

VIRTUAL SERVER

VIRTUAL DESKTOP

DATA CENTER

BRIANMADDEN

CHANNEL

CLOUD

**SearchVMware.com**

The Web's independent resource for managing VMware environments

ADVERTISEMENT

HOME

NEWS

TOPICS

ITKNOWLEDGE EXCHANGE

TIPS

BLOGS

MULTIMEDIA

WHITE PAPERS

EVENTS

SEARCH this site and the web

SEARCH

Search Powered by Google

SITE INDEX

ADVERTISEMENT

[Home](#) > [VMware Tips](#) > [VMware management, migration and performance](#) > [Installing and configuring vShield Zones](#)

## VMware Tips:

[EMAIL THIS](#)

### TIPS & NEWSLETTERS TOPICS

VMWARE MANAGEMENT, MIGRATION AND PERFORMANCE

### Installing and configuring vShield Zones

Eric Siebert, Contributor

07.30.2009

Rating: -4.57- (out of 5)

[Enterprise IT tips and expert advice](#) [Digg This!](#) [StumbleUpon](#) [Del.icio.us](#) [Google™](#)[VMware Migration Tips - White Papers](#)

VMware addressed the growing virtual machine (VM) security concern with two vSphere releases: VMsafe and vShield Zones. While VMsafe's application programming interfaces are designed to help third-party vendors create virtualization security products that better secure VMware ESX, vShield Zones is a security tool targets the VMware administrator.

vShield Zones is essentially a virtual firewall designed to protect VMs and analyze virtual network traffic. This three-part series describes vShield Zones, explains how to install it and provides useful management tips.

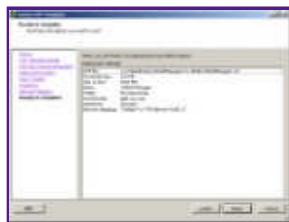
In the first part of this series, I provided [an overview of vShield Zones and explained how it works](#). Now I'll go over how to install and configure vShield Manager and the vShield agents.

Before you begin installing vShield Zones you should have the product documentation handy in case you need to refer to it, including the [vShield Zones release notes](#), [introduction to vShield Zones](#), [the Quickstart Guide](#) and the [Administration Guide](#).

Once you are ready to begin installing vShield Zones, perform the following steps.

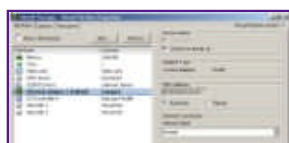
1. Download the 759 MB [ISO installation file](#) from VMware's website. vShield Zones is included on the same ISO image as VMware Data Recovery. (If you have the vSphere DVD media bundle, vShield Zones is included so there is no need to download it.)
2. You can burn the ISO file to a physical DVD or mount it to a virtual CD-ROM. The autorun program will bring up an installer wizard where you can choose to install vShield Zones. The installer extracts the Open Virtualization Format (OVF) templates/VMDK files and the PDF file documentation from the 455 MB VMware-vShieldZones.exe file to a directory that you specify.
3. Once you have extracted the files you can use them to create your vShield Manager VM appliance on a host server using the vSphere Client.
  - Launch the vSphere Client and connect to the vCenter Server (do not connect directly to the ESX/ESXi host).
  - Select File from the top menu and then the Deploy OVF Template option.
  - Select the Deploy from File option, click the Browse button and browse to the directory that you extracted the files to. The vShield Manager template is in a sub-directory called vShieldManager-R1.0G68 (the vShield-R1.0G68 directory

- is for the agent).
- Select the vShieldManager.ovf file.
- Click Next to create the new VM with a 8 GB virtual disk. The template details will display.
- Continue through the prompts selecting a destination host, data store and destination network for the new VM (if you click on the Destination Networks field you can change the value).
- Click Finish to create your new vShield Manager VM.



*Click to enlarge.*

4. Next, edit the vSwitch where the vShield Manager VM is connected. Add a new port group called vsmgmt and give it a VLAN ID if needed. This is a special port group recognized by the vShield agents that prevents them from moving the vShield Manager VM when they are installed. Once you are done editing the settings of vShield Manager VM, select the network adapter and change the network label to the newly created vsmgmt network.



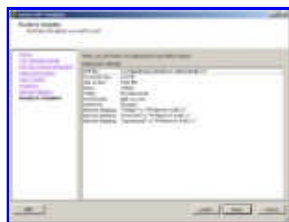
*Click to enlarge.*

5. Power on the vShield Manager VM. Once it boots, log in with 'admin' as the username and 'default' as the password. Once you are logged in you will be at a manager prompt. Type 'setup' to run the command-line interface wizard that configures the network settings. Enter your IP address information. Once completed, select 'y' to save the settings. It will prompt you to log out and back in again but that is not necessary. You should be able to ping the vShield Manager now to verify network connectivity. Type 'quit' to log out once you are done.



*Click to enlarge.*

6. Next you will need to create a new VM from the vShield agent OVF file and convert it into a template so it can be used to create vShield agents. To do this, you again use the vSphere Client.
  - Select File, Deploy OVF Template, browse to the vShield-R1.0G68 sub-directory from the extracted installation files and select the vShield.ovf file.
  - Click Next and the template details will be display. The new VM will have a 5 GB virtual disk.
  - Continue through the wizard by selecting a destination host and data store. On the network mapping screen you will see multiple network adapters (vsmgmt, protected and unprotected).
  - Accept the defaults and don't worry about changing the destination networks.
  - Once you have completed the wizard click Finish to create your new vShield agent VM. Once the VM has been created, **do not power it on**.
  - Right-click on it and select Template, then Convert to Template.



*Click to enlarge.*

7. Now it's time to log in to the vShield Manager and configure it.
  - Using a Web browser, enter the URL <https://<vShield Manager IP Address>>. A log in screen will display.
  - Log in using the username 'admin' and the password 'default'.
  - Once you are logged in, on the right pane under the Configuration tab, select vCenter, enter the IP address and log-in information for your vCenter Server, and click the Commit button.

Once you are logged in, the left pane of the inventory tree should match that of your vCenter Server. You should also go

through and configure the DNS and Date/Time settings using the links under the Configuration tab.



*Click to enlarge.*

8. Now that vShield Manager is set up and configured, it's time to deploy the vShield agents.

- Select an ESX host that you want to protect in the left pane.
- In the right pane, select the Install vShield tab.
- Click the Configure Install Parameters link. You will see a page where you specify the clone information for the new vShield agent along with its IP address and the vSwitch to protect. You have the option to either clone an existing vShield agent or choose the existing template that we created earlier.
- Choose a data store to store the new agent on and provide it a unique name.
- Choose a vSwitch for the vShield's management interface (vsmgmt) and enter the IP address information for it. In the bottom section select a vSwitch that you want to protect from the drop-down menu. The analysis at the bottom will list all your existing vSwitches and provides comments on whether or not they are candidates for protecting with vShield.
- Once you have entered all the information, click Continue to begin the installation.



*Click to enlarge.*

9. The next screen will show you a general example of the before and after configuration of the vSwitch along with the installation steps. Click the Install button at the bottom to begin the installation. The installation will proceed and you can track the progress in the Web browser or by viewing the tasks that are created in the vSphere Client.



*Click to enlarge.*

10. Once the installation is complete in the right pane listed under your host that you deployed the agent to you will see the agent's name. If you select the agent and click the VM Discovery tab you can configure the discovery process for the VMs. The discovery process analyzes the traffic for the VM and also runs a port scan to identify open ports. You can either do a manual one-time scan on specific IP addresses or set up a scheduled scan that is either periodic or continuous.



*Click to enlarge.*

### Navigating the VM Wall and VM Flow tabs

Once everything is installed and configured you can go to the VM Flow and VM Wall tabs to look at traffic analysis and firewall rules. These tabs will appear in the right pane when you select a data center, cluster, resource pool or virtual machine (not host) in the left pane.

If you select the VM Wall tab you will see that the default firewall rules are set to 'any' for the source and destination IP addresses as well as for the source and destination ports, which subsequently allows all traffic through the vShield agent. When you configure rules you will notice that the source and destination are not limited to IP addresses and can use vCenter Server objects such as the data center and cluster. You can create additional VM Wall rules by using the buttons at the top of the page or directly from the VM Flow analysis screen as seen below.



[Click to enlarge.](#)

The traffic monitoring (VM Flow) is performed at the data center, cluster, port group, VLAN, and virtual machine levels, while the blocking (VM Wall) is enforced at the data center, cluster, and VLAN levels. In the left lane, you can configure different rules for various levels and also look at traffic analysis for that level. The VM Wall rules are hierarchical so data center rules have a higher precedence than the lower level cluster rules.

It can take some time to get comfortable with vShield Zones and to get everything configured properly. The vShield Zones administration guide provides detailed instructions on setting up and using the VM Wall and VM Flow components. Stay tuned, in the final part of this series we will cover some valuable usage tips.



**Eric Siebert** is a 25-year IT veteran with experience in programming, networking, telecom and systems administration. He is a guru-status moderator on the [VMware community VMTN forums](#) and maintains [VMware-land.com](#), a VI3 information site.

Rate this Tip

(BAD) ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 (EXCELLENT)



**DISCLAIMER:** Our Tips Exchange is a forum for you to share technical advice and expertise with your peers and to learn from other enterprise IT professionals. TechTarget provides the infrastructure to facilitate this sharing of information. However, we cannot guarantee the accuracy or validity of the material submitted. You agree that your use of the Ask The Expert services and your reliance on any questions, answers, information or other materials received through this Web site is at your own risk.



[About Us](#) | [Contact Us](#) | [For Advertisers](#) | [For Business Partners](#) | [Site Index](#) | [RSS](#)

**SEARCH**

TechTarget provides technology professionals with the information they need to perform their jobs - from developing strategy, to making cost-effective purchase decisions and managing their organizations' technology projects - with its network of [technology-specific websites, events and online magazines](#).

[TechTarget Corporate Web Site](#) | [Media Kits](#) | [Reprints](#) | [Site Map](#)



All Rights Reserved, [Copyright 2007 - 2010](#), TechTarget | [Read our Privacy Policy](#)