VMware vCloud Security

Make your datacenter secure and compliant at every level with VMware vCloud Networking and Security

Foreword by Harish Chilkoti, Staff Engineer in VMware vShield Networking R&D

Prasenjit Sarkar

[PACKT] PUBLISHING enterprise professional expertise distilled

VMware vCloud Security

Make your datacenter secure and compliant at every level with VMware vCloud Networking and Security

Prasenjit Sarkar

[PACKT] PUBLISHING enterprise professional expertise distilled

BIRMINGHAM - MUMBAI

VMware vCloud Security

First published: October 2013

Production Reference: 2171013

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham B3 2PB, UK.

ISBN 978-1-78217-096-9

www.packtpub.com

Cover Image by Aniket Sawant (aniket_sawant_photography@hotmail.com)

Credits

Author
Prasenjit Sarkar

Reviewers
Harish Chilkoti
Muhammad Zeeshan Munir
Preetam Zare

Acquisition Editors
Erol Staveley
Ashwin Nair

Commissioning Editor
Poonam Jain

Technical Editors
Krutika Parab
Hardik B. Soni

Copy Editors
Gladson Monteiro
Alfida Paiva
Mradula Hegde

Project Coordinator
Akash Poojary

Proofreader
Maria Gould

Indexer
Mariammal Chettiyar

Graphics
Ronak Dhruv
Valentina Dsilva
Disha Haria

Production Coordinator
Arvindkumar Gupta

Cover Work
Arvindkumar Gupta

Foreword

Security is the biggest concern in cloud environments for end users as well as cloud administrators. VMware has security solutions that try to solve all the security concerns.

Prasenjit is a technical evangelist who has authored some books that help readers to understand the key concepts and design considerations. Prasenjit provides the technical guidance in implementing VMware's cloud datacenters.

This book gives readers a step-by-step guide to install, configure, and understand the security in vCloud datacenters. The book starts with the basic architecture of vCloud Director and key concepts associated with it, and goes on to explain the setup and configuration of the vCloud Director. After installing vCloud Director, the book talks about how to secure the interior of your virtual datacenter using vCloud Networking and Security App. There are good details on how to manage the vCloud Networking and Security App firewall. The book then talks about how vShield Endpoint strengthens security for virtual machines by offloading antivirus and anti-malware agent processing to a dedicated Security Virtual Appliance. The book also has details about how to protect the sensitive data using VMware vCloud Networking and Security Data Security.

I believe this book would be very useful for the novice as well as the experienced reader. This is not yet another how-to book. The author has written the book based on his experience when implementing VMware's cloud datacenter, so he is aware of the challenges and issues faced when designing cloud datacenters. I hope that readers will get a thorough understanding of the cloud security configuration and that would eventually make cloud computing more secure.

Harish Chilkoti

About the Author

Prasenjit Sarkar is a senior member of the technical staff in VMware Service Provider Cloud R&D, where he provides architectural oversight and technical guidance to design, implement, and test VMware's Cloud datacenters. He is an author, R&D guy, and a blogger focusing on virtualization, cloud computing, storage, networking, and other enterprise technologies.

He has more than 10 years of expert knowledge in R&D, professional services, alliances, solution engineering, consulting, and technical sales, with expertise in architecting and deploying virtualization solutions, and rolling out new technology and solution initiatives. His primary focus is on VMware vSphere Infrastructure and the public cloud using VMware vCloud Suite.

One of his other focuses is to own the entire life cycle of a VMware-based IaaS (SDDC), in particular, vSphere, vCloud Director, vShield Manager, and vCenter Operations. He is one of the VMware vExperts in 2012 and 2013 and well known for his acclaimed virtualization blog, `http://stretch-cloud.info`. Prasenjit holds certifications from VMware, Cisco, Citrix, RedHat, Microsoft, IBM, HP, and Exin. Prior to joining VMware, Prasenjit has served other fine organizations (such as Capgemini, HP, and GE) as a solution architect and infrastructure architect.

You can follow him on Twitter at `@stretchcloud`.

Acknowledgement

I would like to thank and dedicate this book to my family. Without their endless and untiring support, this book would not have been possible.

I want to thank Michael Haines for his review and guidance. Michael is a Senior Cloud Networking and Security Architect and Engineer for the Global Technical Services Engineering team at VMware. Michael provides security architecture and development of VMware's Cloud solutions for service providers, enterprise customers, and partners throughout Europe and Asia Pacific. He is also responsible for providing deep technical expertise and interfacing directly with engineering and product Management to support and develop current and future vCloud Networking and Security products and initiatives.

About the Reviewers

Harish Chilkoti is a staff engineer at VMware. He has been with VMware since 2006. Harish joined VMware fresh out of college after completing a Bachelor's degree in Computer Science and Engineering. He has worked in all the areas related to virtual networking; server virtualization, cloud computing, and resource management to name a few. He has been part of VMware's journey from server virtualization to cloud computing. He has worked on all major product releases in VMware starting from ESX 3.0. He has a solid background in virtual networking and has seen how virtual networking evolved over a period to be known as SDN, Network Virtualization. His areas of interests are programming, virtualization, distributed systems, and networking.

Muhammad Zeeshan Munir is a freelance ICT consultant and solution architect. He has established his career as a System Administrator in 2004, and since then has acquired and executed many successful projects in the multi-million dollar ICT industry. With more than 10 years' experience, he now provides ICT consultancy services to different clients in Europe. He regularly contributes to different wikis and produces various video tutorials, which can be found on his website, `http://zee.linxsol.com/system-administration`. He has traveled all over the world and speaks English, Urdu, Punjabi, and Italian.

To my parents, who taught me how to write.

Preetam Zare is a technical architect who specializes in virtualization. He has worked in a variety of technical roles for over 13 years and achieved several industry certifications including VMware Certified Professional – Datacenter Virtualization (VCP3/4/5 – DV) and VMware Certified Advanced Professional 5 – Datacenter Design (VCAP5-DCD). He also blogs at `vcp5.wordpress.com` during his free time, and loves to share knowledge. He has been awarded vExpert by VMware in the years 2012 and 2013 for his contribution to a wider community. You can follow his blog at `vcp5.wordpress.com` and follow him on Twitter at `@techstarts`.

www.PacktPub.com

Support files, eBooks, discount offers and more

You might want to visit `www.PacktPub.com` for support files and downloads related to your book.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at `www.PacktPub.com` and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at `service@packtpub.com` for more details.

At `www.PacktPub.com`, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.

`http://PacktLib.PacktPub.com`

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can access, read and search across Packt's entire library of books.

Why Subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print and bookmark content
- On demand and accessible via web browser

Free Access for Packt account holders

If you have an account with Packt at `www.PacktPub.com`, you can use this to access PacktLib today and view nine entirely free books. Simply use your login credentials for immediate access.

Instant Updates on New Packt Books

Get notified! Find out when new books are published by following `@PacktEnterprise` on Twitter, or the *Packt Enterprise* Facebook page.

Table of Contents

Preface

Welcome to *VMware vCloud Security*. In this book, you will learn how to mitigate the security threats on a private cloud running VMware vCloud Director. This book will enable the reader with the knowledge, skills, and abilities to build a highly secured private cloud running VMware vCloud. We will also look at a detailed step-by-step coverage with screenshots, which are usually not available in Cloud Security product manuals.

You will learn how to configure and manage vCloud Networking and Security App, which is a hyper-based firewall. You will also learn how to use vShield Endpoint, which can help you to strengthen your cloud security by mitigating threats from virus and malware attack.

In the last chapter, you will learn some advanced concepts of cloud assessment for maintaining compliance standards that are available across the world. You will also learn how to run a data security scan and review the violation report that is generated by vCloud Networking and Security Data Security and take necessary action to mitigate those risks.

What this book covers

Chapter 1, *Installation and Configuration of VMware vCloud Director*, covers installing vCloud Director and configuring it for first-time use. It also introduces security roles in VMware vCloud Director, integration of LDAP servers with vCloud, and security hardening of vCloud Director.

Chapter 2, *Securing Your vCloud using vCloud Networking and Security*, will walk you through a hypervisor-based firewall that protects applications in the virtual datacenter from network-based attacks. It also focuses on creating access control policies based on logical constructs such as VMware vCenter Server containers and VMware vCloud Networking and Security Security Groups, but not just physical constructs such as IP addresses.

Chapter 3, *Mitigating Threats Using VMware vShield Endpoint*, will help you to strengthen security for virtual machines while improving performance for Endpoint protection. It also talks about vShield Endpoint that offloads antivirus and anti-malware agent processing to a dedicated Security Virtual Appliance that is delivered and supported by VMware partners. In this chapter, you will see the architecture of EPSEC and how to implement it.

Chapter 4, *Overview of VMware vCloud Networking and Security Data Security*, will talk about visibility of sensitive data stored within your organization's virtualized environments. It shows you how to use reports from data scans performed by vCloud Networking and Security Data Security, and ensures that sensitive data is adequately protected. It also shows you how to assess compliance with regulations around the world. In this chapter, you will see how to define data security policies, run scans, and analyze results.

What you need for this book

You need VMware vSphere 5.1, which includes VMware vSphere ESXi, vCenter Server, any SSH Client (Putty), and vSphere Client. Also, you need the VMware vCloud Director and vCloud Networking and Security (vCNS) product suite.

Who this book is for

This book is a valuable addition for technical professionals with Cloud Security administration skills and some amount of VMware vCloud experience, who wish to learn about advanced Cloud Networking and Security products and where they fit and how to configure them as well to mitigate risks in the VMware vCloud based private cloud.

Conventions

In this book, you will find a number of styles of text that distinguish between different kinds of information.

Code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles are shown as follows: "To prevent loading it on the next reboot, the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\vsepflt` key needs to be modified, and the value of `DWORD` changed to `4`."

Any command-line input or output is written as follows:

```
# /opt/vmware/vcloud-director/jre/bin/keytool -keystore
certificates.ks -storetype JCEKS -storepass vmware123 -genkey
-keyalg RSA -alias http
```

New terms and **important words** are shown in bold. Words that you see on the screen, in menus or dialog boxes for example, appear in the text like this: "Once you add the vCenter Server, you can see it under the **Manage & Monitor** tab.".

Warnings or important notes appear in a box like this.

Tips and tricks appear like this.

Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book—what you liked or may have disliked. Reader feedback is important for us to develop titles that you really get the most out of.

To send us general feedback, simply send an e-mail to `feedback@packtpub.com`, and mention the book title via the subject of your message.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide on `www.packtpub.com/authors`.

Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books—maybe a mistake in the text or the code—we would be grateful if you would report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting `http://www.packtpub.com/submit-errata`, selecting your book, clicking on the **errata submission form** link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded on our website, or added to any list of existing errata, under the Errata section of that title. Any existing errata can be viewed by selecting your title from `http://www.packtpub.com/support`.

Piracy

Piracy of copyright material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works, in any form, on the Internet, please provide us with the location address or website name immediately so that we can pursue a remedy.

Please contact us at `copyright@packtpub.com` with a link to the suspected pirated material.

We appreciate your help in protecting our authors, and our ability to bring you valuable content.

Questions

You can contact us at `questions@packtpub.com` if you are having a problem with any aspect of the book, and we will do our best to address it.

1
Installation and Configuration of vCloud Director

VMware provides a complete end-to-end cloud platform and solution using VMware vCloud Director, which is built on VMware technologies and solutions to deliver cloud computing. Cloud computing brought a new approach to computing that leverages efficient pooling of an on-demand, self-managed virtual infrastructure to provide resources consumable as a service.

In this chapter, we will cover the following aspects:

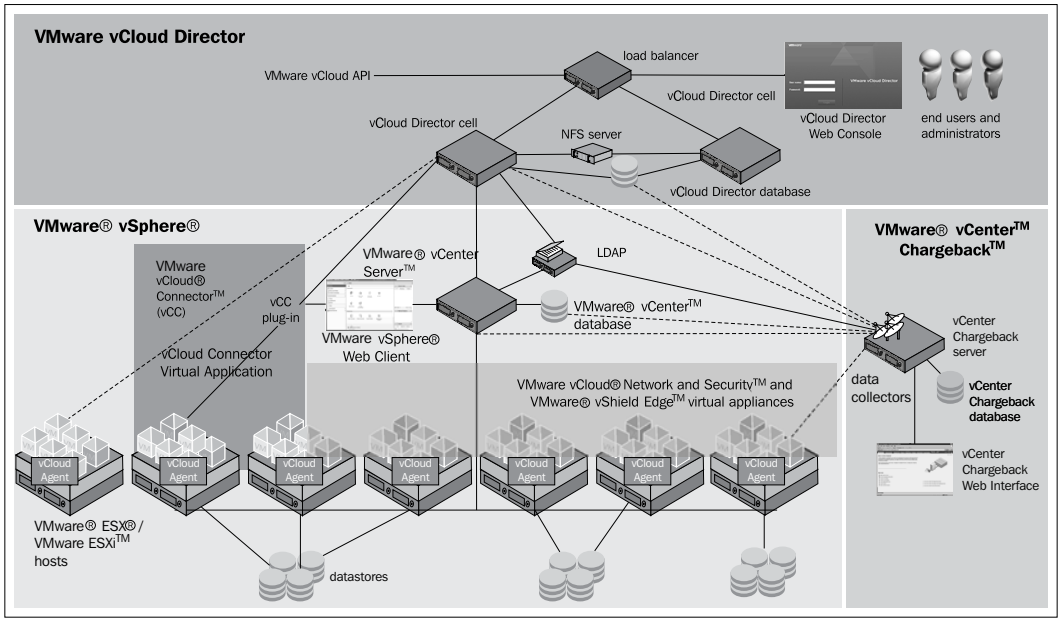
- Installing vCloud Director
- Basic vCloud configuration
- Security hardening of vCloud in a nutshell

VMware vCloud Director architecture

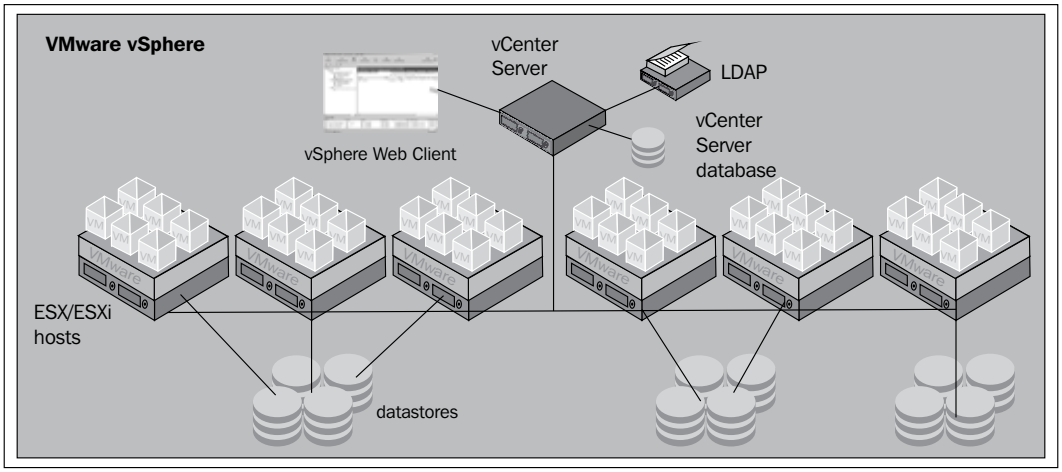
Looking at a simple high-level cloud architecture, it might contain a VMware vCloud Director server or a group comprising of multiple vCloud Director servers. Each server can run a collection of services called a vCloud Director cell.

The following figure shows the vCloud architecture and depicts the core architecture and the optional components of vCloud. Though you can have multiple vCloud Director servers in a group, all the vCloud Director servers in the group share a single vCloud Director database. To provide resources for cloud tenants, **vCloud Director** (**vCD**) connects to one or more VMware vCenter Server systems and the VMware ESXi hosts.

VMware uses one VMware vCloud Networking and Security server for each vCenter Server instance, that is, the vCloud Networking and Security manager always has a one-to-one relationship with vCenter. vCloud Networking and Security servers provide network security services and deploy VMware the vCloud Networking and Security Edge devices (virtual appliances) on demand from vCloud Director to provide static routing, VPN, NAT, DHCP, gateway, and firewall services. This not only enables vCloud Director to provide multitenancy but also a provides a foundation for Software Defined Networking (SDN), which allows network connectivity that is programmable and decoupled from the physical infrastructure. Thus it enables workloads to be placed and moved anywhere.



vCloud Director uses vSphere to provide the CPU and memory to run virtual machines. For virtual machine networking, it uses vSphere's Distributed Switches and Standard vSwitch as well. However, the vSphere Distributed Switch must be used for cross-host fencing and network pool allocation. vSphere **VMFS** (**Virtual Machine File System**) datastores provide storage for virtual machine files and other files necessary for virtual machine operations. These underlying vSphere resources are used by vCloud Director to create cloud resources. This is depicted in the following figure:



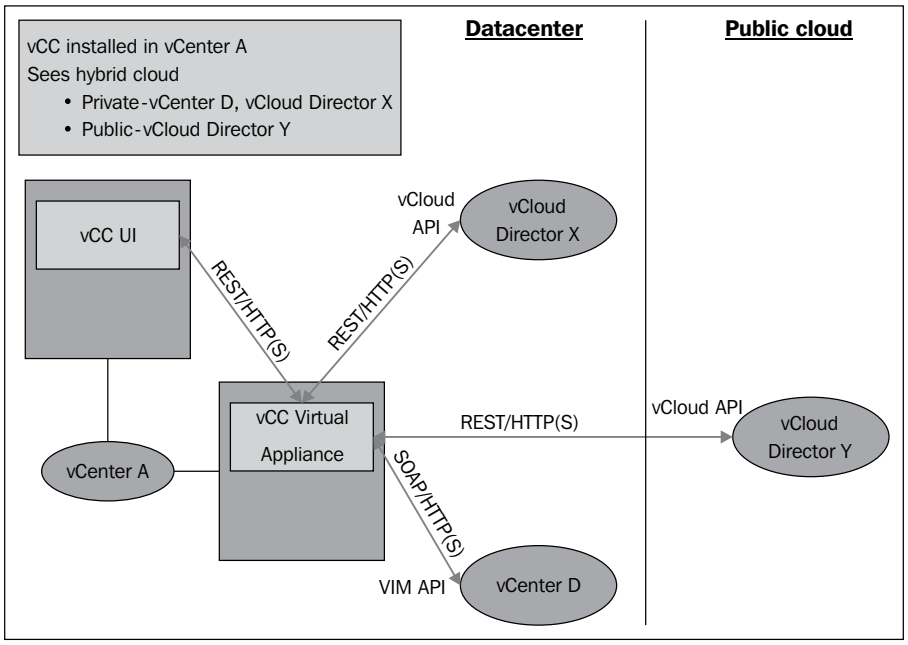
vSphere clusters should be enabled with VMware vSphere **Distributed Resource Scheduler** (**DRS**) that should set to balance the vCloud Director deployed workloads across the physically compute resources of the vSphere DRS cluster. You can define a single cluster for the cloud provider resource or use multiple vSphere resource pools to provide the cloud provider resource. Though resource pools are supported, the best way to use them is in a cluster-wise format from a scaling perspective.

Let us take a closer look at the vCloud side. A vCloud Director Server group consists of one or more vCloud Director servers, which are also called vCloud cells. These servers share a common database and are linked to the vCenter Server systems and ESXi hosts. The **vCloud Networking and Security** servers provide network services for vCloud Director. If you want to segregate and allocate vCloud resources to the organizations, there is a web-based portal for vCloud administrators to do this. This web-based portal can be used for each organization as well and can provide consumers with the means to create and manage their own virtual machines. However, access is controlled through a role-based model set up by the organization administrator. A vCloud administrator has the ability to set the lease time to control how long vApps can run and be stored.

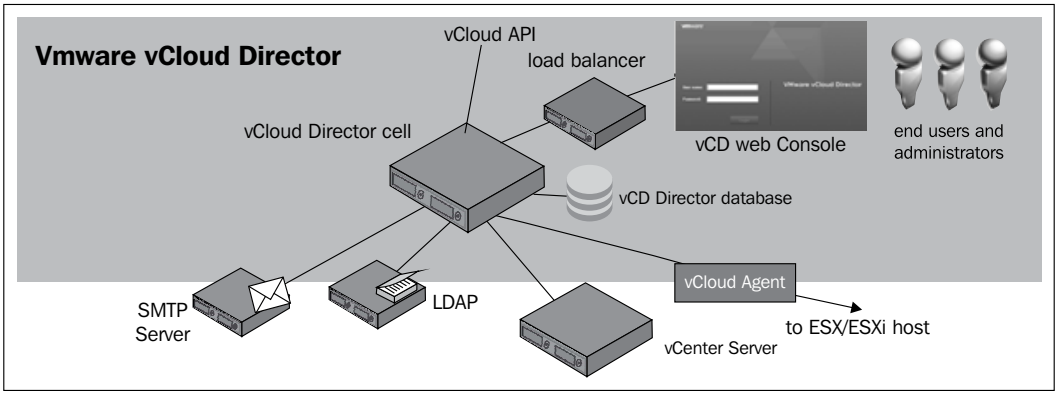
Let us look at the hybrid cloud scenario:

- vCloud Connector (vCC) is a key differentiator in the vCloud Suite for making hybrid cloud.
- vCC helps customers realize the hybrid cloud vision by providing them with a single pane of glass to view, operate, and copy VMs/vApps/templates across vSphere/vCloud Director and vCloud Service Providers.

The following diagram gives an overview of this scenario:



vCloud administrators can also set quotas that limit the number of virtual machines that an organization can have, define an isolated or shared network, have complete control of the network flow, have preestablished pools of resources, and implement security policies. The following figure shows the vCloud components and the integration of them:



Other than the core vCloud components, you can also add other VMware components to increase the capabilities or control. One example is VMware vCenter Chargeback. vCenter Chargeback provides resource metering and reporting to facilitate resource chargeback. vCenter Chargeback comprises of the vCenter Chargeback server and vCenter Chargeback data collector. Though a Chargeback component is optional, it is a must to meet the NIST (National Institute of Standards and Technology) cloud computing definition. Another additional component is VMware vCloud Connector. vCloud Connector helps facilitate the transfer of a "powered-off" vApp in the **Open Virtualization Format** (**OVF**) format from a local cloud (this could also be vSphere) to a remote cloud or a vSphere instance. vCloud Connector is a virtual appliance that is installed in vSphere and handles all the logic of dealing with other clouds. The GUI is displayed in the VMware vSphere Web Client or the C# client through the vCloud Connector browser plugin.

vCloud management and resource clusters

vCloud management cluster is a VMware vSphere High Availability (HA) and vSphere DRS (Distributed Resources Scheduler) cluster that is created to manage a vCloud architecture. A management cluster contains the standard management components, such as ESXi hosts, vCenter Server system, vCloud Director cell servers, database server/s for vCloud Director, and vCenter. A management cluster should have its own shared storage that will store the virtual machines running inside the management cluster. The management cluster should also be separated into a single physical site. We would like to emphasize that for the cloud, it is a must to have a separate management cluster. It is a best practice to place the management components in a management cluster.

You should use vSphere HA and DRS on the management cluster to provide availability for all the management components. For vSphere HA, use the Percentage of Cluster Resources Reserved admission control policy in an *n + 1* fashion instead of defining the amount of host failures a cluster can tolerate or specifying the failover hosts. This approach will help you to allow management workloads run evenly across the hosts in the cluster without the need to dedicate a host strictly for host failure situations. But this is not just limited to *n + 1*; for higher availability, you can add a host for an *n + 2* cluster, although doing so is not a requirement of the vCloud private or public service definitions.

You may be wondering why you need a vCenter Server inside your vCloud management cluster. This management vCenter Server will carry clusters that will host cloud workloads. These resources are allocated by vCloud Director as a provider datacenters. Within a distinct vSphere cluster, a provider datacenter translates into a resource pool that is created automatically by vCenter, issued on a request from vCloud Director.

Although you can physically separate the management cluster and resource cluster, it is not a good practice to do so. You should put the management cluster and vCloud consumer resources on the same physical site. If you use a single site, it ensures a consistent level of service. Otherwise, latency issues might arise if workloads must be moved from one site to another.

vCloud Director installation prerequisites

Even before you start the installation of the vCloud, you should remember that this is a complex system and thus requires proper planning for the installation. If you choose the correct steps and choices, you can save a lot of time during the installation.

For installing vCloud Director, there are lots of prerequisites that have to be in place before you can proceed further. Let us look at those:

- vCenter Server for the resource cluster should set HA, DRS, and Storage DRS.
- vCenter Server should trust their ESXi hosts.
- Use proper vSphere licenses. If you use vSphere Distributed Switch, the Enterprise Plus license is necessary. If not, you need to use the Enterprise license for DRS. For the private or public cloud, the Enterprise Plus license is a must to provide cloud-level scaling.
- vCloud Networking and Security Manager needs to be installed before installing vCloud. The vCloud Networking and Security Manager can be downloaded as an OVF appliance and can be easily deployed as a VM in your management network. The vCloud Networking and Security Manager manages the vCloud Networking and Security Edge appliances and Virtual Extensible LAN (VXLAN) (software-defined Layer 2 networking) for providing redundancy and isolation of the network inside your cluster. In other components, vShield also provides the Endpoint and Data Security components for your VMs. vCloud Networking and Security Manager should be properly licensed. A basic license for the vCloud Networking and Security is included with vCloud Director 5.1, but it does not include advanced features. If you would like to know more, take a look at this article: `http://kb.vmware.com/kb/2042799`.

- VMware strongly recommends that vCenter Server 5.1 and ESXi 5.1 be used with vCloud Director 5.1. Although earlier versions are supported, some features are not available if these earlier versions are used.
- Check the supported operating system for the vCloud Director cell. vCloud Director Server requires Linux OS. Red Hat Enterprise Linux 5 (64 bit), update 4, 5, or 6 is supported. In addition, Red Hat Enterprise Linux 6 (64 bit), update 1 or 2 is supported.
- The minimum hardware requirement for a vCloud Director cell requires 950 MB free on disk and 1 GB of memory (RAM). For better performance, 2 GB of RAM is recommended as with 1 GB RAM, it sometimes becomes irresponsive.
- The minimum Java version required for the cell is Java Runtime Environment (JRE) 1.6.0 update 10 or later. Only the 32-bit version is supported.
- vCloud Director requires Adobe Flash Player version.
- The database that will be used by vCloud Director must be created before installing the first vCloud Director cell.
- Before configuring vCloud Director, you must install security certificates.
- You must use the JRE `keytool` command to create your certificate requests.
- Transfer Server Storage is used as a temporary storage for uploads and downloads. It must be mounted at `$VCLOUD_HOME/data/transfer`.
- On the internal networks, only a few ports should be open for vCloud Director servers. See the *VMware knowledge base article 1030816* at `http://kb.vmware.com/kb/1030816`.

For more information, please see the *VMware vCloud Director 5.1 Documentation Center* at `http://pubs.vmware.com/vcd-51/index.jsp`.

Preparing for installation

vCloud Director uses both Microsoft SQL Server and Oracle Database. In this section, we will consider SQL Server only. VMware suggests that a database server configured with 16 GB of memory, 100 GB of storage, and four CPUs should be adequate for most vCloud Director clusters.

SQL Server databases have specific configuration requirements when you use them with vCloud Director. Install and configure a database instance, and create the vCloud Director database user account before you install vCloud Director.

The vCloud Director database performance is an important factor in the overall vCloud Director performance and scalability. vCloud Director uses the SQL Server `tempdb` file when storing large result sets, sorting data, and managing data that is being concurrently read and modified. This file can grow significantly when vCloud Director experiences a heavy concurrent load. It is a good practice to create the `tempdb` file on a dedicated volume that has fast read/write performance. To do so, follow the given steps:

1. Create the master instance.
    - The following script creates the database and log files, specifying the proper collation sequence:

```
USE [master]
GO
CREATE DATABASE [vcloud] ON PRIMARY
(NAME = N'vcloud', FILENAME = N'C:\vcloud.mdf', SIZE =
100MB, FILEGROWTH = 10%)
LOG ON
(NAME = N'vcdb_log', FILENAME = N'C:\vcloud.ldf', SIZE =
1MB, FILEGROWTH = 10%)
COLLATE Latin1_General_CS_AS
GO
```

    - The values shown for `SIZE` are suggestions. You might need to use larger values.

2. Set the transaction isolation level.
    - The following script sets the database isolation level to `READ_COMMITTED_SNAPSHOT`:

```
USE [vcloud]
GO
ALTER DATABASE [vcloud] SET SINGLE_USER WITH ROLLBACK
IMMEDIATE;
ALTER DATABASE [vcloud] SET ALLOW_SNAPSHOT_ISOLATION ON;
ALTER DATABASE [vcloud] SET READ_COMMITTED_SNAPSHOT ON WITH
NO_WAIT;
ALTER DATABASE [vcloud] SET MULTI_USER;
GO
```

3. Create the vCloud Director database user account.
    - The following script creates the database username `vcloud` with the password `vcloudpas`:

```
USE [vcloud]
GO
CREATE LOGIN [vcloud] WITH PASSWORD = 'vcloudpass',
DEFAULT_DATABASE =[vcloud],
DEFAULT_LANGUAGE =[us_english], CHECK_POLICY=OFF
GO
CREATE USER [vcloud] for LOGIN [vcloud]
GO
```

4. Assign permissions to the vCloud Director database user account.
    - The following script assigns the `db_owner` role to the database user created in step 3:

```
USE [vcloud]
GO
sp_addrolemember [db_owner], [vcloud]
GO
```

Installing vCloud Director

The vCloud Director installer verifies that the target server meets all the platform prerequisites and installs the vCloud Director software on it. The vCloud Director software is distributed as a digitally signed Linux-executable file named `vmware-vcloud-director-5.1.0-nnnnnn.bin`, where `nnnnnn` represents a build number. You should first upload this bin file to the vCloud Director VM. Let's get started:

1. Log in to the target server using SSH as the root user.
2. Change the folder where you have uploaded the bin file with the following command:

```
# cd <Path>
```

3. Enable the installation file for execution as this installation file requires permission to execute:

   # chmod u + x installation-file

```
[root@vcd-cell1         ]#
[root@vcd-cell1         ]# chmod u+x vmware-vcloud-director-5.1.0-810718.bin
[root@vcd-cell1         ]#
[root@vcd-cell1         ]# ls -la
total 281664
drwxr-xr-x  3 root root      4096     17 03:20 .
drwxr-xr-x 28 root root      4096     18 02:58 ..
-rw-r--r--  1 root root        75      6 06:47 MD5Sums.txt
drwxr-xr-x  2 root root      4096      8 04:42    Certs
-r-xr-xr-x  1 root root 288115734     17 03:20 vmware-vcloud-director-5.1.0-810718.bin
[root@vcd-cell1         ]#
[root@vcd-cell1         ]#
```

4. Run the installation file:

   # ./vmware-vcloud-director-5.1.0-810718.bin

```
[root@vcd-cell1         ]#
[root@vcd-cell1         ]# ./vmware-vcloud-director-5.1.0-810718.bin
Checking architecture...done
Checking for a supported Linux distribution...Detected Red Hat Linux system
done
Checking for necessary RPM prerequisites...done
Checking free disk space...done
Extracting VMware vCloud Director. Please wait, this could take a few minutes...
vmware-vcloud-director-5.1.0-810718.x86_64.rpm
vmware-vcloud-director-rhel-5.1.0-810718.x86_64.rpm
done
Verifying RPM signatures...done
Installing the VMware vCloud Director RPMs...
warning: vmware-vcloud-director-5.1.0-810718.x86_64.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
Preparing...                ########################################### [100%]
   1:vmware-vcloud-director-########################################### [ 50%]
   2:vmware-vcloud-director ########################################### [100%]

You should now run the configuration script
(/opt/vmware/vcloud-director/bin/configure) to perform other required
post-installation configuration.

If you will be deploying a vCloud Director cluster you must mount the shared
transfer server storage prior to running the configuration script. If this
is a single server deployment no shared storage is necessary.

If you are not ready to do this right now, you may run the script later
prior to starting the vmware-vcd service.

Would you like to run the script now? (y/n)?
```

5. After the software is installed, the installer prompts you to run the configuration script, which configures the server's network and database connections.

6. For the question **Would you like to run the script now (y/n)?**, answer `n`. We will first need to create the SSL certificates for vCloud Director 5.1.

```
Would you like to run the script now? (y/n)? n

Skipping. You may run the configuration script at a later time by executing
/opt/vmware/vcloud-director/bin/configure
[root@vcd-cell1         ]#
```

At this time, we need to create the SSL/TLSv1 certificates. Cloud computing has become one of the hottest technologies today. It is being used by service providers and enterprises alike. As more and more people have been accessing cloud services via the Internet or within their corporate environments, traffic passing through the cloud has multiplied. Along with this growth and proliferation have come heightened security risks and resulting attacks to the information being shared. Security has become a paramount concern, because authenticity, confidentiality, and integrity of the information are vital and must be guaranteed.

Network security leverages numerous techniques to aid in the protection of transmitted information. Traditionally, it relies on the principles of cryptology to provide the foundation of security. This involves the conversion of information into an incomprehensible form factor that is usable only to selected recipients capable of transforming the information back into a usable form. Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL) are cryptographic protocols commonly used today to aid in network security.

Complex infrastructures such as cloud computing involve multiple connections between various hosts and external communication channels. The use of TLSv1/SSL certificates is an important tool to encrypt those connections to provide data privacy.

TLSv1/SSL certificates also provide for two-way authentication. This enables a host to validate that it is connected to the intended recipient. This decreases the ability of an imposter to intercept the information transmitted.

vCloud Director requires SSL to secure communications between clients and servers. Before you install and configure a vCloud Director Server group, you must create two certificates for each member of the group and import the certificates into the host keystores. This certificate installation requires that you create a Java keystore file using the keytool utility for certificate installation. The resulting keystore file will contain two SSL certificates along with the necessary certificates.

Each vCloud Director Server that you intend to use in a vCloud Director cluster requires two SSL certificates we just mentioned, one for each of its IP addresses. Self-signed certificates can provide a convenient way to configure SSL for vCloud Director in environments where trust concerns are minimal.

Each vCloud Director Server requires two SSL certificates, one for each of its IP addresses, in a Java keystore file. The vCloud Director installer places a copy of a keytool in `/opt/vmware/vcloud-director/jre/bin/keytool`.

The console proxy and the HTTP alias use the same hierarchy of certificates. Because this one keystore file contains both certificates, you can use this single file wherever it is needed after it has been created.

Because this file contains private keys and is protected by a single password, it is strongly recommended that you do not keep copies of this file in unsecured locations. You should maintain a copy of a keystore file only where absolutely needed.

Prerequisites

Before beginning the procedures, the following prerequisites must be fulfilled:

- Obtain the IP addresses for the vCloud Director Server and the fully qualified domain name (FQDN) for each. The configured IP addresses on the vCloud Director host can be identified through the use of the `ifconfig –a` command. The FQDN for the IP addresses can be displayed using the `nslookup_<ip address>` command, where `<ip address>` equates to a configured IP address.

  Note the FQDN names for each IP address because this name will be used for the HTTP server and console proxy service SSL certificates. Noting the IP addresses will assist in the installation of the SSL certificate.

- Access the keytool utility. This utility is installed with vCloud Director by default. It is possible to use the keytool utility on another computer that has the Java Runtime Environment (JRE) version 6 or later installed, and then import the created Java keystore file onto your vCloud Director Server.

This assumes you are using the keytool installed on your vCloud Director Server as in the following example:

1. Create an untrusted certificate for the HTTP service:

```
 # /opt/vmware/vcloud-director/jre/bin/keytool -keystore
certificates.ks -storetype JCEKS -storepass vmware123 -genkey
-keyalg RSA -alias http
```

2. Create an untrusted certificate for the proxy service console:

   ```
   # /opt/vmware/vcloud-director/jre/bin/keytool -keystore
   certificates.ks -storetype JCEKS -storepass vmware123 -genkey
   -keyalg RSA -alias consoleproxy
   ```

3. At this time, we can go back and configure vCloud Director. To run the configuration script, we now need to run the following script:

   ```
   # /opt/vmware/vcloud-director/bin/configure
   ```

   The required information is as follows:

   ```
   HTTP service IP Address:
   Remote Console Proxy IP Address:
   Java Keystore path:
   Java Keystore password:
   ```

4. Now you will be asked to configure the Syslog server. Specify the IP address and press *Enter*.
5. Enter `2` for a **Microsoft SQL Server** database type.

   The required database information is as follows:

   ```
   Database host:
   Database Port:
   Database Name:
   Database Instance:
   Database Username:
   Database Password:
   ```

```
The following database types are supported:
        1. Oracle
        2. Microsoft SQL Server
Enter the database type [default=1]: 2
Enter the host (or IP address) for the database:
Enter the database port [default=1433]:
Using default value "1433" for port.

Enter the database name [default=vcloud]:
Using default value "vcloud" for database name.

Enter the database instance [Press enter to use the server's default instance]:
Using server's default instance name.

Enter the database username: vcloud
Enter the database password:
```

It will connect to the database through JDBC and database script will run.

Once the scripts have been completed, you will be presented with the link to the vCloud Director cell. You will also be asked to start the vCloud Director service; answer `Y` to start the service, and the vCloud Director service will be started.

vCloud Director setup

Once you have completed with the vCloud Director configuration, you can use the vCloud Director Web Console to complete the initial provisioning of your cloud. However, before you use the vCloud Director Web Console, you have to go through the setup wizard. The setup wizard gathers the information that the Web Console requires before it can start. Thus, once the wizard is finished, the web console starts and displays the login screen. The vCloud Director Web Console provides a set of tools for provisioning and managing a cloud environment. It includes a quickstart feature as well that guides you through steps such as attaching vCloud Director to vCenter and creating an organization.

Open a web browser and connect to `https://<FQDN>/cloud`. (This is the web IP address.)

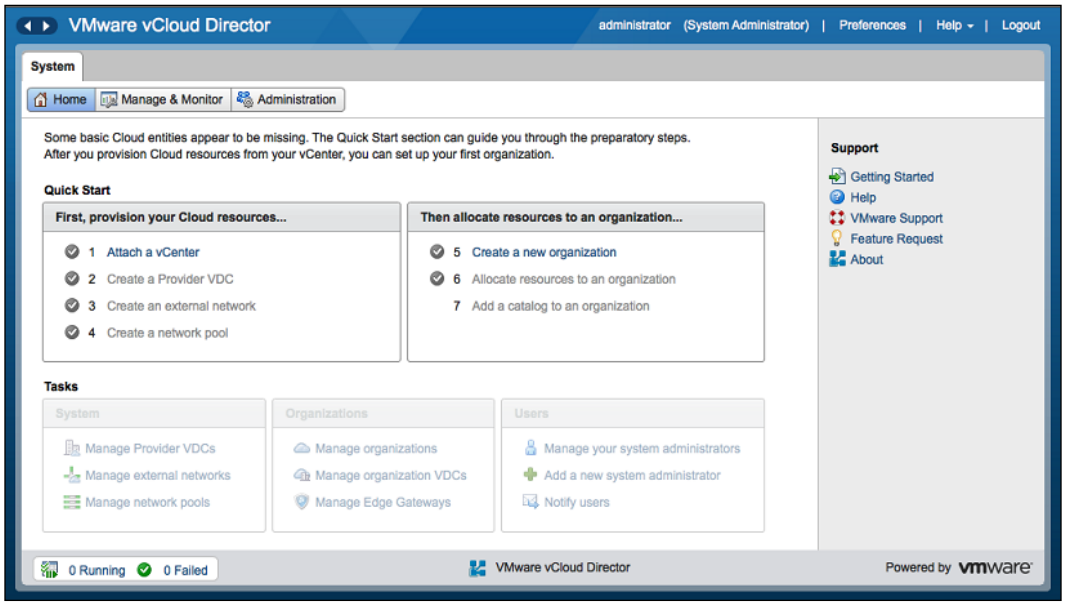
Follow the prompts to complete the setup:

1. Accept the terms of the license agreement.
2. Enter the license key.
3. Enter the administrative account username, password, full name, and e-mail address.
4. Specify the system name and the installation ID. A vCloud Director installation ID is used to ensure the network addressing uniqueness and network traffic separation between distinct vCloud Director instances that happen to utilize the same Layer 2 network.

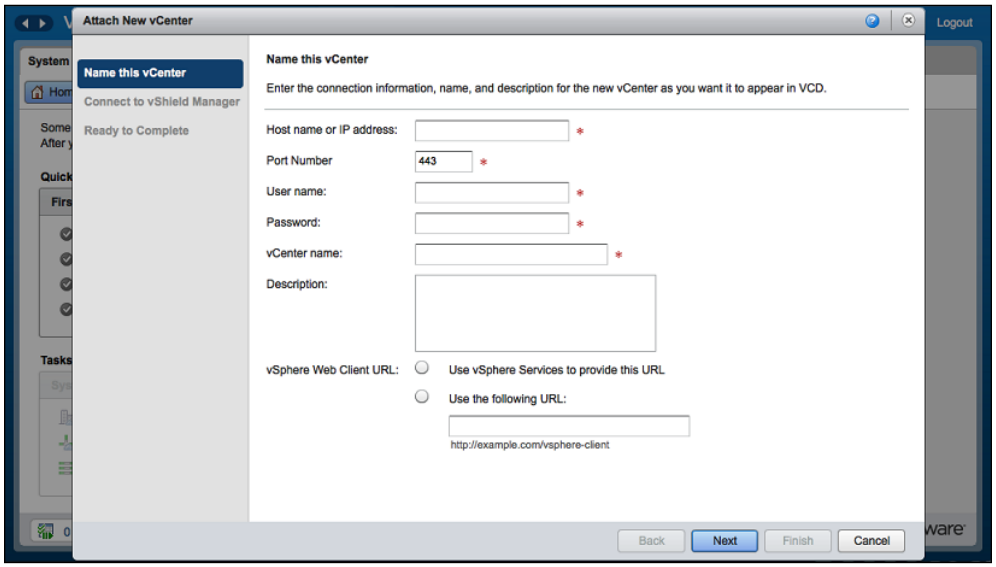
The installation ID permeates the vCloud Director system seeding the network identity of various components as mentioned in the preceding steps. For example, the MAC addresses that vCloud Director assigns VM NICs will have IID embedded. vCloud Director Network Isolation also uses this.

5. At this time, you will get a login prompt. Log in to this vCloud Director using the system admin credentials just created.

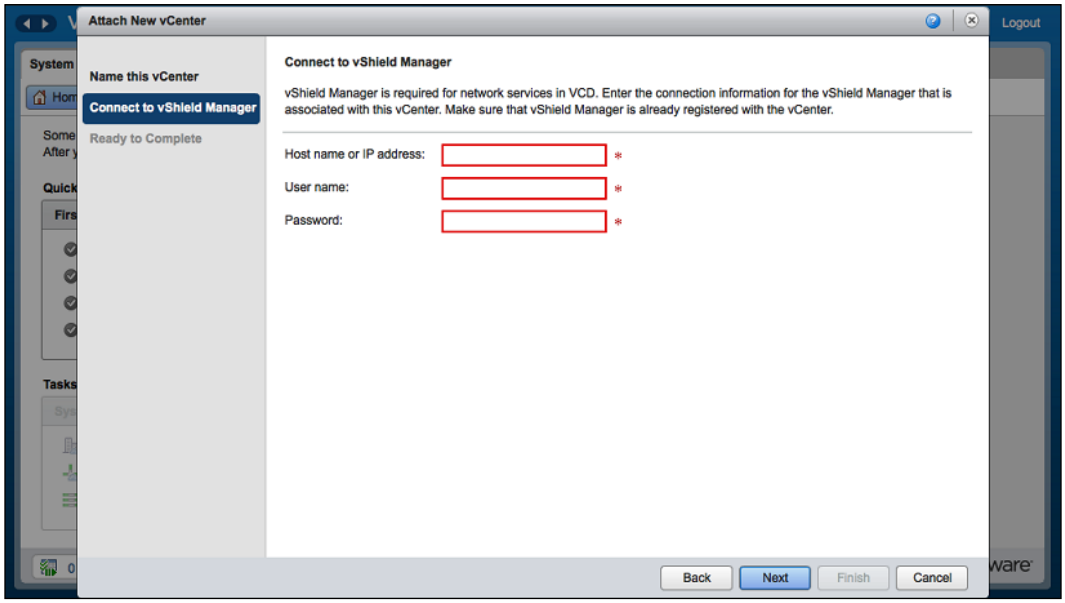
6. You will see the first screen asking you to attach a vCenter Server as shown in the following screenshot:



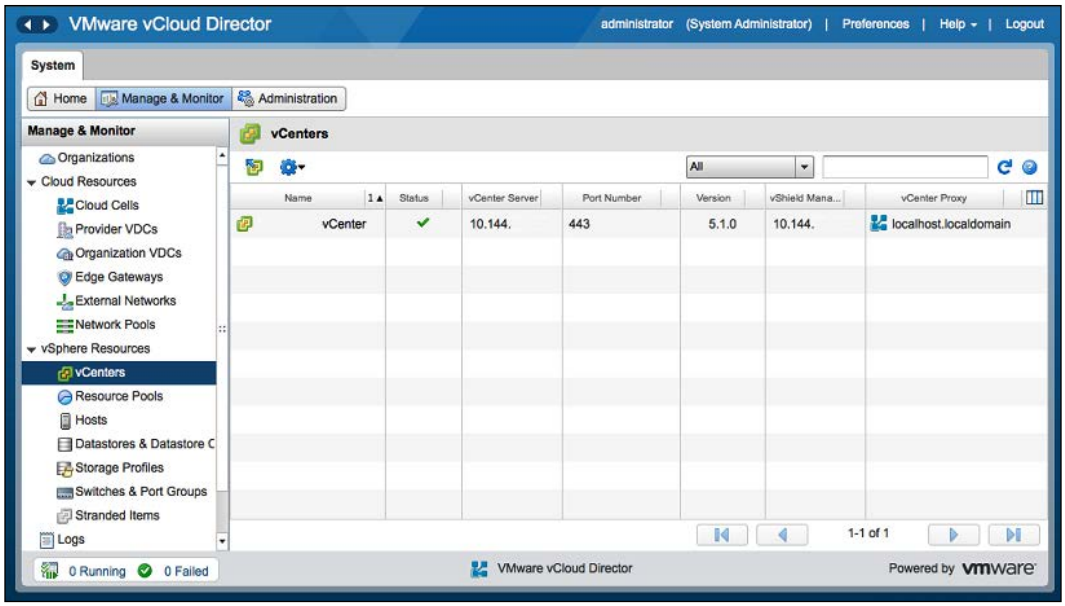
7. Click on **Attach a vCenter**.
    - You will be presented with the following screen where you have to input the vCenter Server information:



8. Specify the vCenter connection information and click on **Next**.
9. You will be presented with the following screen where you have to put the vCloud Networking and Security Manager information:



10. Specify the vCloud Networking and Security Manager server connection information and click on **Next**.
11. On the final screen, click on **Finish**.
12. Once you add the vCenter Server, you can see it under the **Manage & Monitor** tab.
13. Go to the **Manage & Monitor** tab and under the **vSphere Resources** section, click on **vCenters**. You will see a similar screen as follows:



As a prerequisite, vCenter Server has to be registered with your vCloud Networking and Security Manager. If not, you will see an error, **vShield Manager is not registered with the VC <VC Name>. Perform VC registration in vShield Manager and retry**. Open the vCloud Networking and Security Manager URL in a supported browser.

If you get this error, follow the given steps to register your vCenter Server with the vCloud Networking and Security Manager:

1. Log in to the cloud as the administrator. This should have been done as part of the initial configuration.
2. In the main **Settings and Reports** section, find the **vCenter** Server section, and you will see there is no vCenter Server registered with the vCloud Networking and Security Manager.
3. Click on the **Edit** button.
4. Specify the vCenter Server information and its credentials.
5. Click on **OK**.
6. Click on **Yes** on the security warning.
7. vCenter Server should now be configured.

vCloud Director security

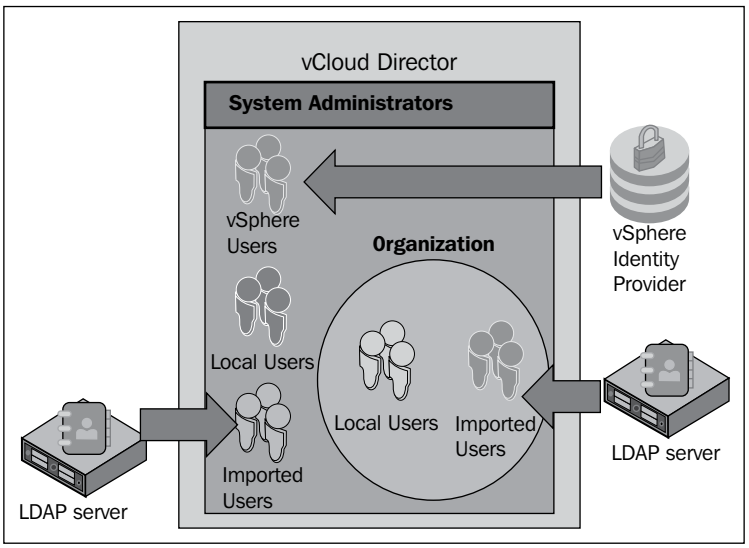
VMware vCloud Director has been designed to be a really secured environment right from the bottom to the top layers. However, it is up to the vCloud Director administrators how they can use security roles, and the LDAP integration to keep VMware vCloud secure. However, this was based in vCloud Director Version 1.5.

The vCloud Director security guide is available at `http://www.vmware.com/files/pdf/techpaper/VMW_10Q3_WP_vCloud_Director_Security.pdf`, which covers in detail how to address the security needed for specific environments.

If you look at the vCloud Director Security model and see how a user can be identified, you will see that user identification can happen from five possible locations and those are:

- Locally defined in vCloud Director (not desirable from a security standpoint)
- Imported users from a **Lightweight Directory Access Protocol** (**LDAP**) server into vCloud Director
- Locally defined users in each organization (not desirable from a security standpoint)
- Imported users from an LDAP server into a specific organization
- Imported users from either the VMware vSphere identity provider (IdP) or the external identity provider (IdP)

System administrators have been defined at the system level, and they carry full system-level access.



As VMware vSphere, vCloud Director also uses roles and permissions to determine what actions a user can perform in an organization. vCloud Director comes with a number of predefined roles with specific rights. System administrators and organization administrators have the ability to assign each user or group a role. It is possible to have the same user imported into different organizations from one LDAP system. That user can then be assigned different rights in each organization if desired. System administrators can also create roles and modify existing ones. Also all the roles can be modified by the system administrator. They can also create custom roles.

By default, vCloud Director ships with some predefined roles and those are:

- System Administrator
- Organization Administrator
- Catalog Author
- vApp Author
- vApp User
- Console Access Only

Directory (LDAP) services integration

The main benefit of using LDAP is that you can use it to provide a directory of users and groups to import into an organization. Otherwise, you have to create a user account for each user in the organization. However, it is limited to the system administrator only, that says, an organization admin cannot modify this. A system administrator can set the LDAP in such a way that each organization will have its own LDAP configuration. They should import users and groups into the organization and assign roles before they can be used.

Another good part here is that with the release of vCloud Director 5.1, it supports importing users from VMware vCenter Single Sign-On. A **Single Sign-on**, also known as SSO capability, is where a user can have a single user ID and password that works throughout the system. vCloud Director provides SSO by integrating either LDAP or vCenter SSO identity. It is a system administrator's job to import users from LDAP or vCenter SSO as vCloud Director does not import users automatically.

vCloud Director does not support hierarchical domains in LDAP. Also, vCloud Director cannot modify the information in an LDAP directory.

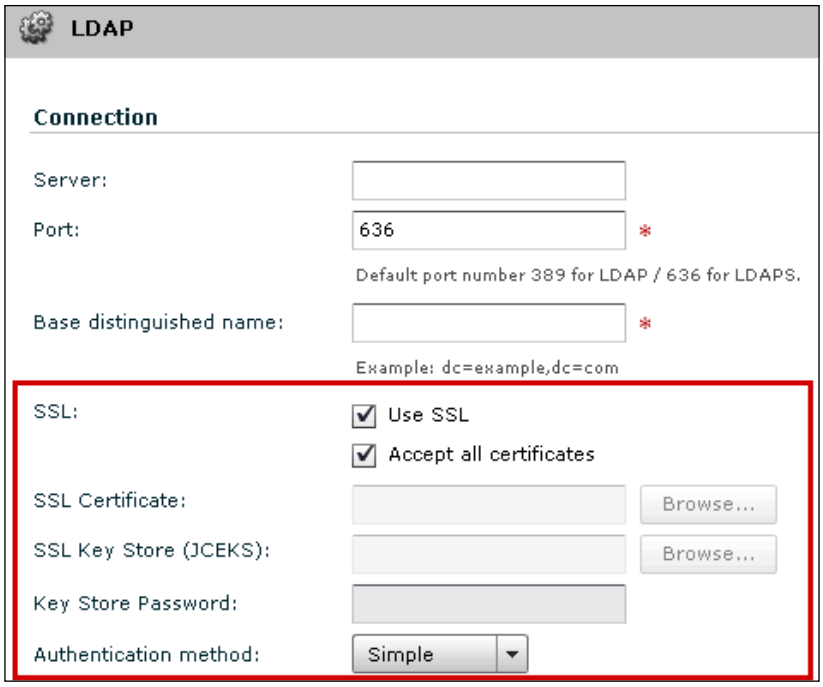
vCloud Director does not import users' passwords from external LDAP systems. Instead, vCloud Director will confirm that a password is correct when a user logs in by checking the supplied hashed password against the hashed password currently stored in the LDAP directory.

vCloud Director has the ability to use LDAP at both the system level and the organization level. At the system level, you can either connect to an external LDAP system or create and use users who are internal to vCloud Director. You can use an external LDAP system to bring in users, but VMware recommends that you create at least one system user, which is only internal. The existence of at least one internally defined system administrator allows you to log in to your vCloud Director console even if the LDAP system is offline.

There are two ways to log in to the LDAP server. One is simple authentication and the other one is with Kerberos authentication. Simple authentication is, well, simple. However, Kerberos is a ticket-based system of client and server authentication. In Kerberos, both parties must prove their identity to each other. Kerberos uses symmetric key cryptography and can also leverage public key cryptography. If you are using Kerberos authentication, you must add a Kerberos realm to the vCloud Director Server first.

If you use simple authentication without at least combining it with SSL, the user ID (DN) and the password are sent in clear text on the network.

In order to use SSL, you must select it. You must then determine whether you will automatically accept all the certificates, or you will insist on browsing to a specific certificate. Using all certificates is much easier to configure. If your LDAP server has a certificate, it is accepted automatically. The use of SSL also provides an encrypted password exchange with the LDAP server. But the certificate from the LDAP server must be located on your system (the one the vCloud Director console is running from) and you must know the location of your SSL keystore file and have the password.

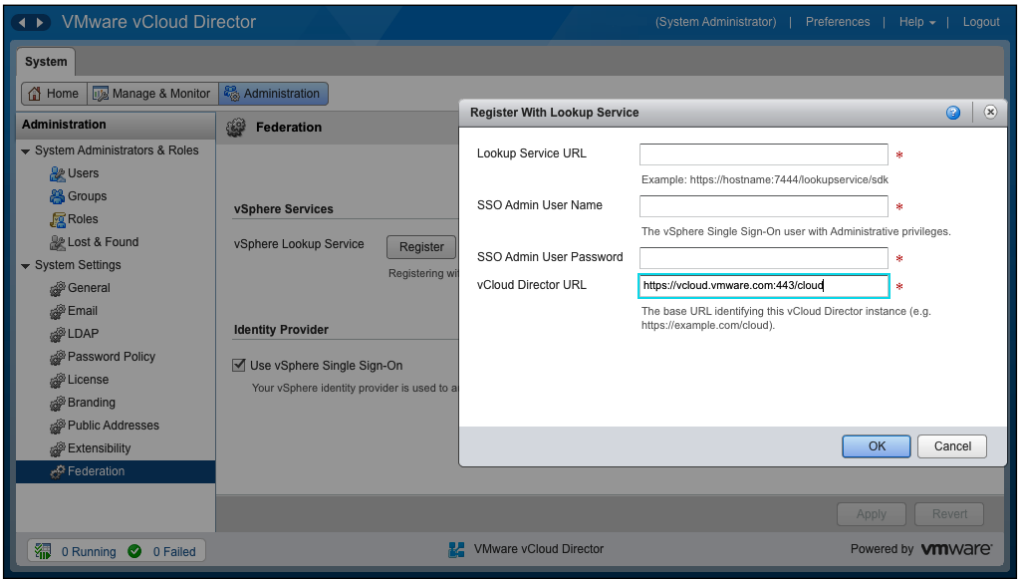


At the organization level, vCloud Director presents the following three options:

- Do not use LDAP. In this case, all the users in this organization are internally defined in the vCloud Director system.
- Use the vCloud Director system LDAP service. The organization leverages the LDAP service that has been configured at the system level. In order to leverage the system-defined LDAP, all the organization users must be defined in the same Organization Unit (OU) in the LDAP database.

- Use a custom LDAP server. A custom LDAP server allows an organization to use its own LDAP service. VMware recommends the use of custom LDAP servers in public cloud implementations.

vCloud Director system administrators are authenticated by the vSphere identity provider when you use vCenter SSO. However, as a prerequisite, vCenter SSO must be configured in vSphere. **vSphere Lookup Service** must be registered in the vCloud Director **Administration** tab under **Federation**. vCloud Director should also be configured with the vSphere Lookup Service URL. vCloud Director system administrator users must be imported (either as a user or a group) from the vSphere identity provider. Only vCloud Director's system administrator users can be authenticated through vCenter SSO.



Auditing and logging

One of the most important factors for the overall system security is to record and monitor the activities of the users. The organization maintains their compliance with rules by maintaining an audit log of significant activities. Using audit logs, an organization verifies and detects any violations and initiates remediation activities.

Audit logs can also help the organization in detecting attempts, whether successful or not, to gain illegitimate access to the system, probe its information, or disrupt its operation.

VMware vCloud Director includes the following two types of logs:

- Diagnostic logs that are maintained in each cell's log directory. You can export it to a centralized Syslog server as well
- Audit logs that are maintained in the database, and optionally, in a Syslog server

As a vCloud system administrator, you can view the system log to monitor system-level tasks that are in progress. Also, you can find and troubleshoot failed tasks as well. You can also analyze vCloud Director logs to monitor vCloud Director cells.

As a vCloud organization administrator, you can view the log for an organization to monitor organization-level tasks that are in progress. In addition, you can find and troubleshoot failed tasks.

So essentially, we are talking about system-level and organization-level tasks.

vCloud Director provides logging information for each cloud cell in the system. You can view the logs to monitor your cells and to troubleshoot issues.

You can find the logs for a cell at `/opt/vmware/cloud-director/logs`.

The following table shows the log names and their purposes:

Log name	What the log shows
`cell.log`	The console output from the vCloud Director cell
`vcloud-container-debug.log`	Debug-level log messages from the cell
`vcloud-container-info.log`	Warnings or errors encountered by the cell
`vmware-vcd-watchdog.log`	When the cell crashed, restarted, and so on
`diagnostics.log`	Diagnostics information (but this first needs to be enabled in the local logging configuration)
`YYYY_MM_DD.request.log`	HTTP request logs in the Apache common log format

Apart from the diagnostics logs in the vCloud Director, you have audit logs mentioned in the preceding table as well. However, by default, these files are not forwarded to the centralized logging server. You have to manually configure the vCloud cell to forward these to the centralized logging server.

It is recommended that you configure this option for the following reasons:

- It allows audit logs from all the cells to be viewed together at a central location at the same time.
- Database logs are not retained after 90 days, but logs transmitted via Syslog can be retained as long as desired.
- It protects the audit logs from loss on the local system due to failure, lack of disk space, compromise, and so on.
- Supports forensics operations in the face of problems as those listed previously.
- Logging to a remote system, instead of the system the cell is deployed on; provides data integrity by inhibiting tampering. Even if the cell is compromised, it does not necessarily enable access to or alteration of the audit log.
- For enabling a centralized Syslog server in vCloud Director 5.1, follow this knowledge base article from VMware, `http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1026815`.

Summary

In this chapter, we have installed VMware vCloud Director and performed a basic configuration of it. We have successfully installed and configured vCloud Director. Also, we looked into the basic security hardening aspects. We discussed basic security aspects of vCloud Director systems. This security aspect includes the user and different security roles, integrating different types of LDAP servers, and its options at various levels, which include the system level and the organization level.

In the next chapter, we will talk about VMware the vCloud Networking and Security App, and how we can integrate it to vCloud Director. We will also discuss the installation steps of the vCloud Networking and Security App, the vCloud Networking and Security App firewall management, and flow monitoring.

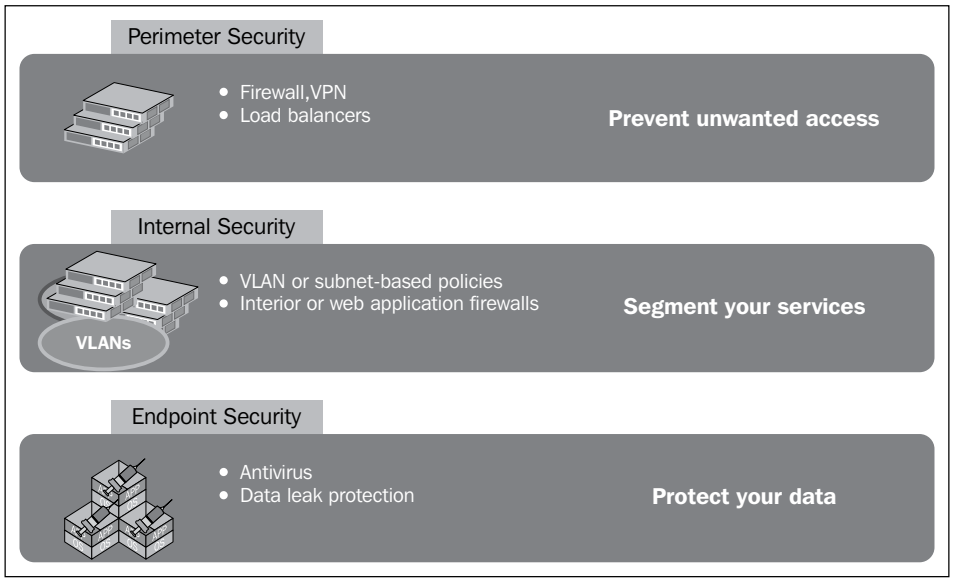
2

Securing Your vCloud Using the vCloud Networking and Security App Firewall

The general, well-accepted approach to securing IT is to employ a layered approach—shown in the following figure—often referred to as defense-in-depth. Physical datacenters have traditionally been protected using a combination of hardware appliances external to the system and agents that run within a system's operating system.

The use of technologies such as firewalls, **Intrusion Protection System** (**IPS**), and **Intrusion Detection System** (**IDS**) greatly enhances the corporate security environment when deployed and managed effectively. Inclusion of these is critical to the corporate IT defense-in-depth strategy as mentioned earlier.

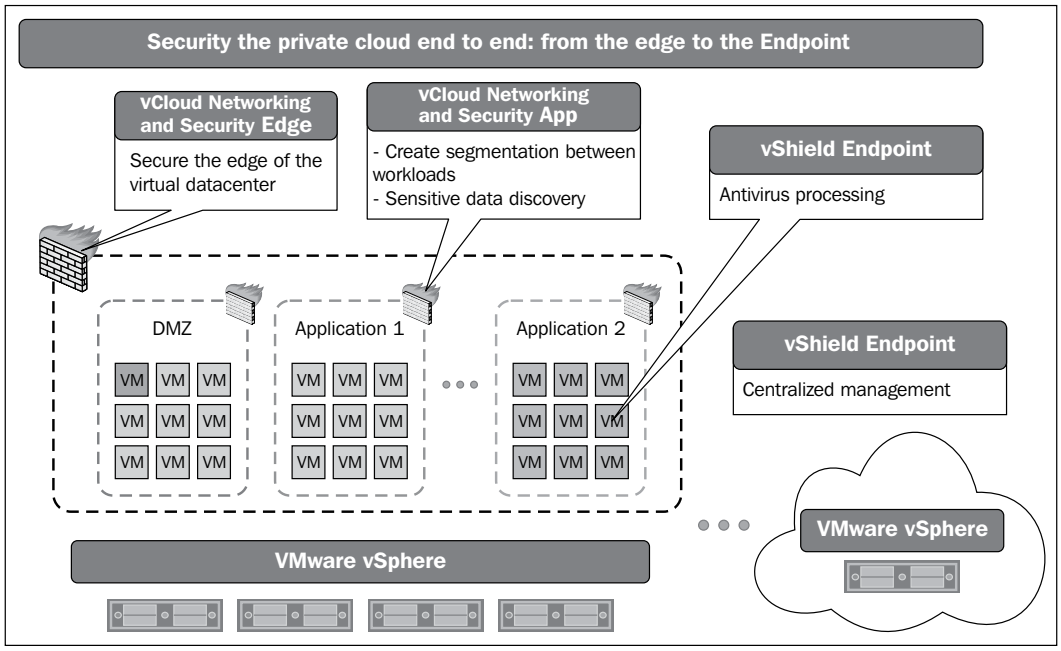
Without a doubt, this is one of the most important aspects of a security and defense-in-depth strategy. The term defense-in-depth has been used extensively in a myriad of security papers over the years in one way or another, but the key message is still the same—providing multiple levels of security.



Cloud security is a combination of security protocols, security controls, methodologies, and technologies, which protects the availability of the cloud resources and checks the confidentiality, integrity, accountability, and the use of security controls (typically involving compliance issues) of the data stored in a cloud environment. Cloud security also addresses issues of identity access management and privacy.

VMware's vCloud Networking and Security solutions including vCloud Networking and Security Edge, App, Endpoint, and Data Security provide the ability to secure the edge of **vDC** (**virtual datacenter**), protect virtual applications from network-based threats, discover sensitive data residing in virtual machines (VMs), and streamline antivirus protection for VMware View deployments by offloading antivirus processing to dedicated security VMs.

If you adopt these networking and security products, you will see that it can start securing your infrastructure almost immediately since all the underlying compute resources are already present in the vSphere environment. If you look at the traditional datacenter security aspects, these same solutions would have taken months to authorize and provision in the physical datacenter. Let us look at the overall security aspects and their components in a private cloud shown in the following figure:



In this chapter, we will talk about vCloud Networking and Security App Firewall and show you how to segment your different workload traffic and discover the application's sensitive data.

vCloud Networking and Security App Firewall – use case

vCloud Networking and Security App helps you overcome the challenges of securing the interior of your virtual datacenter.

The vCloud Networking and Security App Firewall is comprised of three entities and vCloud Networking and Security Manager, which provides centralized management for all vCloud Networking and Security products.

Within the context of vCloud Networking and Security App Firewall, the vCloud Networking and Security Manager is a centralized management console, which allows users to do the following activities:

- Defining firewall policies to control the traffic in/out of the environment
- Defining SpoofGuard policies
- Defining Namespace configuration (also known as realm)
- Viewing the historical flow data going in/out of the environment
- Managing the lifecycle of the vCloud Networking and Security App appliance

The three components of vCloud Networking and Security App Firewall are as follows:

- **The vCloud Networking and Security dvFilter module**: This module is an ESX **Loadable Kernel Module** (**LKM**) that sits in the ESX/ESXi hypervisor and provides hooks to channelize virtual machine traffic to the vCloud Networking and Security App service VM using the VMware dvfilter APIs. The LKM module is also known as fastpath, while its counterpart, the Service VM is known as slowpath.
- **The vCloud Networking and Security App Service VM**: This component is also known as VSA. It is a Service VM or an appliance that performs network traffic introspections. It reports, allows, or denies traffic for a virtual machine based on the policies configured by end user via vCloud Networking and Security Manager. The vCloud Networking and Security dvFilter module redirects all the traffic for protected VMs to this Service VM.

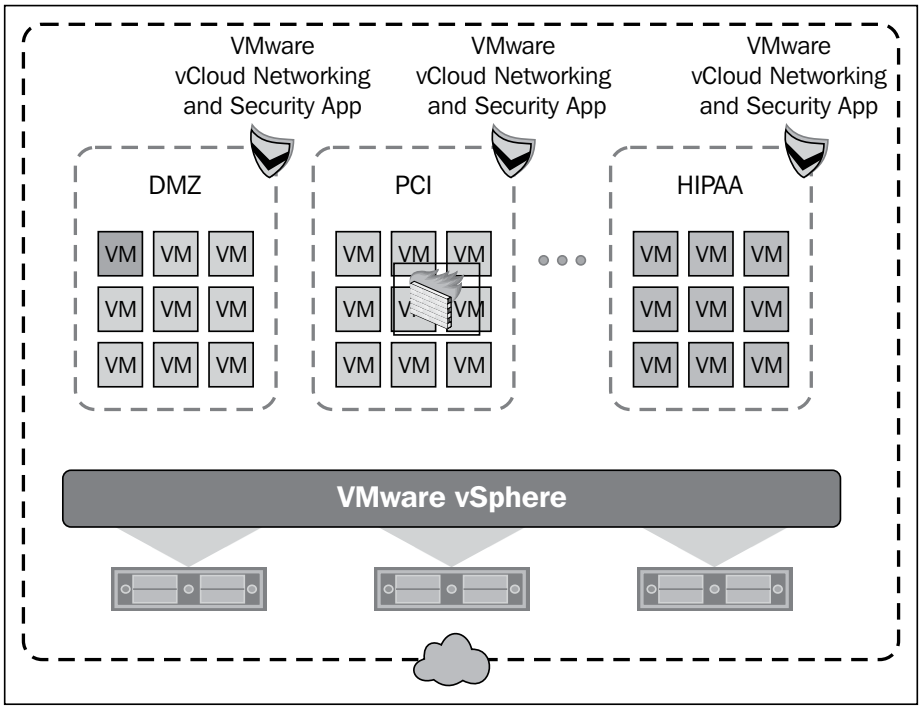
    - The vCloud Networking and Security App Service Appliance Service VM provides both control and data-path processes. The control path process, also known as Sysmgr, communicates with vCloud Networking and Security App Manager (a Java process) over a secured, encrypted channel to receive the control information, that is, firewall configurations, SpoofGuard configuration, flow configuration, and other data.

- **vCloud Networking and Security App dvFilter properties on protected virtual machines**: These properties and associated values are added to the .vmx configuration file of every vNIC of every virtual machine that is on a host where vCloud Networking and Security App has been installed. These values inform the VMs on a given ESX/ESXi host that vCloud Networking and Security App is present. All vCloud Networking and Security appliances are excluded from receiving these properties.

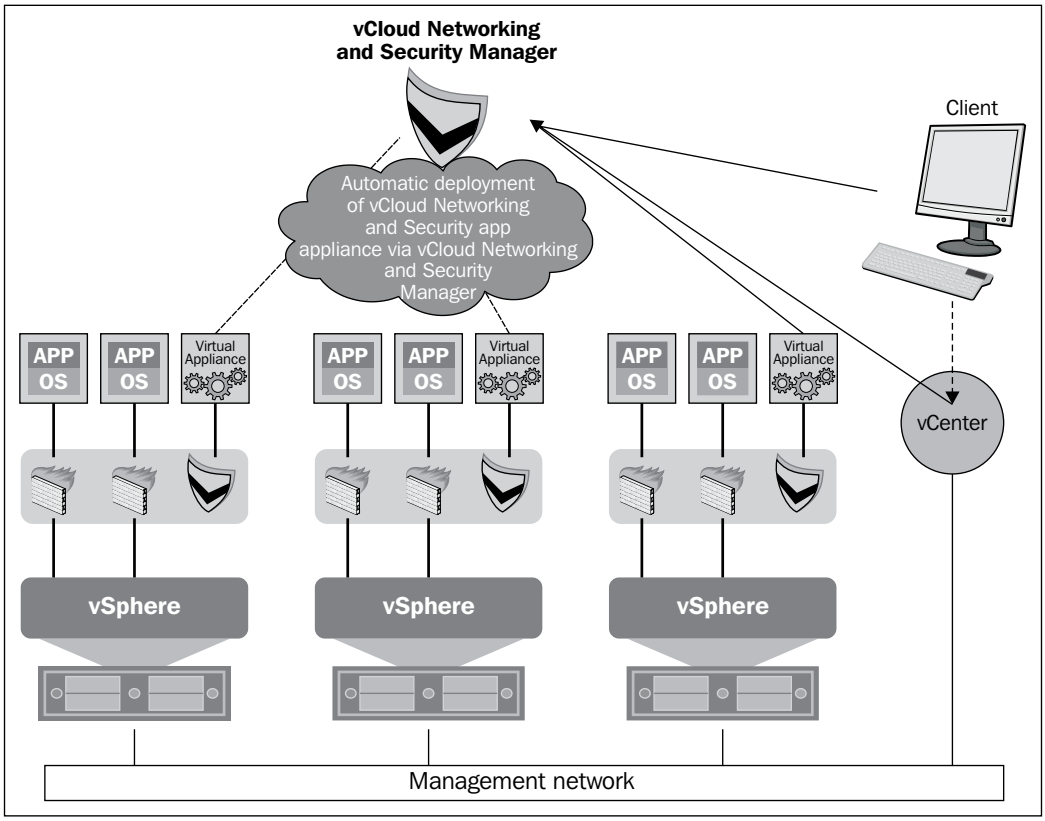
If you take a closer look at vCloud Networking and Security App, it is a software-based and protocol-based firewall app that is directly installed on the network adapter of a virtual machine and monitors all the traffic between a VM network adapter and vSwitch. It deploys as a virtual appliance. vCloud Networking and Security App is in essence a hypervisor-based firewall that protects applications in the virtual datacenter from network-based attacks. vCloud Networking and Security App is better than physically securing the virtual datacenter because it is a lot less expensive than buying a number of physical firewalls and segmenting them into different security zones. Access control policies can be created based on logical constructs, such as VMware vCenter Server containers and VMware vCloud Networking and Security Security Groups, and not just physical constructs, such as IP addresses. Another major benefit of using vCloud Networking and Security App is that, as you install vCloud Networking and Security App on each VMware ESXi host within a cluster, VMware vSphere vMotion operations work seamlessly and virtual machines remain protected as they migrate between ESXi hosts. Some of the key benefits of vCloud Networking and Security App are:

- vCloud Networking and Security App provides complete visibility and control of inter-virtual machine traffic in logical security zones (as shown in the following figure)
- vCloud Networking and Security App provides hypervisor-level introspection into the inter-VM traffic
- vCloud Networking and Security App enables multiple trust zones in the same ESXi cluster

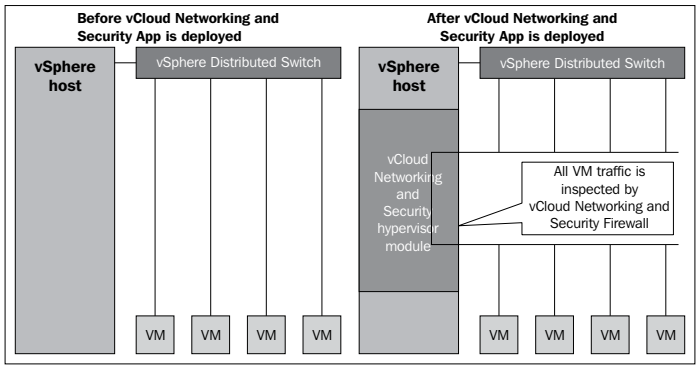
- vCloud Networking and Security App also allows you to create intuitive, business-language policies using the vCenter Server inventory for convenience



Now what you should be interested in is to understand how it works or who manages a vCloud Networking and Security App appliance and how to control the environment; this is shown in the following figure. Well, the answer is vCloud Networking and Security Manager. vCloud Networking and Security Manager is a central point of management. For an RBAC (Role-based Access Control) model, it stores flow data and manages the rule base. You can connect to vCloud Networking and Security Manager directly via the web interface or via the VMware vCenter plugin; however, it cannot be managed via the vSphere Web Client.

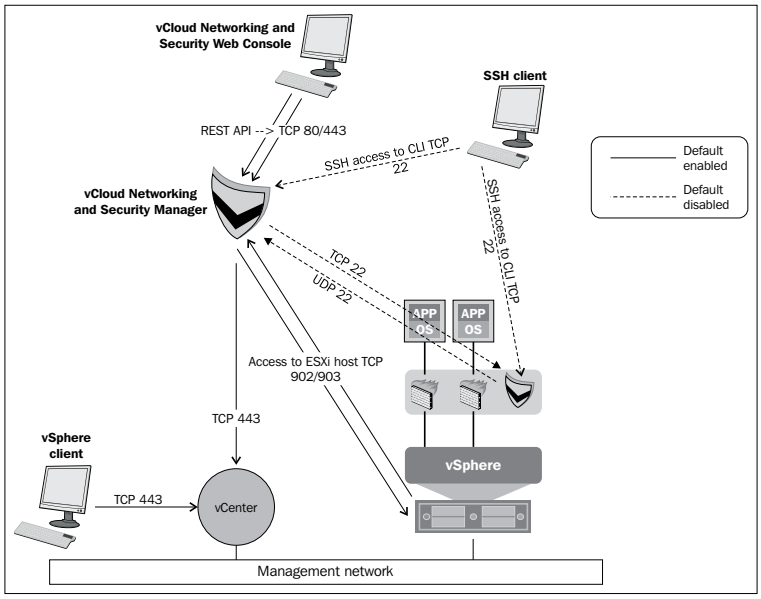


The following figure depicts the before and after effects of vCloud Networking and Security App deployment and its service architecture.



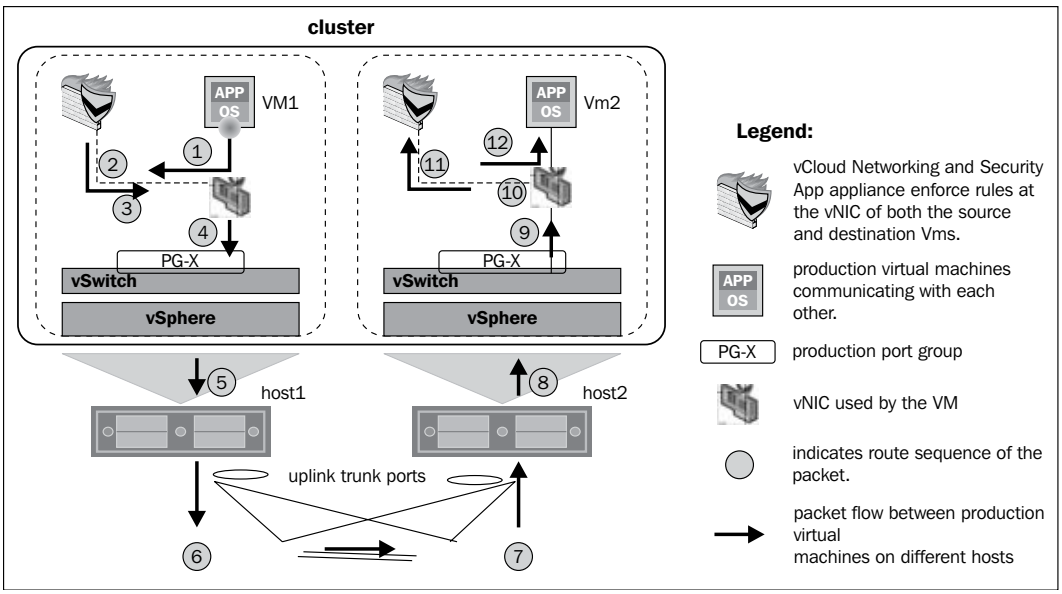
vCloud Networking and Security App – communication flow

Let us look at the communication flow in between various actors in vCloud Networking and Security deployment, such as vCloud Networking and Security Manager, vSphere Client, REST API, and vCloud Networking and Security App appliance. The following diagram shows the ports used and the way the communication happens:



By default, you cannot manage vCloud Networking and Security Manager using SSH as it is disabled by default. Also as a best practice, you should segment vCloud Networking and Security Manager traffic from non-management traffic. vCloud Networking and Security Manager handles the bulk of management communications for vCloud Networking and Security, including vCloud Networking and Security App. Downloading and uploading files, such as flow monitoring files from vCloud Networking and Security App appliances to vCloud Networking and Security Manager, is done over the ESXi host's local link, 127.0.0.1.

Now let us look at typical traffic flow and understand how it happens from one VM to another VM through vCloud Networking and Security App.



In this scenario, **VM1** must communicate with **VM2**. vCloud Networking and Security App is deployed. **VM1** and **VM2** are located on two different ESXi hosts. Communication flows over the wire are described in detail as follows:

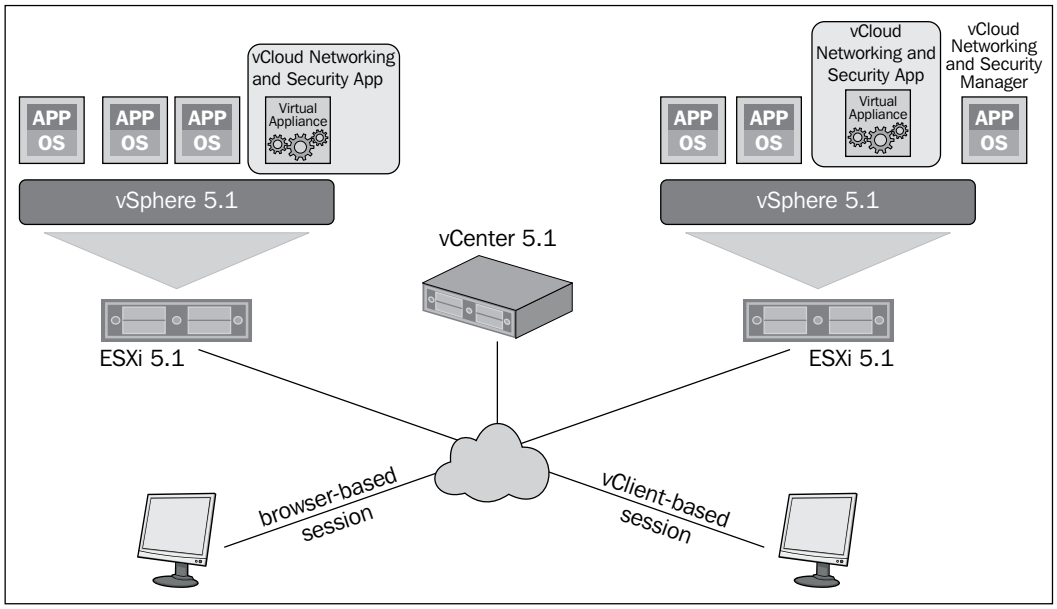
1. When **VM1** sends a packet out, it is intercepted by the kernel module of the virtual network adapter-level firewall. This kernel module is registered in VMkernel of the ESXi host.
2. Then the kernel module gets forwarded to the vCloud Networking and Security App appliance on that host.

3. The vCloud Networking and Security App appliance will inspect the packet. If the security profile allows the packet to flow through, the packet is sent back to the virtual network adapter-level firewall.
4. The virtual network adapter-level firewall sends the packet to the vSwitch or DVSwitch port groups. In this example, it is PG-X on **host 1**, that is, a vSwitch port group.
5. The vSwitch port group looks up the MAC address in its MAC table and accordingly sends the traffic out on the uplink port of **host 1**.
6. After the packet is out of the ESXi host, physical switches will carry this packet.
7. The external physical switch will look at the MAC table and then send the packet to the **host 2** network adapter.
8. The vSwitch on **host 2** receives the packet, looks up the MAC address table, and accordingly sends the traffic out to the virtual machine on **host 2**.
9. The virtual network adaptor-level firewall intercepts the packet and forwards it to the vCloud Networking and Security App appliance.
10. Once the packet gets forwarded to the vCloud Networking and Security appliance, it is inspected and based on a profile that is configured at appliance-level, then it is allowed or disallowed.
11. In this case, it is allowed once the accepted packet is forwarded to the VM.
12. The virtual network adaptor-level firewall sends the packet to the VM.

Installing vCloud Networking and Security App

The next task is to install vCloud Networking and Security App on each ESXi host that you want to protect in your vSphere environment. vCloud Networking and Security App uses vCloud Networking and Security Manager 5.1. The steps that we will take to install a vCloud Networking and Security App instance on an ESXi host are to add a management port group for the vCloud Networking and Security instances to use, install vCloud Networking and Security App on each host, and verify that the functions specific to vCloud Networking and Security App, such as flow monitoring and security groups, are enabled.

The following figure is a typical vCloud Networking and Security App deployment model:



You need to install vCloud Networking and Security App on each ESXi host that has virtual machines that you want to protect. As a prerequisite, you need to verify that you have a unique IP address for the management port of each vCloud Networking and Security App appliance.

The network connection of a virtual machine is interrupted when you protect it with vCloud Networking and Security App. So in a similar case, if vCenter Server is running on a virtual machine and it becomes disconnected from the network, the vCloud Networking and Security App installation process might halt without completing. When vCloud Networking and Security App is deployed on the ESXi host, it adds a new configuration option to the VMX files of all VMs running on that particular host. This entry is made by vCenter. So if vCenter is a VM, it might not be able to make this entry for itself and might get disconnected. If vCenter is disconnected, vCloud Networking and Security App deployment hangs. To mitigate this risk, VMware recommends that you place vCenter Server, the vCenter Server database, and third-party or internal service virtual machines that you do not want to be protected in the virtual machine's exclusion list.

Another thing that you can do is if the vCenter Server or vCenter Server database virtual machines are on the ESXi host on which you are installing vCloud Networking and Security App, migrate vCenter Server to another host before installing vCloud Networking and Security App. This exclusion can be added before the installation of vCloud Networking and Security App.

Another thing to note is that there is as such no issue with vCloud Networking and Security Manager and vCloud Networking and Security App being hosted on the same host because vCloud Networking and Security Manager is not protected by the vCloud Networking and Security App appliance. owever, in case you want to uninstall vCloud Networking and Security App, you have to move vCloud Networking and Security Manager to another host for the uninstallation to complete as uninstalling vCloud Networking and Security App requires a host reboot; so, it's not recommended. Both vCenter Server and vCloud Networking and Security Manager should not be on the host protected by the vCloud Networking and Security App appliance.

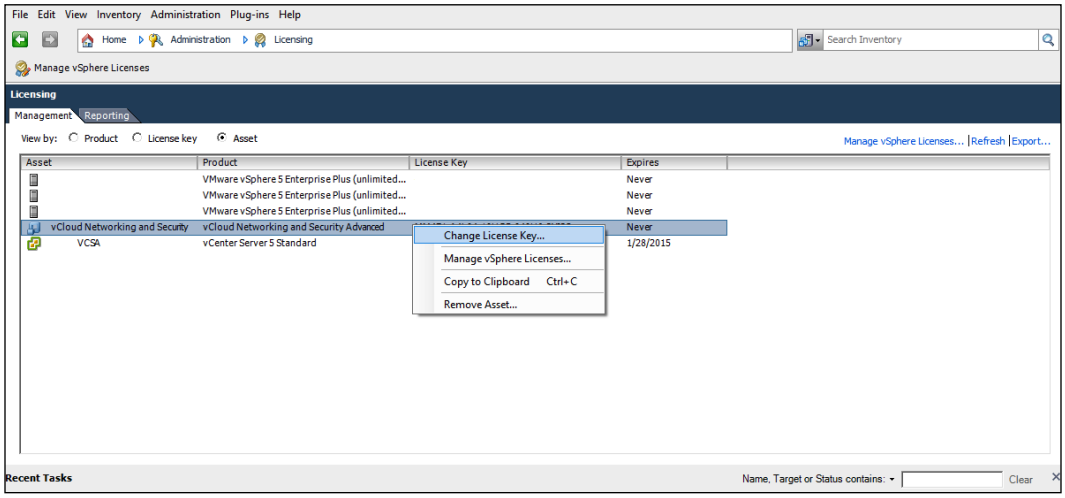
You may ask why both vCenter Server and vCloud Networking and Security Manager should not be on the host protected by the vCloud Networking and Security Manager App appliance?

In general, there are two primary reasons. Firstly, VMs on a host where vCloud Networking and Security App is installed are always protected by vCloud Networking and Security App. Their traffic will flow through the vCloud Networking and Security App appliance, pass through the SpoofGuard policies and firewalls, and will be reported in flow monitoring. Ideally, solutions do not want their management or control plane traffic to fall into their own data plane path. For vCloud Networking and Security Manager, the host is not protected by vCloud Networking and Security App (no vmx parameters are set on vCloud Networking and Security Manager), so it's not affected by this. Though for vCenter Server the user has to put the vCenter Server VM explicitly in the exclude list. If not, then it will be protected and user might experience network disruption between vCloud Networking and Security Manager and vCenter Server due to some rule kicked in or vCloud Networking and Security App is down or something similar.

Secondly, vCloud Networking and Security App requires rebooting the host during uninstallation. If, for some reason, the user has to uninstall or upgrade vCloud Networking and Security App, the host needs to be rebooted for successful completion of the process. You cannot bring down vCloud Networking and Security Manager and vCenter Server in this process, so now it becomes a chicken and egg problem. So, you have to move it to a different host.

Before you install vCloud Networking and Security App, you need to first put the vCloud Networking and Security App license on the host as you will not be able to use these features without licensing your vCloud Networking and Security suite. To do so, follow these steps:

1. Log in to the vCenter Server instance where you have vCloud Networking and Security Manager registered.
2. On the **Home** screen click on **Licensing**.
3. Click on **Asset**. Here you will find the **vCloud Networking and Security Advanced** product.
4. Right-click on it and go to **Change License Key...**.

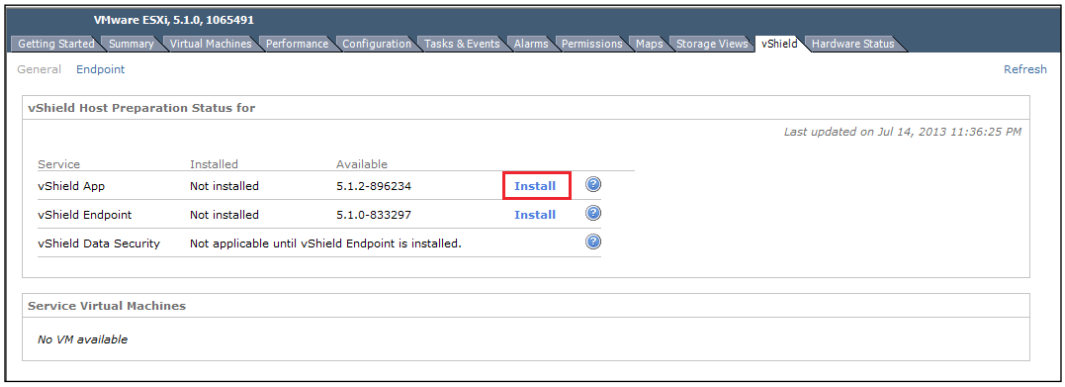


5. Click on **Assign a new license key to this solution**.
6. Click on **Enter Key**.
7. Specify a key and click on **OK**.
8. Click on **OK** again.

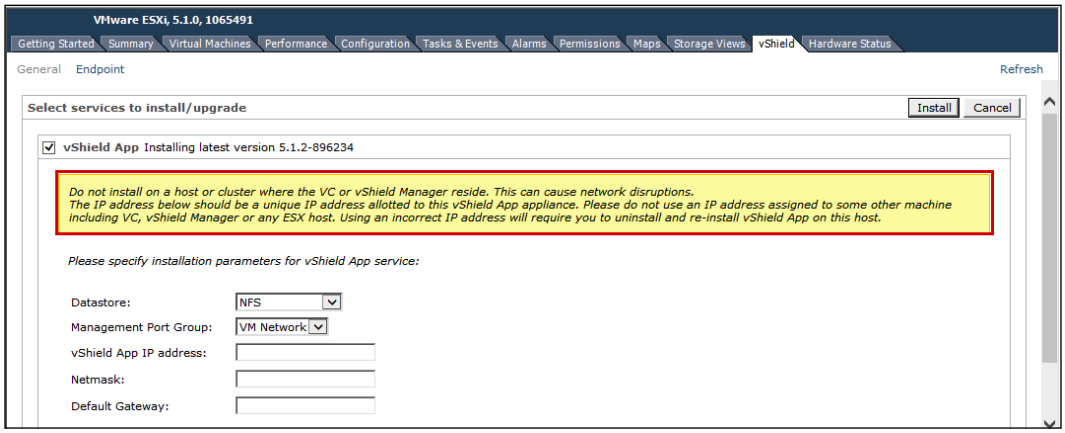
After the licensing is done, you should install vCloud Networking and Security App on each ESXi host where you want to protect your VMs. To do so, follow these steps:

1. Log in to the vCenter Server instance where you have vCloud Networking and Security Manager registered.
2. On the **Home** screen, go to **Hosts and Clusters**.
3. Navigate to the ESXi host where you want to install vCloud Networking and Security App.

4. At the top on the right, go to **vShield**.
5. Click on the **Install** link for vCloud Networking and Security App.



6. Configure the following vCloud Networking and Security App installation settings:
    - **Datastore**
    - **Management Port Group**
    - **vShield App IP address**
    - **Netmask**
    - **Default Gateway**
    - **vShield Endpoint**



Note the warning there.

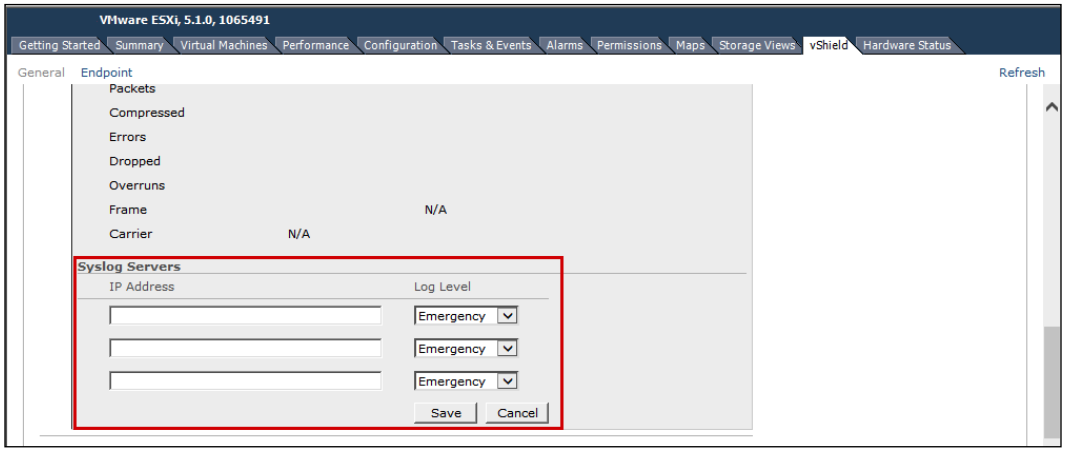
7. Click on **Install**.

8. Monitor the installation process through all the three phases to completion.

Once you have completed with the installation of vCloud Networking and Security App, the first thing what you should do is configure the Syslog server. vCloud Networking and Security App requires (though this step is optional) a Syslog server to capture logs from vCloud Networking and Security App. Three Syslog servers can be defined per vCloud Networking and Security App. Each vCloud Networking and Security App instance can report to a Syslog server; this is based on vCloud Networking and Security App use. You can designate a logging level per Syslog server.

The Syslog traffic is sent over the management network that was defined when deploying the vCloud Networking and Security App. Follow these steps:

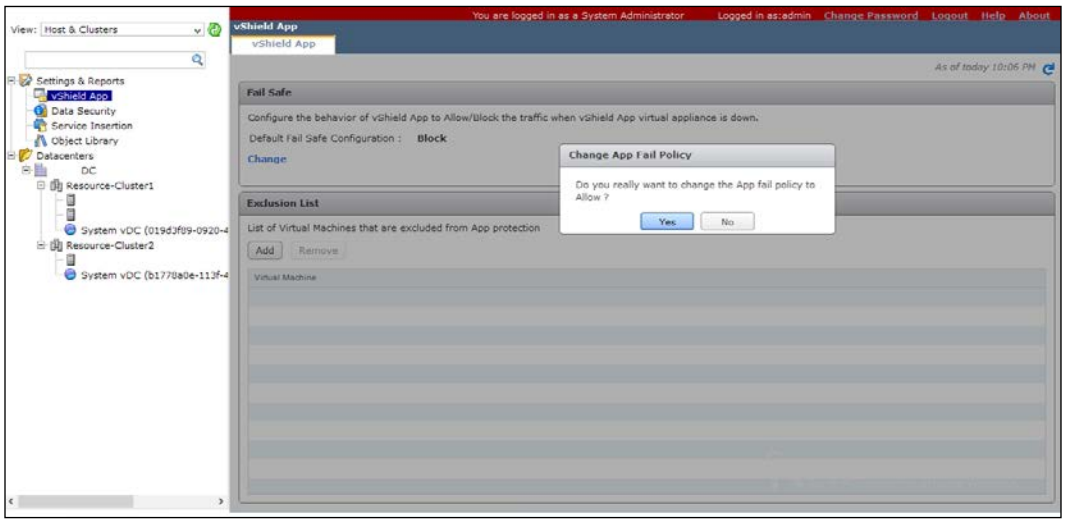
1. Click on the **ESXi** host in the **Hosts and Clusters** screen.
2. Click on the **vShield** tab on the right-hand side.
3. Scroll down and go to **Service Virtual Machine**.
4. Expand that and scroll further down.
5. Specify the IP in the **IP address** fields in the **Syslog Servers** section, choose the **Log Level**, and click on **Save**.



It is recommended that you deploy the two Syslog servers to protect against network disruption and potential loss of important logs.

After you install vCloud Networking and Security App, your next immediate task should be to configure vCloud Networking and Security Fail Safe behavior. Fail Safe is a behavior of vCloud Networking and Security App to allow/block traffic when a vCloud Networking and Security App virtual machine is down. By default, it is set to **Block**. To change this behavior, follow these instructions:

1. Log in to the vCloud Networking and Security Manager web portal.
2. On the left-hand pane, under **Settings & Reports**, go to **vShield App**.
3. On the right-hand pane, in the **Fail Safe** section, click on the **Change** link.
4. When prompted, click on **Yes** to change the App fail policy to allow.



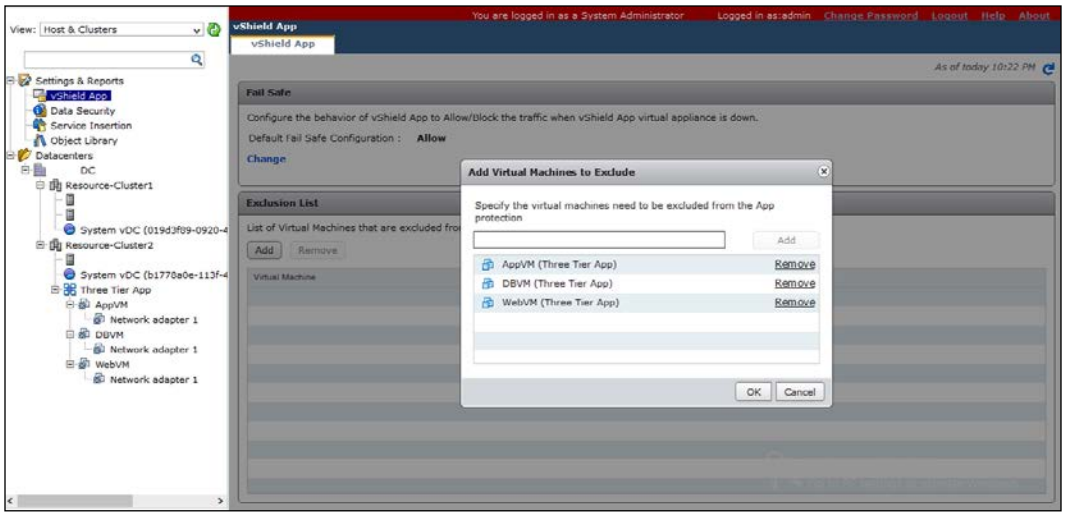
You can exclude a set of virtual machines from vCloud Networking and Security App protection. The exclusion list is applied across all vCloud Networking and Security App installations within vCloud Networking and Security Manager. If a virtual machine has multiple vNICs, all of them are excluded from protection.

vCloud Networking and Security Manager and service virtual machines are automatically excluded from vCloud Networking and Security App protection. You should exclude vCenter Server and other service virtual machines.

Excluding virtual machines from vCloud Networking and Security App protection is useful for instances in which vCenter Server resides in the same cluster where vCloud Networking and Security App is being utilized. After enabling this feature, no traffic from excluded virtual machines can pass through the vCloud Networking and Security App appliance.

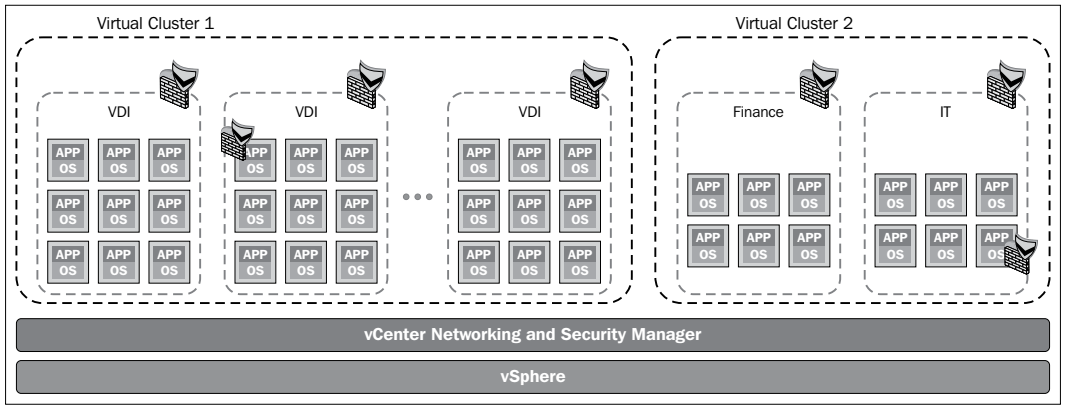
To add a virtual machine to the exclusion list, follow this procedure:

1. Log in to the vCloud Networking and Security Manager user interface.
2. Click on **Settings & Reports** | **vShield App** in the vCloud Networking and Security Manager inventory panel.
3. Click on the **App Global Configuration** tab
4. In **Virtual Machines Exclusion List**, click **Add**. The **Add Virtual Machines to Exclude** dialog box opens.
5. Click on the field next to **Select** and click on the virtual machine you want to exclude.
6. Click on **Select**. The selected virtual machine is added to the list.
7. Click on **OK**.



vCloud Networking and Security App – firewall management

vCloud Networking and Security App comes with a distributed firewall that can protect all workloads from network threats. You can use either containers or individual workloads to apply segmentation. vCloud Networking and Security App will be effective when the vCloud Networking and Security Manager plugin is installed in the vCenter Server and the vCloud Networking and Security App agent gets installed on the ESXi host and uses the VMSAFE API for hypervisor protection.



vCloud Networking and Security App provides a centralized and hierarchical firewall service for ESXi hosts. The vCloud Networking and Security App interface with VM's virtual **NIC** (**network interface card**) allows you to create access control policies regardless of network topology. All traffic in and out of an ESXi host, including between virtual machines in the same port group, will be monitored by your vCloud Networking and Security App because vCloud Networking and Security App gets installed as a hypervisor module and firewall service virtual appliance.

Every VM virtual NIC gets protection by a firewall filter.

vCloud Networking and Security App implements an IP-based stateful firewall and application layer gateway. The firewall filter operates transparently and does not require network changes or modification of IP addresses to create security zones.

You can add a firewall rule for various containers such as datacenter and virtual wire levels. The rules are applied hierarchically and matched in the same order as well. You can reduce the total number of firewalls if you add multiple objects per rule at the source and destination levels.

If you want to add a firewall rule at the datacenter level, you have to go to the vCloud Networking and Security Manager inventory and navigate to the datacenter. Then go to the **App Firewall** tab.

One of the other benefits of using the vCloud Networking and Security App firewall is you are not dependent on application installation; you can configure and publish Layer 3 and Layer 2 firewall rules even before installing an application. vCloud Networking and Security App allows for rules to be defined at the datacenter, cluster, port group, and vNIC levels. When a rule is added, removed, or modified, vCloud Networking and Security Manager determines which vCloud Networking and Security App firewalls are affected and those vCloud Networking and Security App firewalls will get updated rule sets. Each vCloud Networking and Security App firewall inherits global firewall rules set in vCloud Networking and Security Manager.

vCloud Networking and Security App rules are published as a low-level job on the vCloud Networking and Security App firewall; the main benefit of this type of publishing is that it allows traffic flowing through vCloud Networking and Security App to be uninterrupted during rule application. After the rule set is published to the vCloud Networking and Security App, the rules take effect immediately, which includes active network sessions. That means those rule sets will also affect the active network sessions already established.

The default firewall rule allows all traffic to pass through all vCloud Networking and Security App instances. The default rule for Layer 3 traffic appears in the firewall table in the **General** tab, and the default rule for Layer 2 traffic appears in the firewall table in the **Ethernet** tab. The default rule is always the last rule in the table and cannot be deleted or added to. However, you can change the **Action** element of each rule from **Allow** to **Block** (or vice versa), comments for the rule, and whether traffic for that rule should be logged.

vCloud Networking and Security App provides firewall protection through access policy enforcement. Policies can be created automatically from the flow monitoring (which will be discussed shortly) report. Policies can also be created manually from the **App Firewall** tab. The **App Firewall** tab represents the vCloud Networking and Security App firewall access control list.

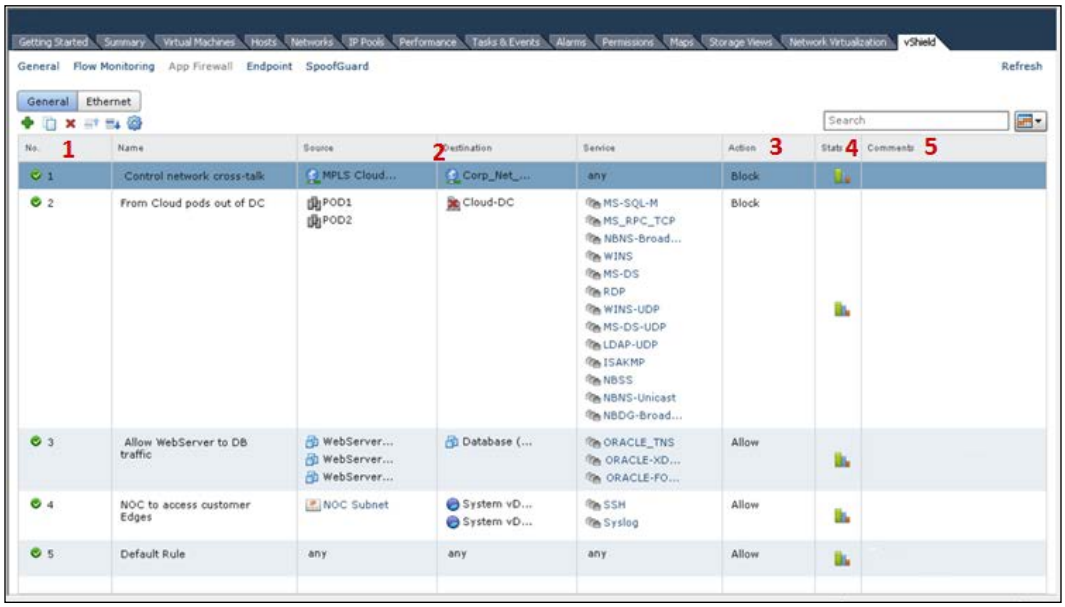
The **App Firewall** tab offers two sets of configurable rules: Layer 3 rules and Layer 2 rules. "Layer" refers to layers of the Open Systems Interconnection (OSI) reference model.

Layer 3 rules govern TCP and UDP transport of Layer 7 or application-specific traffic. The protocols that Layer 3 rules monitor are DHCP, DNS, FTP, HTTP, and SNMP. Layer 3 rules also monitor application-specific traffic including Oracle, Sun Remote Procedure Call (RPC), Microsoft RPC, LDAP, and SMTP. These rules improve security by opening ports only as needed.

Layer 2 rules monitor traffic from protocols such as ICMP and ARP. Layer 2 firewalls protect against multiple types of attacks, for example, password sniffing, DHCP snooping, ARP spoofing/poisoning attacks, and so on. You can configure Layer 3 and Layer 2 rules at the datacenter level only. By default, all Layer 3 and Layer 2 traffic is allowed to pass.

A vCloud Networking and Security App checks each traffic session against the top rule in the App firewall table before moving down the subsequent rules in the table.

Let's look at the App firewall standard UI.

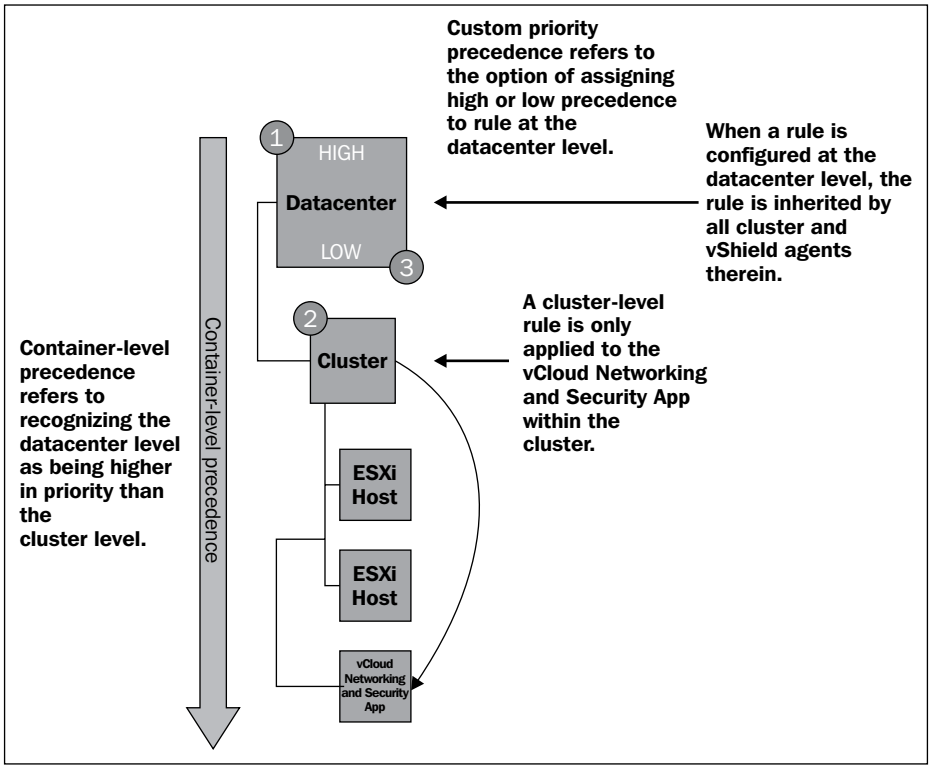


The firewall rules are enforced in the following hierarchy:

1. The datacenter high precedence rules.
2. The cluster-level rules.
3. The datacenter low precedence rules.

   Rules below this level have a lower precedence than cluster-level rules when a datacenter resource is selected.

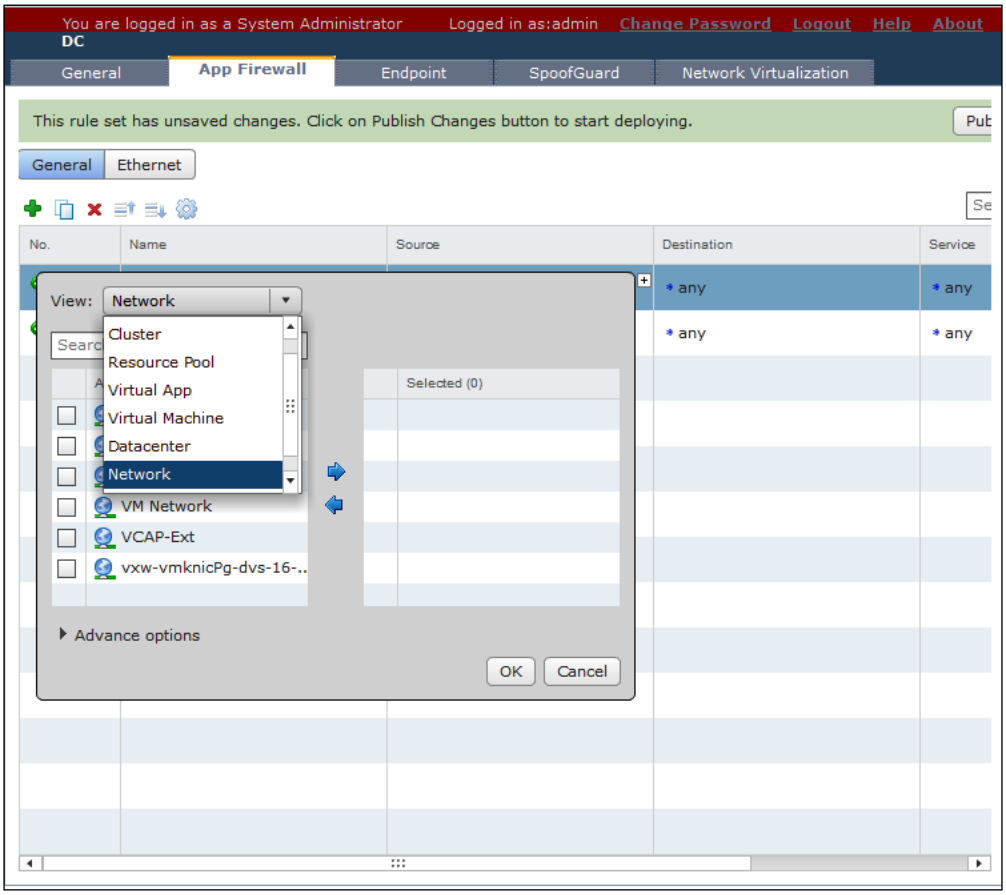
4. The default rules.



As discussed earlier, you can create rules based on traffic to or from a specific container that encompasses all of the resources within that container. For example, you can create a rule to block any traffic from inside a cluster that targets a specific destination outside the cluster. When you specify a container as the source or destination, all IP addresses within that container are included in the rule.

The management of security policies are handled using vCenter Server as well as vCloud Networking and Security Manager containers. These containers could be dynamic or static in nature. By dynamic, we mean the IP/MAC list can change over time or not. All vCenter Server containers as well as vCloud Networking and Security containers, such as Security Group, are dynamic, while IPSet/MacSet are static containers. Security Group is the strongest of all as it allows for nesting of vCenter Server and vCloud Networking and Security Manager containers (both static and dynamic).

Security groups are containers, such as vApp, cluster, or resource pool are trust zones that you create and assign resources to for App firewall protection. Security groups enable you to create a container by assigning resources arbitrarily, such as virtual machines and network adapters. After the security group is defined, you add the group as a container in the **Source** or **Destination** field of an **App Firewall** rule.



You can also define rules based on MAC and IP set. Both follow the same procedure to create a rule. All we have to select is IP range or MAC range. Before that let's understand where we use this type of rule. A virtual machine is identified by its port group, MAC address, and IP address. If you want to configure a rule based on virtual machine identity, MAC set, IP set, and Port Group set are the right types of rules to configure. In this case, even if the virtual machine follows any part of the resource pool, the cluster rule will always apply. Set rules are not true when you define rules based on the resource pool, vApp, or the cluster. The moment a VM is moved from one resource pool to another, the rule no longer applies.

vCloud Networking and Security App rules are organized around Layer 2 and Layer 3. vCloud Networking and Security App refers to Layer 2 rules as ethernet rules and Layer 3 rules as general rules. General rules use five-tuple As the name implies, it allows firewall policies to allow or deny traffic based on five pieces of information. Five-tuple is a unique set of information for each connection and consists of the source, source port, destination, destination port, and protocol, which are described as follows:

- **Source**: This is an IP address with a subnet mask from which communication originates.
- **Source port**: This is the port from which communication originates.
- **Destination**: This is an IP address with subnet mask which communication is targeting.
- **Destination port**: This is the port which communication is targeting.
- **Protocol**: This is the transport protocol, TCP or UDP, used for the communication of Layer 7, or application-specific, traffic.

In addition, the source and destination can be identified using a vCloud Networking and Security App security group or a vSphere grouping, such as datacenter or cluster.

All ethernet rules are enforced globally for that datacenter and act before all general rules. Use caution when deploying ethernet rules as they control all low-level and higher-level protocols relying on them.

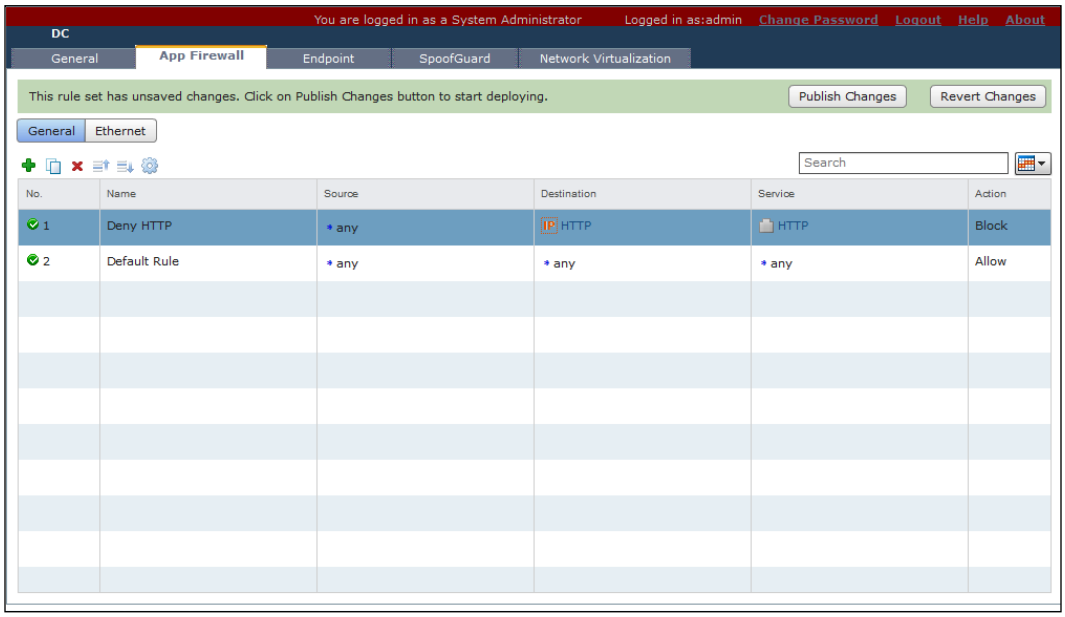
Ethernet rules can be utilized to limit IPv6 traffic as well as other Layer 2 protocols. Unless the client has a well-defined set of rules for Layer 2 filtering, the system-defined rule should remain **allow-any-to-any**. With Layer 2 filtering, all network traffic is commonly blocked until a rule is removed.

Creating a vCloud Networking and Security App firewall rule

In this example, we will create a VMware vCloud Networking and Security App firewall rule that restricts inbound HTTP traffic destined for a web server:

1. Open the vCloud Networking and Security Manager URL in a supported browser, or it can also be accessed from the vCenter client.
2. Log in to vCloud Networking and Security as **admin**.
3. In the vCloud Networking and Security Manager inventory pane, go to **Datacenters** | **Your Datacenter**.
4. In the right-hand pane, click on the **App Firewall** tab.
5. Click on the **Networks** link.
6. On the **General** tab, click on the **+** link.
7. Point to the new rule **Name** cell and click on the **+** icon.
8. In the rule **Name** panel, type `Deny HTTP` in the textbox and click on **OK**.
9. Point to the **Destination** cell and click on the **+** icon.
10. In the input panel, perform the following actions:
    1. Go to **IP Addresses** from the drop-down menu.
    2. At the bottom of the panel, click on the **New IP Addresses** link.
    3. In the **Add IP Addresses** panel, configure an address set that includes the web server.
    4. Click on **OK**.
11. Point to the **Service** cell and click on the **+** icon.
12. In the input panel, perform the following actions:
    1. Sort the **Available** list by name.
    2. Scroll down and go to the **HTTP** service checkbox.
    3. Click on the blue right-arrow to move the **HTTP** service from the **Available list to the Selected** list.
    4. Click on **OK**.

13. Go to the **Action** cell and click on the **+** icon.
14. In the input panel, click on **Block** and **Log**.
15. Click on **OK**.
16. Click on the **Publish Changes** button, located above the rules list, on the green bar.



In general, create firewall rules that meet your business needs. In addition, you might consider the following guidelines:

- Where possible, when identifying the source and destination, take advantage of vSphere groupings in your vCenter Server inventory, such as the datacenter, cluster, and vApp. By writing rules in terms of these groupings, the number of firewall rules is reduced, which makes the rules easier to track and less prone to configuration errors.

- If a vSphere grouping does not suit your needs because you need to create a more specialized group, take advantage of security groups. Like vSphere groupings, security groups reduce the number of rules that you need to create, making the rules easier to track and maintain.
- Finally, set the action on the default firewall rules based on your business policy. For example, as a security best practice, you might deny all traffic by default. If all traffic is denied, vCloud Networking and Security App drops all incoming and outgoing traffic. Allowing all traffic by default makes your datacenter very accessible, but also insecure.

vCloud Networking and Security App – flow monitoring

Flow monitoring is a traffic analysis tool that provides a detailed view of the traffic on your virtual network and that passed through a vCloud Networking and Security App. The flow monitoring output defines which machines are exchanging data and over which application. This data includes the number of sessions, packets, and bytes transmitted per session. Session details include sources, destinations, direction of sessions, applications, and ports used.

Session details can be used to create firewall rules to allow or block traffic.

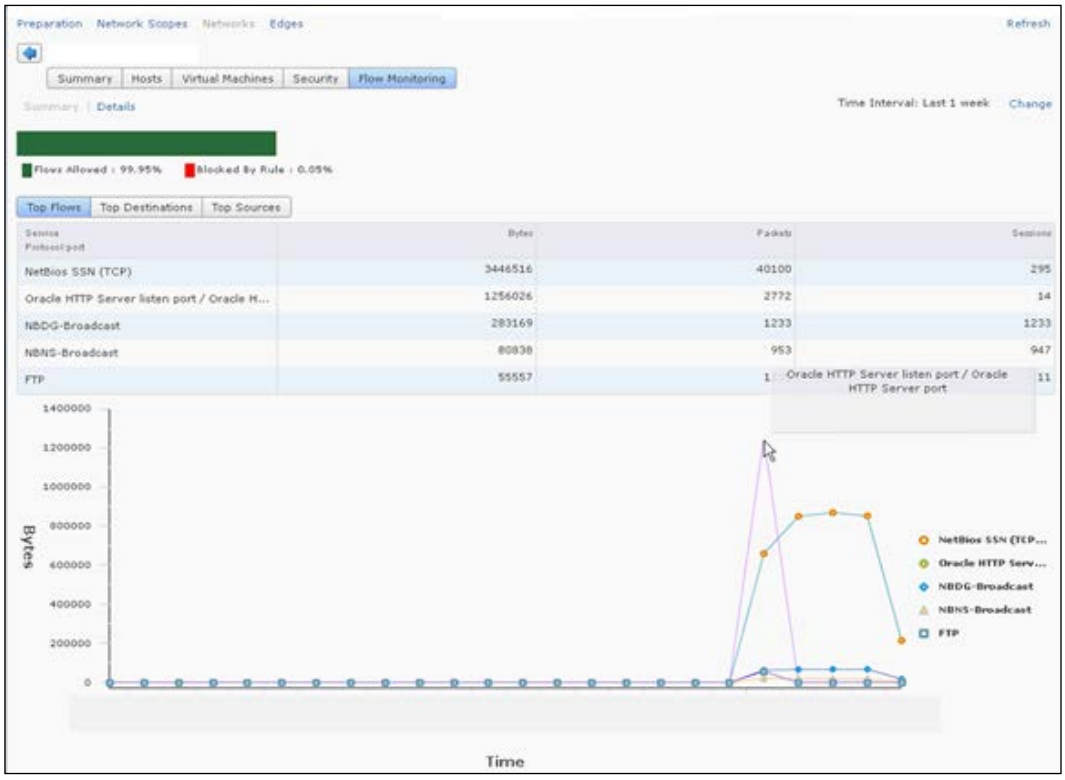
You can use flow monitoring as a forensic tool to detect rogue services and examine outbound sessions.

The main advantages of flow monitoring are:

- You can easily analyze inter-VM traffic
- Dynamic rules can be created right from the flow monitoring console
- You can use it for debugging network related problems as you can enable logging for every individual virtual machine on an as-needed basis

You can view traffic sessions inspected by a vCloud Networking and Security App within the specified time span. The last 24 hours of data are displayed by default; the minimum time span is 1 hour, and the maximum is 2 weeks.

The bar at the top of the page shows the percentage of allowed traffic in green and blocked traffic in red.

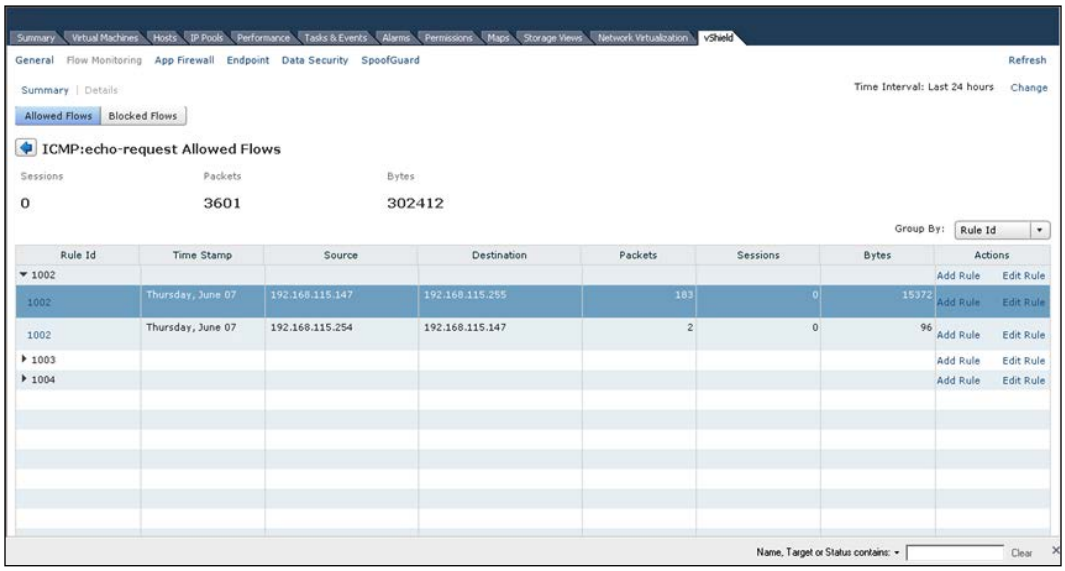


Examining flow monitoring statistics

Let us examine the statistics for the **Top Flows**, **Top Destinations**, and **Top Sources** categories.

1. Open the vCloud Networking and Security Manager URL in a supported browser.
2. Log in to vCloud Networking and Security as **admin**.
3. In the vCloud Networking and Security Manager inventory pane, go to **Datacenters | Your Datacenter**.
4. In the right-hand pane, click on the **Network Virtualization** link.
5. Click on the **Networks** link.
6. In the networks list, click on the network where you want to monitor the flow.

7. Click on the **Flow Monitoring** button.
8. Verify that **Flow Monitoring | Summary** is selected.
9. On the far right side of the page, across from the **Summary** and **Details** links, click on the **Time Interval Change** link.
10. On the **Time Interval** panel, select the **Last 1 week** radio button and click on **Update**.
11. Verify that the **Top Flows** button is selected.
12. Use the **Top Flows** table to determine which flow has the highest volume of bytes and which flow has the highest volume of packets.
13. Use the mouse wheel or the vertical scroll bar to view the graph.
14. Point to the apex of three different colored lines and determine which network protocol is reported.
15. Scroll to the top of the form and click on the **Top Destinations** button.
16. Use the **Top Destinations** table to determine which destination has the highest volume of incoming bytes and which destination has the highest volume of packets.
17. Use the mouse wheel or the vertical scroll bar to view the graph.
18. Scroll to the top of the form and click on the **Top Sources** button.
19. Use the **Top Sources** table to determine which source has the highest volume of bytes and which source has the highest volume of packets.
20. Use the mouse wheel or the vertical scroll bar to view the graph.



Summary

We have successfully installed and configured vCloud Networking and Security App, which is a hypervisor-based firewall that protects applications from network-based attacks.

vCloud Networking and Security App works with vSphere to provide protection, no matter where a virtual machine resides in a cluster. Virtual machines can be excluded from vCloud Networking and Security App protection.

We also learned that vCloud Networking and Security App firewall controls traffic based on the security group that contains vSphere objects in addition to network objects. We have also learned about flow monitoring, which is a traffic analysis tool that provides a detailed view of the traffic that passes through a vCloud Networking and Security App.

In the next chapter, we will talk about VMware vShield Endpoint and how we can use it to protect your cloud workloads from virus attacks. We will describe the benefits of vShield Endpoint and show how to monitor vShield Endpoint health status.

3
Mitigating Threats Using vShield Endpoint Security

VMware vShield Endpoint strengthens security for virtual machines while still improving performance for endpoint protection. The **vShield Endpoint Security** (**EPSEC**) does this by offloading the antivirus and anti-malware agent processing to a dedicated Security Virtual Appliance that is delivered and supported by VMware partners. EPSEC is a framework of different elements, including **Application Programming Interfaces** (**APIs**) that are developed by VMware Engineering to enable Endpoint security partners to integrate these solutions into the VMware vSphere (SVM) platform. This integration is performed at the hypervisor layer that provides the introspection.

It's important to note that customers do not consume EPSEC, but they benefit from the integration of EPSEC through Endpoint products and solutions.

In this chapter, we will look into the benefits of vShield Endpoint over traditional antivirus solutions for a virtual environment. We will also showcase how the **Security Virtual Appliance** (**SVA**), the Thin Agent in the virtual machine, and the vShield Endpoint hypervisor module work together to support virus detection and remediation.

Also, we will talk about the installation process of vShield Endpoint and monitor its health status.

EPSEC – use case

Traditional antivirus solutions require an agent in each virtual machine. All of those agents manage an antivirus signature. You can either configure a client-side schedule to do the virus scanning or you can use a centralized schedule running on the master server. In this approach, if you look at the consolidation ration, your memory, CPU, and network overhead may become a significant overkill.

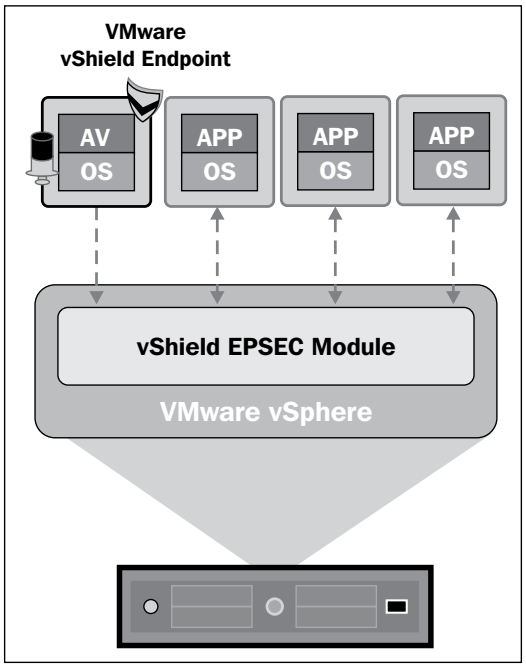
However, there are other solutions as well, which can be configured for a distributed scan over a configurable time interval. It can reduce the resource usage in VMs and in your ESXi as well.

You can still get exposed to a threat in this model if your antivirus signature is not up-to-date. Until the time you update your signature in guest machines, your VM is at risk. Some antivirus software comes with the automated process of pushing the antivirus signature to the guest machines (registered clients).

So, as you see, there are lots of caveats as to why VMware does not recommend using an antivirus on the VMs that are your vCloud workloads.

VMware vCloud Networking and Security does a fabulous job in protecting virtual machines from virus and malware. As mentioned earlier, it does that by offloading virus scanning activities from each VM to a SVA that has a virus scanning engine as well as the stored antivirus signatures.

For antivirus and anti-malware functions, this architecture, as shown in the following screenshot, eliminates the software agent's footprint in guest virtual machines, frees up system resources, improves performance, and eliminates the risk of antivirus storms (overloaded resources during scheduled scans and signature updates).



EPSEC – key benefits

The vCloud Networking and Security Endpoint product allows you to offload the following security functions from the VM to a dedicated appliance on the host:

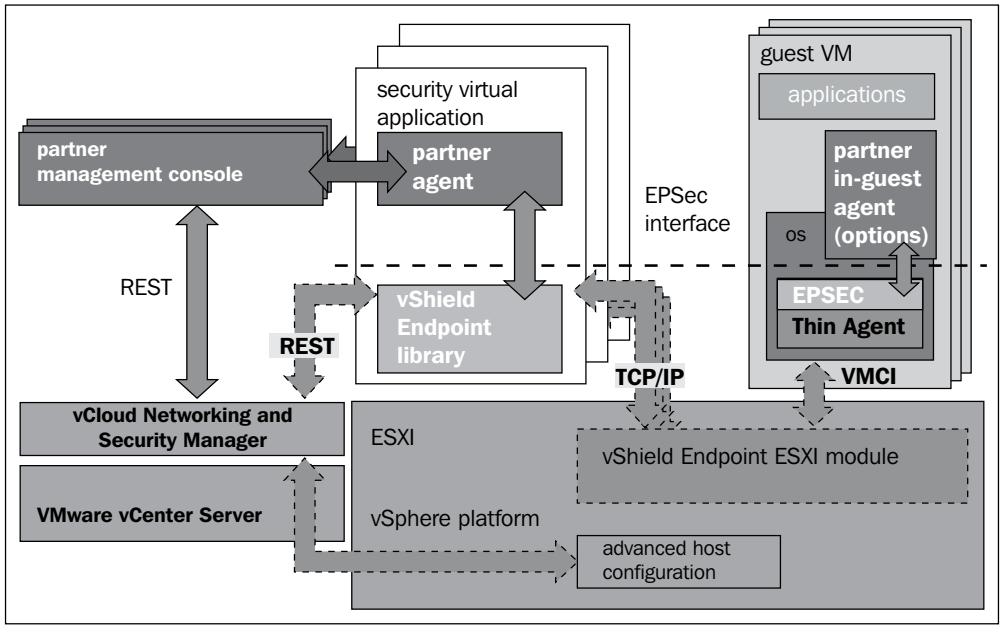
- **Protection**: Virus definitions can be kept up-to-date easily as they are stored on an always-on appliance. So if an attacker is targeting a particular VM, the virus engine is not compromised.
- **Efficiency**: You don't need to install an agent on each guest on the host. An agent is provided with a driver, which is included in VMware Tools. You just need one appliance per host. So you need just one scanning engine and one signature database per host. There is also no antivirus storm.
- **Assurance**: As there is no need to install the software, deployed VMs are protected as soon as they are switched on.
- **Centralized management**: Using a single management console, vCloud security administrators can manage policies and see if the antivirus is functioning correctly.

In a nutshell, it provides:

- On-access scans
- On-demand scans
- Remediation
- Caching and filtering

vShield Endpoint architecture

Let us look at the various architectural components of vShield Endpoint as shown in the following figure:



You can configure and control the partner's software hosted in the SVA using the management console provided by the VMware partner. VMware partners can provide a user interface that makes the management experience (including policy management) exactly like managing software hosted on a dedicated physical security appliance.

Your vSphere administrators will put in less effort on this as they do not need to manage agents on the virtual machines. All of the policy management and AV management is done through a partner-provider SVA. Your vSphere administrators also don't need to update the AV definition inside the guest.

Virtual infrastructure administrators can easily monitor deployments to determine, for example, whether an antivirus solution is operating properly.

The EPSEC and REST interfaces allow partner-provided services to integrate with vSphere and vCloud Networking and Security services.

The **partner in-guest agent** is an agent that can provide additional virtual machine assessments. The virtual machine communications interface (VMCI) API facilitates fast and efficient communication between guest virtual machines and the host.

vShield Endpoint components and intercommunication

To plug in Endpoint directly into the vSphere, which is the backbone of a vCloud environment, the following components are needed:

- A SVA that will be hardened and delivered by VMware partners, such as Bitdefender, Symantec, Trend Micro, McAfee, and Kaspersky
- The Thin Agent for virtual machines to offload security events, which is included in VMware Tools
- vShield Endpoint ESXi hypervisor module (MUX) that enables communication between the first two components in the hypervisor layer

For example, in the case of an antivirus solution, vShield Endpoint monitors the virtual machine's file events, such as a file open request, and notifies the antivirus engine, which scans and returns a disposition. The solution supports both on-access and on-demand (scheduled) scans initiated by the antivirus engine in the SVA.

VMCI is an inter-process communication used between the thin agent and the MUX component. However, there are caveats around this. If you use VMCI, which will be used by MUX, you cannot use vSphere Fault Tolerance (FT) on the same host, and more precisely, you cannot enable FT on that VM. MUX talks to the library within the virtual appliance over TCP/IP. A private VMkernel interface will be created on the host and will be allocated an IP address.

The MUX will also communicate with VMware vCloud Networking and Security Manager in order to get configuration information and health monitoring. This is done over REST (Representational State Transfer) API calls.

We know that vShield Endpoint offloads the antivirus and anti-malware protection; however, it handles the remediation and logging tasks on its own. vShield Endpoint enforces antivirus policies that dictate whether a malicious file should be deleted, quarantined, or otherwise handled. The Thin Agent manages file remediation activity within the virtual machine.

vShield Endpoint prerequisites

Installing only vShield Endpoint is not enough. You need to install an SVA (partner solution) as well. So let us see what would be the proper flow for installing vShield Endpoint:

1. Install vShield Endpoint on each ESXi host. This will effectively install the MUX module on each host. When you install the MUX module on each host, it opens ports 48651 to 448666 for communication between the host and partner SVA.
2. Deploy and configure an SVA to each ESXi host according to the instructions from the VMware antivirus partner. However, in our example, we will use vCloud Networking and Security Data Security as the SVA.
3. Install VMware Tools 8.6.0 or later on all virtual machines that are to be protected. VMware Tools include the vShield Thin Agent, which must be installed on each guest virtual machine to be protected.

Make sure that the guest virtual machine has a supported version of Windows installed. The following Windows operating systems are supported:

- Windows Vista (32 bit)
- Windows 7 (32/64 bit)
- Windows XP (32 bit)
- Windows 2003 (32/64 bit) and Windows 2003 R2 (32/64 bit)
- Windows 2008 (32/64 bit) and Windows 2008 R2 (64 bit)

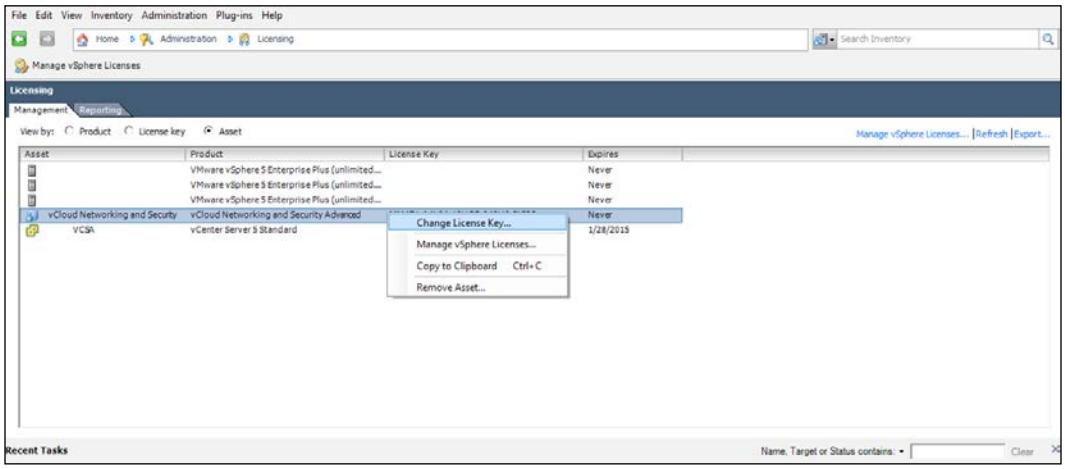
Installing vShield Endpoint

First of all, we need to install the vShield Endpoint in the hypervisor of an ESXi host, before deploying the SVA. In this case, it is the VMware vCloud Networking and Security Data Security SVA. Finally, we need to install the Thin Agent in the guest VM. You should keep in mind that it is that Thin Agent that enables protection on the guest VM, where interesting security events are passed to the SVA for processing and possible threat mitigation.

You should also remember that each host should have the EPSEC module installed. Even if a guest has the Thin Agent installed, if the host does not have the Endpoint module installed or the SVA VM, then the guest VM is not protected.

Before you install vShield Endpoint, you need to first put the vCloud Networking and Security App license there. To do so, perform the following steps:

1. Log in to the vCenter Server where you have vCloud Networking and Security Manager registered.
2. On the **Home** screen, click on **Licensing**.
3. Click on **Asset**. Here you will find the **vCloud Networking and Security** product.
4. Right-click on it and select **Change License Key...**.

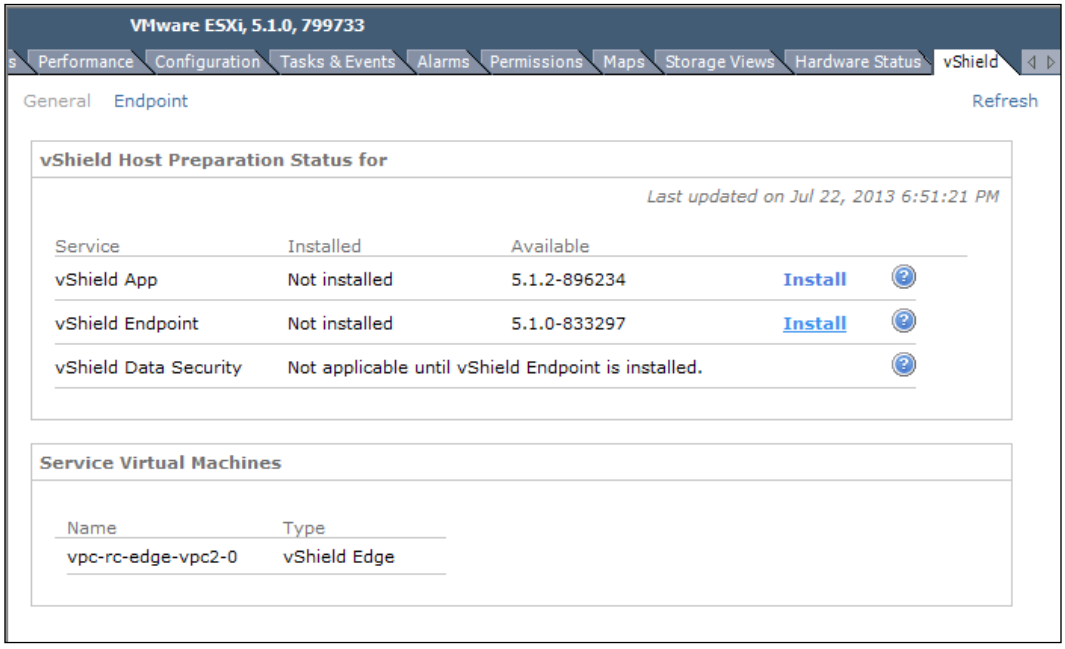


If you upgrade your vSphere environment to vSphere 5.1 from vSphere 4.1 Update 3 or 5.0, or if you are performing a new install of vSphere 5.1, your vSphere 5.1.x license enables the vShield Endpoint 5.1.x functionality, and no additional Endpoint license is required.

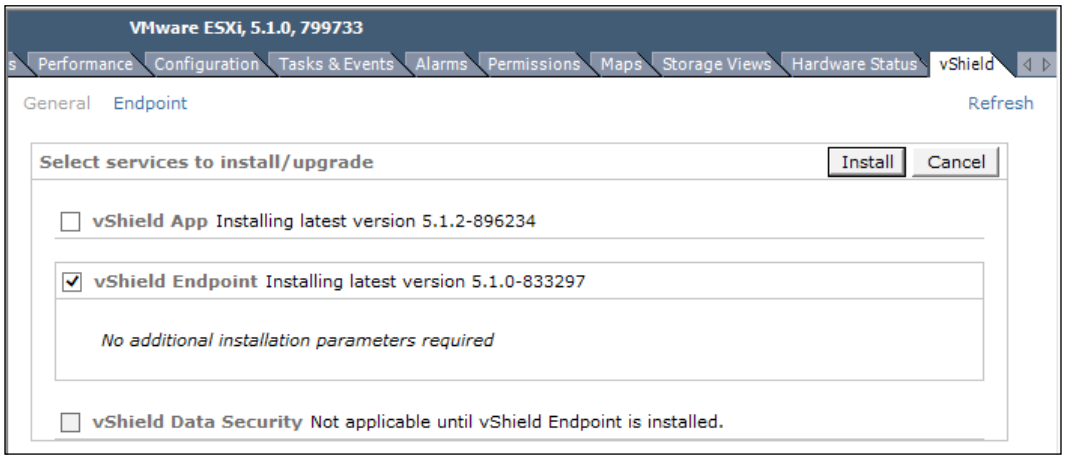
5. Click on **Assign a new license key to this solution**.
6. Click on **Enter Key**.
7. Specify a key and click on **OK**.
8. Click on **OK**.

After the licensing is done, you should now install vShield Endpoint on each ESXi host where you want to protect your VMs. To do so, perform the following steps:

1. Log in to the vCenter Server where you have vCloud Networking and Security Manager registered.
2. On the **Home** screen, select **Hosts and Clusters**.
3. Select the ESXi host where you want to install vShield Endpoint.
4. On the right-hand pane, click on the **vShield** tab, and then click on the vShield Endpoint's **Install** link.



5. You will see the following screen. Just click on the **Install** button.



6. Now log in to the ESXi host using SSH.
7. This step is optional. Navigate to the `/etc/init.d` directory. Note that the MUX is listed there; that means the Endpoint module has been installed on this ESXi host.

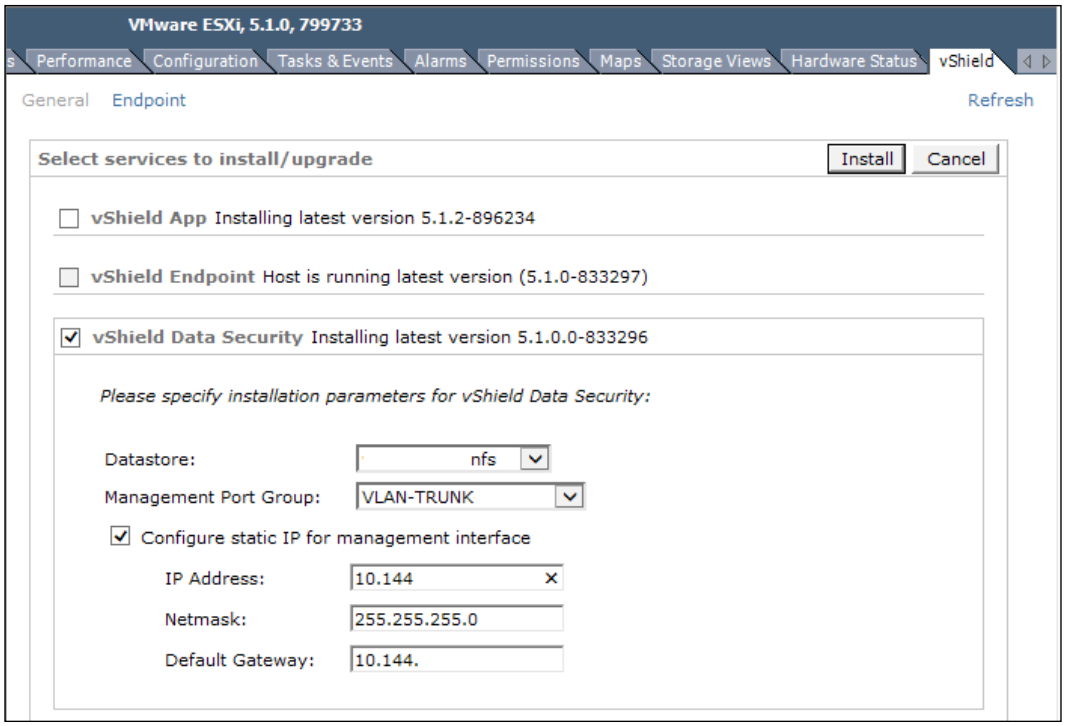
```
~ # cd /etc/init.d/
/etc/init.d # ls
DCUI                hostd               lwiod               sensord             snmpd               vobd
ESXShell            iked                memscrubd           sfcbd               storageRM           vprobed
SSH                 lacp                netlogond           sfcbd-watchdog      usbarbitrator       vpxa
cdp                 lbtd                ntpd                slpd                vShield-Endpoint-Mux wsman
dcbd                lsassd              rhttpproxy          smartd              vmamqpd             xorg
/etc/init.d #
```

As discussed earlier, once the Endpoint module has been installed, the next step is to install the SVA. In this case, we will install VMware vCloud Networking and Security Data Security SVA that provides visibility into sensitive data stored within your organization's vCloud environments. This is discussed in great detail in the next chapter. This is for demo purposes only. If there is no SVA, there is no mechanism for EPSEC to protect the VMs on a host.

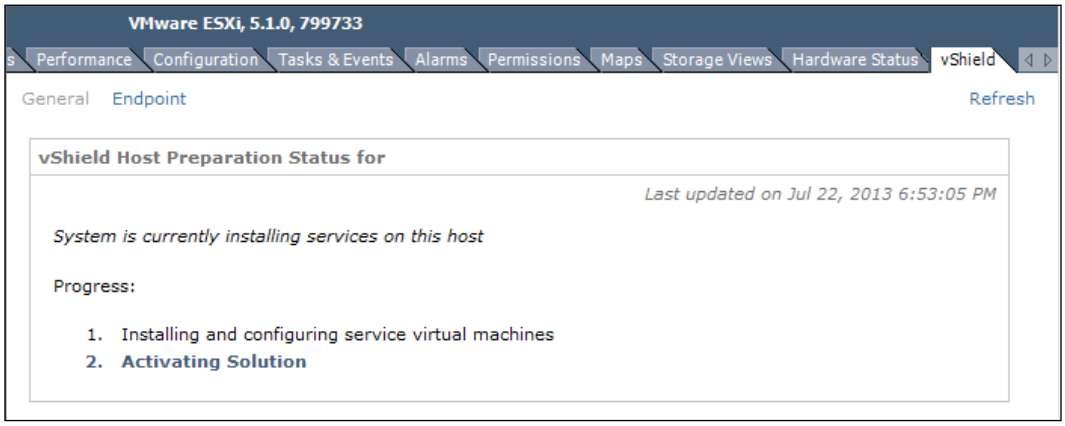
The following steps are performed for installing the VMware vCloud Networking and Security Data Security SVA:

1. Select the ESXi host in the inventory panel, and go to the **vShield** tab. Here you can see the relevant EPSEC-related information (currently Endpoint is installed).
2. Now click on **Install** to begin the installation process for vCloud Networking and Security Data Security.

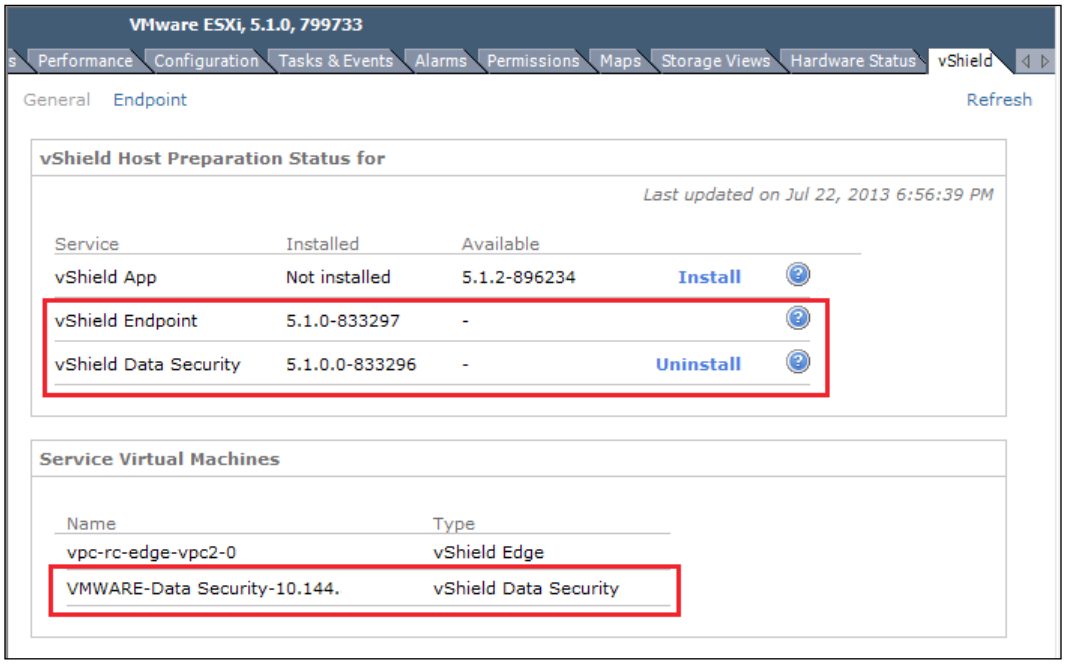
3. You then have to select some installation settings. Choose the values for **Datastore** where you need to have this SVA placed, and **Management Port Group**. You can also specify a value for **IP Address** (optional) and then click on **Install**.



4. During the install, the **SVM** (**Secure Virtual Machine**) for Data Security is deployed.

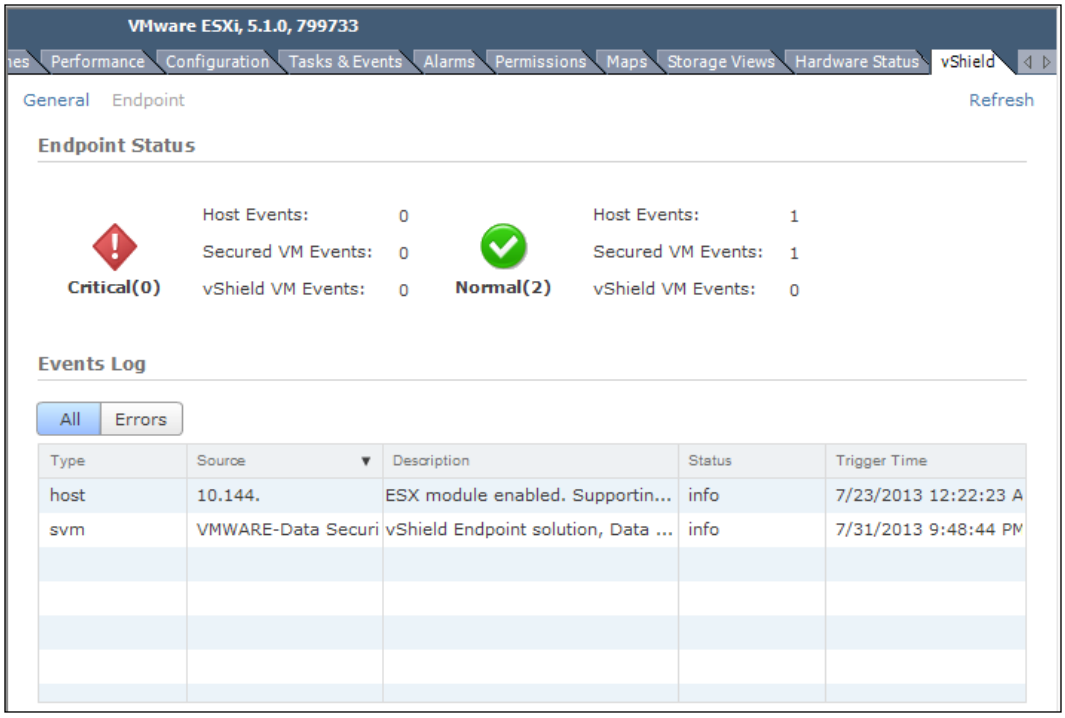


5. When the installation has completed successfully, you will see the SVM listed in the **vShield** tab.



Once the Endpoint component is installed, a new vSwitch is deployed automatically, which will be used to facilitate communication between the host and any SVM deployed. So a private port group is created on the host, which is then allocated an IP address. This is the VMkernel port group `vmservice-vmknic-pg`.

Having Endpoint installed will not enable protection for your VMs. From the host level, you can see that the SVM is not operating. There are VMs on the host, but it's not listed as protected. You should see both the SVM and the VM in a functioning system.

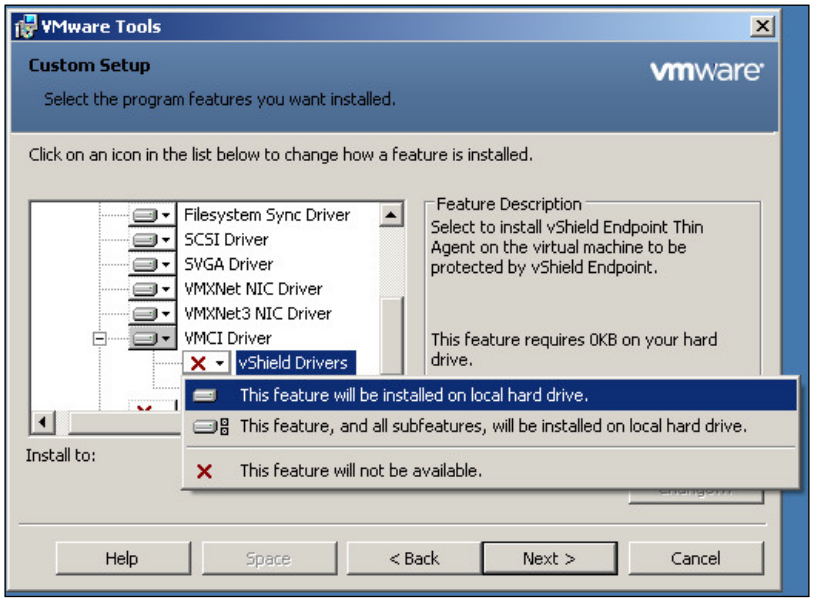


Now you need to install the Thin Agent on the hosted VM. This is necessary to enable protection on the VM. In addition, it will trigger the SVM's operation. You will do this in the next task.

VMware Tools include the vShield Thin Agent that must be installed on each guest virtual machine to be protected. Virtual machines with VMware Tools installed are automatically protected whenever they are started up on an ESXi host that has the security solution installed; that is, protected virtual machines retain the security protection through shutdowns and restarts, and even after a vMotion moves to another ESXi host with the security solution installed. The following steps have to be performed to install the Thin Agent on the hosted VM:

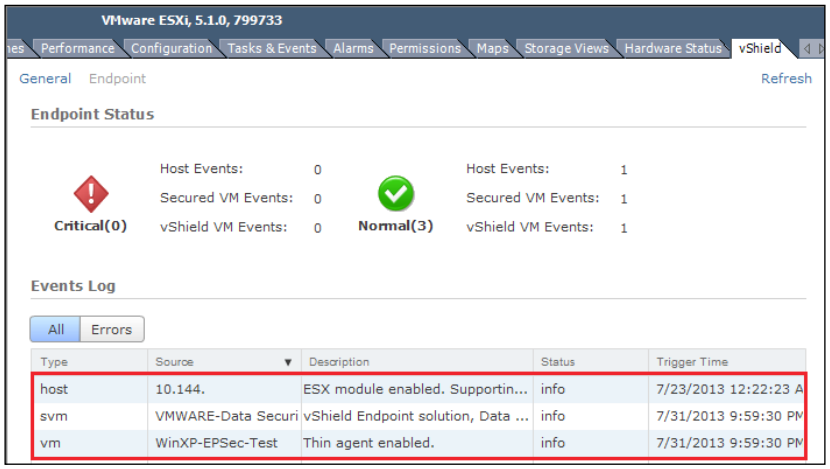
1. Open a console to the guest VM in vCenter and navigate to **Virtual Machine | Guest | Install/Upgrade VMware Tools**.

2. In the **Setup Type** wizard, select the **Custom** option from the **VMware Device Drivers** list, select **VMCI Driver**, and then select **vShield Drivers**. Choose the **This feature will be installed on local hard drive.** option. This driver does not get installed with the default VMware Tools installation, so this step is necessary.

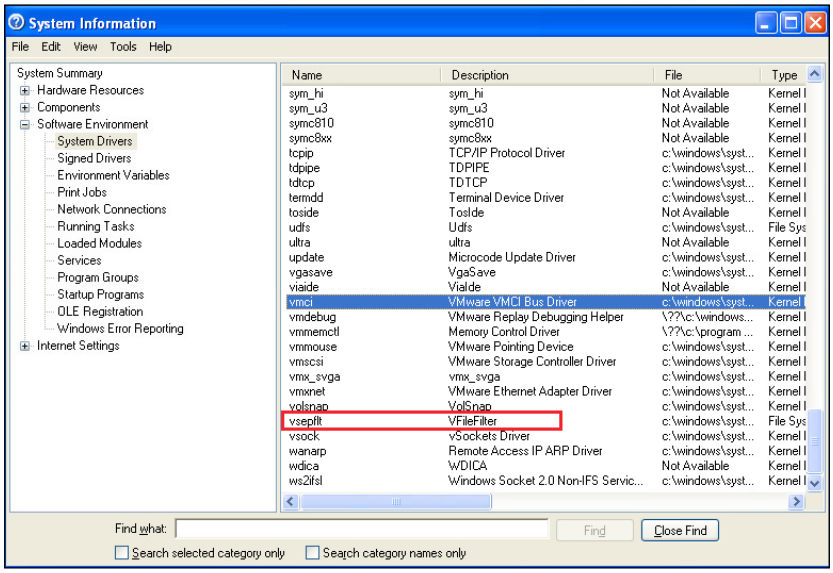


The use of the VMCI channel for communication here means that it's not available for VM fault tolerance. You cannot enable FT and Endpoint on the same host, where Endpoint uses the VMCI channel. This, however, doesn't affect HA.

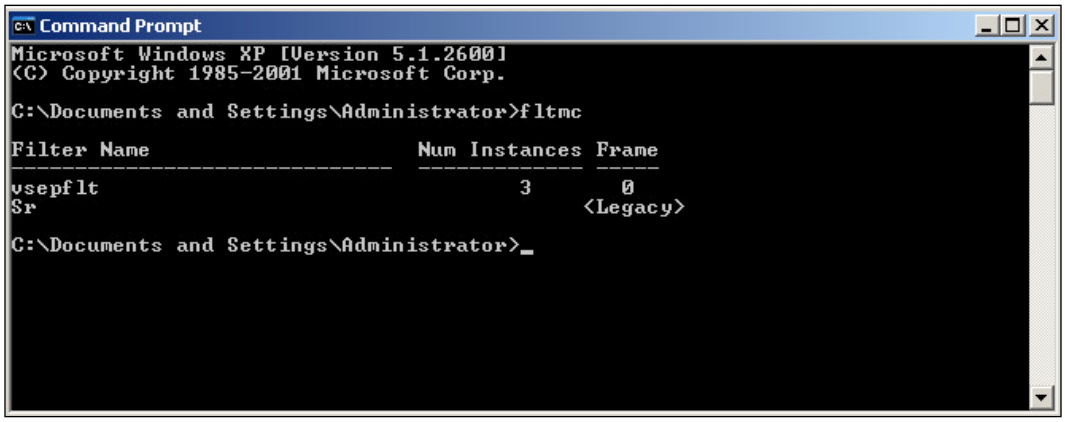
3. Return to the host in vCenter, and notice that the SVM is now enabled, and that the VM is listed.



4. Now just for double confirmation, check the filter driver on the guest OS.
5. Open up the guest OS console. Go to **Run** and type `msinfo32`.
6. Now expand **Software Environment** and select **System Drivers**.
7. Note the two components installed, that is, the VMCI Driver (`vmci`) and the Thin Agent filter (`vsepfilt`). Both of these are required for the Thin Agent to function.



8. By running `fltmc` on a VM, you can confirm if the `vsepflt` filter is loaded. If you want to stop the filter driver, then from a command prompt on the VM in your vAPP, run the `fltmc unload vsepflt` command to unload the filter.
9. To prevent loading it on the next reboot, the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\vsepflt` key needs to be modified, and the value of `DWORD` changed to `4`.



Enable logging on the guest VM

You can also enable Thin Agent logging on the protected VM. Two registry values are read at boot time from the Windows registry. They are polled again periodically. To enable this, you need to change the appropriate registry values on the VM.

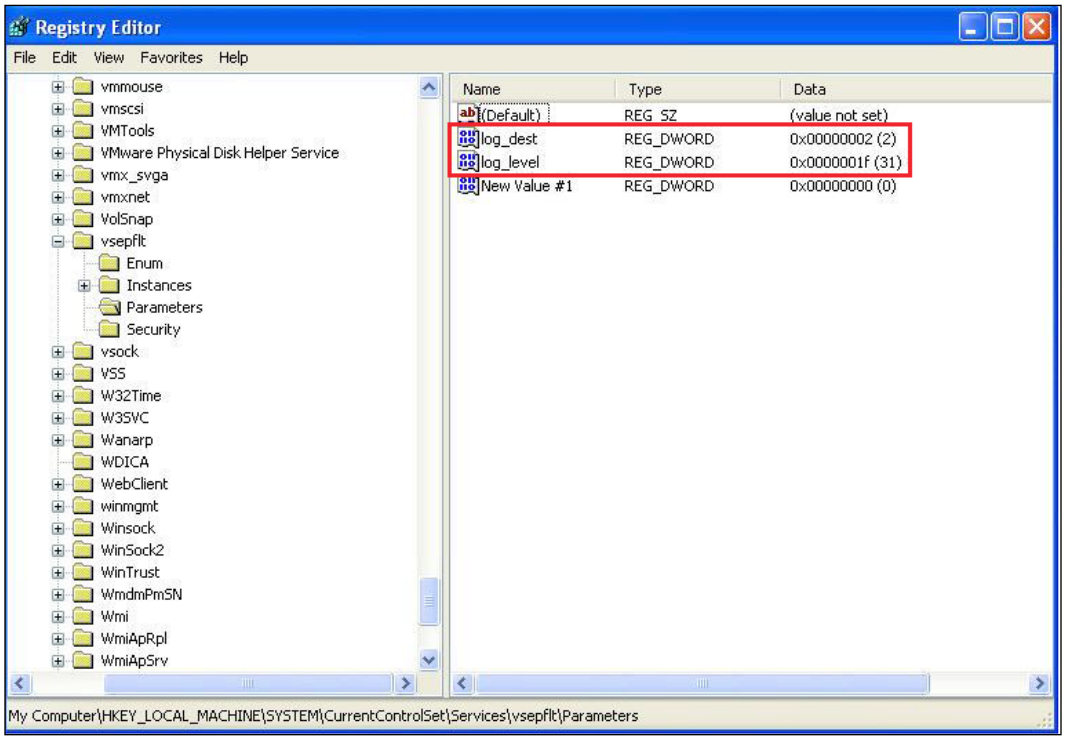
However, there is a considerable performance penalty that will be incurred when these values are enabled. This should only be performed for troubleshooting and debugging purposes.

The following table shows the Thin Agent logging details:

DWORD	Value	Description
`log_dest`	`0 X 1`	WINDBLOG requires the DEBUG mode
	`0 X 2`	Logfiles are stored on the root directory of the VM
`log_level`	`0 X 1`	AUDIT
	`0 X 2`	ERROR
	`0 X 4`	WARN
	`0 X 8`	INFO
	`0 X 10`	DEBUG

The steps to view these logging details are as follows:

1. From vCenter, open a console session to the protected VM in your vApp.
2. From the protected VM in your vApp, launch the registry editor using `regedit`.
3. In the registry editor, navigate to **HKEY_LOCAL_MACHINE** | **SYSTEM** | **CurrentControlSet** | **Services** | **vsepflt**.
4. Now you need to create a new key. Click on **Edit** | **New** | **Key** | **Parameters**.
5. Now create the following for the new parameters key:
   - `log_level= 0000001f`
   - `log_dest= 00000002`
6. Here is how the registry will look. Finally, exit the registry and reboot the Windows VM.



vShield Endpoint – health monitoring

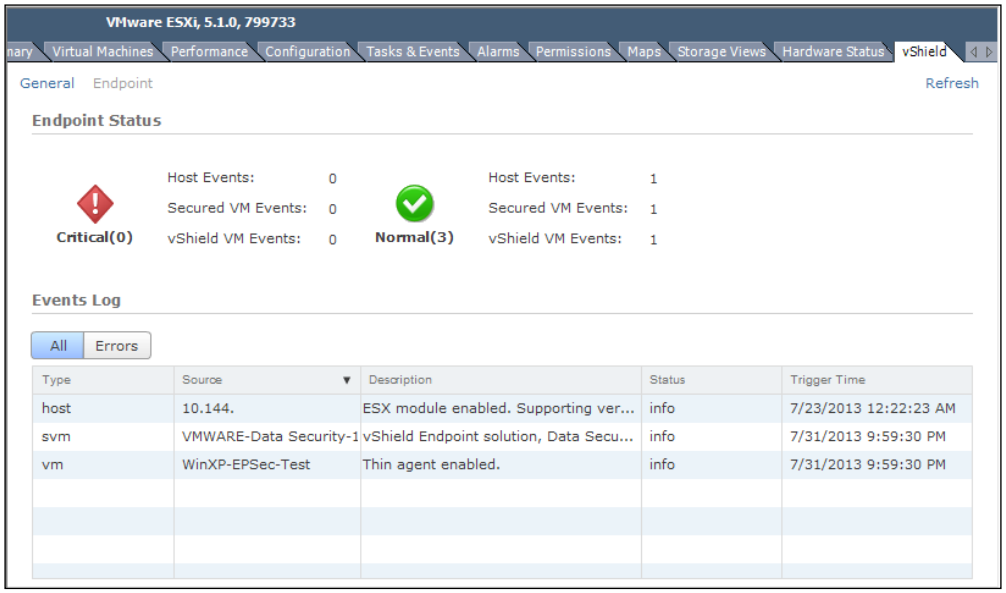
If you want to monitor the vShield Endpoint health status, you need to look at alarms that are shown in red on the vCenter Server. You can also look at the event logs to gather more status information. To get these, you need to configure your vCenter Server correctly. The following are the points that need to be taken care of:

- Not all guest operating systems are supported by vShield Endpoint. Virtual machines with unsupported operating systems are not protected by the security solution. Refer to the KB article, which is available at `http://kb.vmware.com/kb/1036847`.
- All hosts in a resource pool containing protected virtual machines must be prepared for vShield Endpoint, so that virtual machines continue to be protected as they are moved with vSphere vMotion from one ESXi host to another within the resource pool.

To properly monitor a vShield Endpoint environment, you need to look at the following three components:

- The SVA
- VMware ESXi host-resident vShield Endpoint module
- Protected virtual machine

In the following screenshot, the initial startup status is reported for each component. There has been one event posted for each component, as shown in the **Events Log** pane:



Summary

VMware vShield Endpoint strengthens security for virtual machines while improving performance for endpoint protection. vShield Endpoint offloads the antivirus and anti-malware agent processing to a dedicated SVA that is delivered and supported by VMware partners. In this chapter, we have seen the architecture of EPSEC and how to implement it.

In the next chapter, we will talk about VMware vCloud Networking and Security Data Security. We will walk through the installation and configuration process. We will create a Data Security policy and show you how to perform a data scan. We will also review the violation reports that are generated by the vCloud Networking and Security Data Security scan.

4

Overview of VMware vCloud Networking and Security Data Security

VMware vCloud Networking and Security Data Security provides visibility into sensitive data stored within your organization's virtualized environments.

You can ensure that sensitive data in your vCloud environment is adequately protected and assess compliance with regulations around the world, and you can do it by using reports from data scans performed by vCloud Networking and Security Data Security.

In this chapter, we will discuss the following:

- The use cases of vCloud Networking and Security Data Security
- Installing vCloud Networking and Security Data Security on a VMware ESXi host
- Creating a Data Security policy by selecting regulations or content blades, specifying the inventory to be scanned, and configuring the file filter
- Performing a data scan
- Reviewing the violation reports that are generated by a vCloud Networking and Security Data Security scan

VMware vCloud Networking and Security Data Security enables you to choose from built-in templates for standards and regulations governing the most common types of sensitive data, including **PII** (**Personally Identifiable Information**), **PCI-DSS** (**Payment Card Industry Data Security Standard**), and **PHI** (**Patient Health information**) within your organization's virtualized and cloud environments. You can use the violation reports from vCloud Networking and Security Data Security and make sure that sensitive data is adequately protected and assess compliance with regulations around the world.

To get vCloud Networking and Security Data Security into action, you should create a policy that defines the regulations that apply to data security in your organization and specifies the areas of your environment and files to be scanned. A regulation is composed of content blades that identify the sensitive content to be detected. vCloud Networking and Security supports PCI, PHI, and PII related regulations only.

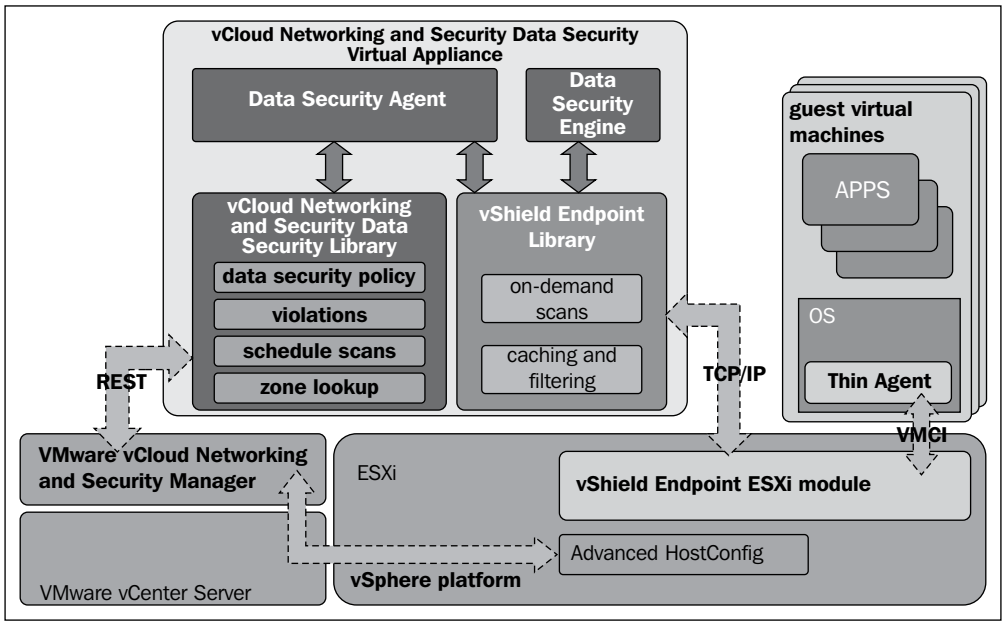
Once you start a vCloud Networking and Security Data Security scan, it analyzes the data on the virtual machines in your VMware vSphere inventory that you define as a boundary, and then generates a report that contains the number of violations detected and the files that violated your policy.

You can perform all data security tasks using REST APIs.

For more information, see the vCloud Networking and Security API programming guide available `https://www.vmware.com/support/pubs/vshield_pubs.html` and the complete documentation suite can be found at `https://www.vmware.com/support/pubs/vshield_pubs.html`.

vCloud Networking and Security Data Security architecture

The vCloud Networking and Security Data Security architecture has been defined in the following figure, where you will find similarities with the architecture of other solutions that work with vShield Endpoint, which we described in the previous chapter.



You cannot deploy vCloud Networking and Security Data Security unless you install vShield Endpoint for each ESXi host on your vSphere Datacenter. Once you install vShield Endpoint, you can use VMware vCloud Networking and Security Manager to deploy a vCloud Networking and Security Data Security virtual appliance on each ESXi host. The virtual appliance is based on the EPSEC framework, so it includes an agent that works with the vShield Endpoint service to scan virtual machines by communicating with them through the vShield Thin Agent that is included in VMware Tools. The Thin Agent driver is the software in the guest VM that offloads security events via the hypervisor to the vShield Endpoint Virtual Appliance. If we were discussing antivirus, it would represent say the Trend Micro Virtual Appliance. In general terms, vShield Endpoint is required to run partner antivirus solutions and/or our vCloud Networking and Security Data Security solution.

This way it exposes introspection at the hypervisor layer. The EPSEC API also delivers a rich toolset to perform particular file activities within the hypervisor. For example, it monitors access to a rich set of capabilities to access specific file activities within the hypervisor.

Discovery and reporting of sensitive data has been taken care of by the vCloud Networking and Security Data Security virtual appliance, which includes an analysis engine. vCloud Networking and Security Data Security leverages the capabilities included in the EPSEC Endpoint Library for on-demand scans, caching, and filtering.

This Data Security virtual appliance includes a Data Security library, which enables the creation and management of the data security policies, such as regulations. You can use this Data Security library to enable scanning and reporting on violations.

You can leverage this Data Security library for scheduling scans, and move the virtual machines that host sensitive information to a designated VMware vCloud Networking and Security App security group so that proper policies can be applied to it. However, there is a small caveat in it, and that is that vCloud Networking and Security Data Security does not currently include these capabilities in the user interface; however, you can use REST APIs to create scripts to automate these two functions.

vCloud Networking and Security Data Security installation

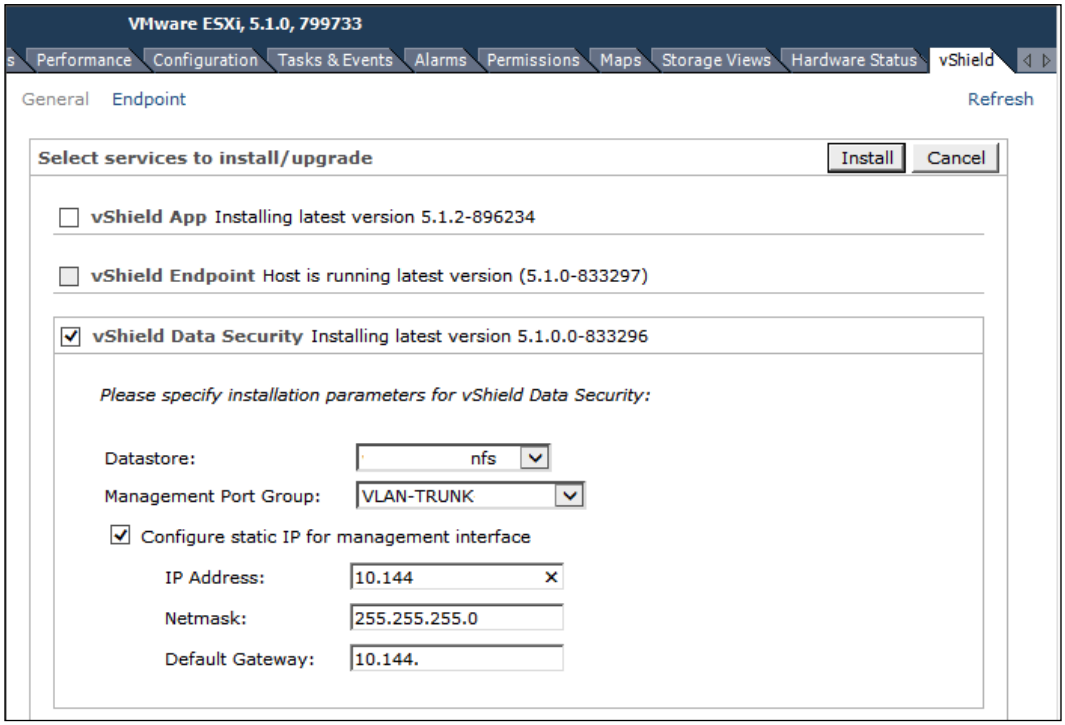
As mentioned previously, you can install vCloud Networking and Security Data Security only after installing VMware vCloud Networking and Security Endpoint. vShield Data Security requires the vShield Endpoint Thin Agent (included in the VMware Tools) and the hypervisor module (MUX module) for communication between the service virtual machine and the virtual machines that are being scanned.

So, before you start the Data Security installation, first verify that the vShield Endpoint has been installed on the host and guest virtual machines.

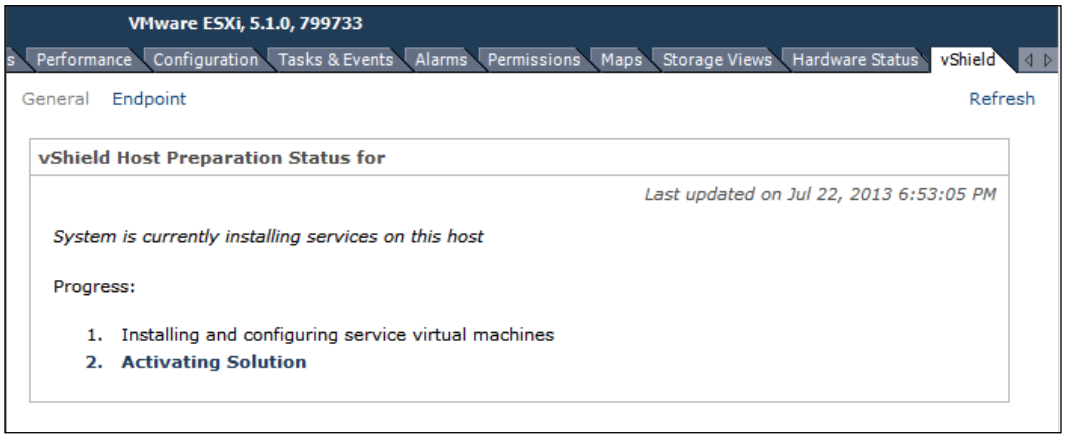
Let us get started with the installation process:

1. Log in to the vCenter Server where you have vCloud Networking and Security Manager registered.
2. On the **Home** screen, select **Hosts and Clusters**.

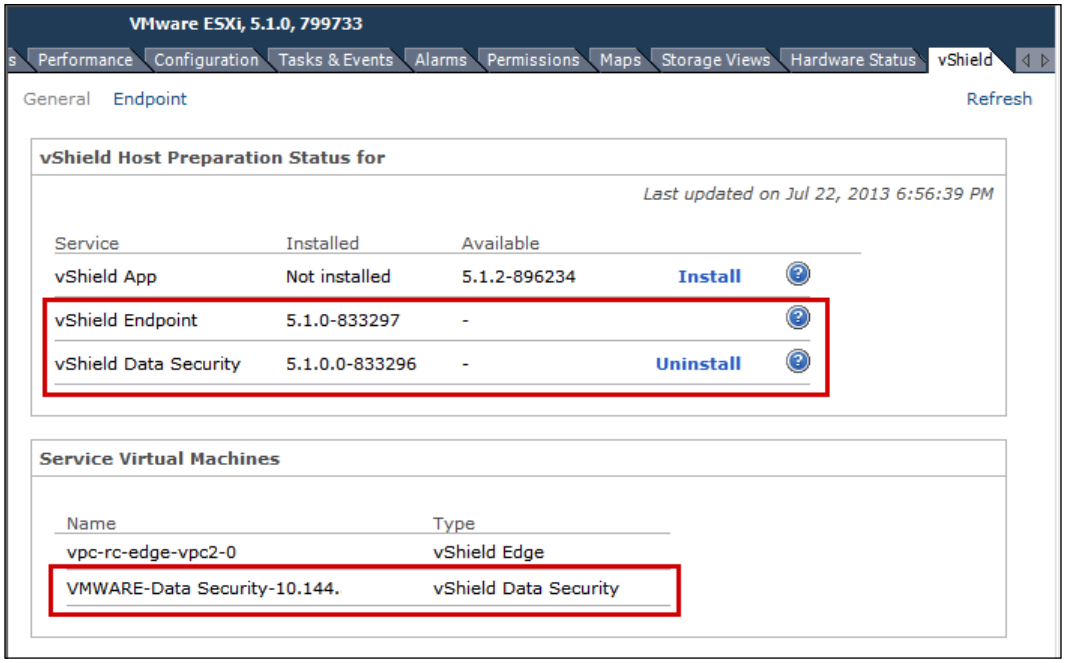
3. Select the ESXi host where you want to install the vCloud Networking and Security App.
4. On the right-hand pane, click on the **vShield** tab. Here you can see the relevant EPSEC-related information (currently, Endpoint is installed).
5. Now click on **Install** to begin the installation process for vCloud Networking and Security Data Security.
6. You then have to select some installation settings. Choose the values for **Datastore** where you need to place this SVA and **Management Port Group**. You can also specify a value for **IP Address** (optional), and then click on **Install**.



7. During the installation, the SVM for Data Security is deployed.



8. When the installation has completed successfully, you will see the service virtual machine listed in the **vShield** tab.



Defining the vCloud Networking and Security Data Security policy

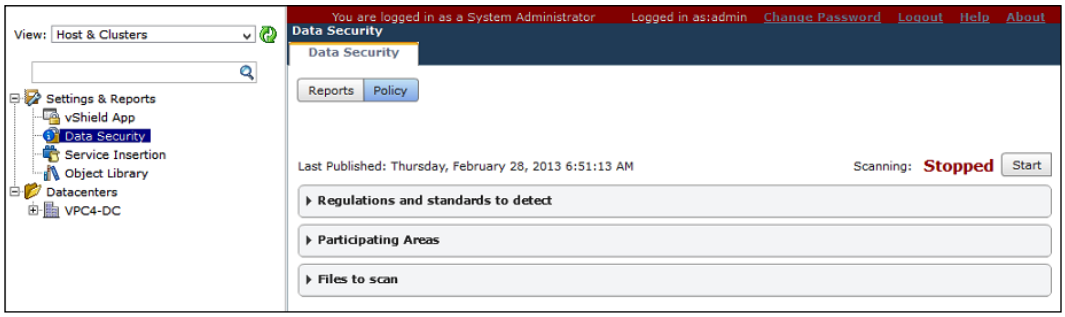
In order to detect sensitive data in your vCloud environment, you need to first define a security policy. There are three things to be specified when you create a Data Security policy:

- **Regulations and standards**: A regulation is a data-privacy law. It is used for protecting PCI, PHI, and PII information. Your company may need different regulations for data compliance. vCloud Networking and Security Data Security gives an option to select the regulations that your company needs to comply with. When you run a scan, vCloud Networking and Security Data Security identifies sensitive data in your organization that violates the regulations in your policy. As discussed earlier, all available regulations are incorporated in the vCloud Networking and Security Data Security library.
- **Participating zone**: By default, your entire vSphere infrastructure is scanned by vCloud Networking and Security Data Security. If you want to scan a subset of the entire inventory, you can include or exclude security groups. For example, if you want to scan only the virtual machines in a certain resource pool, create a security group that includes only the resource pool. This is the perfect use case for a vCloud environment where different organizations will have different resource pools. If a resource (cluster, datacenter, or host) is part of both an excluded and included security group, the exclude list takes precedence, and the resource is not scanned.
- **File filters**: You can create data security scan filters to limit the data being scanned and exclude the file types that are unlikely to contain sensitive data from the scan.

You need to select the regulations that you want your company data to comply with, and then vCloud Networking and Security Data Security can help you identify files that contain information that violates these particular regulations.

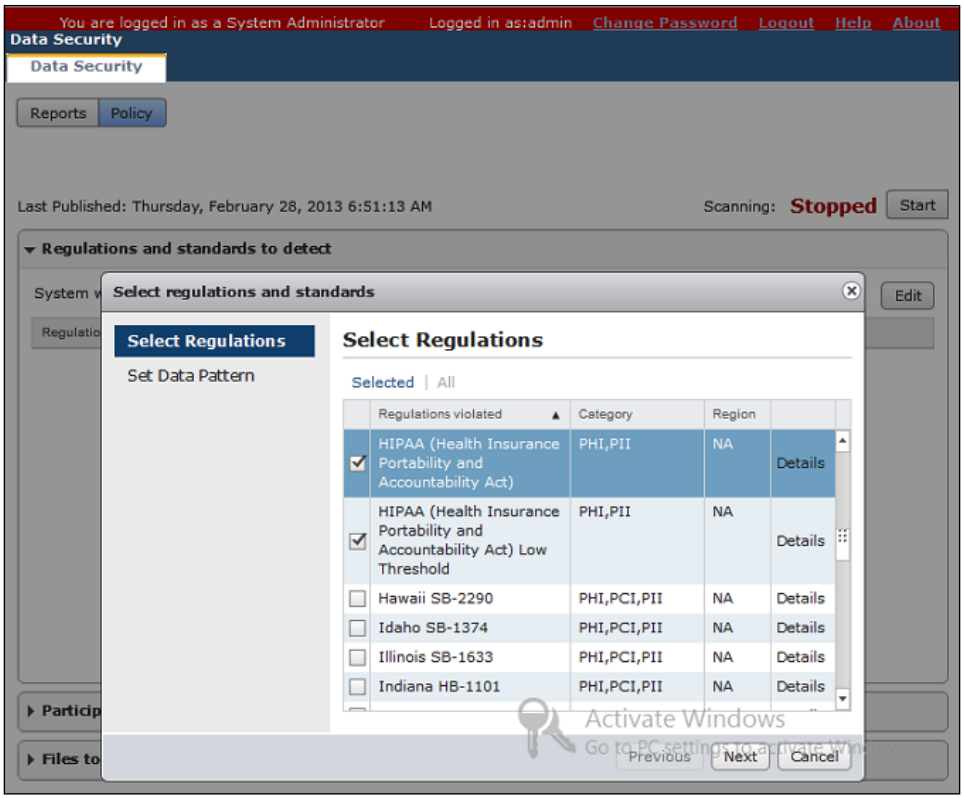
Let us look at the steps you need to perform for defining the vCloud Networking and Security Data Security policy:

1. Log in to the vCloud Networking and Security Manager web interface.
2. Click on the **Data Security** option under the **Settings and Reports** section on the left-hand side.



You can see that the scanning has stopped under the **Policy** tab. There are also no regulations and standards defined. To define them, perform the following steps:

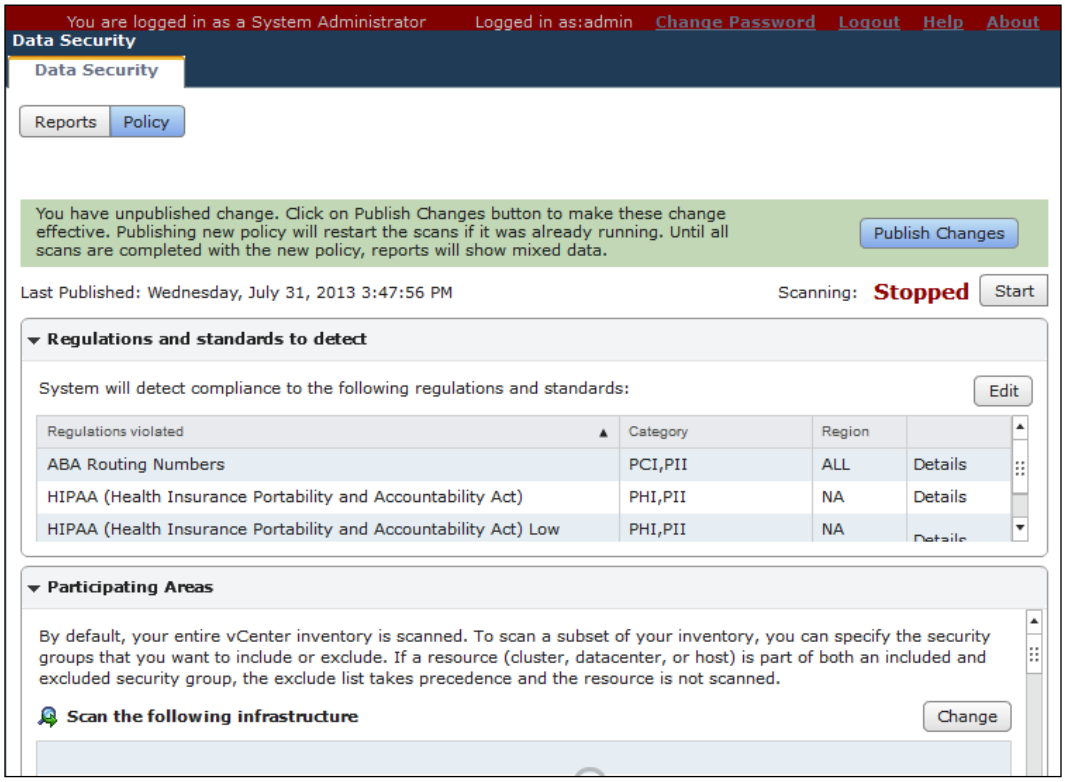
1. Expand the **Regulations and standards to detect** section.
2. Click on the **Edit** button.
3. A new window named **Select regulations and standards** will appear.
4. On this window, click on the **All** link to get all the regulations from the Data Security library.
5. For this example, select **HIPAA (Health Insurance Portability and Accountability Act)** and **HIPAA (Health Insurance Portability and Accountability Act) Low Threshold**.



6. Click on **Next**.
7. As these regulations do not require you to specify a pattern for recognizing sensitive data, click on **Finish** to complete the change.

In this example, we did not set a data pattern as it was not required for HIPAA. However, vCloud Networking and Security Networking and Security Data Security requires additional information to recognize sensitive data for certain regulations. You must provide a search pattern, which can be a regular expression.

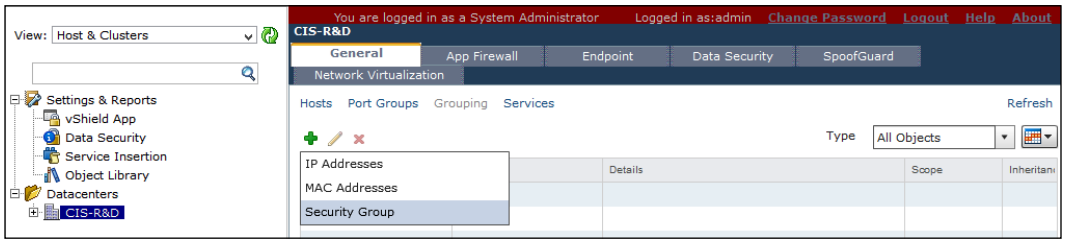
If you selected a regulation that monitors Group Insurance Numbers, Patient Identification Numbers, Medical Record Numbers, Health Plan Beneficiary Numbers, US Bank Account Numbers, Custom Accounts, or Student Identification Numbers, the **Select regulations and standards** wizard prompts you to set a data pattern for identifying that data. To make it effective, click on **Publish Changes**.



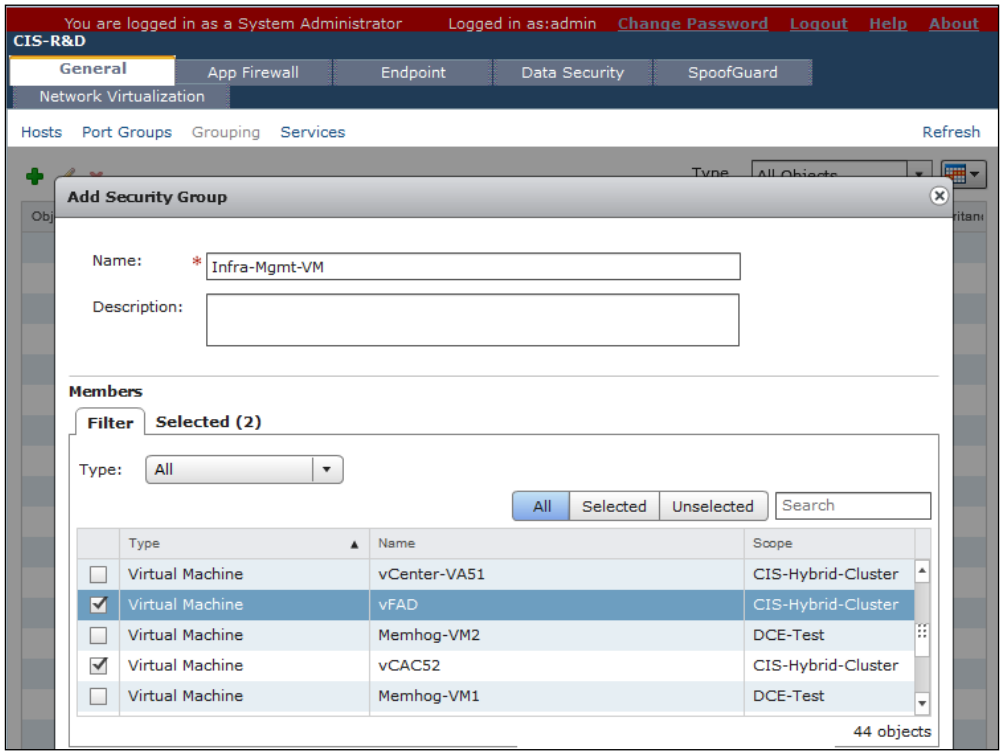
As discussed earlier, by default, your entire vSphere infrastructure is scanned by vCloud Networking and Security Data Security. To scan a subset of the inventory, you can include or exclude security groups. To create a security group, perform the following steps:

1. Select a datacenter from the **Datacenters** section on the left-hand side, navigate to **General | Grouping**, and click on the **+** icon.

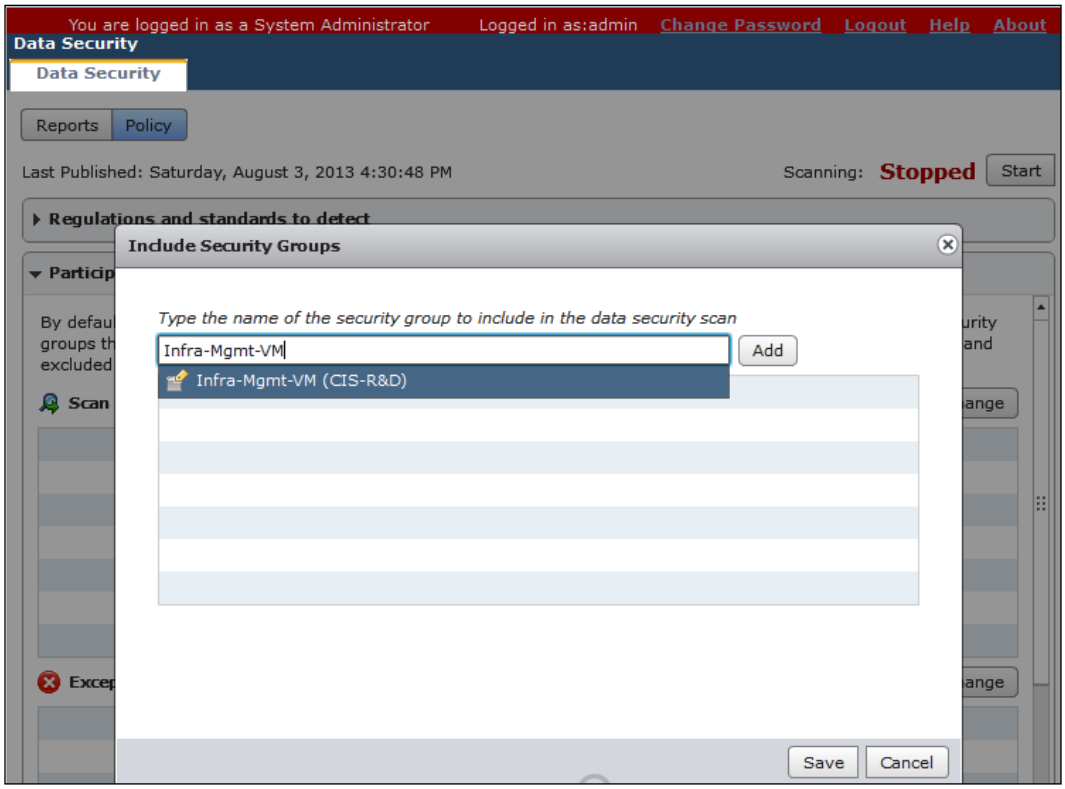
2. Select **Security Group**.



3. Specify a name for this security group.
4. Select the VMs that need to be part of it and click on **OK**, as you can see in the following screenshot:



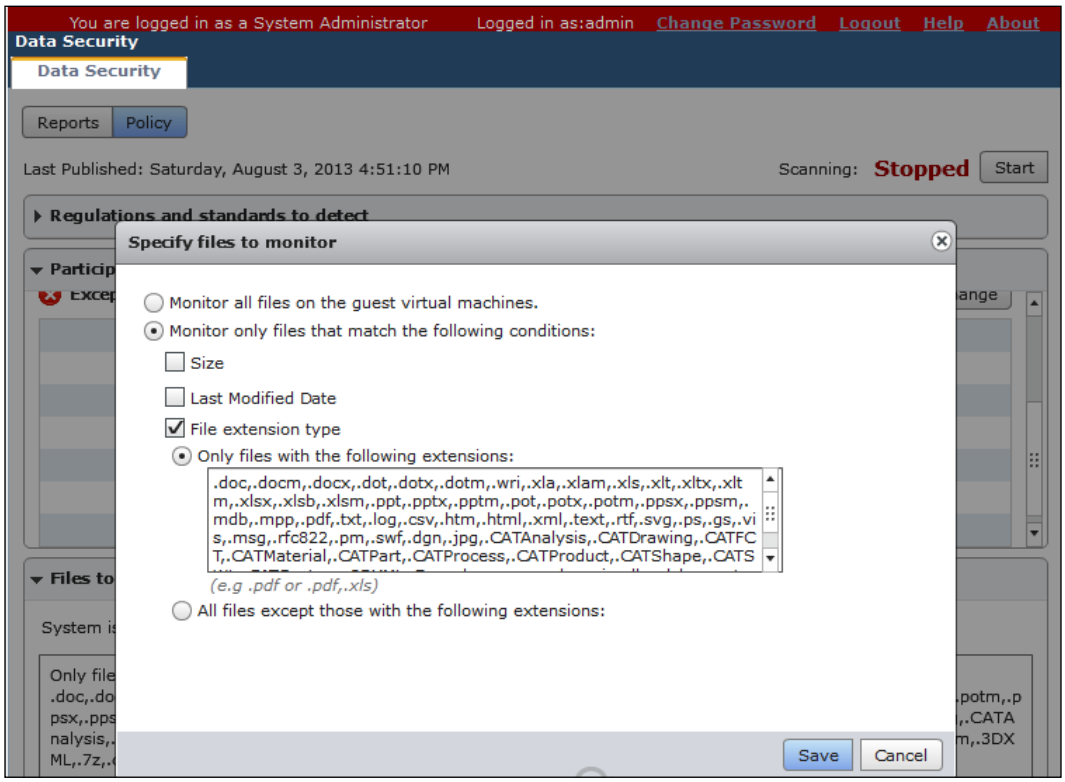
5. In the **Policy** tab of the **Data Security** panel, expand **Participating Areas**.
6. To include a security group in the Data Security scan, click on **Change**, which is next to **Scan the following infrastructure**.
7. Click on the **Include Security Groups** dialog box, which displays a list of security groups.
8. Select the security group to include in the scan and click on **Add**.



9. Click on **Save**.
10. If you are updating an existing policy, click on **Publish Changes** to apply it.

You can either monitor all files on the virtual machines in your inventory, or select and configure the restrictions that you want to apply. You can restrict the files that you want to scan based on the size, last modified date, or file extensions. All common file formats are permitted. To specify the file restrictions for scanning, perform the following steps:

1. In the **Policy** tab of the **Data Security** panel, expand the **Files to Scan** section and click on **Edit**.
2. Select either **Monitor All Files** or **Only files that match the following conditions**.
3. Click on **Save**.



4. Click on **Publish Changes** to make it effective.
5. Now click on **Start**.

When you start a security scan, vCloud Networking and Security displays the start and end time of each scan, the number of virtual machines scanned, and the number of violations detected. It also identifies data in your virtual environment that violates your defined regulations and standards.

There is a limitation to the Data Security scan; that is, if a virtual machine is powered off, it will not be scanned until it is powered on.

All virtual machines in your datacenter are scanned once during a scan, if not edited. If the Data Security policy is edited and published while a scan is running, the scan restarts. The rescan ensures that all virtual machines comply with the edited policy. A rescan is triggered by publishing an edited policy, not by data updates on the virtual machines.

vCloud Networking and Security Data Security reduces the number of virtual machines scanned on a host, one at a time, to minimize the impact on performance. VMware recommends that you pause the scan during normal business hours to avoid any performance overhead.

Scanning statistics and reports

There are a number of items displayed in the **Reports** tab that include the following:

- **Current scan status**: This mentions the status of the current scan.
- **Scan statistics**: This is a pie chart that displays the number of virtual machines that have been scanned, are being scanned, and are waiting to be scanned.
- **Violation information**: This displays information about the top regulations that have been violated and the virtual machines on which the most violations have been reported.
- **Scan history**: This mentions the start and end time of each scan, the number of virtual machines scanned, and the number of violations detected. You can click on **Download Complete Report** in the **Action** column to download the complete report for any scan.

After a Data Security scan completes, vCloud Networking and Security displays two reports:

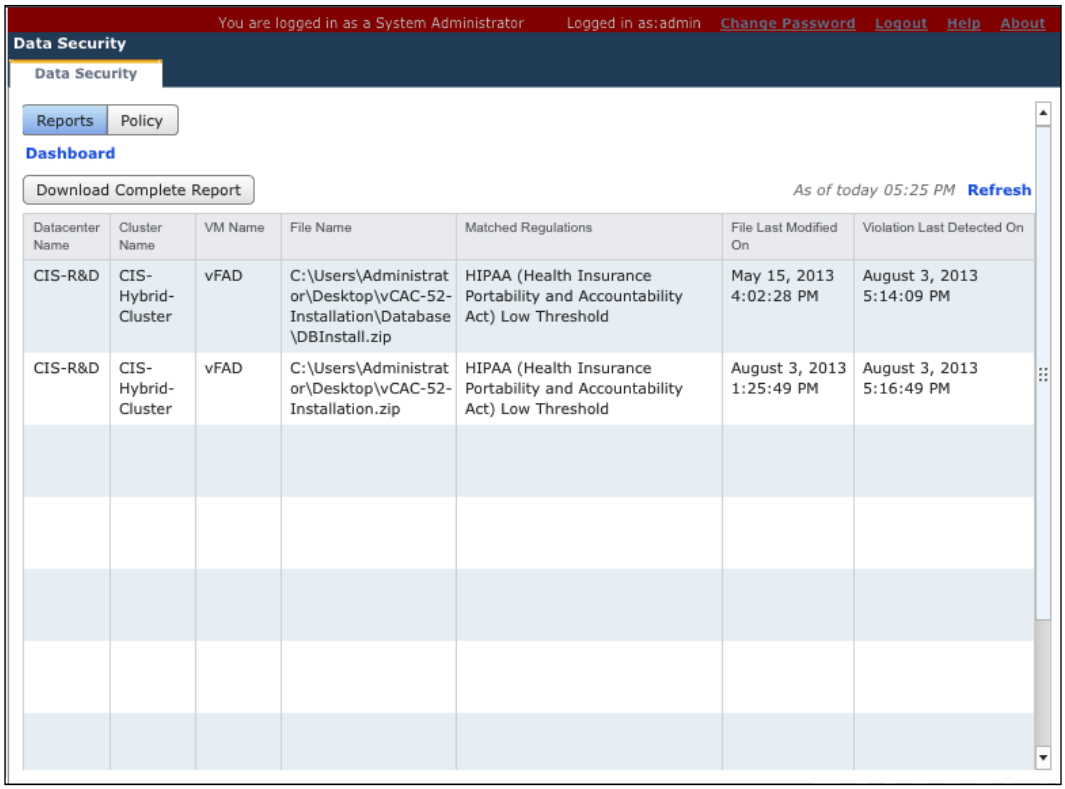
- **The violation counts report**: This displays each regulation or standard in your policy that is violated, and the number of times it is violated.

- **The violating files report**: This lists the datacenter, cluster, and virtual machine containing the files that violated the policy, the regulations or standards they violated, and the date and time at which the violations were detected. If you fix a violating file by deleting sensitive information from the file, deleting or encrypting the file, or editing the policy, the file continues to display in the violating files section until the next scan is completed.

Let us see how to generate the report and interpret it:

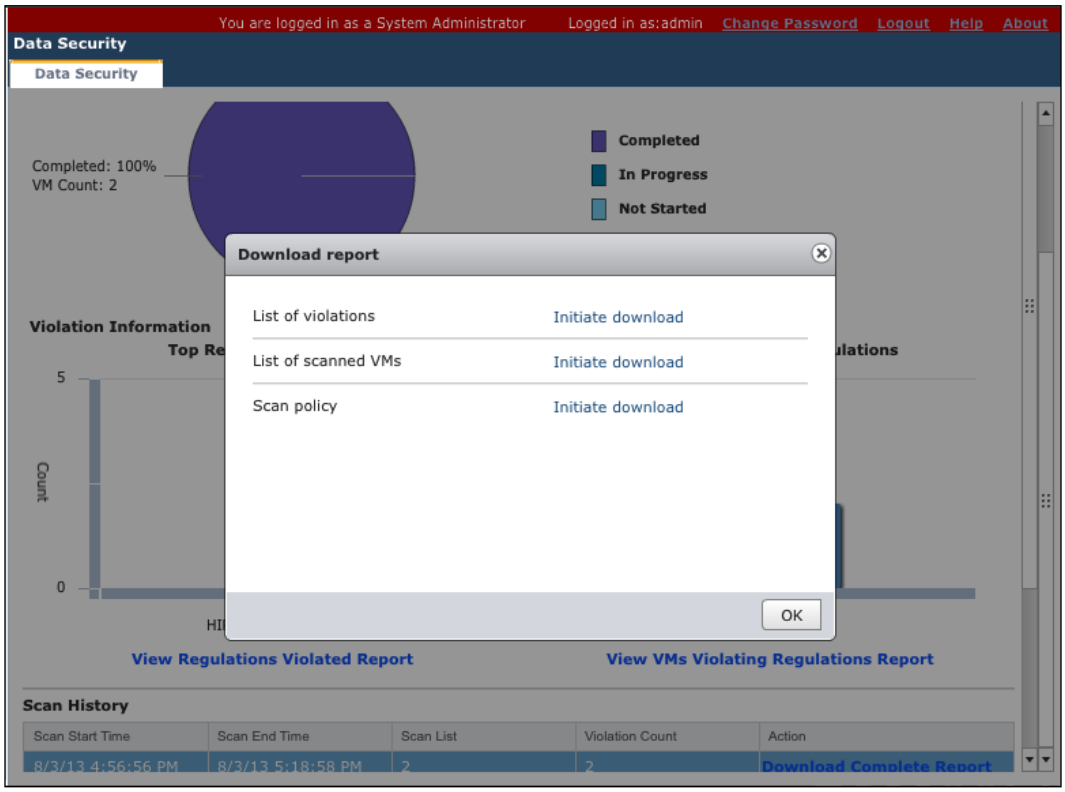
1. Log in to the vCloud Networking and Security Manager web interface.
2. Click on **Data Security** under the **Settings and Reports** section.
3. At the right-hand side, select the **Reports** tab. Here you can see **Last Scan Statistics**, **Violation Information**, **Top VMs Violating Regulations**, and **Scan History**.

4. If you want to view the VMs that violate the regulations, click on the **View VMs Violating Regulations Report** link in the bottom-right corner. It will show you which VM has violated regulations and which file is the culprit. It will also tell you which regulations have been violated.



5. If you want to have complete reports, go to the **Scan History** section and click on **Download Complete Report**.
6. You will be able to generate three reports here. They are **List of violations** (a CSV file), **List of scanned VMs** (a CSV file), and **Scan policy** (an XML file).

7. Click on **Initiate Download** on each section to get the complete report.



8. Once it is done, you will see the **Download** link there. Click on each link to download the report.

Summary

vCloud Networking and Security Data Security analyzes the data on the virtual machines in your vSphere inventory, which is the base of your vCloud environment, and reports the number of violations detected and the files that violated your data security policy.

You can install vCloud Networking and Security Data Security only after installing vShield Endpoint.

A data security policy determines the inventory to scan and which regulations are applied to the data. You can use the violation reports to determine where data resides so that you can verify whether it is adequately protected.

Index

T

V

W

Thank you for buying

VMware vCloud Security

About Packt Publishing

Packt, pronounced 'packed', published its first book "Mastering phpMyAdmin for Effective MySQL Management" in April 2004 and subsequently continued to specialize in publishing highly focused books on specific technologies and solutions.

Our books and publications share the experiences of your fellow IT professionals in adapting and customizing today's systems, applications, and frameworks. Our solution based books give you the knowledge and power to customize the software and technologies you're using to get the job done. Packt books are more specific and less general than the IT books you have seen in the past. Our unique business model allows us to bring you more focused information, giving you more of what you need to know, and less of what you don't.

Packt is a modern, yet unique publishing company, which focuses on producing quality, cutting-edge books for communities of developers, administrators, and newbies alike. For more information, please visit our website: `www.packtpub.com`.

About Packt Enterprise

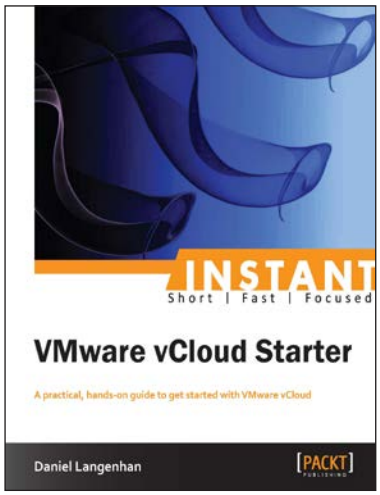
In 2010, Packt launched two new brands, Packt Enterprise and Packt Open Source, in order to continue its focus on specialization. This book is part of the Packt Enterprise brand, home to books published on enterprise software – software created by major vendors, including (but not limited to) IBM, Microsoft and Oracle, often for use in other corporations. Its titles will offer information relevant to a range of users of this software, including administrators, developers, architects, and end users.

Writing for Packt

We welcome all inquiries from people who are interested in authoring. Book proposals should be sent to `author@packtpub.com`. If your book idea is still at an early stage and you would like to discuss it first before writing a formal book proposal, contact us; one of our commissioning editors will get in touch with you.

We're not just looking for published authors; if you have strong technical skills but no writing experience, our experienced editors can help you develop a writing career, or simply get some additional reward for your expertise.

[PACKT] enterprise
professional expertise distilled
PUBLISHING



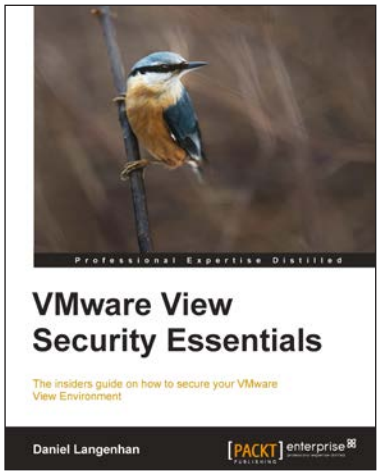
Instant VMware vCloud Starter

ISBN: 978-1-84968-996-0 Paperback: 76 pages

A practical, hands-on guide to get started with VMware vCloud

1. Learn something new in an Instant! A short, fast, focused guide delivering immediate results
2. Deploy and operate a VMware vCloud in your own demo kit
3. Understand the basics about the cloud in general and why there is such a hype
4. Build and use templates to quickly deploy complete environments

---



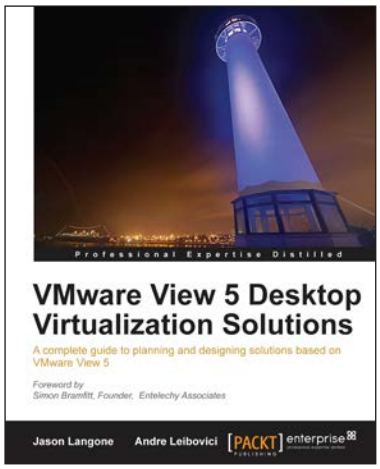
VMware View Security Essentials

ISBN: 978-1-78217-008-2 Paperback: 130 pages

The insiders guide to how to secure your VMware View Environment

1. Discover how to correctly implement View connection, security, and transfer servers
2. Understand all the firewall rules and the basics of multi-layered security
3. Secure all your connections between client and desktop

[PACKT] enterprise
professional expertise distilled
PUBLISHING



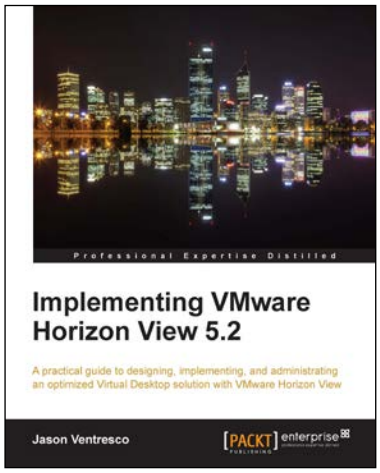
VMware View 5 Desktop Virtualization Solutions

ISBN: 978-1-84968-112-4 Paperback: 288 pages

A complete guide to planning and designing solutions based on VMware View 5

1. Written by VMware experts Jason Langone and Andre Leibovici, this book is a complete guide to planning and designing a solution based on VMware View 5
2. Secure your Visual Desktop Infrastructure (VDI) by having firewalls, antivirus, virtual enclaves, USB redirection and filtering and smart card authentication
3. Analyze the strategies and techniques used to migrate a user population from a physical desktop environment to a virtual desktop solution

---



Implementing VMware Horizon View 5.2

ISBN: 978-1-84968-796-6 Paperback: 390 pages

A practical guide to designing, implementing, and administrating an optimized Virtual Desktop solution with VMware Horizon View

1. Detailed description of the deployment and administration of the VMware Horizon View suite
2. Learn how to determine the resources your virtual desktops will require
3. Design your desktop solution to avoid potential problems, and ensure minimal loss of time in the later stages