



No-x Linux

KECIL-KECIL CILI PADI

**OCT
24**

VSPHERE - vSHIELD ZONES FOR DUMMIES

Category: [vSphere](#)

Yesterday I spent most of the time in my office just to figure out another vSphere features called "vShield Zones". Though the test was running smoothly, the installation & configuration of vShield is not so easy & straight forward as other features that I shared before. There was quoted also in vShield documentation that "vShield Zones installation is a multi step process". To successfully install all vShield components, we have to do it in correct sequence.



What is vShield and how vShield could help us to protect our datacenter?

vShield Zones is an application

critical security component for protecting virtualized datacenters from attacks and misuse helping you achieve your compliance

Notes: Even until now I still cant list out in details the advantages of vShield except this :

- You can gain control incoming & outgoing traffic of your virtual environment
- You can monitor open & listening port & services each of your virtual machines

vShield Zones Components

The following components comprise the vShield Zones solution:

- vShield Manager: The vShield Zones management center that manages all of the distributed vShield instances. Provides for monitoring, configuration, and software updating of your vShields.
- vShield: The active security component of vShield Zones that inspects traffic flow and provides firewall protection. You install a vShield on each ESX host you want to protect. A vShield installs within the traffic path to monitor all traffic into and out of an ESX host, as well as between virtual machines on the host.

Requirements

You can get the full lists of vShield requirements from "vShield Quick Start" documentation but below is my short list :

- vSphere 4.0 environment
- Static IP (One for vShield Manager & each for vShield) – You could have multiple vShield for each vSwitch but not vShield Manager
- At least one vmnic attached per vSwitch
- vShield Manager & vShield .ovf (appliance)

Installation & Setup

Based on my previous testing, the installation & configuration process can be divided into sequence as below :

- Pre-requisite
- vShield Manager Deployment
- vShield Deployment
- vShield Manager Configuration UI
- vShield Configuration



VMWARE

\$ 610.52



SEARCH

CALENDAR

August 2010

M T W T F S S

1

2 3 4 5 6 7 8

9 10 11 12 13 14 15

16 17 18 19 20 21 22

23 24 25 26 27 28 29

30 31

« Jul

CATEGORIES

- > [FAQ](#)
- > [Linux How to](#)
- > [News](#)
- > [Nox](#)
- > [Personal](#)
- > [VMware](#)
- > [vSphere](#)

ARCHIVES

- > [August 2010](#)
- > [July 2010](#)
- > [June 2010](#)
- > [May 2010](#)
- > [April 2010](#)
- > [March 2010](#)
- > [February 2010](#)
- > [January 2010](#)
- > [December 2009](#)
- > [November 2009](#)

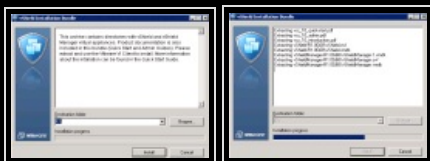
- vShield Configuration
- Virtual Machine Discovery

Pre-Requisite:

Create a port group named **"vsmgmt"** for the vShield Manager on the ESX host where the vShield Manager installed. Each installed vShield recognizes this port group name, which prevents the vShield from moving the vShield Manager virtual machine during vShield installation.

vShield Manager Deployment

First, we have to extract vShield Manager & vShield folder to your client from vShield installer as below :



Deploy vShield Manager appliance (.ovf) to your hosts by login to vCenter → File → Deploy OVF Template. Browse your vShield Manager .ovf image from your client. Don't forget to choose **"port group"** which you are going to protect and as for this tutorial I'm going to protect my **"Testing"** port group.



Once you finished importing vShield Manager appliance to your host, make sure your network adapter pointing to **"vsmgmt"** network and then power-on.



Open your console and login to your vShield Manager with username **"admin"** & password **"default"** and configure your vShield Manager network with by running **"setup"** command.

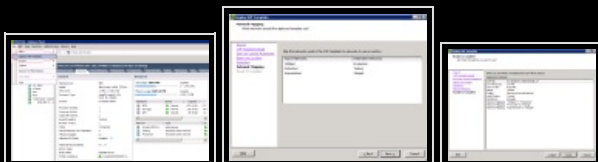
Once everything configured, test your appliance network with **"ping"** command to your gateway & other machine available on your network.



vShield Deployment

Deploy vShield .ovf template to your host with same steps as vShield Manager above. Remember, first imported vShield image to your host can become the only one or template for the next vShield deployment for other ESX hosts. This can be done via vShield Manager web access.

Note: Do not power on your vShield appliance until we finished with vShield Manager configuration.



vShield Manager Configuration UI

Now this is the time we configure vShield Manager via web access. Just open Internet Browser, then pointing the url to your vShield Manager appliance IP Address **"https://192.168.1.70"**. When come to vShield Manager Login page, please use your vShield Manager username=admin and password=default.



Next, we have to configure vShield Manager setting for vCenter under **"Configuration"**, give your vCenter IP Address, username & password then click **"Commit"**. I think this is mandatory configuration we have to set before vShield Manager can synchronize with vCenter and list out all virtual machines in vSphere inventory.

- > [October 2009](#)
- > [September 2009](#)
- > [August 2009](#)
- > [July 2009](#)
- > [June 2009](#)
- > [May 2009](#)
- > [April 2009](#)
- > [March 2009](#)
- > [February 2009](#)
- > [January 2009](#)
- > [December 2008](#)
- > [October 2008](#)
- > [September 2008](#)
- > [August 2008](#)
- > [June 2008](#)
- > [May 2008](#)
- > [April 2008](#)
- > [March 2008](#)
- > [February 2008](#)
- > [January 2008](#)
- > [December 2007](#)

LINK

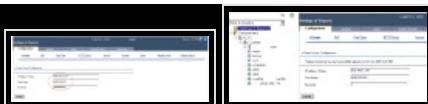
- > [Server Info](#)
- > [Minux](#)
- > [Download](#)
- > [Forum](#)
- > [LinuxForums.Org](#)

LINUX DISTRO

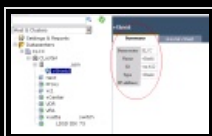
- > [Slax](#)
- > [Ubuntu](#)
- > [Slackware](#)
- > [Debian](#)
- > [PCLinuxOS](#)
- > [Opensuse](#)
- > [Knoppix](#)
- > [DSL Linux](#)
- > [Puppy Linux](#)

META

- > [Login](#)



If you click your ESX host, you should have at least one vShield appliance as shown in the picture below. Remember, we have to configure at least one vShield VM before it can track all incoming and outgoing traffic within our virtual environment.

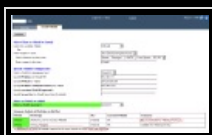


vShield Configuration

Now, we going to configure our first vShield appliance. Go to ESX host → Install vShield → Configure install parameters

You can choose your vShield from available one or clone it from template if any.

Under vSwitch to protect, choose the one which your port group sitting with. Since my "vsmgmt & Testing" port group under vSwitch1, I have to choose this one as my protected vSwitch. Once finished, click button "continue".



Review your vSwitch diagram before and after vShield installation then click "install". Few things you will notice after you installed vShield :

- New vSwitch will be created as vSwitch1_VS
- Port group (Testing) will be moved to vSwitch_VS
- All vmnic will be remained in original vSwitch1
- vShield Manager will stay in management vSwitch (vSwitch0)
- vShield VM will automatically power-on



Now, we already finished with mandatory vShield components installation and configuration. There are few others additional configuration could be done as below which will be discussed later.

- Virtual Machine Discovery (Discover your virtual machine open, listening ports & services)
- vsphere plug-in (plug-in for vSphere client)
- Custom VMWall (Firewall)

This is what you will get when you configured correctly your VMDiscovery. vShield can provide you with some useful information such as virtual machine ip address, OS, protocol, listening port, services & etc.



This is how I'm blocking incoming RDP connection for one of my win2k3 virtual machines



ariyossss

athlon_crazy 25/10/2009 2:40am

UPDATE 1

For vNetwork Distributed Switch environments, you must install a vShield manually. Manual vShield installation requires the creation of a second vNetwork Distributed Switch and two distributed virtual port (dvPort) groups. Once you create these items, you install the vShield and move the virtual machines to the second vNetwork Distributed Switch for protection. (reference : vsz 1.0 administration guide.pdf-pg32)

UPDATE 2

Layer 4 rules govern TCP and UDP transport of Layer 7, or application rules monitor traffic from ICMP, ARP, and other Layer 2 and Layer 3 protocols. You can configure Layer 2/Layer 3 rules at the datacenter level only. By default, all Layer 4 and Layer 2/Layer 3 traffic is allowed to pass. (reference : vsz 1.0 administration guide.pdf-pg41)

No Comments

Leave a comment

name (required)

email (non sarà visibile) (required)

sito web

Send

No-x Linux is proudly powered by [WordPress](#) and themed by [Mukka-mu](#)