Chapter No 11
"Configuring vShield Data Security"
In this package, you will find:

The author’s biography

A preview chapter from the book, Chapter no.11 "Configuring vShield Data Security"

A synopsis of the book’s content

Information on where to buy this book

About the Author

Mike Greer is an accomplished IT Security Practitioner and Enterprise architect with a proven track record of successful, highly-complex projects over the past 20 years. Infusing security into the core infrastructure is one of his greatest concerns while enabling customers to achieve and preserve a secure business posture. As a consultant or instructor in his professional career, he continues to provide consultancy services on a number of subject matters that include strategy, virtualization, messaging, database, and infrastructure optimization. He is the founder of Evolution Security Solutions, a start-up company focusing on strategy, virtualization, and security. His industry certifications include CCSK, CISM, CISSP, ITIL, VCP, MCSE, and MCITP.

Evolution Security Solutions provides vCIO services in addition to strategy, security, cloud, and virtualization consulting.

I'd like to thank Gloria, Declan, and Colin for their support and understanding during the course of this project.

For More Information:

VMware vSphere Security Cookbook

This book features two topics that I have a keen interest in: security and virtualization. The virtualization space can be complex in its own right, and like other technological areas, adding sufficient security can prove to be quite labor intensive and often frustrating. As technology evolves, the idea of building an infrastructure or project in a secure manner from the beginning is still somewhat novel in its approach. While more security controls are available in products, I find that such controls and features continue to be underutilized or not implemented at all.

Consider the following: on receiving a plate of pasta at your local restaurant, you are generally asked, "Would you like cheese with that?" This simple scenario and the relationship between pasta and cheese is an apt metaphor for the way security is applied to the Information Technology (IT) infrastructure in many businesses today.

My core philosophy is to help those in need. By and large, given my profession, ensuring privacy and providing some form of data security seems the logical approach. I hope this cookbook that deals with security tasks specific to the VMware vSphere 5.5 product set will enable you to get a better understanding of the virtualization environment with step-by-step instructions.

This book covers implementing specific security features of the vSphere 5.5 virtualization platform in a step-by-step format. Each topic contains a high-level overview to give context to the cookbook recipes. This book is not intended to provide reference architectures or theories behind specific security topics implemented by vSphere.

What This Book Covers

Chapter 1, Threat and Vulnerability Overview, provides you with an overview of threats and vulnerabilities specific to the virtualization infrastructure. This chapter covers a high-level review of hypervisor, virtual machine, network, storage, and physical threats and vulnerabilities.

Chapter 2, ESXi Host Security, introduces you to hardening the ESXi host from both the console and the vSphere client. This chapter covers the host firewall and configuration of services.

Chapter 3, Configuring Virtual Machine Security, focuses on security of the guest virtual machine, covering both management of the virtual machine and configuration of the virtual machine. Configuration of guest operating system security and virtual machine isolation controls are covered in this chapter.

For More Information:
Chapter 4, Configuring User Management, guides you through the secure user administration of a virtualization environment using vCenter. Topics include configuring Active Directory integration, configuring Single Sign-On, assigning permissions, and administrative roles.

Chapter 5, Configuring Network Security, introduces you to security options in the configuration of virtual network switches and port groups.

Chapter 6, Configuring Storage Security, introduces you to the configuration of storage security from a vSphere perspective. The majority of this chapter covers iSCSI authentication between source and target systems. On completion of this chapter, you will be able to configure iSCSI authentication on a vSphere 5.5 host.

Chapter 7, Configuring vShield Manager, introduces you to the installation and configuration of vShield Manager, from downloading and installing the virtual appliance to configuration of user and group access—including SSL certificate configuration.

Chapter 8, Configuring vShield App, introduces you to vShield App configuration and setup on the ESXi host. The common application firewall settings are also covered.

Chapter 9, Configuring vShield Edge, introduces you to the setup and configuration of vShield Edge. In addition, adding and managing appliances and interfaces is covered, along with VPN, firewall, and gateway configurations.

Chapter 10, Configuring vShield Endpoint, introduces you to vShield Endpoint protection, installation, and configuration, and the importance of endpoint protection in securing the virtual infrastructure.

Chapter 11, Configuring vShield Data Security, introduces you to the configuration of vShield Data Security options and policies. Customizing data policies and reports are also covered.

Chapter 12, Configuring vSphere Certificates, guides you through the tasks involved in assigning issued X.509 certificates to vSphere component services. The SSL tool is used to assign certificates to vCenter, Update Manager, Web Client, Log Manager, Inventory Manager, and Single Sign-On services.

Chapter 13, Configuring vShield VXLAN Virtual Wires, introduces the prerequisites for implementing VXLAN virtual wires, configuring virtual wires and configuring firewall rules for virtual wires.

For More Information:
In this chapter, we will cover the following recipes:

- Installing vShield Data Security
- Configuring the vShield Data Security policies
- Managing vShield Data Security reports

Introduction

The vShield Data Security component of the vShield suite is specifically designed to scan virtual machines for governance and compliance violations. vShield Data Security runs at the hypervisor level and provides Data Loss Prevention (DLP) functionality. Specific to each organization's regulatory requirements, over 80 predefined templates are included, covering compliance regulations from around the world. These predefined templates enable the discovery and reporting of sensitive data in unstructured files.

The importance of data regulation is an increasing requirement of internal and external systems. As more mission-critical applications and their associated data move out into the cloud, it is imperative to monitor data integrity and confidentiality. In a pure virtualization environment, all of the data is presumably owned by the same company with virtualization hardware stored in their datacenter. The public cloud, on the other hand, puts forth the concern of data commingling where multiple companies have data and virtual machines running on the same physical host. The ability to segment and control data and communication is key in providing a compliant environment.

For More Information:
Governance and compliance data are required to satisfy requirements such as Payment Card Industry Data Security Standard (PCI-DSS) (https://www.pcisecuritystandards.org) and Health Insurance Portability and Accountability Act (HIPAA) (http://www.hhs.gov/ocr/privacy/index.html) regulations. vShield Data Security provides a control framework that allows the scanning of virtual machines from a central point. While vShield Data Security doesn't provide an active defense mechanism, it does provide a robust set of predefined regulations and standards-based reports. These reports can be used by the compliance team to evaluate the virtual machines being monitored, or as a proof of compliance to auditors.

vShield Data Security installation and configuration requires vSphere, vShield Manager, and vShield Endpoint. The vShield driver option in VMware Tools is also required, much like vShield Endpoint Protection, in order to gain access to the data within the virtual machine.

**Installing vShield Data Security**

vShield Data Security provides the ability to identify and monitor sensitive data stored in the virtualization environment. In this recipe, we will install the vShield Data Security module using vShield Manager.

**Getting ready**

The installation of vShield Data Security requires a previously installed and running vShield Manager (Version 5.5). The vShield Manager installation steps are covered in Chapter 7, Configuring vShield Manager.

In order to proceed, we require access to vShield App through the vSphere Client plugin. The plugin can be enabled through the Plug-ins menu in vSphere Client. The client can be run on any modern Windows desktop operating system or server operating system.

> The vShield vSphere Client plugin requires Adobe Flash, which is not supported on Linux operating systems at this time.

vShield Manager must be installed and the vCenter account used for login must have Enterprise Administrator rights to vShield Manager. vShield Endpoint must be installed in order to install vShield Data Security.

For More Information:

Chapter 11

How to do it...

Perform the following steps:

1. Launch vSphere Client using an account with administrative rights, if it is not already open.
2. Navigate to Home | Inventory | Hosts and Clusters from the menu bar.
3. Navigate to Datacenter | Lab Cluster | esx5501.training.lab.
4. Select the vShield tab.
5. Click on the General option and locate vShield Data Security, and click on Install.

6. Select vShield Endpoint Installing latest version 5.1.0-01255202 and click on Install.
7. Select a Datastore local to the host if possible (in our example, we'll use datastore1).
8. Select a management port group that will allow vShield Data Security to communicate with vShield Manager (in our example, we'll use Internal Network).

For More Information:

9. Enter the proper IP information for the Data Security appliance.

10. Verify that the vShield Endpoint service is installed by ensuring the version number is displayed as shown in the following screenshot; repeat installation for any additional hosts.

How it works...

The completed installation procedure creates a vShield Data Security appliance that is dedicated to a specific host. In our example, we installed to the esx5501.training.lab ESXi host. The resulting vShield Data Security appliance is named VMWARE-Data Security-esx5501.training.lab. A vShield Data Security appliance must be installed on each ESXi host in order to access the virtual machines hosted on that particular host.

For More Information:
The vShield Data Security scan uses the vShield driver that was installed with VMware Tools in Chapter 10, Configuring vShield Endpoint. Each virtual machine must have the vShield driver installed to be successfully scanned and cataloged by vShield Data Security.

**Configuring the vShield Data Security policies**

Configuring the vShield Data Security policies requires some knowledge of current regulations that are applicable to the organization. The governance or compliance group within the organization should be able to provide guidance on which regulatory policies are required. Configuring an incorrect policy will likely cause false positives and confusion as to the secure state of the virtual machines being scanned.

Permissions are often given to the internal audit group to view policy and violation reports. For example, the auditing Active Directory group can be added to the vShield role of Auditor to accomplish this task.

The vShield Data Security policies consist of three components:

- **Regulations and standards to detect**: These predefined content blades are available for standard regulations, including PCI. Custom detection strings can also be used for detection.
- **Areas to exclude**: These components can be excluded from detection by the datacenter, cluster, or resource pool.
- **Files to scan**: The files to scan can be filtered by size, date, and file extension type.

In this recipe, we'll be adding a file to a file server that contains numbers in the Social Security Number (SSN) format. We'll then add a regulation to our scan policy for US Social Security Numbers and observe the results.

**Getting ready**

To proceed, we'll require access to vShield App through the vSphere Client plugin. The plugin can be enabled through the **Plug-ins** menu in vSphere Client. The client can be run on any modern Windows desktop operating system or server operating system.

vShield Manager must be installed and the vCenter account used for login should have Enterprise Administrator rights to vShield Manager. Refer to Chapter 7, Configuring vShield Manager, for additional information.

For More Information:

How to do it...

Perform the following steps:

1. Launch vSphere Client using an account with administrative rights, if it is not already open.
2. Navigate to Home | Inventory | Hosts and Clusters from the menu bar.
3. Navigate to Datacenter and select the vShield tab.
4. Select Policy.
5. Click on the triangle next to Regulations and standards to detect.
6. Click on Edit.
7. Click on All for a listing of all regulations.
9. Click on Next.

For More Information:
Note that this regulation does not have any options for **Set Data Pattern**. Some regulations such as **California AB-1298** have additional data patterns that can be defined.

10. Click on **Finish** to complete the rule creation. For additional rules, repeat the steps to add each additional rule.

For More Information:

11. Click on **Publish Changes** to publish the detection criteria we just added.

12. Click on **Start** to start the regulations scan.

13. Note the options for **Participating Areas** and **Files to scan**.

For More Information:
How it works...

Once the regulations and standards are added to vShield Data Security and published, a scan can be run to detect any violations present within the protected virtual machines. Multiple regulations can also be added to run concurrently. Applicable regulations to your organization should be added during this step to ensure compliance.

The participating area option allows different areas or groups of objects to be excluded from the scan. Currently, the tool does not support enabling different regulations and standards on a per group basis. In other words, a scan for HIPAA on a selected group of virtual machines and a PCI-DSS scan on an alternate group of virtual machines cannot take place simultaneously without reconfiguration after each scan.

The default listing in Files to scan covers the most common file extensions. Specifying files to monitor provides options for the conditional monitoring of files based on the size, last date modified, and file extension type. The default setting is the file extension type and is populated with common file extensions used by current enterprise applications.

Some regulations have an option to specify additional file characteristics through custom expressions. For example, selecting the California AB-1298 regulation will result in the following Set Data Pattern screen. This allows custom expressions to find the data formatted in a certain pattern.

Certain regulations offer the option to search for certain pattern strings through the use of expressions. Custom expressions can be created by visiting http://userguide.icu-project.org/strings/regexp.

For More Information:
Managing vShield Data Security reports

Following the configuration of a vShield Data Security policy, a scan can be initiated. Once a scan is in progress or has completed, the statistics and reporting can be viewed, utilizing the vShield Data Security reports option within vCenter.

Getting ready

To proceed, we'll require access to vShield App through the vSphere Client plugin. The plugin can be enabled through the Plug-ins menu in vSphere Client. The client can be run on any modern Windows desktop operating system or server operating system.

The vShield vSphere Client plugin requires Adobe Flash, which is not supported on Linux operating systems at this time.

VShield Manager must be installed and the vCenter account used for login should have Enterprise Administrator rights to vShield Manager.

How to do it...

Perform the following steps:

1. Launch vSphere Client using an account with administrative rights, if it is not already open.
2. Navigate to Home | Inventory | Hosts and Clusters from the menu bar.
3. Navigate to Datacenter and select the vShield tab.
4. Select Reports. We see the current Scan Statistics option along with violations reported. In this example, the SSN information in a text file on the VM File Server has been detected by the US Social Security Numbers policy.

For More Information:
Scan reports can also be downloaded in their native format of CSV for the list of violations and list of scanned VMs. Scan policies can be downloaded in the XML format.

5. From the vShield Reports screen, select Download Complete Report, as noted in the preceding image.

6. Click on Initiate Download for each report.

For More Information:  
7. Click on Download to open the save file dialog box and save each file.

8. Click on OK to close.

9. The ScannedVMs.csv downloaded file can be viewed in Excel.

10. The violations file shows the name and location of the file in violation.

How it works...

vShield Data Security reporting is straightforward in its implementation and design. As we’ve seen in our example environment, the status can be easily seen graphically in the vShield reports view with the option to see a more detailed status with a single mouse click. Basic reports in the CSV format can be downloaded and saved to a file share for periodic review.

The file used to test the US Social Security Numbers policy was simply a text file with several fictitious numbers in the format of xxx-xx-xxx. During the testing phase, both the PCI and HIPAA rules were used. However, due to the lack of detail of a valid record, a violation cannot be generated.

For More Information:

Where to buy this book


Free shipping to the US, UK, Europe and selected Asian countries. For more information, please read our shipping policy.

Alternatively, you can buy the book from Amazon, BN.com, Computer Manuals and most internet book retailers.