAAS-SNG

monitor-load ica

class EPMAP

distribute service-node-group AUTOWAAS-SNG

monitor-load MS-port-mapper

class NFS

distribute service-node-group AUTOWAAS-SNG

monitor-load nfs

class AUTOWAAS

distribute service-node-group AUTOWAAS-SNG

**! Assign vWAAS Instance to a WAAS Node Group**

service-insertion service-node-group AUTOWAAS-SNG

description "AUTOWAAS"

service-node **192.168.2.10**

node-discovery enable

**! Assign 4K to AppNav Controller Group**

service-insertion appnav-controller-group AUTOWAAS-SCG

description "AUTOWAAS"

appnav-controller **192.168.2.2**

**! Bind AppNav Policy to the AppNav Service Context to activate the Policy. VRF default = all VRFs**

service-insertion service-context waas/1

appnav-controller-group AUTOWAAS-SCG

service-node-group AUTOWAAS-SNG

**service-policy AUTOWAAS**

**vrf default**

enable

**! Enable Interception on the WAN Interface(s)**

interface GigabitEthernet0/0/0

description WAN Interface

ip address 100.2.2.2 255.255.255.0

**service-insertion waas**

! **Use LAN IP for AppNav Controller IP**

interface GigabitEthernet0/0/1

description LAN Interface

ip address 192.168.2.2 255.255.255.0

! **Auto-created Interfaces for traffic to/ from AppNav Controller**

interface AppNav-Compress1

ip unnumbered GigabitEthernet0/0/1

no keepalive

!

interface AppNav-UnCompress1

ip unnumbered GigabitEthernet0/0/1

no keepalive

!

# WAAS Configuration for AppNav:

!WAAS configuration

interception-method appnav-controller

interface virtual 1/0

ip address 192.168.2.10 255.255.255.0

ip default-gateway 192.168.2.2

service-insertion service-node

enable

exit

!