Professional Expertise Distilled

Hyper-V Replica Essentials

Ensure business continuity and improve your disaster recovery policy using Hyper-V Replica

Vangel Krstevski

[PACKT] PUBLISHING enterprise professional expertise distilled

www.allitebooks.com

Hyper-V Replica Essentials

Ensure business continuity and improve your disaster recovery policy using Hyper-V Replica

Vangel Krstevski

[PACKT] PUBLISHING enterprise professional expertise distilled

BIRMINGHAM - MUMBAI

www.allitebooks.com

Hyper-V Replica Essentials

Copyright © 2013 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing, and its dealers and distributors will be held liable for any damages caused or alleged to be caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

First published: October 2013

Production Reference: 1031013

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

ISBN 978-1-78217-188-1

www.packtpub.com

Cover Image by Gerard Eykhoff (gerard@eykhoff.nl)

www.allitebooks.com

Credits

Author
Vangel Krstevski

Reviewers
Adam Ball
Milton Goh

Acquisition Editor
Rebecca Youe

Lead Technical Editor
Sharvari Tawde

Technical Editors
Pragnesh Bilimoria
Sandeep Madnaik
Larissa Pinto

Project Coordinator
Amigya Khurana

Proofreader
Clyde Jenkins

Indexer
Monica Ajmera Mehta

Graphics
Yuvraj Mannari

Production Coordinator
Arvindkumar Gupta

Cover Work
Arvindkumar Gupta

www.allitebooks.com

About the Author

Vangel Krstevski is an IT prodigy, excelling in virtualization and network design. He is an expert in virtualization deployment and management. He is a strong team player with an affinity for details. His strengths are excellent communication skills, hands-on experience with various Microsoft products, ability to manage conflicts, and accomplish demands to agreed standards and timelines.

He has experience in planning, designing, deploying, and managing various Microsoft products. All of this has been acquired in his three years of experience in IT, working as a System and Network Engineer.

His product skills set include Microsoft infrastructure technologies, such as Hyper-V, System Center Suite, Windows Server, MS SQL Server, Exchange Server, IIS, Active Directory, and Forefront. He also has knowledge of configuring DELL, SonicWall, and CISCO networking equipment.

He is CISCO CCNA 640-802 certified.

He currently works at Re-Aktiv, a software consulting company in Skopje, Macedonia.

He led the implementation of Microsoft System Center Operations Manager for the Central Registry of the Republic of Macedonia.

www.allitebooks.com

About the Reviewers

Adam Ball has been in various engineering/leadership roles in IT for more than 15 years. Over the last seven years, he has become focused on virtualization and Microsoft UC products. In addition, he has spent time as a Unix/Linux administrator, and as a storage administrator.

ExtraTeam is a leading provider of innovative IT solutions to corporate and public-sector businesses. They are certified experts at information and communication technologies, and convergent services. ExtraTeam designs, implements, and supports infrastructure projects for customers across a variety of markets. Our engineers are experienced at network architectures, high availability, infrastructure optimization, datacenter virtualization, SharePoint, video conferencing and telepresence, security, storage, and network resource management.

www.allitebooks.com

Milton Goh has been in the Information Technology and Management field since 2005. He started as a Software Developer meddling with Visual Basic .NET and later moved on to Visual C# .NET as his primary programming language. He has played multiple roles throughout the years in his career as a developer, consultant, and architect completing more than two dozens of small to large projects delivered to small- and medium-sized businesses, and enterprise organizations.

He currently works with Dimension Data (Singapore) as a consultant that works with projects that leverage Microsoft products to solve business problems. On top of that, he leads a team of developers that does development work on an IT Service Management Tool that helped enterprise customer to adopt the whole ITIL framework. He also joined the top league players in the organization as a Premier Field Engineer to help enterprise customer solve problem(s) they faced with the Microsoft solutions.

Prior to joining Dimension Data (Singapore), he has worked in a Small and Medium Enterprise (SME) as a Solutions Consultant that deals with Microsoft solutions for the government bodies.

Over the years, he has worked with most Microsoft products but has strong knowledge in Microsoft SharePoint and Windows Servers.

During his free time, he would contribute through user groups in Singapore and through online forum. He also spends time writing articles at his web blog, and he is an author at the Spiffy committee (`www.spiffy.sg`).

I would like to thank the team at Packt Publishing, for they have given me a chance to be a Technical Reviewer for this amazing book. I would like to thank my family for supporting me all along for the time I spent with my lab environment, when I am not at work. Lastly, I would like to thank the most important lady in my life, Cindy Askara, for her understanding all the while when I am busy with my research and development work.

---

www.allitebooks.com

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.

www.allitebooks.com

www.allitebooks.com

Table of Contents

Preface 1

Chapter 1: Introducing Hyper-V Replica 5

- **Understanding virtualization** 5
- **Hyper-V 3.0 features** 5
- **Prerequisites for Hyper-V Replica** 7
- **Installing Hyper-V** 7
- **Hyper-V Replica functionalities** 10
  - Hyper-V Replica replication manager 10
  - Hyper-V Replica replication tracker 10
  - Hyper-V Replica broker manager 11
- **Security considerations** 11
- **Summary** 12

Chapter 2: Failover Clustering 13

- **The Server Message Block protocol** 13
- **Installing and configuring the SMB server** 14
  - Setting up iSCSI connections 18
  - Setting up networking 21
  - Setting up security permissions on SMB file shares 23
- **Setting up a failover cluster** 23
- **Migration of virtual machines** 29
- **Summary** 31

Chapter 3: Configuring Hyper-V Replica 33

- **Hyper-V Replica requirements** 33
- **Hyper-V Replica in standalone Hyper-V hosts environment** 34
  - Configuring Hyper-V replica on a server in a replica site 34
  - Configuring virtual machines for replication 36
  - Configuring firewall rules 46

www.allitebooks.com

Virtual machine replication in Failover Cluster environment **49**
Failover scenarios **51**
Test failover 52
Planned failover 52
Unplanned failovers 53
Summary **53**
Chapter 4: Authentication in Hyper-V Replica **55**
Hyper-V Replica authentication types **55**
Nonencrypted communication **56**
Encrypted communication **57**
Creating a certificate template 58
Requesting and importing a certificate 64
Authenticating with a self-signed certificate 69
Summary **69**
Chapter 5: Administrating Hyper-V Replica **71**
Managing Hyper-V Replica **71**
Primary site management 72
Replica site management 73
Administration of certificates **75**
Summary **76**
Summary **77**
Index **79**

Preface

Hyper-V Replica Essentials is a step-by-step guide for configuring Hyper-V Replica in various deployment scenarios, which will help you learn how to configure this new feature and improve the systems' availability in your datacenter. This book will give you an overview of what Hyper-V Replica is. Then, it will take you through all the prerequisites you need to properly configure it, which will help you take advantage of this easy-to-configure disaster recovery tool. You will learn how to set up a modern datacenter with the help of a new concept called Server Message Block (SMB) from Windows Server 2012. We will also take a look at how you can configure Hyper-V Replica in your existing environment, whether it is a clustered or non-clustered environment, and how to secure your data with the use of certificates.

What this book covers

Chapter 1, *Introducing Hyper-V Replica*, will take a deep dive into virtualization and its importance to the modern enterprises. You will also get to know about the new features of Windows Server 2012 called Hyper-V Replica; its functionalities, values, and components.

Chapter 2, *Failover Clustering*, introduces a new concept for file sharing and application data storage called SMB. It will also show you how install Hyper-V on a server and join servers in a Failover Cluster.

Chapter 3, *Configuring Hyper-V Replica*, is all about different configurations of Hyper-V Replica, depending on the various infrastructure models. This chapter will teach you how to configure Hyper-V in a cluster environment or in a standalone host environment.

Chapter 4, *Authentication in Hyper-V Replica*, will show you how to encrypt the communication between the Primary and the Replica site with the help of certificates.

Chapter 5, *Administration of Hyper-V Replica*, will teach you how to maintain Hyper-V Replica configuration and troubleshoot the Hyper-V Replica issues.

What you need for this book

The only thing you need for this book is a Microsoft Windows Server 2012.

Who this book is for

This book is excellent for Windows Server administrators who want to improve their system availability and speed disaster recovery. It is imperative that you have experience in Hyper-V deployment because Hyper-V Replica is built in the Hyper-V platform.

Conventions

In this book, you will find a number of styles of text that distinguish among different kinds of information. Here are some examples of these styles, and an explanation of their meaning.

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: "clicking the **Next** button moves you to the next screen".

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.

Downloading the example code

You can download the example code files for all Packt books you have purchased from your account at `http://www.packtpub.com`. If you purchased this book elsewhere, you can visit `http://www.packtpub.com/support` and register to have the files e-mailed directly to you.

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
Introducing Hyper-V Replica

In this chapter, we will take a look at how modern data centers are built. We will see what virtualization is, and why it is very appealing to IT departments. We will look at Windows Server 2012, and how we can use some of its new features and functionalities to build a modern data center. We will learn about Hyper-V 3.0, which is the latest edition of Microsoft hypervisor. The main focus on the chapter will be to understand a new feature of Hyper-V 3.0, called Hyper-V Replica which adds business continuity and disaster recovery value to the data center.

Understanding virtualization

Virtualization is a concept in IT that has its root back in 1960 when mainframes were used. In recent years, virtualization became more available because of different user-friendly tools, such as Microsoft Hyper-V, were introduced to customers. These tools allow the administrator to configure and administer a virtualized environment easily. Virtualization is a concept where a hypervisor, which is a type of middleware, is deployed on a physical device. This hypervisor allows the administrator to deploy many virtual servers that will execute its workload on that same physical machine. In other words, you get many virtual servers on one physical device. This concept gives better utilization of resources and thus it is cost effective.

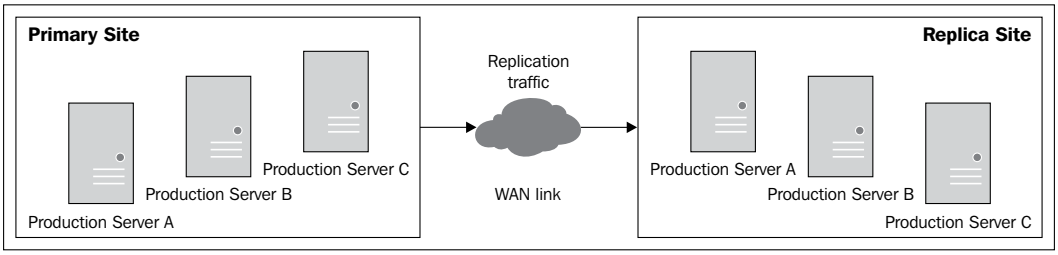
Hyper-V 3.0 features

With the introduction of Windows Server 2008 R2, two new concepts regarding virtual machine high availability were introduced. Virtual machine high availability is a concept that allows the virtual machine to execute its workload with minimum downtime. The idea is to have a mechanism that will transfer the execution of the virtual machine to another physical server in case of node malfunctioning. In Windows Server 2008 R2, a virtual machine can be live migrated to another Hyper-V host. There is also quick migration, which allows multiple migrations from one host to another host.

In Windows Server 2012, there are new features regarding Virtual Machine Mobility. Not only can you live migrate a virtual machine but you can also migrate all of its associated files, including the virtual machine disks to another location. Both mechanisms improve high availability. Live migration is a functionality that allows you to transfer the execution of a virtual machine to another server with no downtime. Previous versions of Windows Server lacked disaster recovery mechanisms. Disaster recovery mechanism is any tool that allows the user to configure policy that will minimize the downtime of systems in case of disasters. That is why, with the introduction of Windows Server 2012, Hyper-V Replica is installed together with Hyper-V and can be used in clustered and in non-clustered environments. Windows Failover Clustering is a Windows feature that is installed from the **Add Roles and Features Wizard** from Server Manager. It makes the server ready to be joined to a failover cluster. Hyper-V Replica gives enterprises great value, because it is an easy to implement and configure a **Business Continuity and Disaster Recovery** (**BCDR**) solution. It is suitable for Hyper-V virtualized environments because it is built in the Hyper-V role of Windows Server 2012. The outcome of this is for virtual machines running at one site called primary site to be easily replicated to another backup site called replica site, in case of disasters. The replication between the sites is done over an IP network, so it can be done in LAN environments or across WAN link. This BCDR solution provides efficient and periodical replication. In case of disaster it allows the production servers to be failed over to a replica server. This is very important for critical systems because it reduces downtime of those systems. It also allows the Hyper-V administrator to restore virtual machines to a specific point in time regarding recovery history of a certain virtual machine.

To create a failover cluster, there must be at least two physical servers.

In the following screenshot, we can see a simple Hyper-V Replica scenario consisting of a **Primary Site** and a **Replica Site**:



Prerequisites for Hyper-V Replica

Hyper-V Replica has a few prerequisites that you must fulfill before you can begin deployment. These prerequisites are as follows:

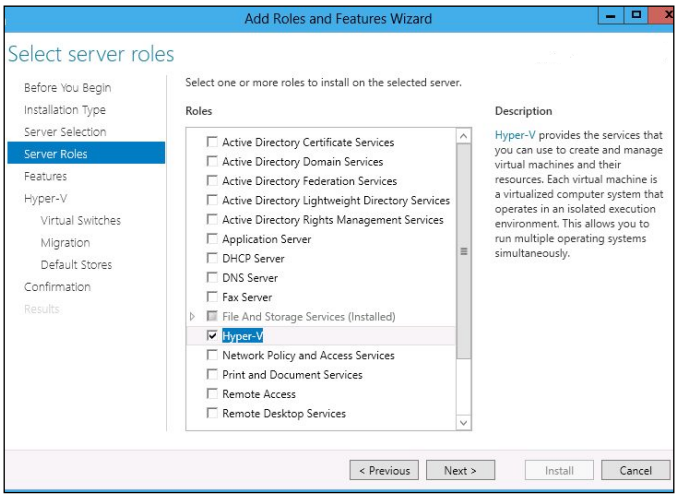
- Windows Server 2012 installed on physical machines
- Certificates for data encryption (optional)
- Network connection between primary and replica sites

It is important to say that for Hyper-V to work, both sides can have vendor-neutral servers and storage. It means that server model and storage model don't have to be the identical on both sides.

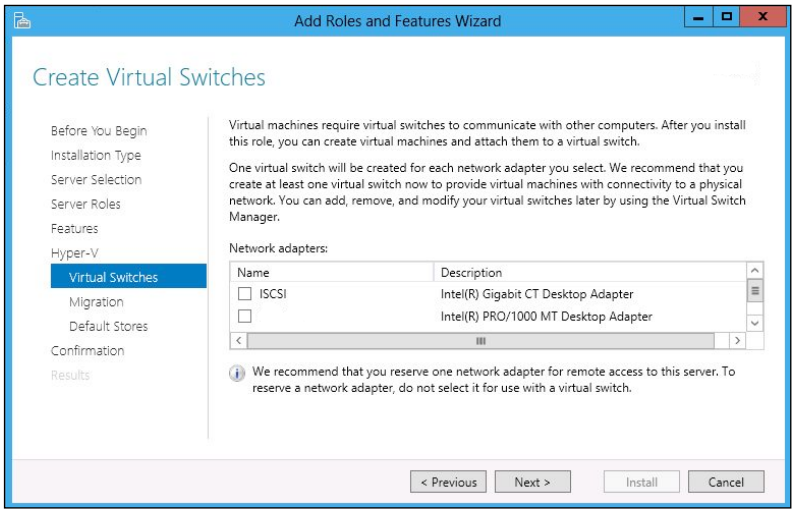
Installing Hyper-V

Hyper-V Replica is a built-in feature of the Hyper-V Role Version 3.0. Hyper-V 3.0 is only available if you have Windows Server 2012. Hyper-V servers can be part of a Workgroup or an Active Directory Domain. When you deploy Hyper-V Replica in standalone hosts environment, primary and replica sites can be in different Active Directory domains. If you deploy Hyper-V Replica in a failover cluster environment then the Hyper-V servers have to be part of a same Active Directory domain. Hyper-V Replica is installed together with the Hyper-V Role. To install the Hyper-V Role on a server, you have to use the **Add Role and Feature Wizard**, found in Server Manager. When the installation of Hyper-V role is finished, the server must be restarted.

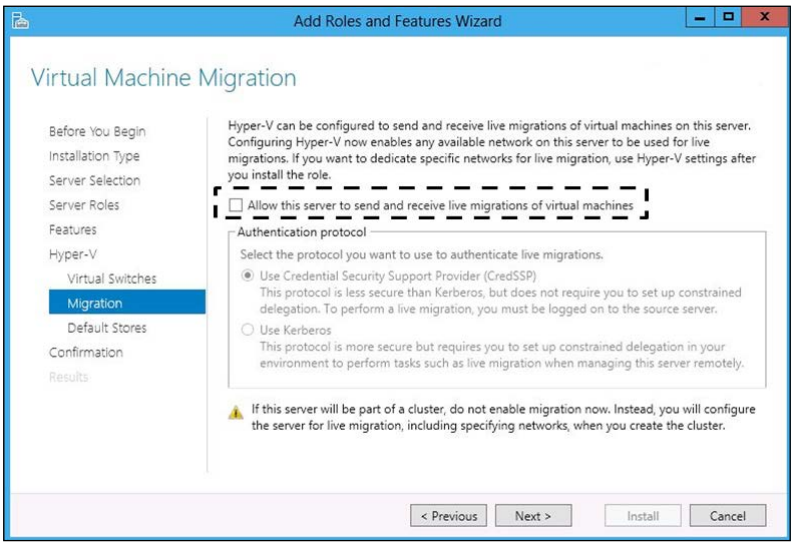
1. Navigate to **Server Manager** | **Add Roles**. When you open it, you will see a window like the following screenshot. From the list of roles select **Hyper-V**.



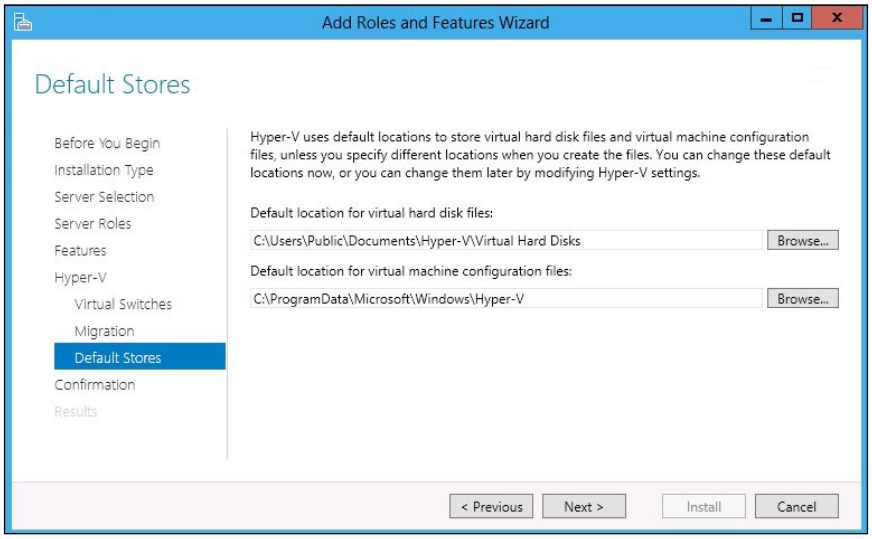
2. The wizard asks you if you want to create **Virtual Switches**. A Virtual Switch is deployed on a physical network adapter to allow multiple virtual machines to use it. If you don't want to create a switch within the wizard, you can do it later from the Hyper-V Management console. The next screenshot shows the virtual switch configuration window:



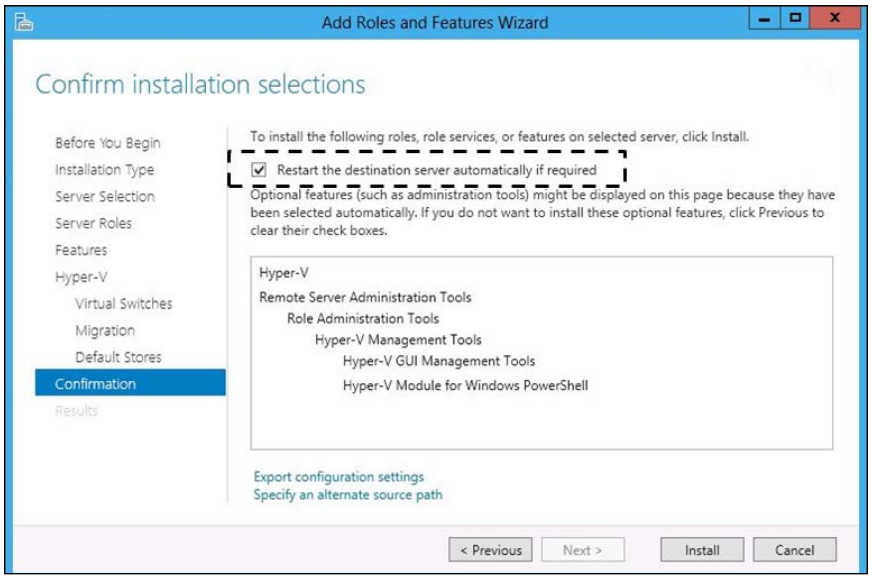
3. Setup your Hyper-V server for live migration. To do this, check the **Allow this server to send and receive live migrations of virtual machines** checkbox. The following screenshot shows the configuration window for live migrations:



4. Specify the default location where virtual machine data files will be stored. The next screenshot shows the configuration window for virtual hard disk location:



5. In the final step, check the **Restart the destination server automatically if required** checkbox, and then click on **Install** to finish configuring and start the Hyper-V installation. You can see the configuration window in the next screenshot:



www.allitebooks.com

Hyper-V Replica functionalities

The main functionality of Hyper-V Replica is to allow virtual machine replication over a LAN/WAN to a remote site with only the functionalities included in Windows Server 2012. For all this to work, there are four core Hyper-V Replica functionalities that allow this. These functionalities are as follows:

- Replication
- Change tracking
- Network
- Hyper-V Replica Broker

Hyper-V Replica replication manager

The main task of Hyper-V Replica replication manager is replication of Hyper-V Replica enabled virtual machines. It is responsible for: initial replication, change replication, failover, failback, and test failover. When a live migration is performed, the replication manager halts replication and resumes it after the migration is completed.

Hyper-V Replica replication tracker

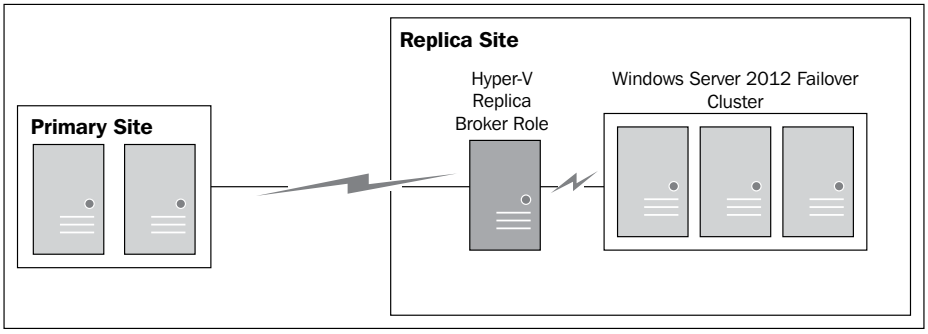
The main tasks of Hyper-V Replica replication tracker are to save the virtual machine state and replicate only the changes to the replica site. The default replication interval is five minutes. All of the changes that happened inside the virtual machine for the last five minutes are replicated to the replica site. Replication tracker also gives you the opportunity to set different recovery history settings for your virtual machines. The following three are the recovery history settings:

- **Store only the latest recovery point**: Only one point-in-time state of the virtual machine is kept at the replica site, which is the current state.
- **Store multiple recovery points**: Multiple recovery point means that there can be more than one point-in-time restore point of the virtual machine. By default, multiple recovery point replication happens every 60 minutes. After the limit of recovery points is reached the oldest recovery point is overwritten.
- **Store multiple recovery points with Application-Consistent**: This type of replication also saves the application data that is running inside the virtual machine. It uses the **WMI** (**Windows Management Instrumentation**) Service to extract the data from the applications.

Hyper-V Replica broker manager

The main tasks of Hyper-V Replica broker manager are to send and receive replication traffic in a failover cluster environment. When you have a failover cluster, whether it is in your primary or replica site, you must install Hyper-V Replica Broker role. The role is installed on the failover cluster like any other failover cluster role. This role looks for live migrations of Hyper-V Replica enabled virtual machines. It provides right and continuous replication of virtual machines in a cluster environment.

In the following image, we can see how Hyper-V Replica Broker role works:



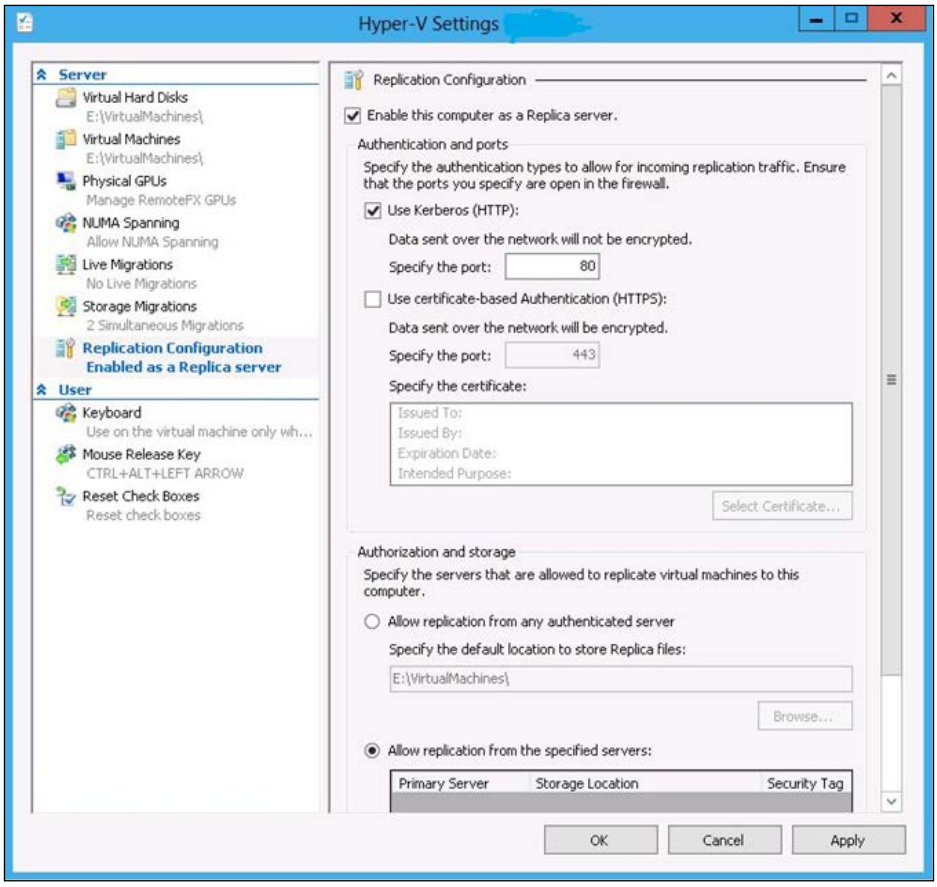
Security considerations

Restricting access to Hyper-V is very important. You want only authorized users to have access to the management console of Hyper-V. When Hyper-V is installed, a local security group on the server is created. It is named Hyper-V Administrators. Every user that is member of this group can access and configure Hyper-V settings. Another way to increase security of Hyper-V is to change the default port numbers of Hyper-V Authentication. By default, Kerberos uses port number 80, and Certificate Authentication uses port number 443. Certificated also encrypts the traffic generated from primary to replica site. And at last, you can create a list of authorized servers from which replication traffic will be received.

Downloading the example code

You can download the example code files for all Packt books you have purchased from your account at `http://www.packtpub.com`. If you purchased this book elsewhere, you can visit `http://www.packtpub.com/support` and register to have the files e-mailed directly to you.

The following screenshot shows the security options that you can configure in Hyper-V Replica:



Summary

In this chapter, we learned about what virtualization is and why is it important to modern enterprises. We learned about Hyper-V, which is a platform for virtualization, how to install it, and what its functions are. We were introduced to a new feature of Windows Server 2012 called Hyper-V Replica. We took a look at its functionalities, its values, and components.

In the next chapter, we will learn how to build a modern data center, and set up a failover cluster environment with Windows Server 2012.

2
Failover Clustering

In this chapter, we will take a look at Windows Failover Clustering, which is a feature of Windows Server. It allows the administrator to join separate Hyper-V servers in one cluster. This failover cluster ensures virtual machine availability in case of Hyper-V host malfunction.

The Server Message Block protocol

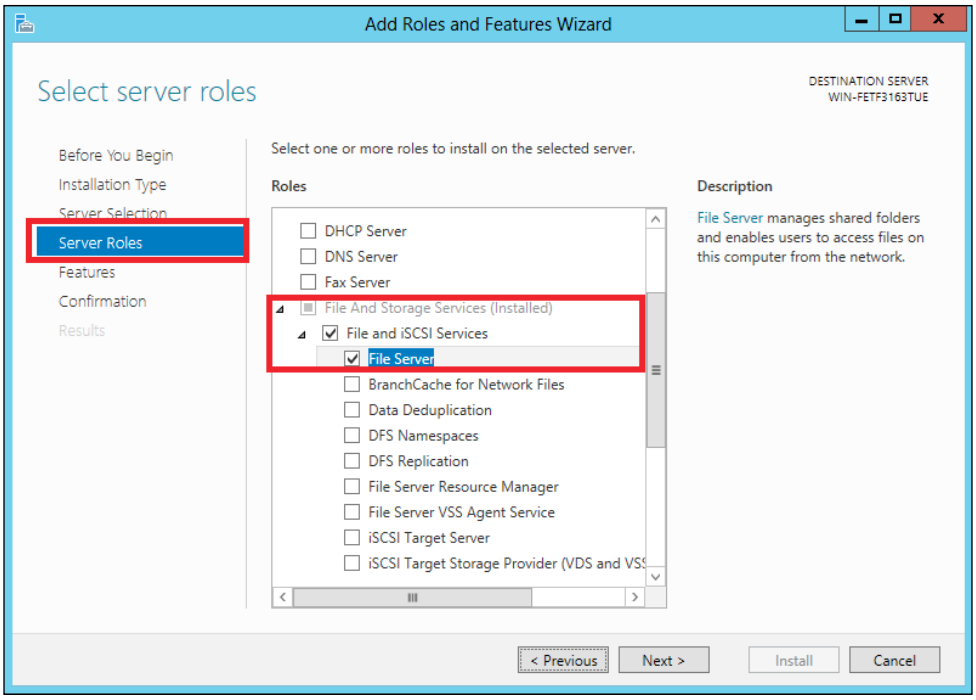
When an enterprise starts to build a modern datacenter, the first thing that should be done is to set up the storage. With the introduction of Windows Server 2012, a new improved version of the **Server Message Block** (**SMB**) protocol is introduced. The SMB is a file sharing protocol. This new version is 3.0 and is designed for modern datacenters. It allows administrators to create file shares and deploy critical systems on them. This is really good, because now administrators have to deal with file shares and security permissions, instead of complex connections to storage arrays. The idea is to set up one central SMB file-sharing server and attach the underlying storage to it. This SMB server initiates connection to the underlying storage. The logical disks created on the storage are attached to this SMB server. Then different file shares are created on it with different access permissions. These file shares can be used by different systems, such as Hyper-V storage space for virtual machine files, MS SQL server database files, Exchange Server database files, and so on. It is an advantage, because all of the data is stored on one location, which means easier administration of data files.

It is important to say that this is a new concept and is only available with Windows Server 2012. It comes with no performance degradation on critical systems, because SMB v3.0 was designed for this type of data traffic.

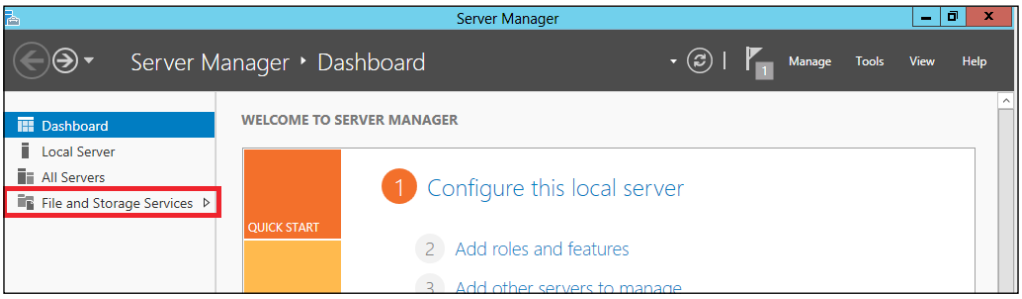
Installing and configuring the SMB server

In order to use SMB v3.0, you have to install Windows Server 2012 on your SMB file-sharing server. After that, it is really simple, because SMB installs as a Windows Server Role from the Add Remove Roles Wizard. The following are the steps to create an SMB file share:

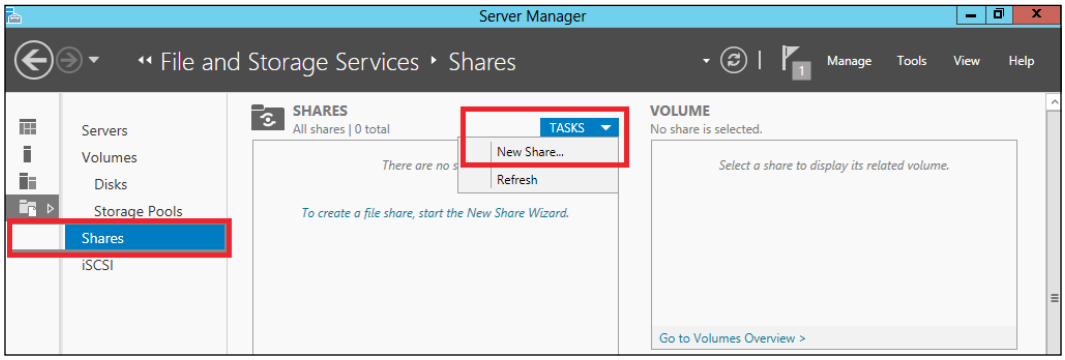
1. From the **Add Roles and Feature Features Wizard**, select **File Server** role under **File And Storage Services (Installed) | File and iSCSI Services**.



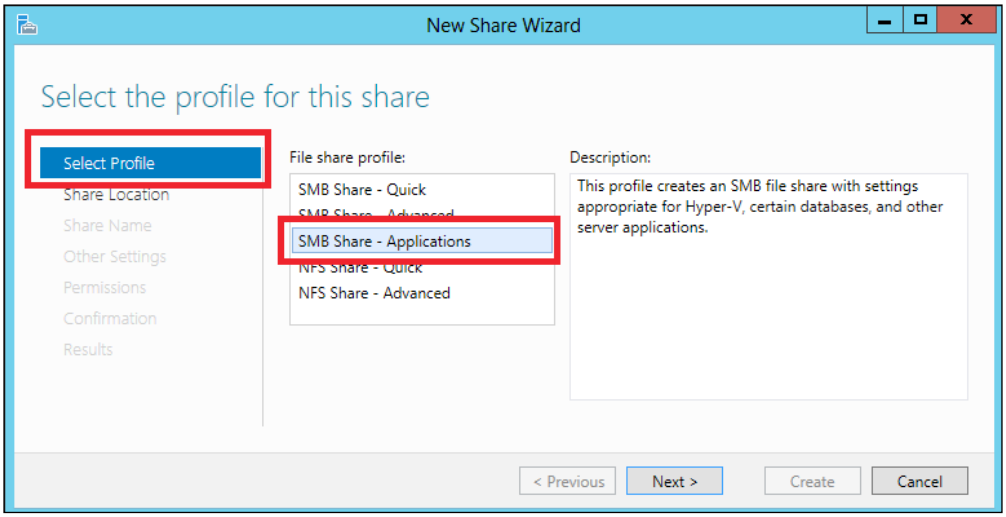
2. After the role is successfully installed from the Server Manager, locate and access on the left-hand side **File and Storage Services**.



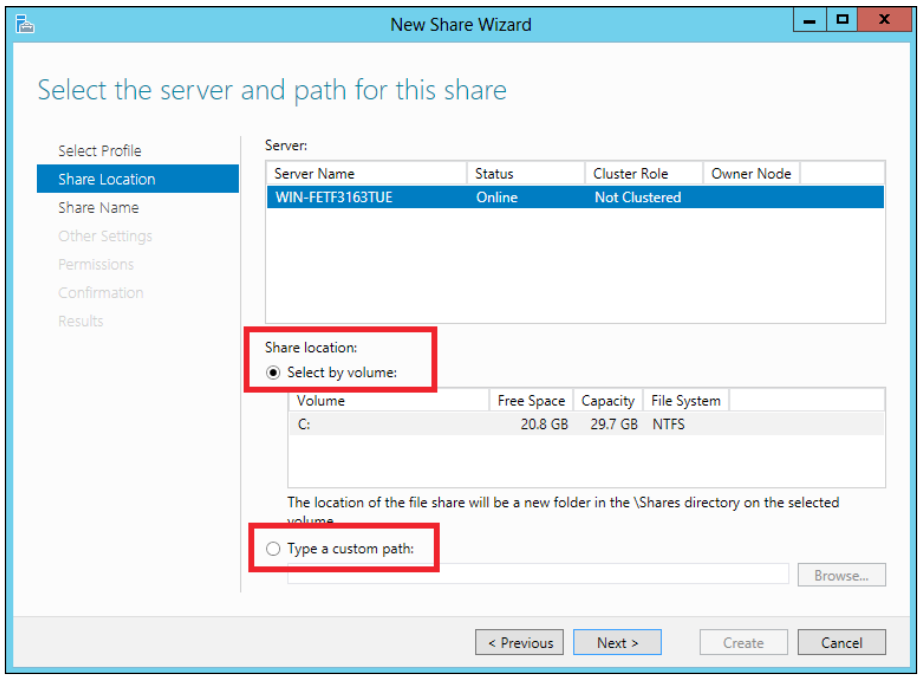
3. From the menu, access **Shares** and then click on **TASKS** on the top of the window. There appears a **New Share** option. Click on it.



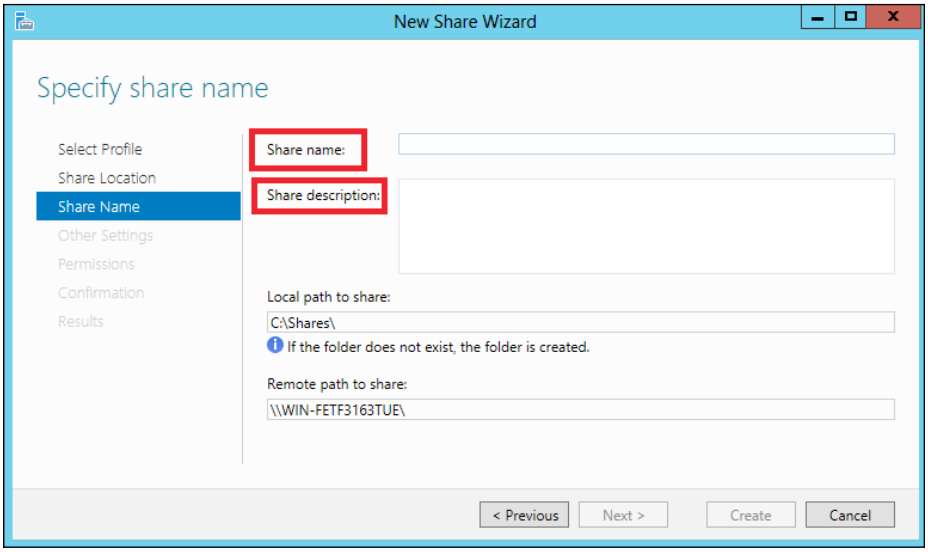
4. Next, in the new menu, there will be five options from which to select. In order to create SMB file share suitable for applications, select the third option **SMB Share - Applications**. The reason we select this type of share is because it can be used for server applications such as Hyper-V and MS SQL.



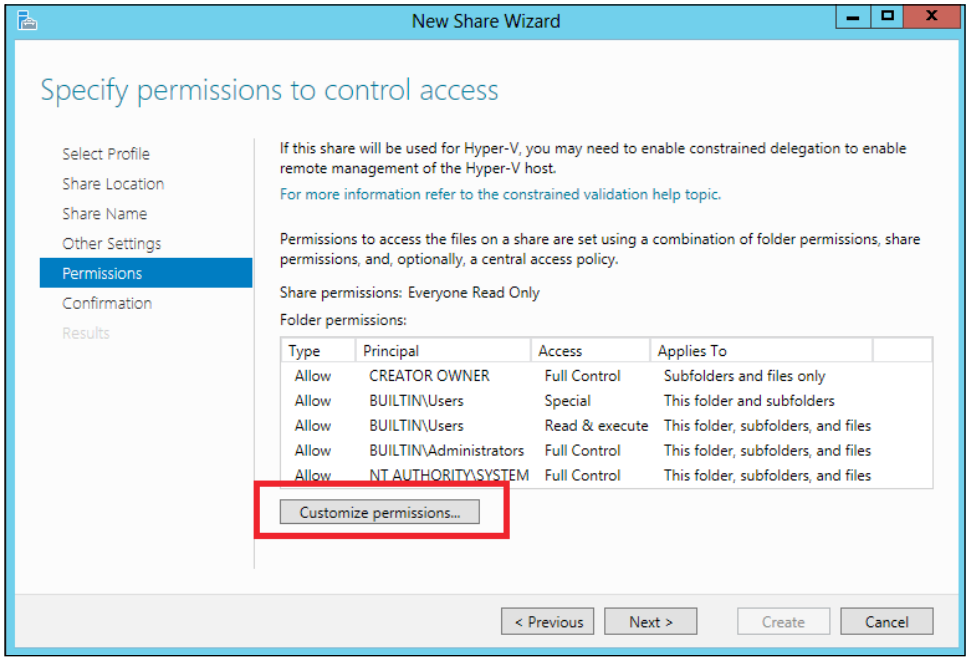
5. Next, select between **Select by volume** or **Type a custom path** for a share location.



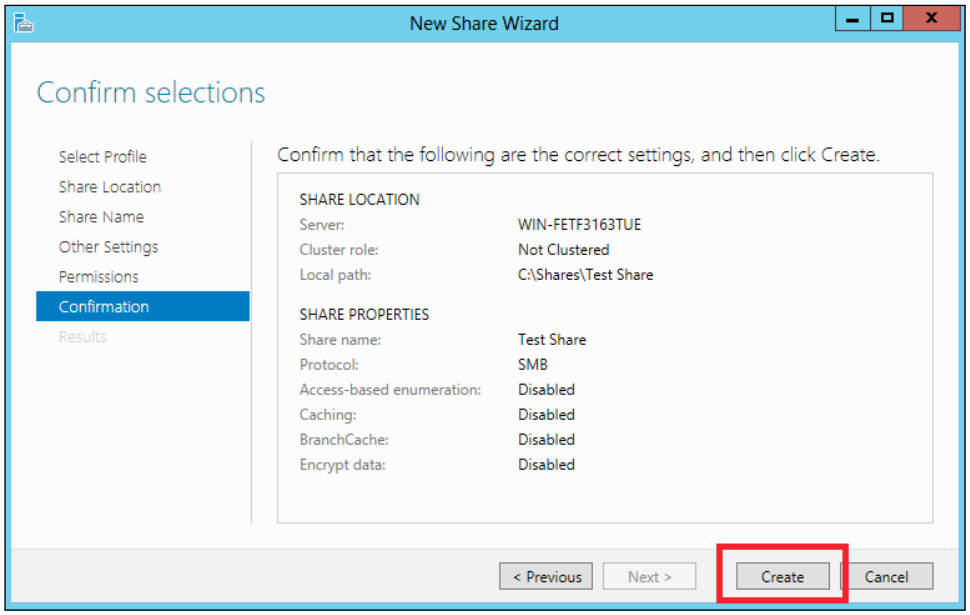
6. In the next step, enter **Share name** and optional **Share description** in the designated fields.



7. The next step is for configuring encrypted data access. Data encryption adds overhead to the entire communication. If you enable data encryption, the server will automatically encrypt all the data with predefined encryption algorithms. In this example, it will be left unchecked.
8. The next step is for setting up the security permissions and defining which server or which service account will have access to the file share. Access permissions are very important, because only authorized users should have access to shares, which contain virtual machine data. You can choose between: **Full Control**, **Modify**, **Read & Execute**, **List folder contents**, **Read**, **Write**, and **Special permissions**. For the purpose of this example, Full Control permissions need to be given to the Hyper-V server's machine accounts. To add permission, click **Customize permissions…**.



9. The final step is an overview of all the settings and confirmation of the setting. To create the share, just click the **Create** button.



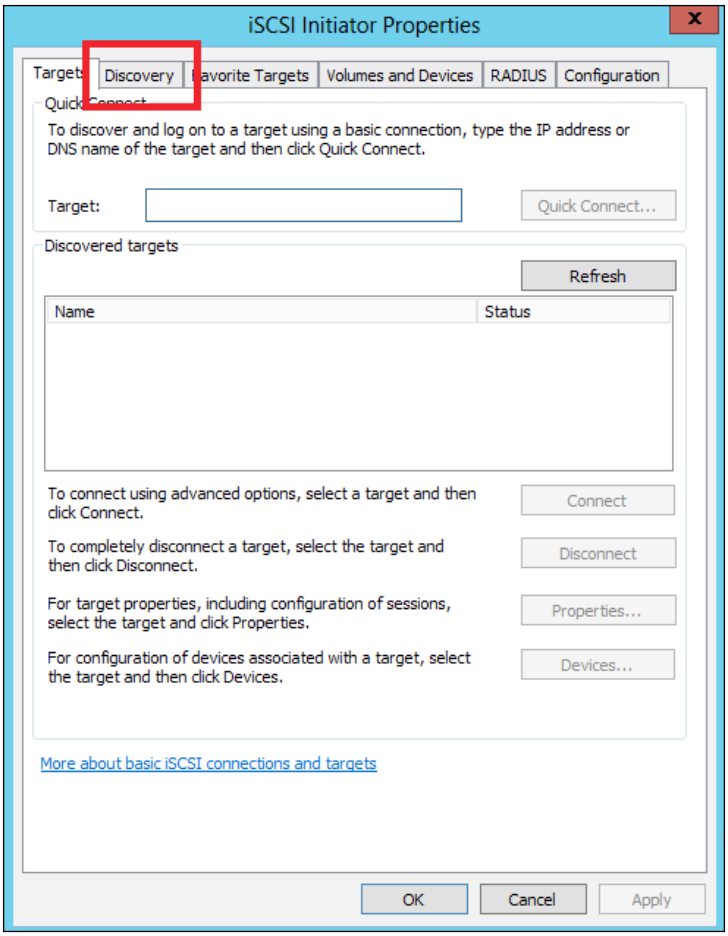
Setting up iSCSI connections

For the purpose of this example, an iSCSI storage will be attached to the SMB file-sharing server. Before file shares are setup, the SMB file sharing server must be connected to an iSCSI or some other kind of storage. The storage has to be configured with **Logical Unit Number** (**LUN**), as per the infrastructure needs. You can create different LUNs for different usage, or create a single LUN and store everything in it. The storage itself has RAID configured on it, so data loss is avoided in case of disk malfunctioning. Also, there are hot spare disks for failover.

In Windows Server 2012, setting up iSCSI is very simple and it is the same as it was on Windows Server 2008 R2. The steps to configure an iSCSI connection are as follows:

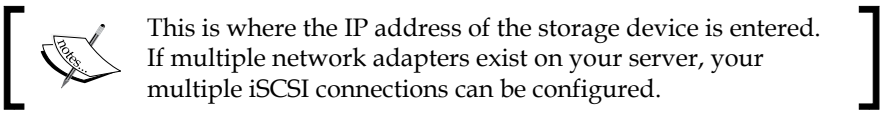
1. From the **Control Panel**, access iSCSI initiator and a menu appears as shown in the next screenshot.

The first menu that appears is only an overview of the entire iSCSI configuration.

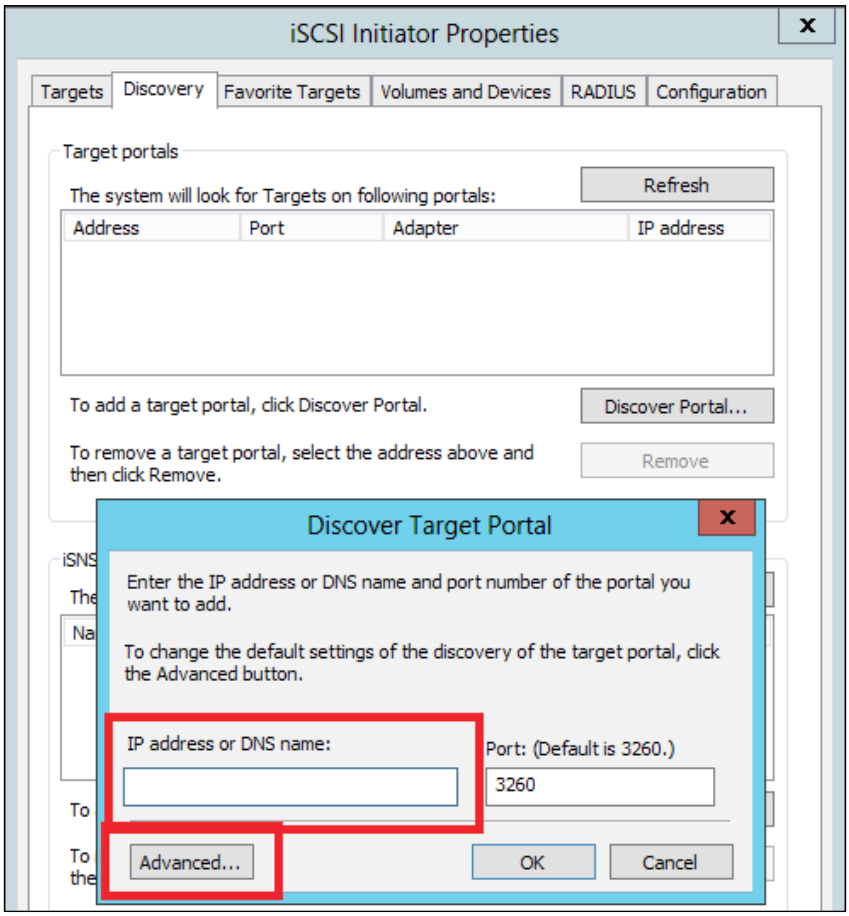


www.allitebooks.com

2. Next, click on the **Discovery** tab and then click on **Discovery Portal…**.



This is where the IP address of the storage device is entered. If multiple network adapters exist on your server, your multiple iSCSI connections can be configured.



3. To set up multiple iSCSI connections, click on **Advanced**. For multiple iSCSI connections there is one prerequisite. Multiple I/O Windows Feature has to be installed. These multiple iSCSI connections will speed up the I/O operations between your SMB file server and iSCSI storage.

With the iSCSI connection active and SMB File shares created all the storage related activities are done. The iSCSI connections will automatically become active every time the system restarts. The same thing happens with the SMB File shares.

Setting up networking

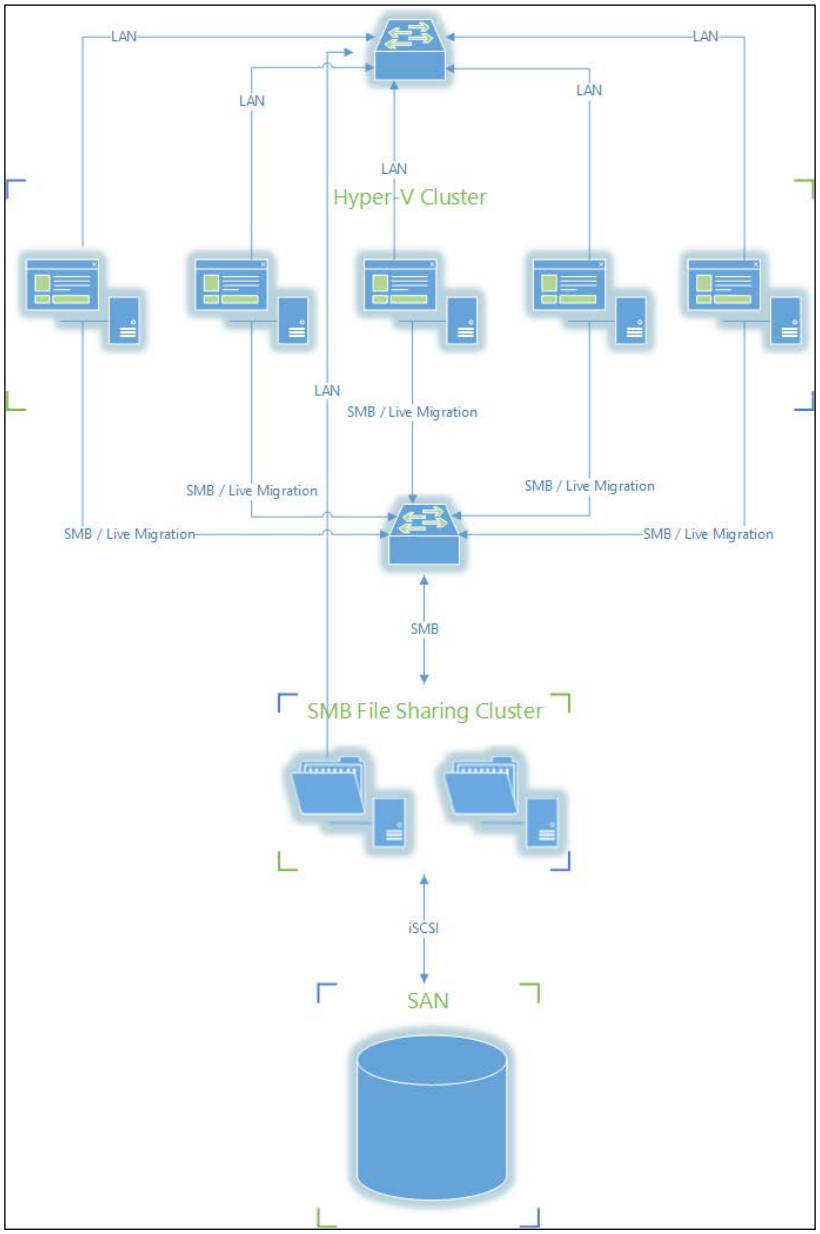
Networking in a failover cluster is very important. There are three different traffic types in the network and all those have to be separated, so there is no congestion. The different traffic that is generated in such environment is as follows:

- **iSCSI traffic**: This is the traffic between SMB File Sharing Server and iSCSI Storage
- **SMB Traffic**: This is the traffic generated from **Hyper-V hosts** and destined for SMB File Sharing Server
- **Failover cluster traffic**: In this traffic, control messages are exchanged between Cluster Nodes and Live Migration dedicated network

An important note on the networking part is that SMB traffic, LAN traffic, and failover cluster traffic are different types of traffic. So, on each Hyper-V cluster node there will have to be separate network adapters for each of them. You can setup VLANs on the central switch to further optimize your traffic. The next diagram shows a simple scenario of such an environment, and a way in which you can organize all this traffic.

The next diagram presents how the traffic will flow in the infrastructure. This is only a logical view of the traffic. It shows that each server must have a connection to the SMB file sharing server and a connection to the LAN. The two networks can be in different subnets.

If LAN and SMB network belong to different subnets, then the SMB file server must have one connection to the LAN because the server must be connected to the Active Directory to authenticate the permissions set on the file shares.



Failover clustering can be implemented in the SMB file sharing server. In this example, only one SMB File Sharing server is used. With failover clustering configured on the SMB server, file shares will be constantly available in case one of the servers malfunctions. To do this, refer to the guide in the following link:

`http://blogs.technet.com/b/clausjor/archive/2012/06/07/smb-transparent-failover-making-file-shares-continuously-available.aspx`

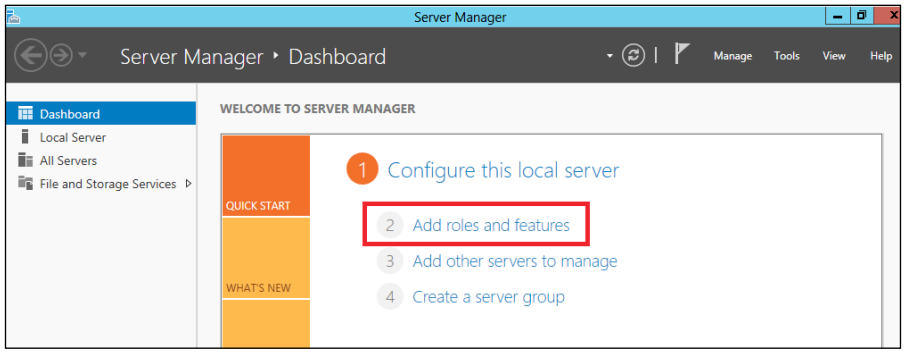
Setting up security permissions on SMB file shares

SMB file shares contain sensitive data files Whether they are virtual machines or SQL server database files, proper security permissions need to be applied to them in order to ensure that only authorized users and machines have access to them. Because of this, SMB File Sharing server has to be connected to the LAN part of the infrastructure as well. Security permissions are read from an Active Directory server. For example, if Hyper-V hosts have to read and write on a share, then only the computer accounts of those hosts need permissions on that share, and no one else. Another example is, if the share holds MS SQL server database files, then only the SQL Server computer accounts and SQL Server service account need permissions on that share.

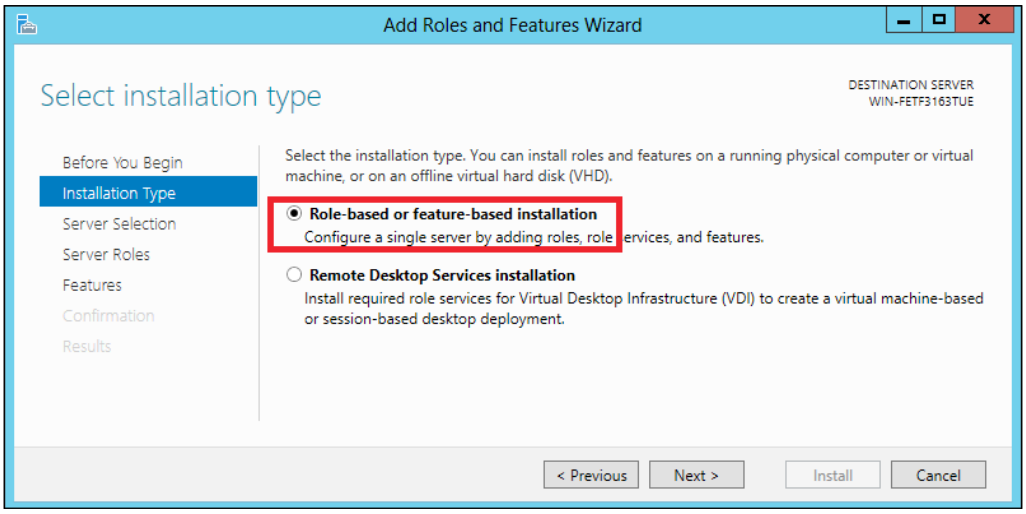
Setting up a failover cluster

When the storage, networking and Hyper-V hosts are up and running, the failover cluster can be setup on top of Hyper-V. Setting up failover cluster in Microsoft Windows Server 2012 is very simple. First, you have to install the Failover Clustering feature from **Add Roles and Features Wizard** on all Hyper-V nodes. Now, perform the following steps:

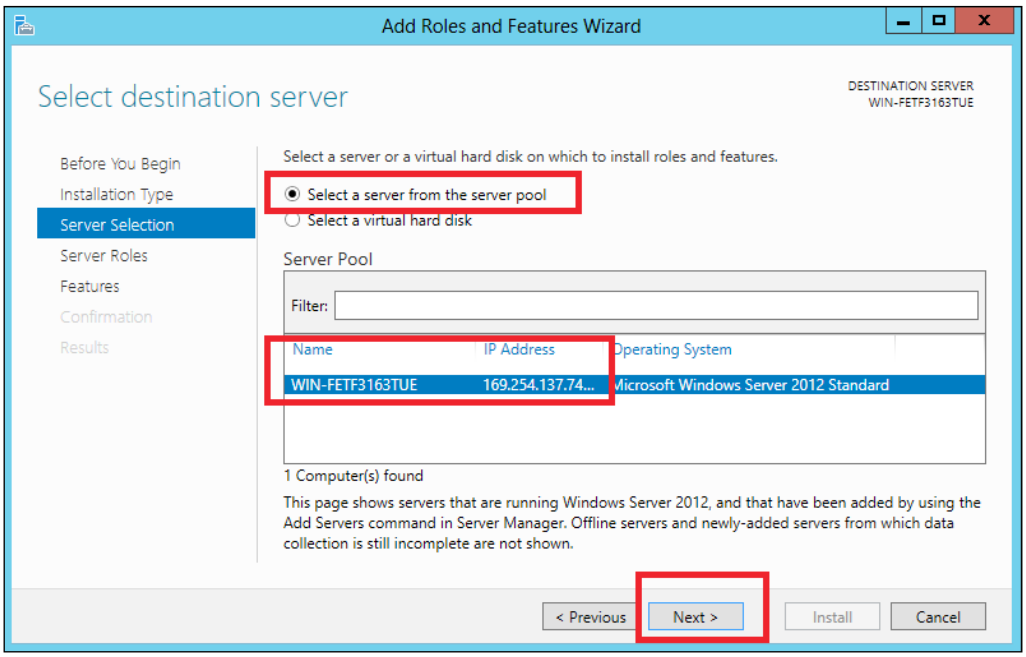
1. Open **Server Manager** and go to **Add Roles and features**.



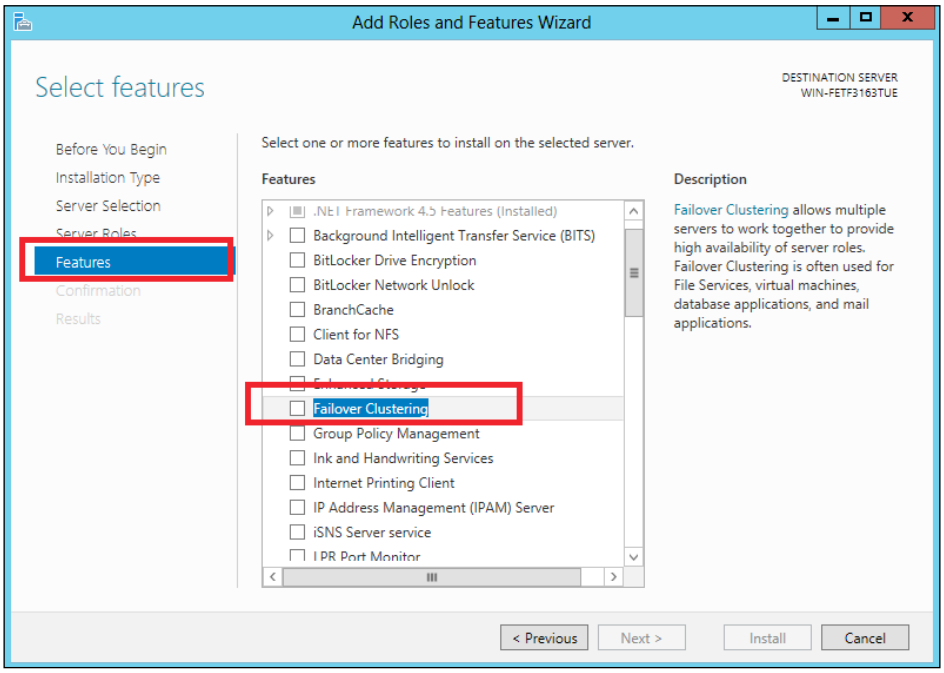
2. Select **Role-Based or Feature-based installation**.



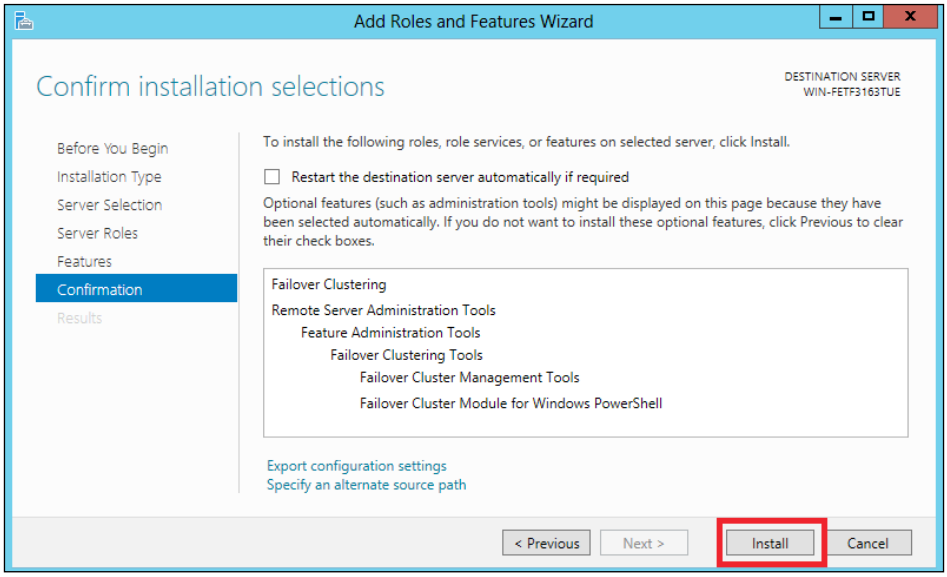
3. Select the server from the list of available servers.



4. From the list of **Features**, select **Failover Clustering**.



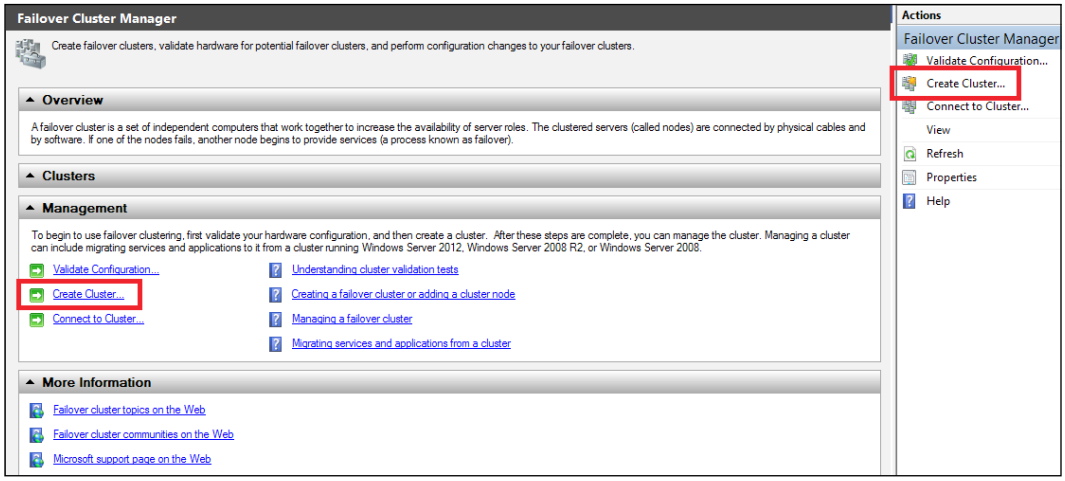
5. In the last step, click on **Install** to complete the installation of the **Failover Clustering** feature.



Next, we can continue with the **Failover Clustering** configuration. From the **Failover Cluster Manager**, there are three ways to create a failover cluster:

1. Right-click on **Failover Cluster Manager** on the left-hand side pane, and click on **Create Cluster…**.
2. From the right-hand side **Actions** pane, click on **Create Cluster…**.
3. From the **Management** pane in the middle, click on **Create Cluster…**.

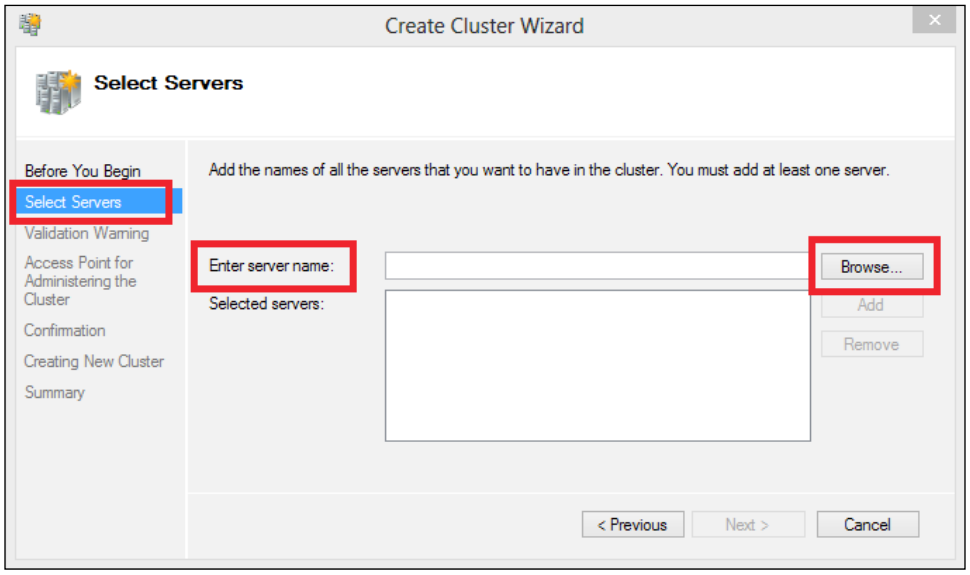
Only the first option isn't shown in the following screenshot:



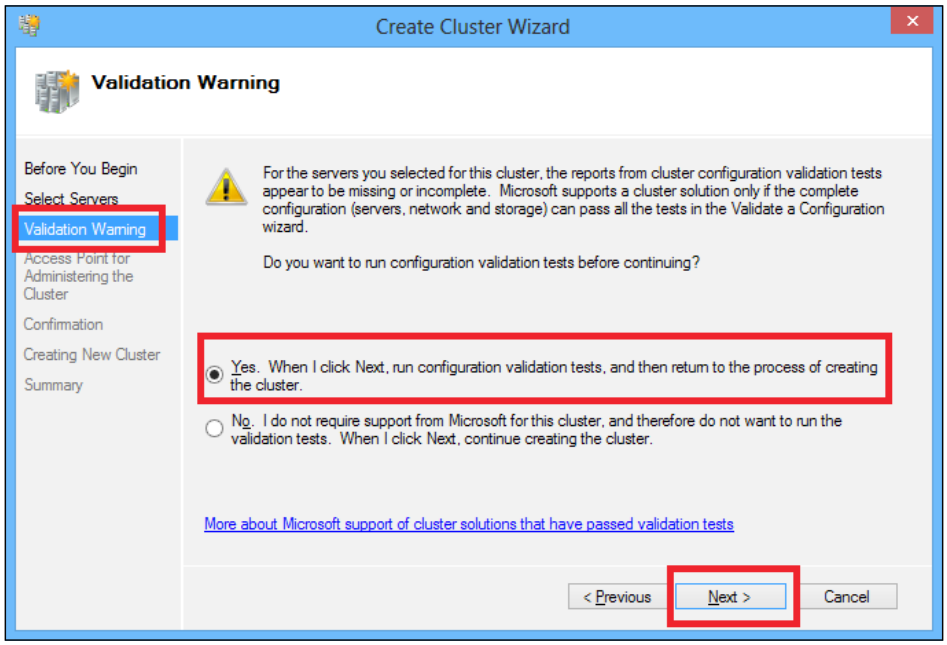
Choose any one of them and the Failover Cluster wizard will start and guide you through the process of cluster creation:

1. In the first step of the wizard, click on **Next**.

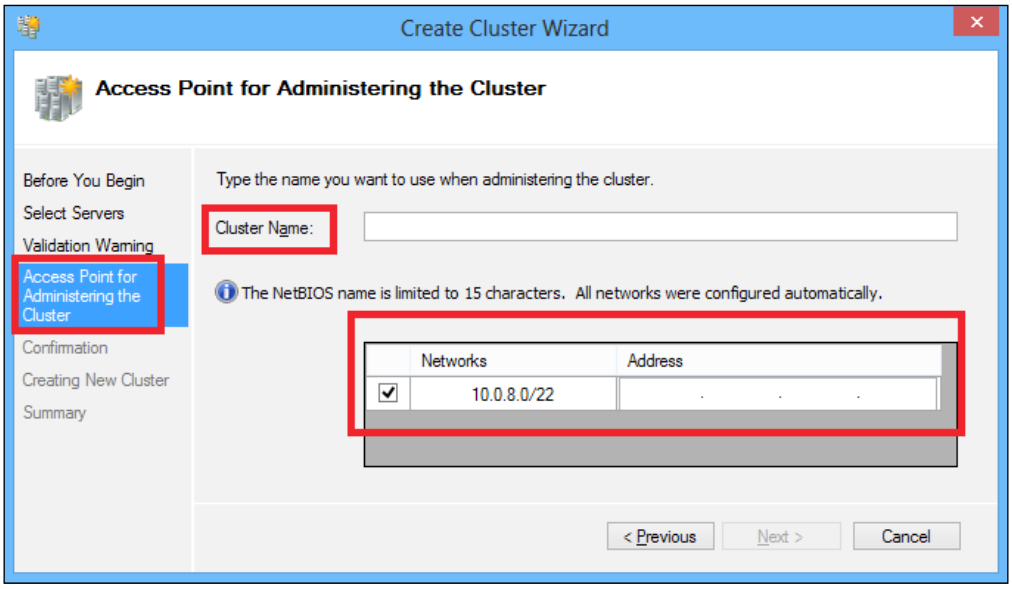
2. In this step, add all the servers that will be a part of the failover cluster by writing the names, or click on **Browse…** to choose the Active Directory.



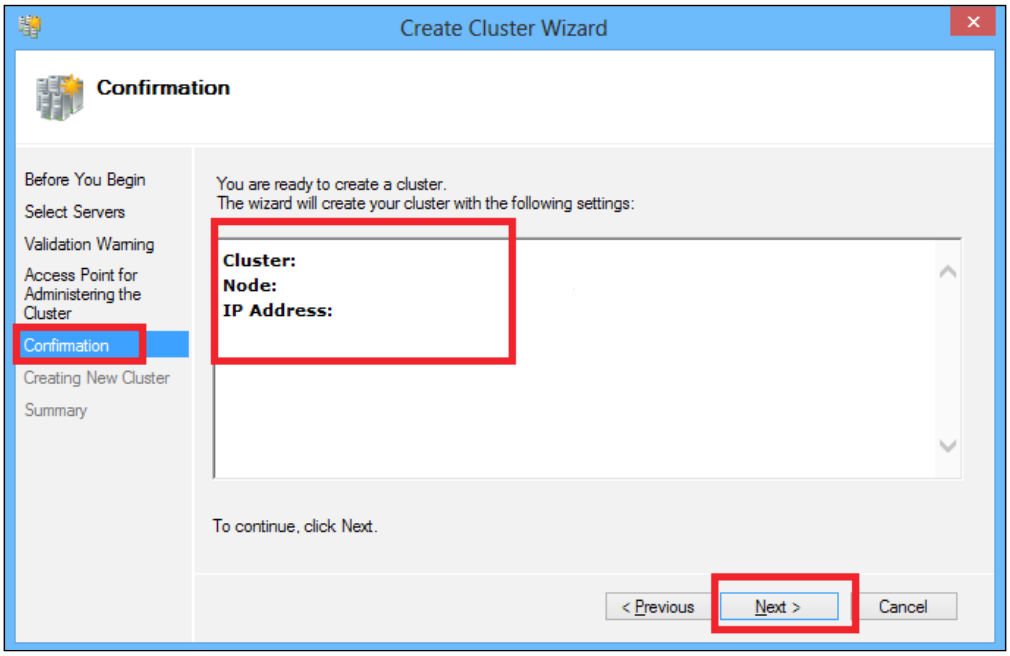
3. After all of the Hyper-V servers are entered, Hyper-V server settings validation is performed. If the configuration is not valid, the wizard will not continue.



4. After the validation is complete, enter **Cluster Name** and IP address for management access.



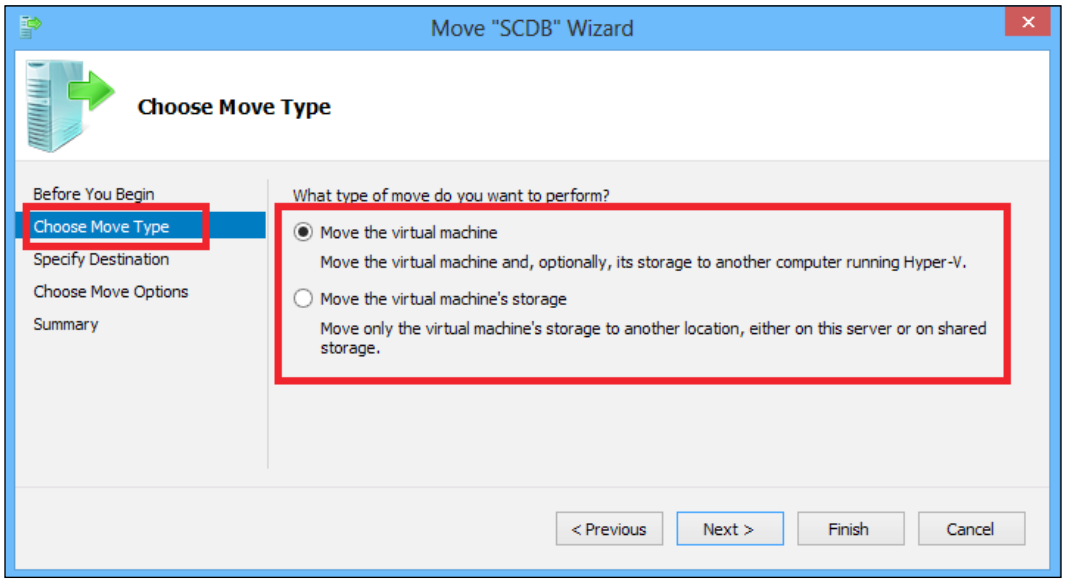
5. Click **Next** to confirm your settings and create the cluster.



Migration of virtual machines

Virtual Machine High Availability is the reason why failover clusters are deployed. High availability means that there is no system downtime or there is minimal accepted system downtime. This is different from system uptime. A system can be up and running but it may not be available. Hyper-V hosts in modern datacenters run many virtual machines, depending on the underlying hardware resources. Each of these systems is very important to the consumer. Let's say that a Hyper-V hosts malfunctions at some bank, and let's say that this host, hosts several critical systems and one of them may be the ATM system. If this happens, the users won't be able to use the ATMs. This is where Virtual Machine High Availability comes into picture. It is achieved through the implementation of failover cluster. A failover cluster ensures that when a node of the cluster becomes unavailable, all of the virtual machines on that node will be safely migrated to another node of the same cluster. Users can even set rules to specify to which host the virtual machines failover should go. Migration is also useful when some maintenance tasks should be done on some of the nodes of the cluster. The node can safely be shut down and all of the virtual machines, or at least the most critical, will be migrated to another host. Hyper-V v3.0 allows the user to choose among the following options:

- **Move the virtual machine**
- **Move the virtual machine's storage**



www.allitebooks.com

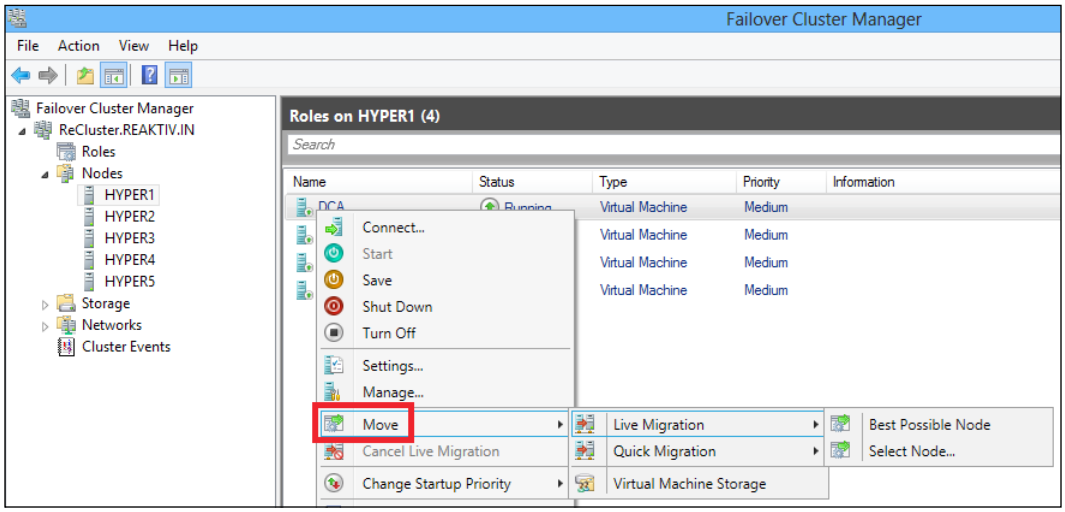
The first option allows the administrator to transfer the execution of a virtual machine from one Hyper-V host to another. This is useful when you want to migrate the virtual machine to a better host with more resources. The second option allows the administrator to transfer the execution of a virtual machine to other Hyper-V hosts and optionally set another location for the virtual machine VHD file. This is useful when you want to free space on your Hyper-V host and migrate your virtual machine VHD file to a host with more storage space. These options are great, but they are manually triggered. If you want to set up rules for automatic failover when disaster happens, you have to use the **Failover Cluster Management** console. If you want to Live Migrate a virtual machine from one node to another from the Failover Cluster Management console, you have to perform the following steps:

1. Open the Failover Cluster Management console.
2. Expand **Nodes** in the left-hand side pane.
3. Select the node on which the virtual machine you want to Live Migrate is located.
4. Right-click on the virtual machine that you want to migrate, click on **Move** and you will see the following options, which you saw previously in the Hyper-V management console:
    - If you navigate to **Live Migration | Select Node…**, the wizard will let you choose to which node you want to Live Migrate the virtual machine
    - If you navigate to **Live Migration | Best Possible Node**, the failover cluster will choose the best node for you depending on its rating (The failover cluster maintains rating for all nodes in the cluster.)
5. After you choose the destination node, the **Live Migration** starts and the virtual machine is transferred to the other node.

Live Migration is performed between hosts that are in the same domain or mutually trusted domain.

The **Quick Migration** option from the **Move** menu is a different type of migration. Live Migration lets you migrate only one virtual machine at a time, but Quick Migration lets you migrate multiple virtual machines at a time. There is also difference in the way the virtual machine is transferred. During Live Migration, the virtual machine is not turned off, and it is available through the entire process. Users working on that virtual machine won't notice that anything has changed.

Virtual Machine Storage is the third option, which allows you to transfer only the virtual machine's VHD file from one storage location to another.



Summary

In this chapter, we were introduced to SMB, a new concept that comes with Windows Server 2012. This new concept allows system administrators to configure file share and use them for application storage. We also learned how to set up an SMB server and configure the file shares and access permissions for those file shares. We learned about different traffic types in the infrastructure and how to isolate it to improve speed. Next, we learned what the advantages of implementing a failover cluster are and how to build a failover cluster with Windows Server 2012, and how to use Live Migration to migrate virtual machines between nodes.

In the next chapter, we will learn how to add disaster recovery and business continuity value to our enterprise with the implementation of Hyper-V Replica.

3
Configuring Hyper-V Replica

Enterprises tend to increase their system availability and deliver end user services. There are various ways how this can be done, such as making your virtual machines highly available, disaster recovery methods, and back up of critical systems. In case of system malfunction or disasters, the IT department needs to react fast, in order to minimize system downtime. Disaster recovery methods are valuable to the enterprise. This is why it is imperative that the IT department implements them. When these methods are built in the existing platform that the enterprise uses and it is easy to configure and maintain, then you have a winning combination. This is a suitable scenario for Hyper-V Replica to step up. It is easy to configure and maintain, and it is integrated with the Hyper-V 3.0, which comes with Windows Server 2012. This is why Hyper-V Replica is becoming more attractive to the IT departments when it comes to disaster recovery methods. In this chapter, we will learn what are the Hyper-V Replica prerequisites and configuration steps for Hyper-V Replica in different deployment scenarios. Because Hyper-V Replica can be used with **failover clusters**, we will learn how to configure a failover cluster with Windows Server 2012.

Hyper-V Replica requirements

Before we can start with the implementation of Hyper-V Replica, we have to be sure we have met all the prerequisites. In the previous chapters, we said that in order to implement Hyper-V Replica, we have to install Windows Server 2012 on our physical machines. Windows Server 2012 is a must, because Hyper-V Replica is a functionality available only with that version of Windows Server. Next, you have to install Hyper-V on each of the physical machines. Hyper-V Replica is a built-in feature of Hyper-V 3.0 that comes with Windows Server 2012. If you plan to deploy Hyper-V on non-domain servers, you don't require an **Active Directory Domain**. If you want to implement a failover cluster on your premise, then you must have Active Directory Domain.

In addition, if you want your replication traffic to be encrypted, you can use self-signed certificates from local servers or import a certificate generated from a **Certificate Authority (CA)**. This is a server running **Active Directory Certificate Services**, which is a Windows Server Role that should be installed on a separate server. Certificates from such CAs are imported to Hyper-V Replica-enabled hosts and associated with Hyper-V Replica to encrypt traffic generated from a primary site to a replica site. A primary site is the production site of your company, and a replica site is a site which is not a part of the production site and it is where all the replication data will be stored. If we have checked and cleared all of these prerequisites, then we are ready to start with the deployment of Hyper-V Replica.

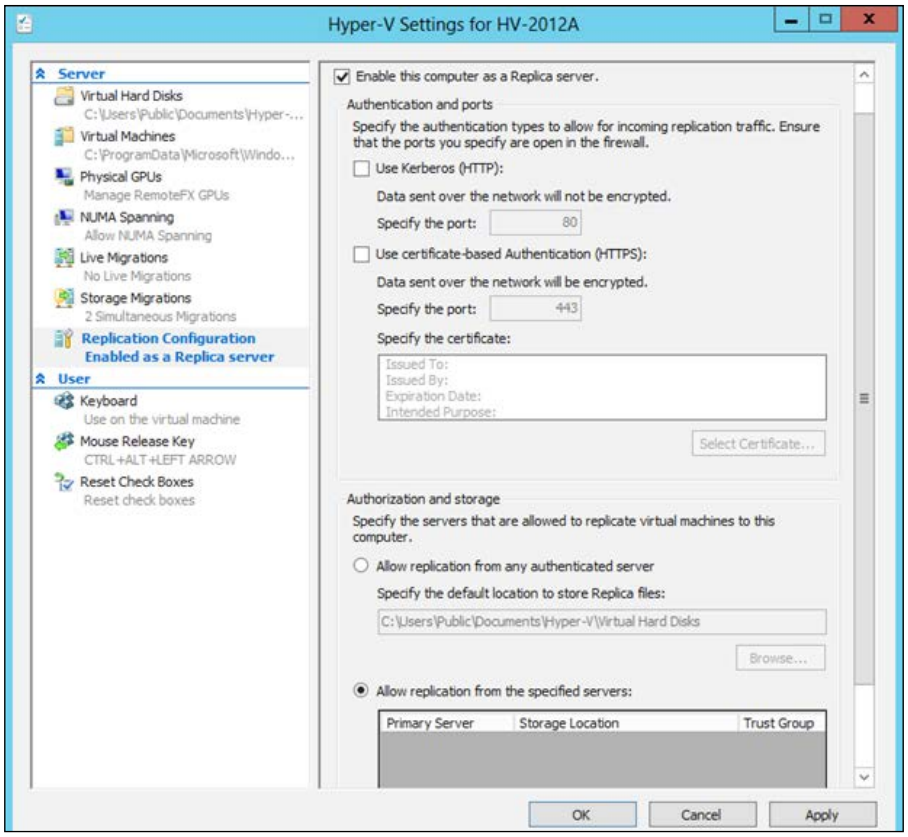
Hyper-V Replica in standalone Hyper-V hosts environment

You must have enough storage space on all of the primary and replica servers to store the files used by primary virtual machines and its replica virtual machines. Between the sites there should be some kind of a network connection, whether it is LAN, leased line, some kind of VP, and so on. You must configure your local firewall on all Hyper-V hosts and intermediate firewall devices to allow replication traffic. There are three steps that have to be done to configure Hyper-V Replica:

- Configuring Hyper-V Replica on a server in a replica site
- Configure virtual machines for replication
- Configure firewall rules

Configuring Hyper-V replica on a server in a replica site

The first step is to enable a server in the replica site as a replica server. The replica server is the server that will receive replication traffic. To enable a server as a replica server, you have to open the **Hyper-V Management** console and from the right-hand side pane, click on **Hyper-V Settings**. You will see a window, such as the one shown in the next screenshot:



This is the configuration window where you configure your server as a replica server. To do this, just select the top checkbox that says **Enable this computer as Hyper-V Replica server**. Next, you can configure authentication and port numbers. There are two ways for site authentication:

- Kerberos
- Certificate authentication

With **Kerberos** authentication, the traffic between sites is not encrypted. By default, Kerberos uses port number 80 or the HTTP protocol. You can always change the port number in this menu.

Kerberos can only be used when Hyper-V hosts are part of a domain or mutually trusted domains.

If you want to encrypt your traffic generated from the primary site, then you must configure certificate authentication. By default, this type of authentication uses port number 443 or the HTTPS protocol.

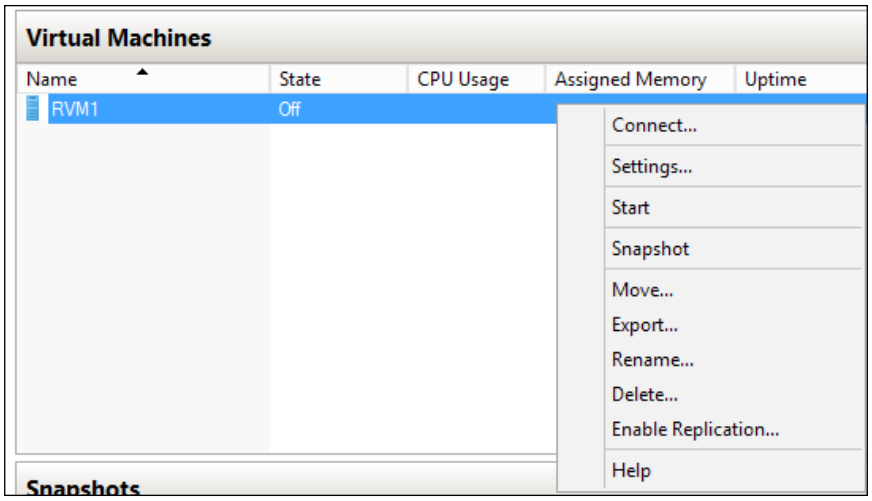
In the third configuration pane, you can setup authorization and storage location where incoming replication traffic will be stored. There are two options for authorization:

- **Allow replication from any authenticated server**: This option allows the replica server to accept traffic from any server that is properly authenticated by Kerberos or certificate authentication.
- **Allow replication from specified servers**: This option allows your replica server to accept traffic only from the designated servers in the list.

It is important to note that you must select some kind of authentication. If you don't, then you cannot enable the server as a replica server. If you click on **Apply**, and then on **OK**, you will receive an error that says you must select an authentication type.

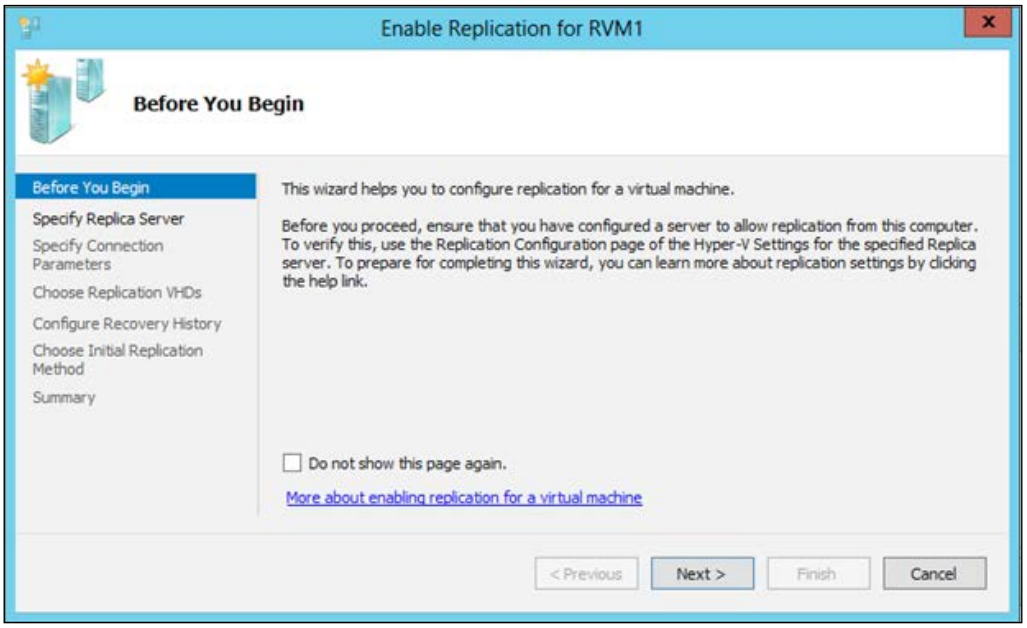
Configuring virtual machines for replication

After you have setup the replica server to receive replication traffic, you can continue with the configuration of the virtual machines in the primary site. A primary server is a server that is located in the primary site, whereas a replica server is any server that is located in a replica site. Enabling virtual machines for replication is done from the **Hyper-V Management** console. When you open it, right-click the virtual machine that you want to enable for replication, and then select **Enable Replication**. The following screenshot shows the options you get when you right-click a virtual machine:



When you click on **Enable Replication**, the **Enable Replication** wizard is started and it will guide you through the configuration process that consists of six steps for the virtual machine:

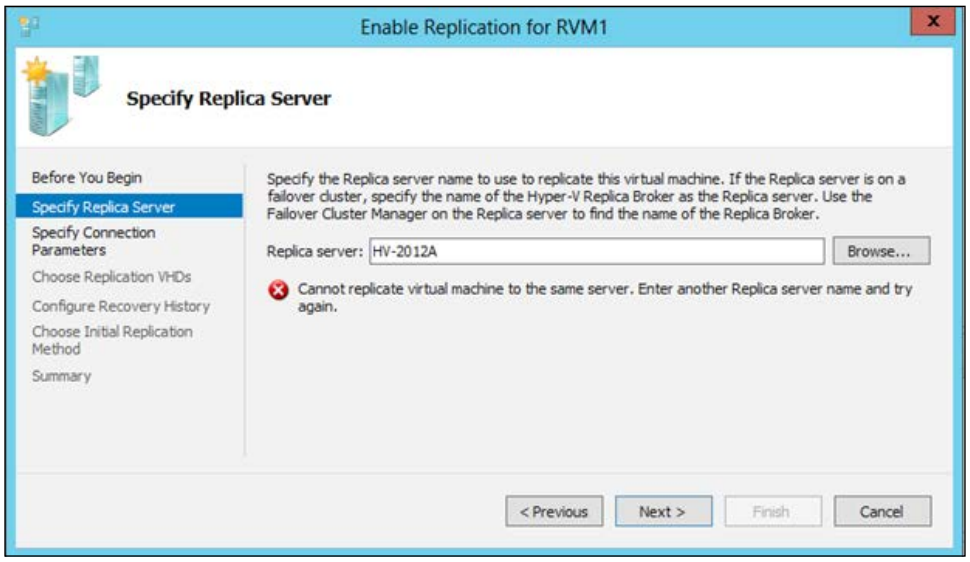
1. On the first screen presented in the following screenshot, click on **Next**:



2. Next, you have to select your replica server.

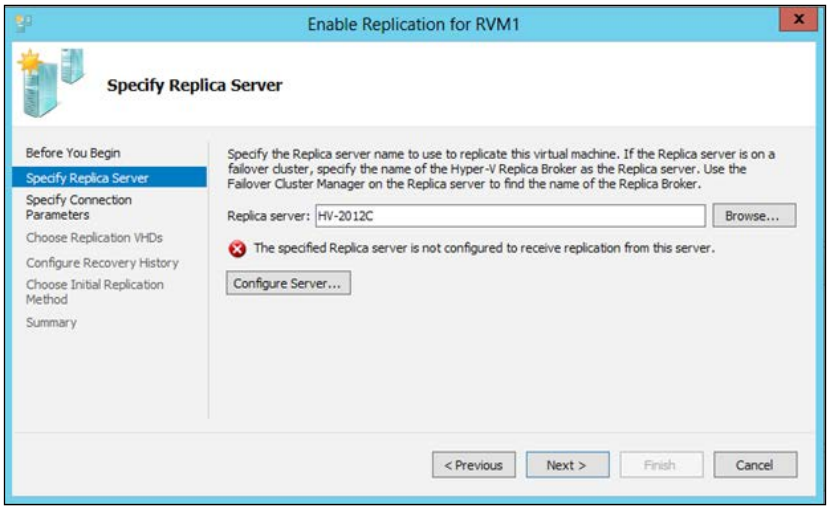
You cannot select the server on which the virtual machine is running as a replica server.

In the next screenshot, you can see the window where you specify the replica server:

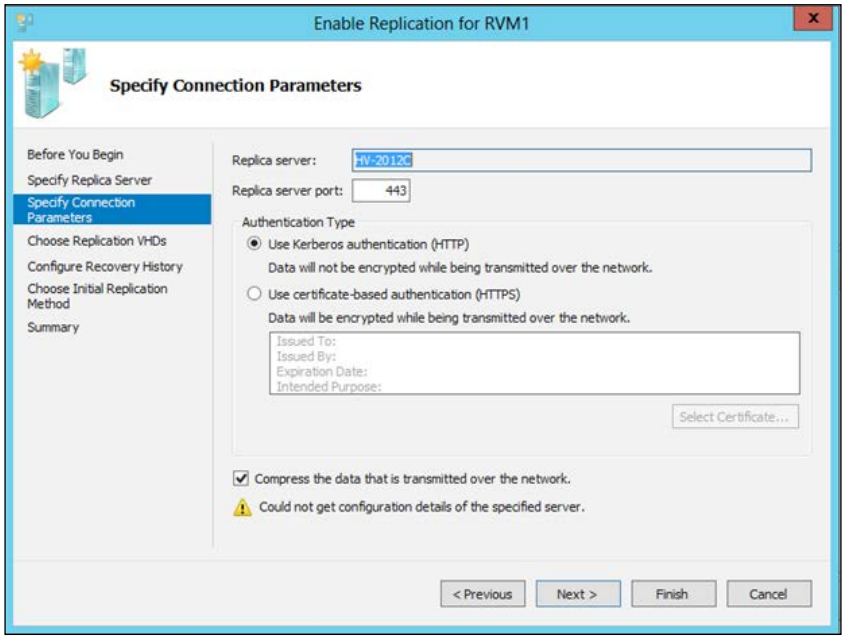


If the replica server that you specified is not configured as a Hyper-V replica server or this primary server is not in the list as an authorized server for replication, you will receive an error and will have an option to configure the destination replica server.

In the following screenshot, you can see the warning you get if your replica server is not properly configured as a replica server:



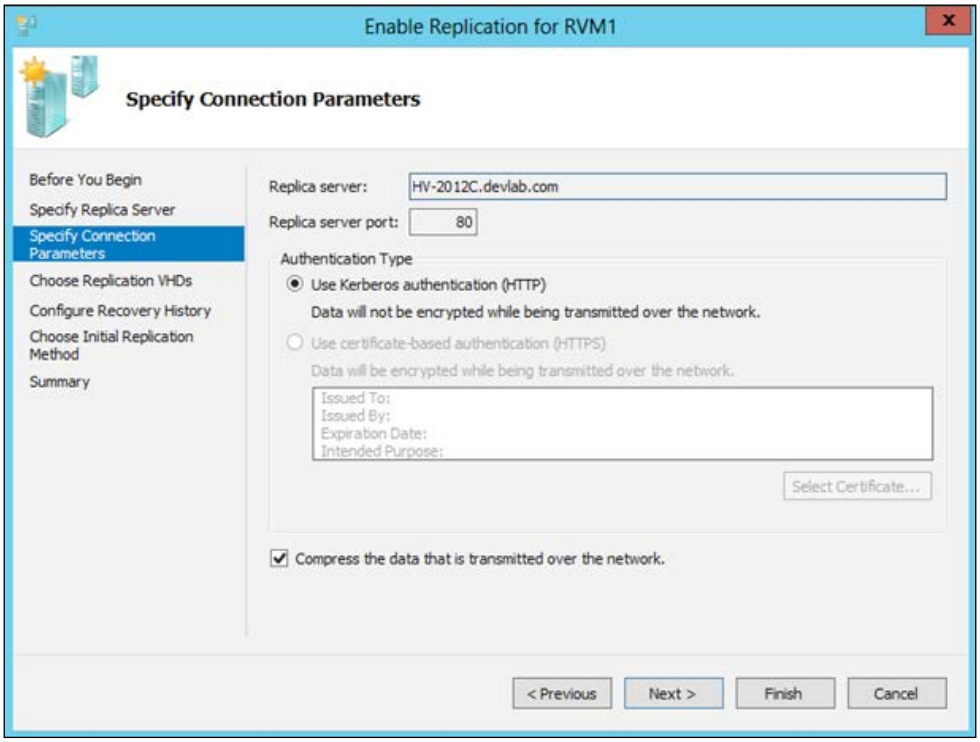
3. In the next step, you configure connection parameters. Here you configure the authentication type and the port number that you specified for the replica server. In the following screenshot, you can see the configuration window for the connection parameters:



www.allitebooks.com

It is important to say that you must have a DNS record in the domain boundary for the replica server. If not, you will receive a warning on the bottom. If you have a DNS record, then no warning will be displayed, and you will see a window like the one shown in the following screenshot.

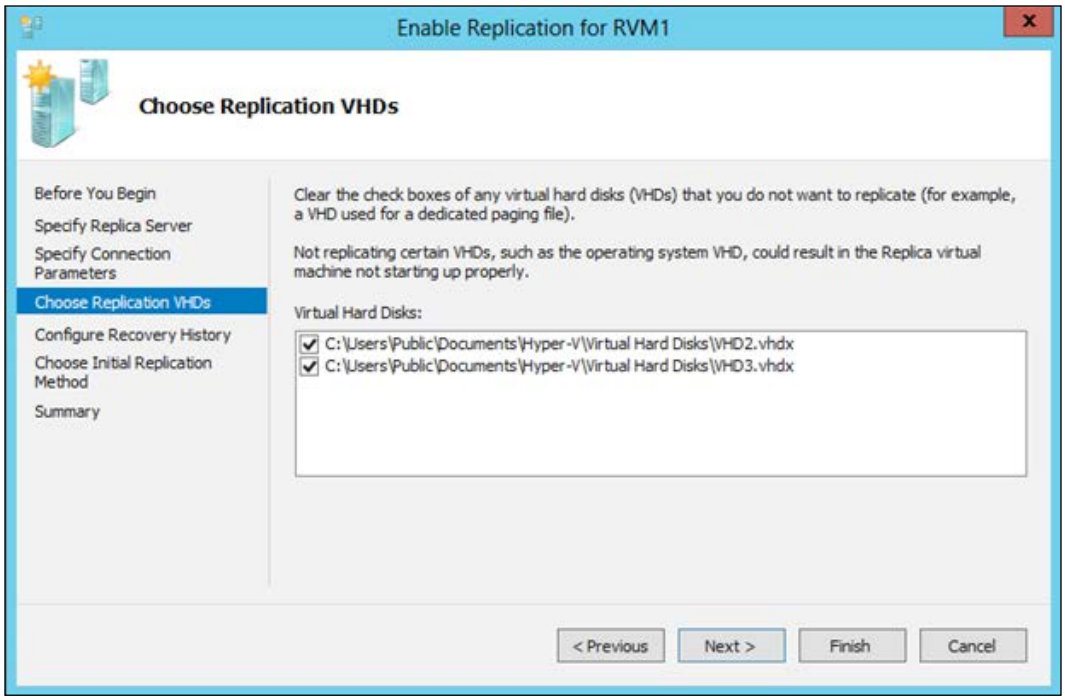
At the bottom of this part you can select the **Compress the data that is transmitted over the network** checkbox if you want to decrease the amount of traffic generated form the primary site. You can see this in the next screenshot:



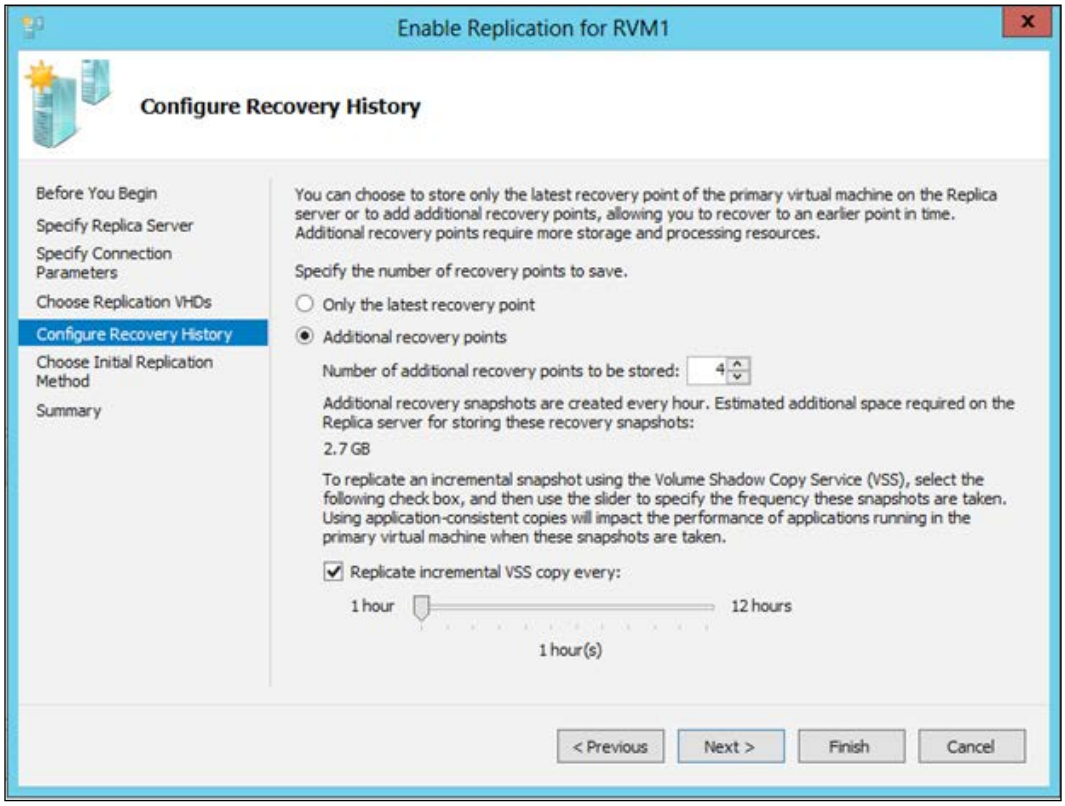
4. In this step, you select all of the VHD files that you want to be part of the replication process.

You can select individual VHD files that need to be replicated, but you have to select the VHD file where the operating system of the virtual machine is installed.

You can see the configuration window in the following screenshot:



5. This step is the most complex one and probably the most important of all. Here you specify recovery history. This means that you can configure point-in-time snapshots of the virtual machine, in order to perform a restore to one of them in case of disaster. When you get to this step, you will see a window like the one in the following screenshot:



There are two types of Hyper-V replica copies:

- Standard replicas
- Application consistent replicas

Standard replicas can be divided to:

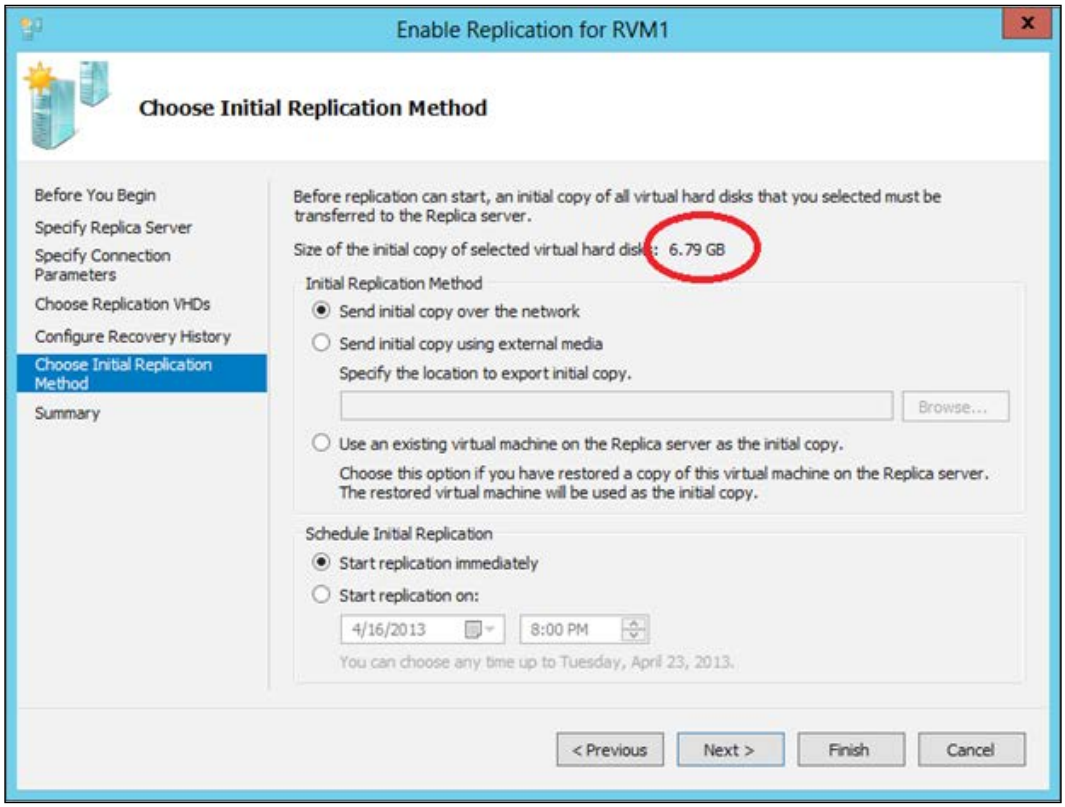
- **To store only the latest recovery point**: This means that there is only one replica for a virtual machine. Only the latest changes of the primary virtual machine are stored on the replica site. When you want to restore there is only one replica to restore.

- **To store additional recovery points**: This means that multiple recovery points can exist for a single virtual machine. This gives you more options when you want to make a restore to a point in time of a single virtual machine. The default interval for standard replicas is one hour and cannot be changed. When you create multiple snapshots, the wizard automatically calculates the storage space needed for all of them and displays it in the configuration windows.

Application-consistent replicas are more complicated. These types of replicas use the **Hyper-V VSS** (**Volume Shadow Copy Services**) writer for the applications running inside the virtual machine. They extract the application state and replicate it to the replica site. You can set the time interval on which you want to create these application-consistent replicas. The default interval for application consistent replicas is one hour and cannot be changed; for example, let's say that you created four multiple recovery points for a single virtual machine and you set up a two-hour application consistency. This means that every other standard replica will be application consistent. To enable application consistency, select the checkbox at the bottom and set your desired time interval for application consistency.

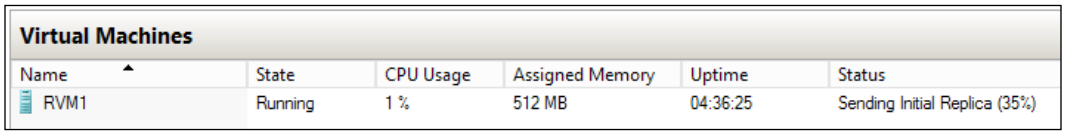
6. In the final configuration step, you choose how the initial replica will be sent to the replica site. Initial replica is the very first replication of a primary virtual machine. The configuration windows also show the size of the initial copy. There are three options to do this:
    - **Send initial copy over the network**: This is suitable for small size virtual machines. This is the default selection and it sends all of the selected VHD files from step 4 to the replica server.
    - **Send initial copy using external media**: This is suitable for large size virtual machines. You can make an export of a virtual machine and use this export as an initial copy.
    - **Use an existing virtual machine on the Replica server as initial copy**: If you have already exported a primary virtual machine, you can import it on the replica server as an initial copy of that virtual machine. This replica virtual machine must be configured with the same parameters as the primary virtual machine. Only then you can select **Use an existing virtual machine on the Replica server as initial copy**.

In the next screenshot, you can see the configuration window for the replication method:

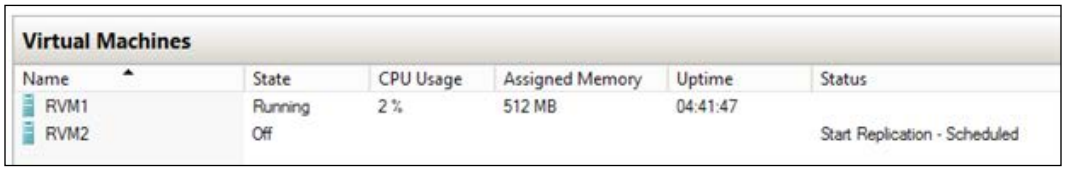


Once you have selected the initial replication method, you have to schedule initial replication. This can be done immediately, or you can schedule the initial replication on a specific date and time from the configuration menu.

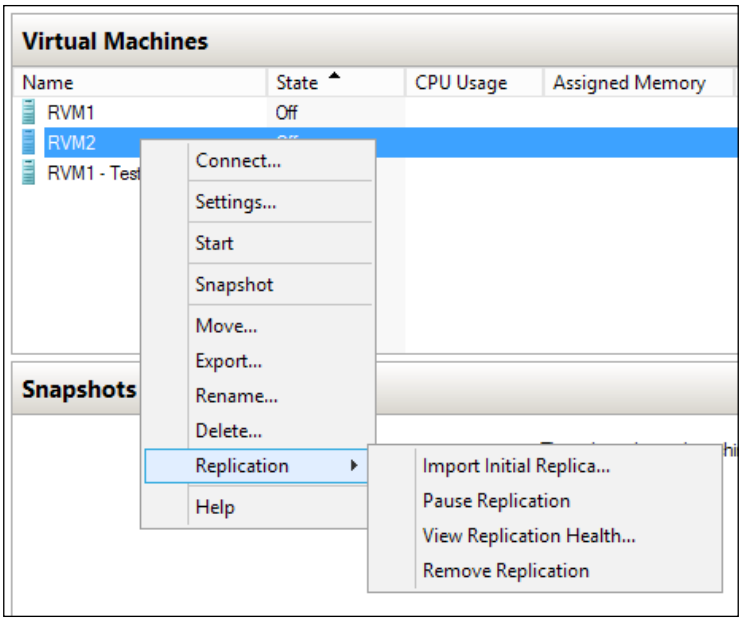
This concludes the Hyper-V Replica configuration for a single virtual machine. All of these steps must be configured on all virtual machines. When the wizard completes, if you have selected immediate replication, you will see the process of replication in Hyper-V as seen in the following screenshot:



If you have selected a scheduled initial copy, the status of the virtual machine will be like the one in the following screenshot:



You don't have to wait for the initial replication to take place. You can always do it manually by right-clicking the virtual machine, choosing replication, and then clicking **Import Initial Replica**. The same window as in Step 6 appears and is shown in the following screenshot:



Once the initial replication takes place, Hyper-V makes standard and application-consistent replicas. The replica virtual machine can only be started using the **Failover** option.

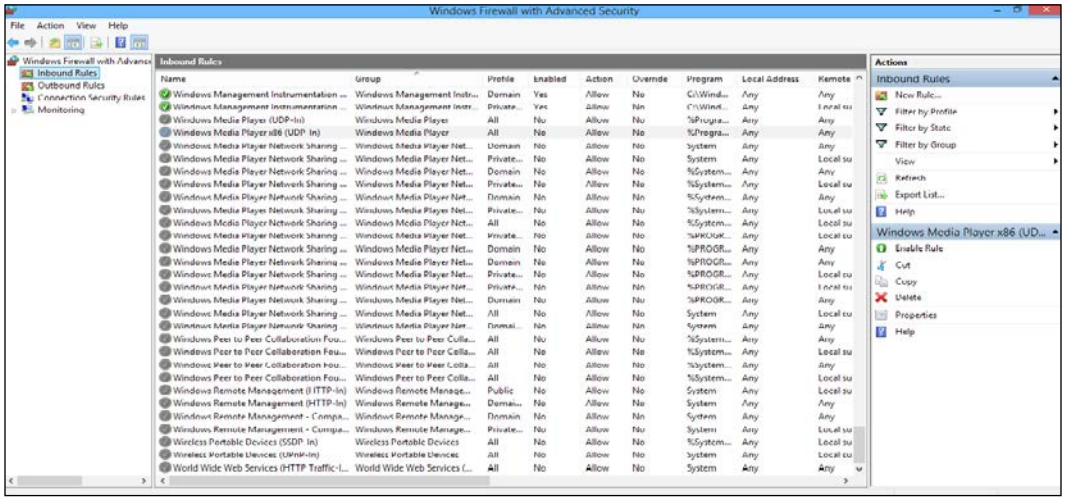
Configuring firewall rules

For replication to take place, the firewall rules must be enabled to allow replication traffic. By default, ports 80 and 443 or HTTP and HTTPS are used for virtual machine replication. When Hyper-V is installed, these rules are created but not enabled. You have to open the **Windows Firewall with Advanced Security** management console, go to **Inbound Rules**, and enable them. The names of these rules are:

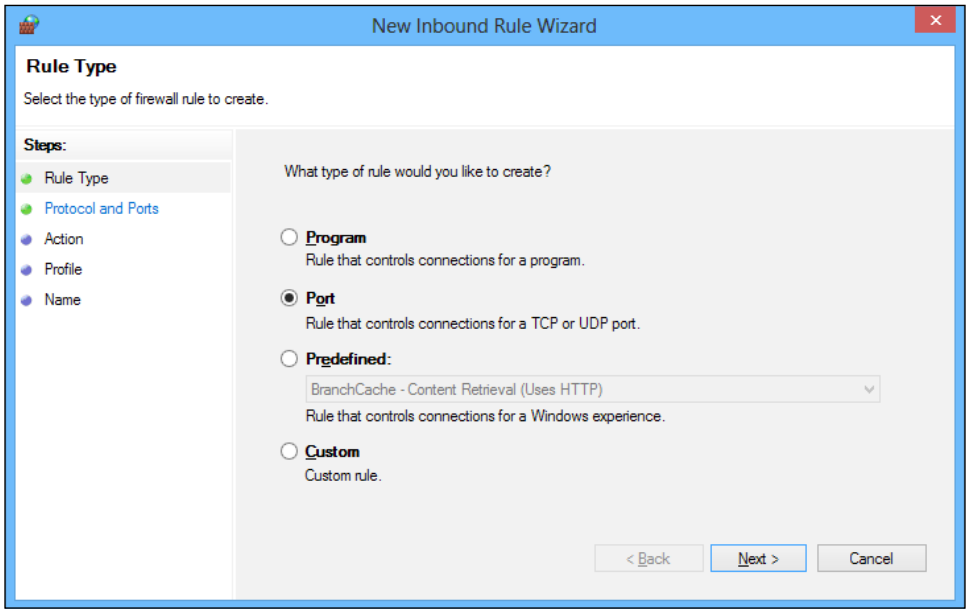
- Hyper-V Replica HTTP listener (TCP-In)
- Hyper-V Replica HTTPS listener (TCP-In)

If you have changed the default port numbers, then you must create custom rules and open the port numbers that you specified in your Hyper-V Replica configuration. To create a custom firewall rule do the following:

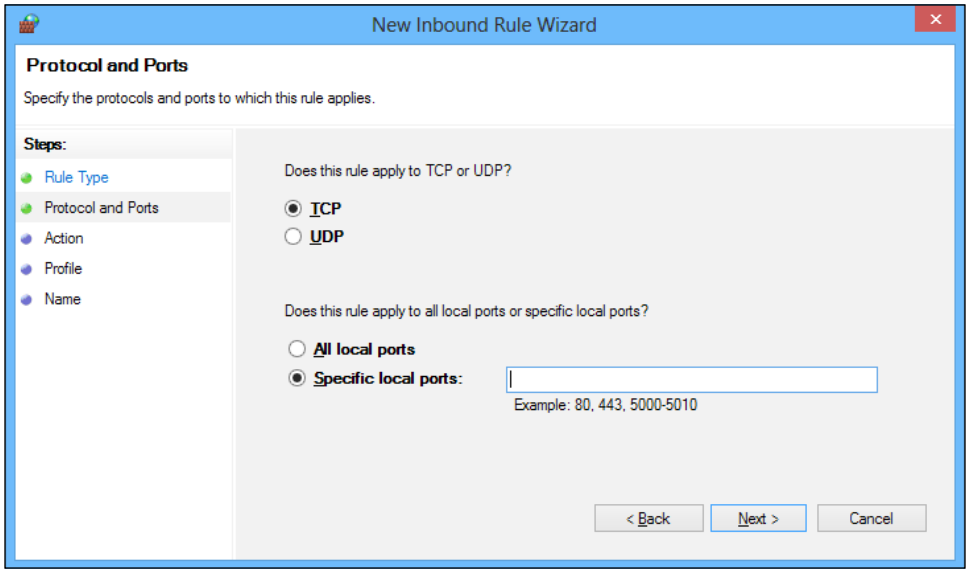
1. Open **Windows Firewall with Advanced Security** and you will see a window, such as the one in the following screenshot:



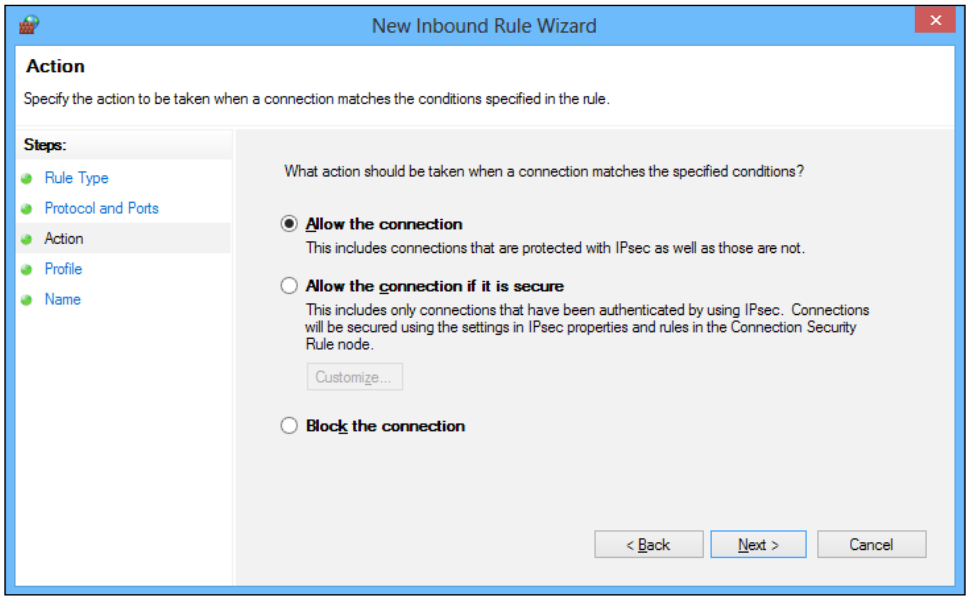
2. Right-click on **Inbound Rules**, and then click on **New Rule**. From the menu, shown in the following screenshot, select **Port Type Firewall Rule**:



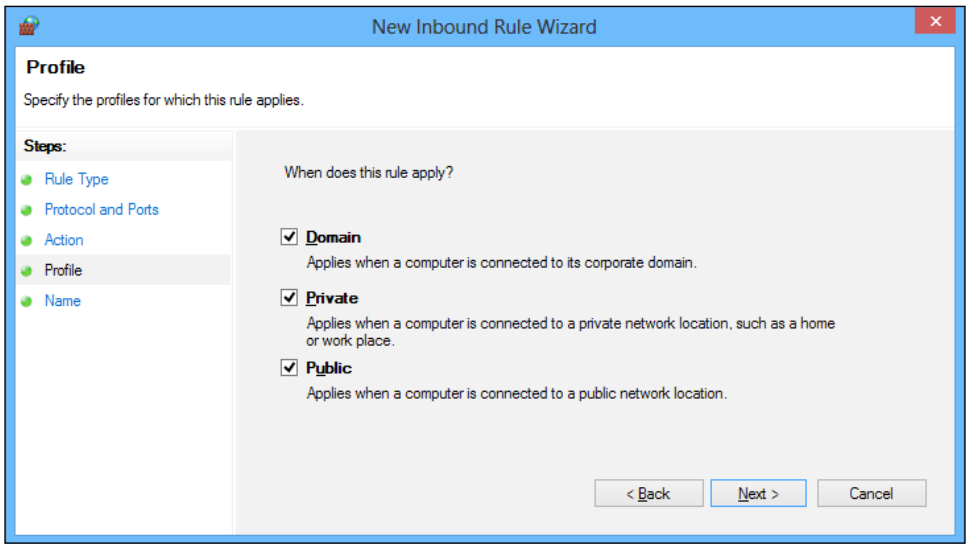
3. Enter the port number that you specified in the Hyper-V configuration. In the following screenshot, you can see the port number configuration window:



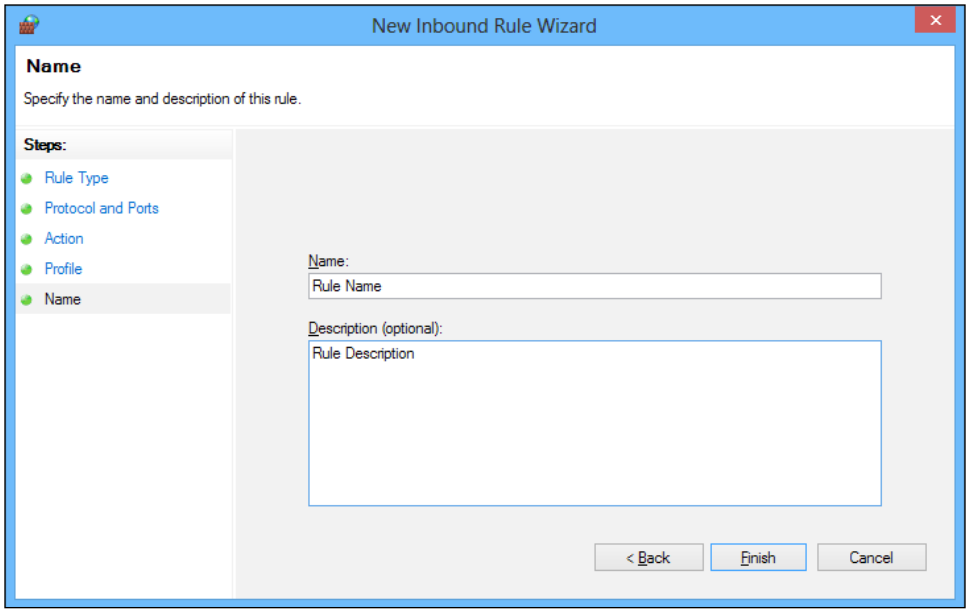
4. In this step, select **Allow this Connection**. The configuration window for this step is shown in the following screenshot:



5. Select the **Network Profile Settings** to which you want to apply this rule. The default selection is all of them so that is recommended. The network profile settings configuration window is shown in the following screenshot:



6. Enter the **Rule Name** and the optional **Rule Description**. In the following screenshot, you can see the configuration window, where you can enter the rule name and description:



Virtual machine replication in Failover Cluster environment

Hyper-V Replica can be used with Failover Clusters, whether they reside in the primary or in the replica site. You can have the following deployment scenarios:

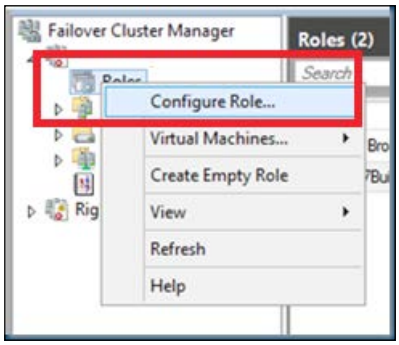
- Hyper-V host to a Failover Cluster
- Failover Cluster to a Failover Cluster
- Failover Cluster to a Hyper-V node

Hyper-V Replica configuration when Failover Clusters are used is done with the Failover Cluster Management console. For replication to take place, the **Hyper-V Replica Broker** role must be installed on the Failover Clusters, whether they are in primary or replica sites. The Hyper-V Replica Broker role is installed like any other Failover Cluster roles. You have to do the following:

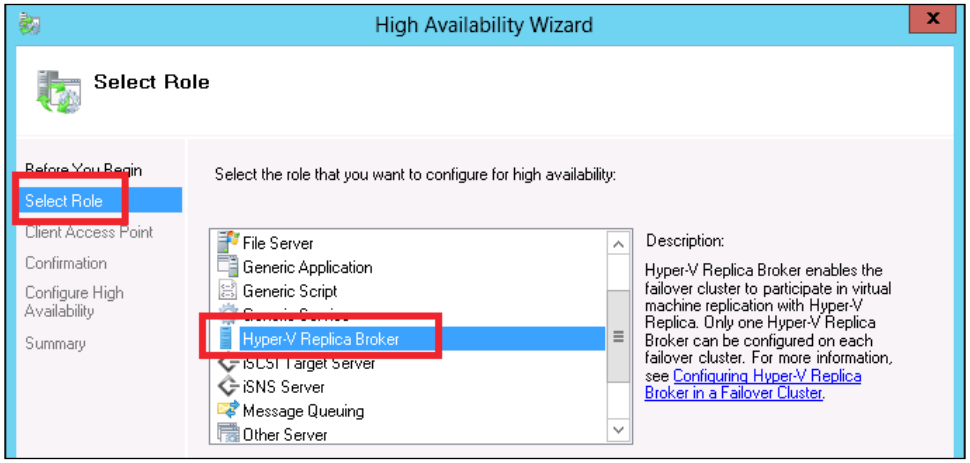
1. Start the Failover Cluster Management console.
2. Select a cluster from the left pane.

www.allitebooks.com

3. In the **Actions** pane, click on **Configure Role**:



4. Choose **Hyper-V Replica Broker** from the list of available roles:

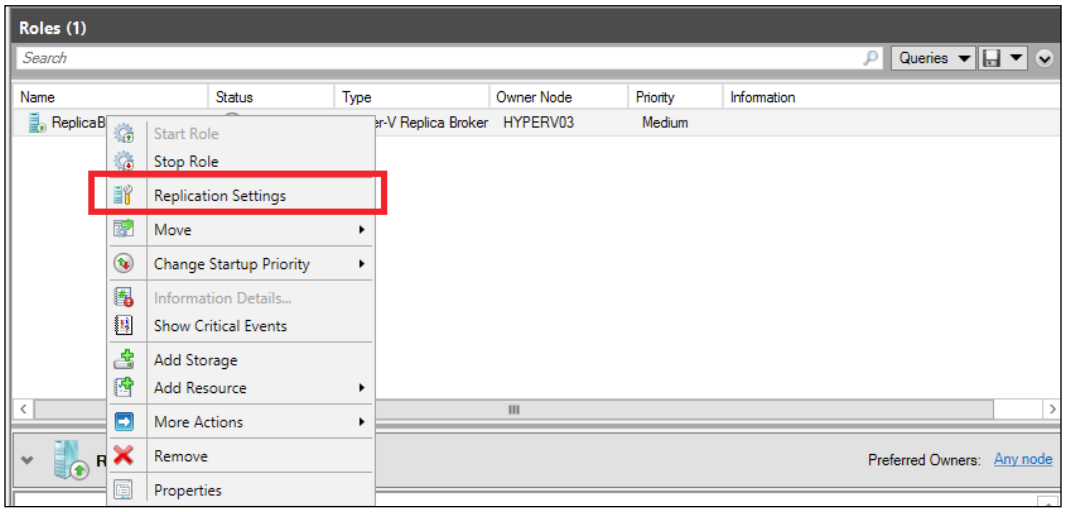


5. You have to enter a NetBIOS name and an IP address of the cluster which is a connection point for management.

Once the Hyper-V Replica Broker is installed, you can continue with the configuration of the cluster as a replica cluster. To do this, perform the following tasks:

1. Start the Failover Cluster Management console.
2. Select a cluster from the left pane.
3. Click on the **Roles in the details** pane.

4. Right-click on the **Hyper-V Broker** role and choose **Replication Settings**:



5. Here, you can configure the Failover Cluster as a replica cluster, just as you would configure a standalone host.

So, when using Failover Cluster in the replica site, you have to enable the **Hyper-V Broker** role on the Failover Cluster. This is done from the Failover Cluster Management console. To configure virtual machines for replication that are running in the cluster, you can do it with the Hyper-V Management console or Failover Cluster Manager, and then follow the procedure to **Configure Virtual Machine for Replication**.

Failover scenarios

In Hyper-V Replica there are three failover scenarios:

- Test failover
- Planned failover
- Unplanned failover

Test failover

As the name says, this is only used for testing purposes, such as health validation and Hyper-V Replica functionality. When test failover is performed, there is no downtime on the systems in the production environment. Test failover is done at the replica site. To perform a test failover on a replica virtual machine do the following:

1. Start the Hyper-V Management console.
2. Right-click on a replica virtual machine for which you want to perform a test failover.
3. Navigate to **Replication** | **Test Failover**.
4. Choose the recovery point.
5. Click on **Test Failover**.

When test failover is in progress, a new virtual machine is created which is a copy of the virtual machine for which you are performing the test failover. It is easily distinguished because the new virtual machine has `Test` added to the name. It is safe for the Test Virtual Machine to be started because there is no network adapter on it. So no one can access it. It serves only for testing purposes. You can log in on it and check the application consistency. When you have finished testing, right-click on the virtual machine and choose **Stop Test Failover**, and then the Test virtual machine is deleted.

Planned failover

Planned failover is the safest and the only type that should be performed. Planned failover is usually done when Hyper-V hosts have to be shut down for various reasons such as transport or maintenance. This is similar to Live Migration. You make a planned failover so that you don't lose virtual machine availability. The first thing you have to do is check whether the replication process for the virtual machine is healthy. To do this, you have to start the Hyper-V Management console in the primary site. Choose the virtual machine, and then at the bottom, click on the **Replication** tab. If the replication health status is `Healthy`, then it is fine to do the planned failover. If the health status doesn't show `Healthy`, then you need to do some maintenance until it says `Healthy`. To make a planned failover:

1. Start the Hyper-V Management console.
2. Right-click on a virtual machine.
3. Navigate to **Replication** | **Planned Failover**.
4. Select the **Start the Replica virtual machine after failover** checkbox.

Unplanned failovers

Unplanned failover is used only as a last resort. It always results in data loss because any data that has not been replicated is lost during the failover. Although planned failover is done at the primary site, the unplanned failover is done at the replica site. When performing unplanned failover, the replica virtual machine is started. At that moment Hyper-V checks to see if the primary virtual machine is on. If it is on, then the failover process is stopped. If the primary virtual machine is off, then the failover process is continued and the replica virtual machine becomes the primary virtual machine. To start an unplanned failover do the following:

1. Start the Hyper-V Management console.
2. Select the virtual machine.
3. Right-click on it and go to **Replication** | **Failover**.
4. Select the recovery point.

The recovery point can be useful because this way you can bring a virtual machine to a point in time where there was no primary site malfunctioning.

Summary

In this chapter, we learned what Hyper-V Replica is and how it can be applied. We examined the different replication scenarios and their advantages. We successfully configured a replica site and configured virtual machines for replication, and learned how to configure the Windows Firewall to allow incoming replication data. We learned how to test the Hyper-V Replica configuration with the test failover functionality and also learned how to failover a virtual machine successfully in case of planned or unplanned failover scenarios.

In the next chapter, we will take a closer look at the security aspects of Hyper-V. We will go deeper in the authentication and authorization stages that occur between replica sites. We will also learn how to generate certificates for data encryption.

4
Authentication in Hyper-V Replica

In this chapter, we will learn how to increase security in Hyper-V Replica. Replication traffic is sensitive traffic because it consists of virtual machine data, which can be very confidential. All this traffic can be intercepted by attackers. That is why the virtual machine replication traffic should be encrypted. We will see how you can create a certificate template in your Certificate Authority and how to import it in your Hyper-V hosts. Also, we will see how to use the Hyper-V hosts' self-signed certificate, which is generated when the server is installed. Not all the replication traffic should be encrypted. That is why there is another option for authentication. It is named **Kerberos** and we will take a look at it also.

Hyper-V Replica authentication types

In Hyper-V Replica, there are two types of authentication. They are as follows:

- Kerberos
- Certificate-based authentication

Although certificate-based authentication provides data encryption, Kerberos doesn't. There are three different types of certificates that you can use in Hyper-V Replica. They are as follows:

- Certificates issued by public Certificate Authority
- Certificates issued by **Enterprise Certificate Authority**
- Self-signed certificates

Note that Hyper-V Replica configuration with certificates issued by public Certificate Authorities will not be covered.

When it comes to authentication, Kerberos is the preferred option. It is easier to administer and it doesn't add an overhead to the communication. This can be very important, so that the link between sites doesn't get congested.

Nonencrypted communication

There are several factors that you have to consider when implementing Hyper-V Replica. For example, you have to choose between encrypted and nonencrypted communication between your primary and Replica site. Nonencrypted communication is faster because there is no overhead on the link between the sites. But, it doesn't protect your data from the attackers. Any attacker can intercept your data and possibly use it to damage your enterprise. This decision, whether or not to use certificates, is influenced by the following factors:

- To what degree is your Data Replication Traffic sensitive
- How fast is your connection between the primary and secondary site

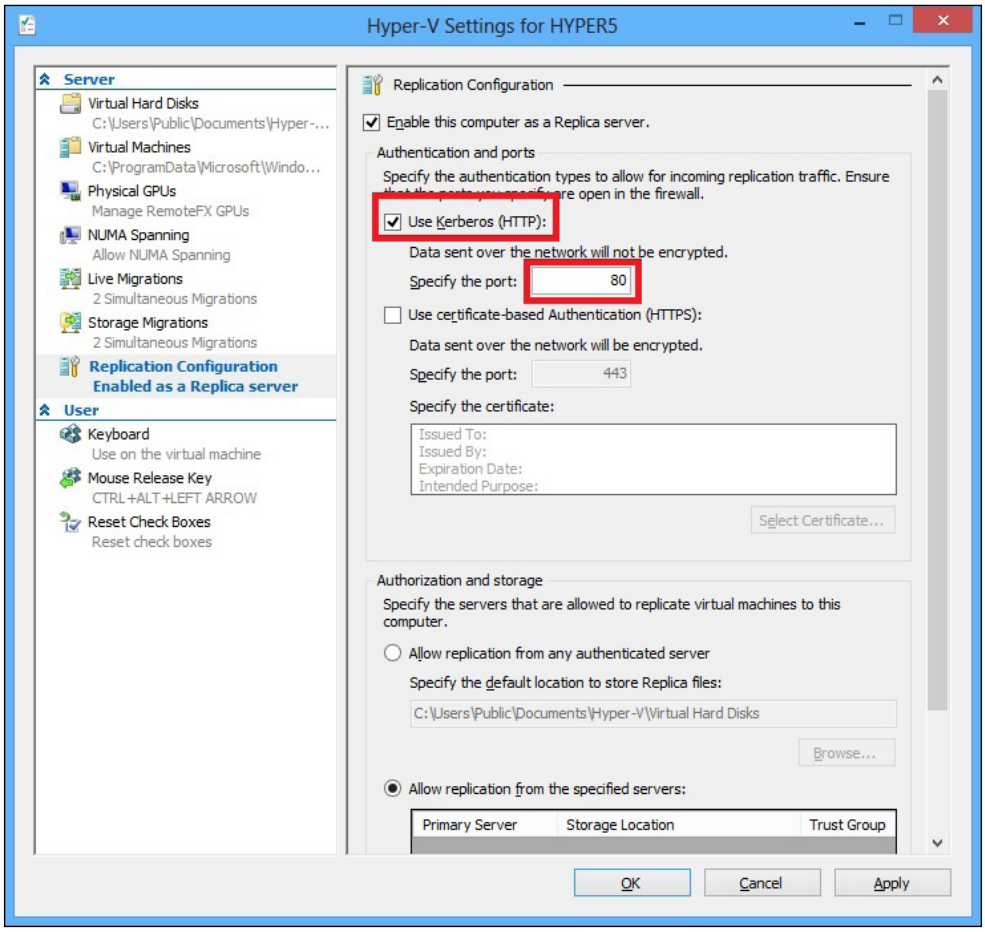
In a perfect scenario, there will be data encryption and a fast connection between the sites, but that is not always the case. So you have to take into consideration these two factors and decide which works best for you. Encryption of replication traffic adds overhead to the traffic, so if the link between the sites is slow then Hyper-V Replica's performance will suffer, especially when there is a slow link between the sites. Link stability is another factor. Before replication starts, you have to perform initial replication. This transfer lasts longer and contains more data than replication of changes in the virtual machine.

When using nonencrypted communication, Hyper-V Replica uses a protocol named Kerberos. Kerberos is a network authentication protocol, which works on the principle of "tickets" to allow devices to communicate in a non-secure network. Kerberos proves the identity of the devices in a secure manner. It uses symmetric key cryptography.

To configure Kerberos authentication on your Replica Server do the following:

1. Start Hyper-V Manager Console.
2. Click **Hyper-V Settings** in the **Actions** pane.
3. Go to **Replication Configuration**.

4. The following screenshot shows the Kerberos configuration. Check **Use Kerberos (HTTP)** and enter another port number or use the default.



Encrypted communication

In order to encrypt your traffic you have to use certificates. Certificates have a double role in this scenario; they are used for the authentication of nodes and also for the encryption of replication traffic.

Note that you must have an Enterprise Certificate Authority server in your domain. Enterprise Certificate Authority is a server with the Active Directory Certificate Services role installed on it.

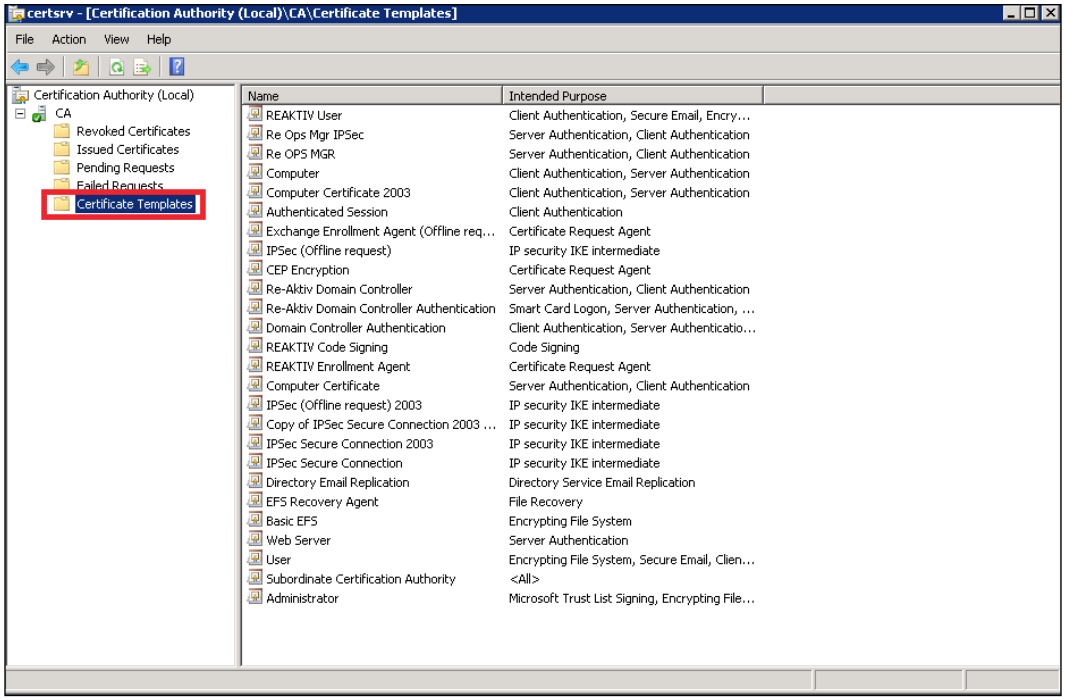
To set up an Enterprise Certificate Authority server, refer to the article at the following link:

`http://technet.microsoft.com/en-us/library/cc772393(v=ws.10).aspx`

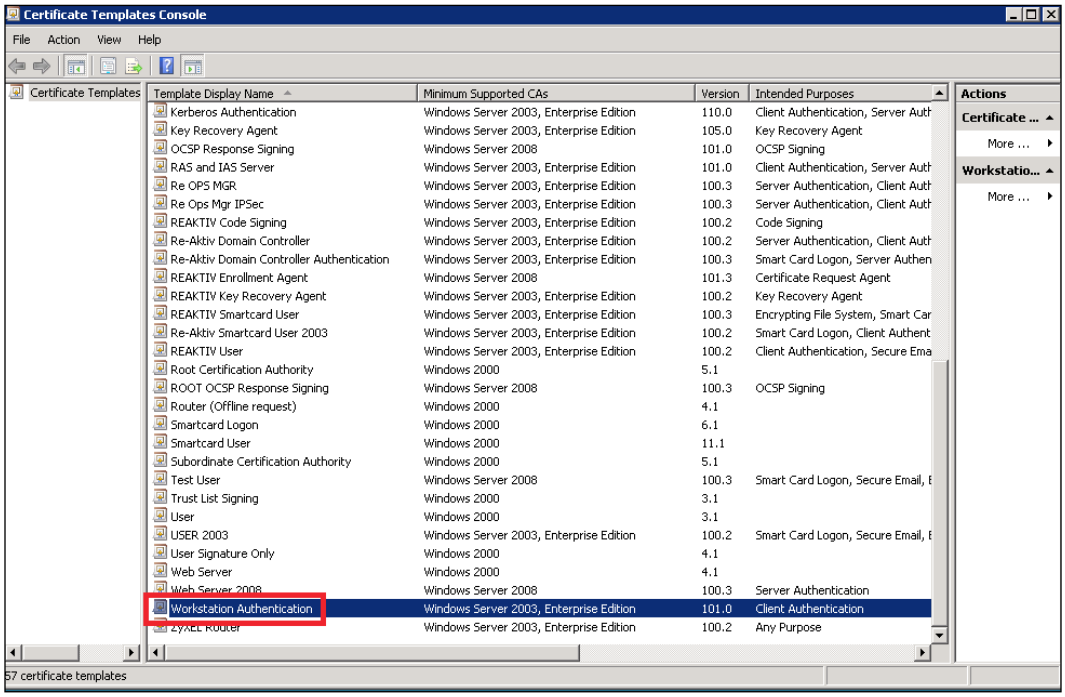
Creating a certificate template

Before we can equip our Hyper-V hosts with a certificate for data encryption, we need to create a certificate template. To do this, we need to log on to our Certificate Authority server and perform the following steps:

1. Navigate to **Start | Administrative Tools | Certificate Authority**.
2. In the left-hand side pane, expand your server and go to **Certificate Templates | Manage**, as shown on the following screenshot:

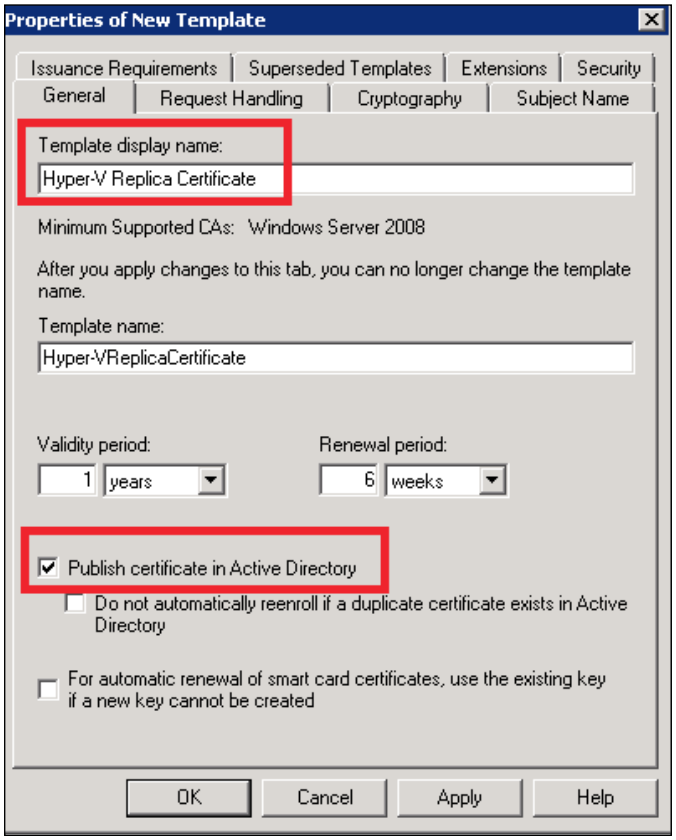


3. In the next screenshot, you can see the list of available templates. Find **Workstation Authentication**, right-click on it and choose **Duplicate Template**.

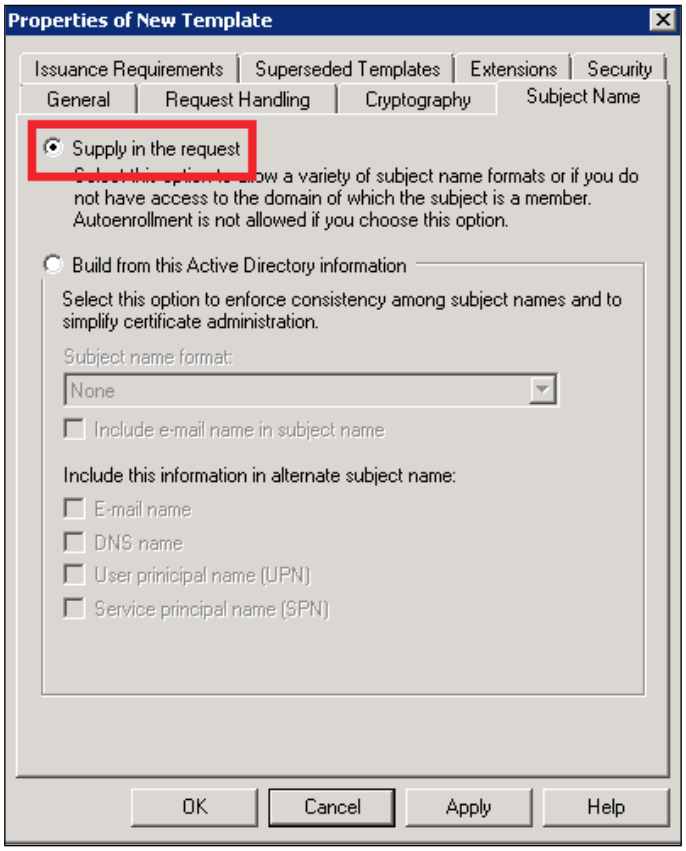


www.allitebooks.com

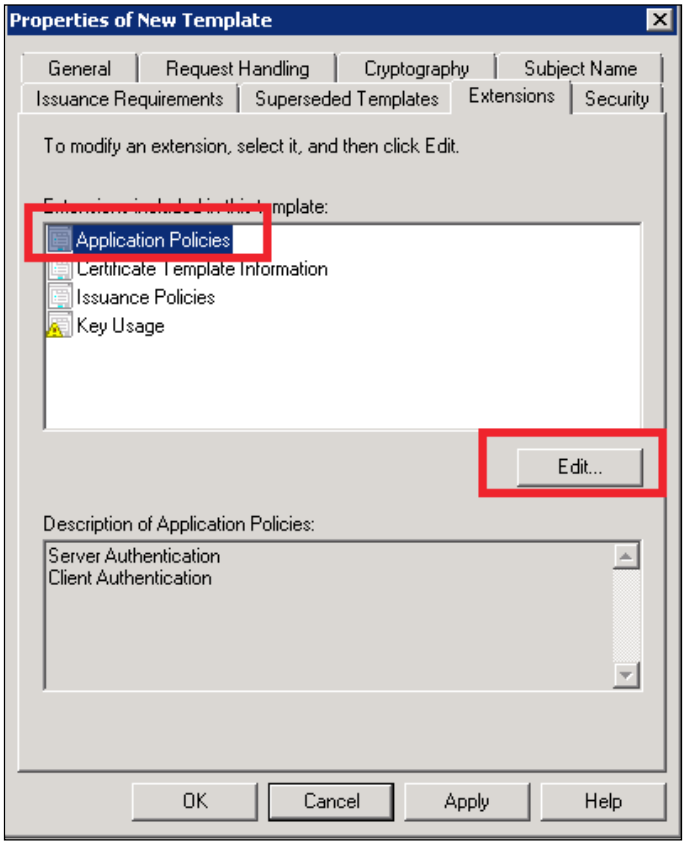
4. In the next screenshot, the configuration window for the certificate name is shown. Enter a name for the template and check **Publish certificate in Active Directory**.



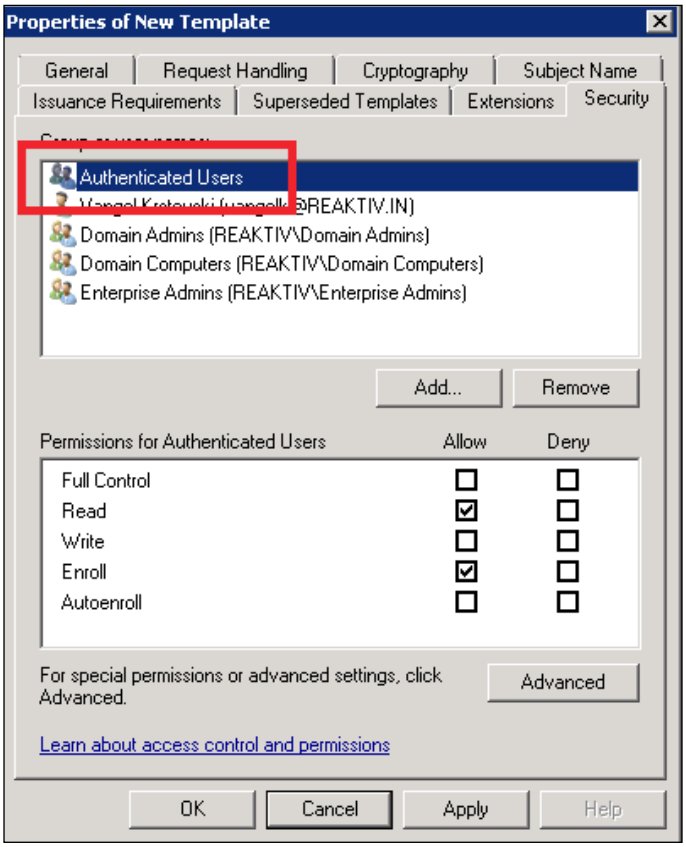
5. In the **Subject Name** tab, select **Supply in the request**, as shown in the following screenshot:



6. In the next screenshot, you can see the configuration window for the use of the template. In the **Extensions** tab, click on **Application Policies**. Then click on **Edit**, and add **Server Authentication** and **Client Authentication**.



7. In the **Security** tab, select **Authenticated Users** and give them **Enroll** and **Read** permissions, as shown in the following screenshot:



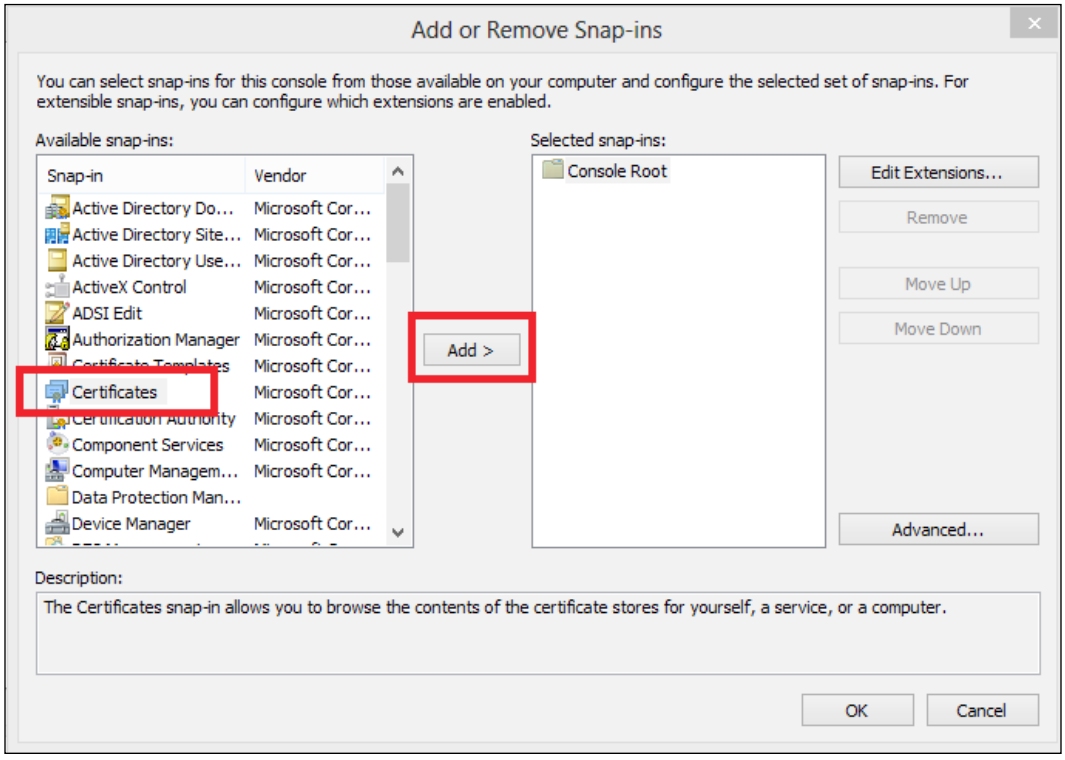
8. Click on **Apply** and then on **OK** to complete the configuration of your template.

This concludes the certificate template configuration. Next, you need you use this certificate template and import it to all of the Hyper-V hosts.

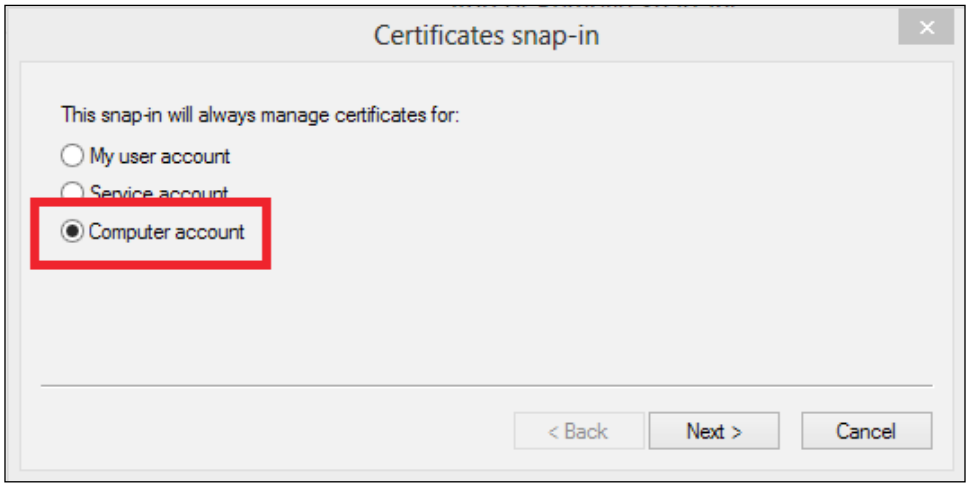
Requesting and importing a certificate

To import a certificate, you need the following:

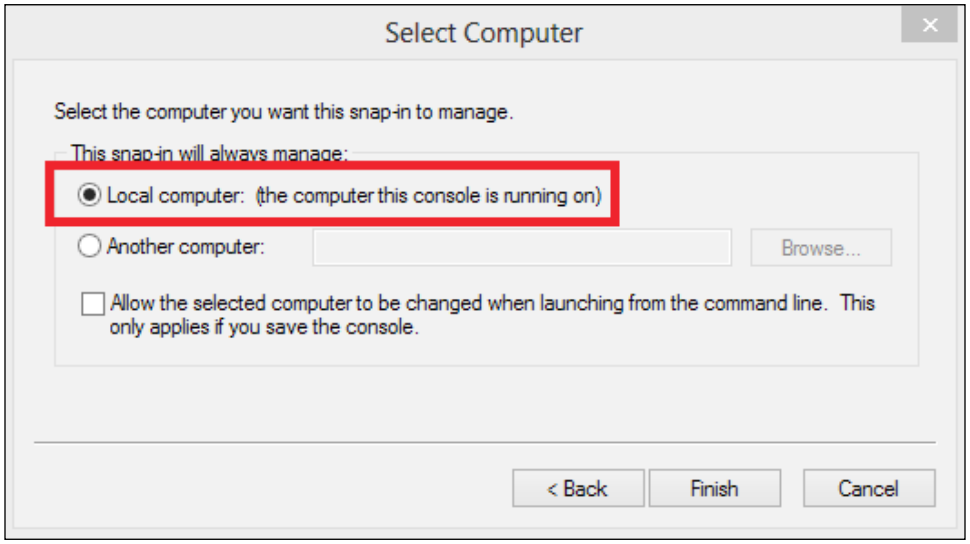
1. Login to your Hyper-V hosts and go to **Start | Run** and enter `mmc.exe`.
2. Go to **File | Add/Remove Snap-ins**.
3. From the list, select **Certificates** and click on **Add**.



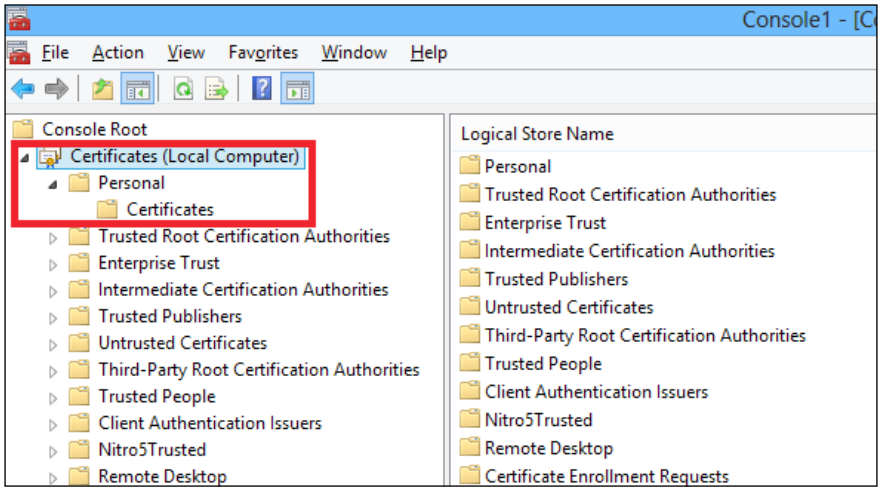
4. A menu such as the one in the next screenshot appears. Choose **Computer account**, and click on **Next**.



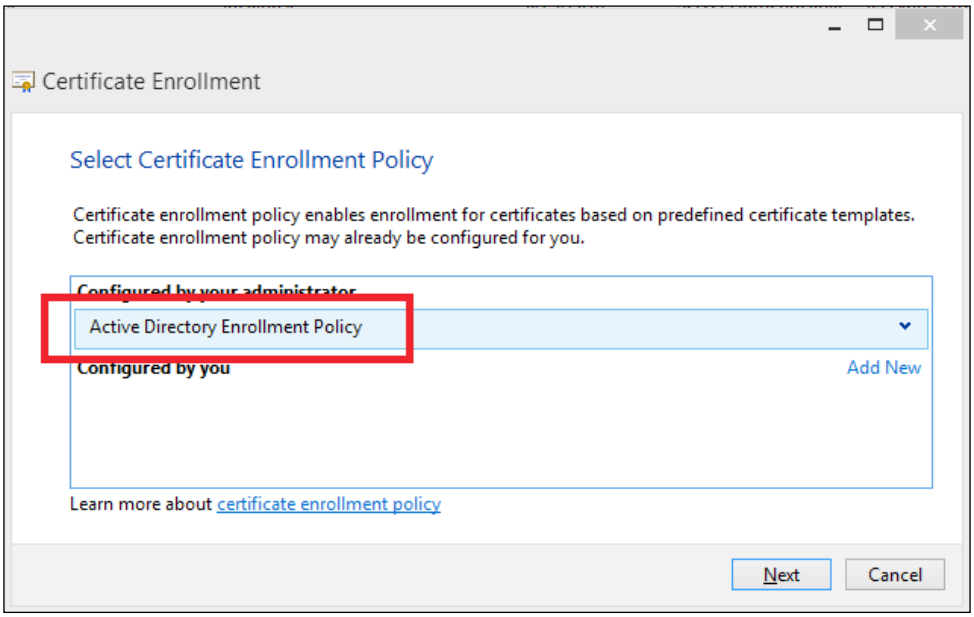
5. When a new menu appears, as the one in the next screenshot, select **Local computer**, and click on **Finish**.



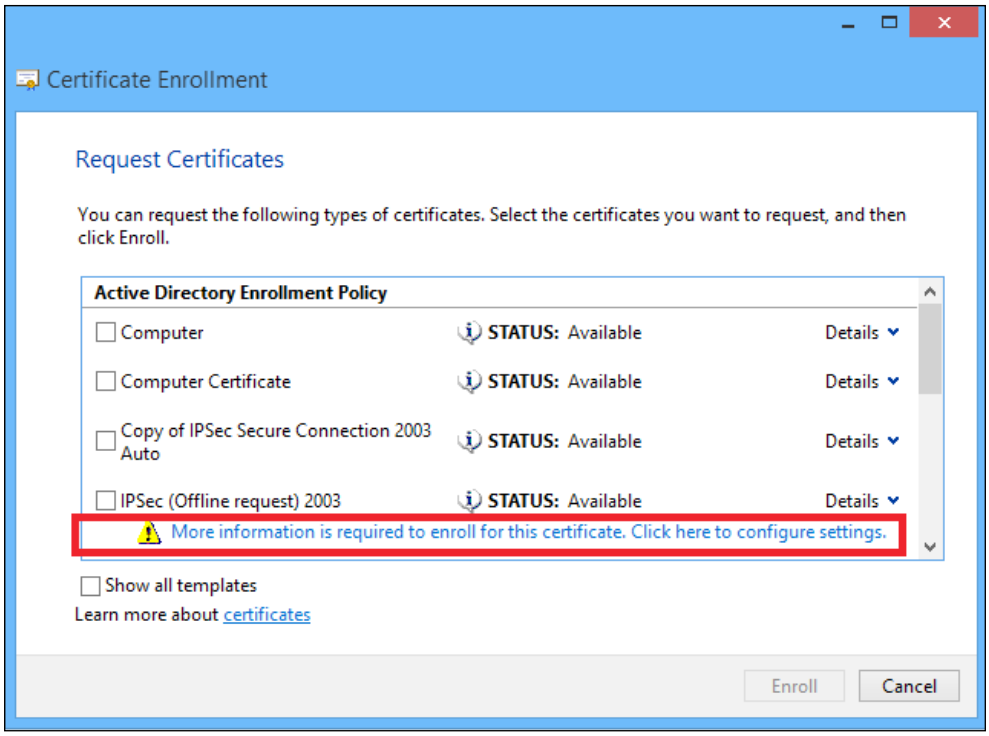
6. In the left-hand side pane, select your server, expand **Personal**, and right-click on **Certificates** and go to **All tasks | Request new certificate**. The configuration window is shown in the following screenshot:



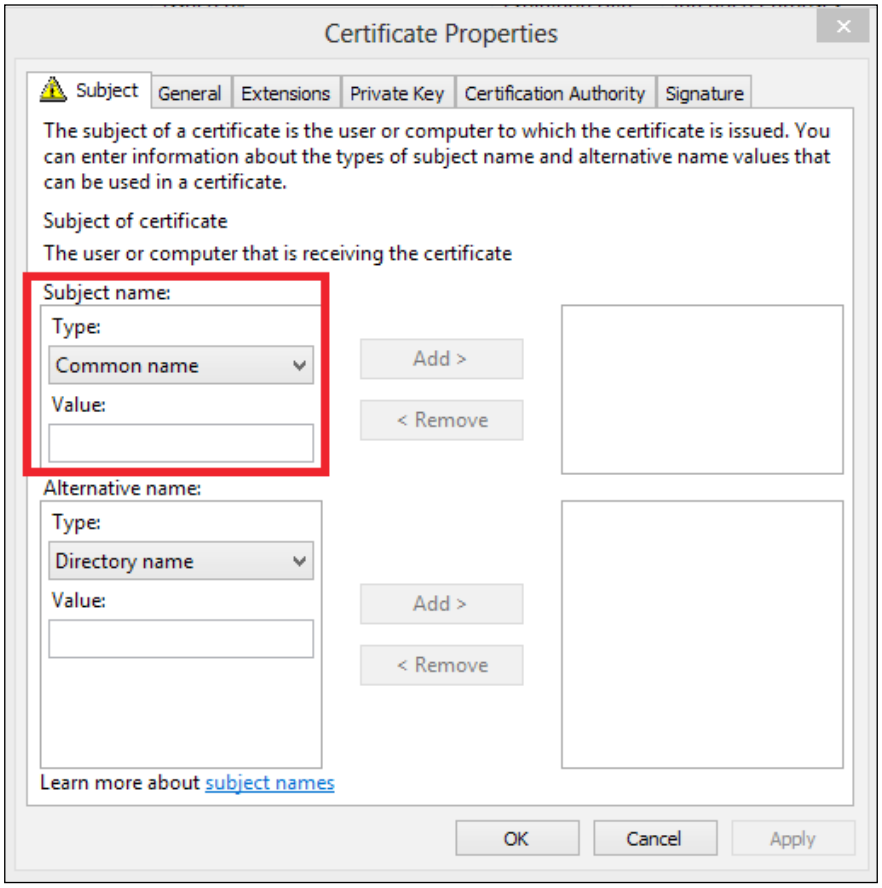
7. In the first step of the wizard, just click on **Next**.
8. In the second step, select **Active Directory Enrolment Policy**, and click on **Next**, as shown in the following screenshot:



9. From the list of certificate templates, such as the one in next screenshot, find the new template that you created, and click on the blue link that says **More information is required to enroll for this certificate. Click here to configure settings**.



10. After that, you will see a window, such as the one in the next screenshot. From the drop-down menu select **Common Name** for **Subject Name** and enter the name of your server in **Fully Qualified Domain Name** (**FQDN**).



11. Click on **Apply** and then click on **Enroll** to finish importing your certificate.

This concludes the import process of a certificate to a Hyper-V host. Now, follow the procedure Enable Hyper-V Replica on Replica site, explained in *Chapter 3*, *Configuring Hyper-V Replica*, to select this certificate for Hyper-V authentication.

Note that certificate authentication is also used when one of the sites reside in untrusted domains. When you have this kind of scenario, then using certificates is the only way to configure Hyper-V Replica.

When configuring Hyper-V Replica between untrusted domains, the request and import of certificates is different. You need to use the web enrolment functionality of Certificate Authority to request and import the certificate. Refer to the following article about request and import of a certificate from a server in untrusted domain:

`http://technet.microsoft.com/en-us/library/hh831649.aspx`

Authenticating with a self-signed certificate

There is also a scenario where the Hyper-V hosts reside in a workgroup and there is no Enterprise Certificate Authority. In this scenario, the use of self-signed certificates is the only solution. To configure Hyper-V Replica with self-signed certificate, refer to the article on the following link:

`http://jsmcomputers.biz/wp/?p=360`

Summary

In this chapter, we learned about why encryption is important for Hyper-V Replica, and defined factors that influence the decision whether or not to use certificates for authentication and encryption. We learned the procedure how to create a certificate template for the purpose of Hyper-V Replica. We also learned how to import this certificate in our Replica Server and associate it with Hyper-V Replica.

In the next chapter, we will learn more about management of Hyper-V Replica and how to troubleshoot common Hyper-V Replica issues.

5
Administrating Hyper-V Replica

In this chapter, we will take a look at the various ways you can manage Hyper-V Replica depending on your scenario. We will learn how to troubleshoot common Hyper-V Replica issues and how to resolve them. Administration takes up most of the operations regarding any platform with any purpose. Daily maintenance of systems is just as important as analyzing and deploying them. If some Hyper-V Replica enabled virtual machine stops being replicated, or if an entire production or replica site is not accessible, you need to know where to look for the problem and how to approach it. This chapter will show you how to do all of this.

Managing Hyper-V Replica

Depending on your deployment scenario, there are two ways to manage Hyper-V Replica. The following are the two management consoles that we have used throughout the configuration process of Hyper-V Replica:

- Hyper-V management console
- Failover cluster management console

If Virtual Machine Manager 2012, which is part of the System Centre 2012 Suite, is deployed in your infrastructure, you can also use it to configure Hyper-V Replica. This management console was not used in the examples because it doesn't come with Windows Server 2012.

If you want to go deeper into what is going on with your Hyper-V Replica servers, you can browse the event log on your server. To view Hyper-V Replica events, do the following steps:

1. Navigate to **Start** | **Run**, and type `eventvwr.exe`.
2. From the navigation pane, navigate to **Application and Services log** | **Microsoft** | **Windows** | **Hyper-V-VMMS**.

Primary site management

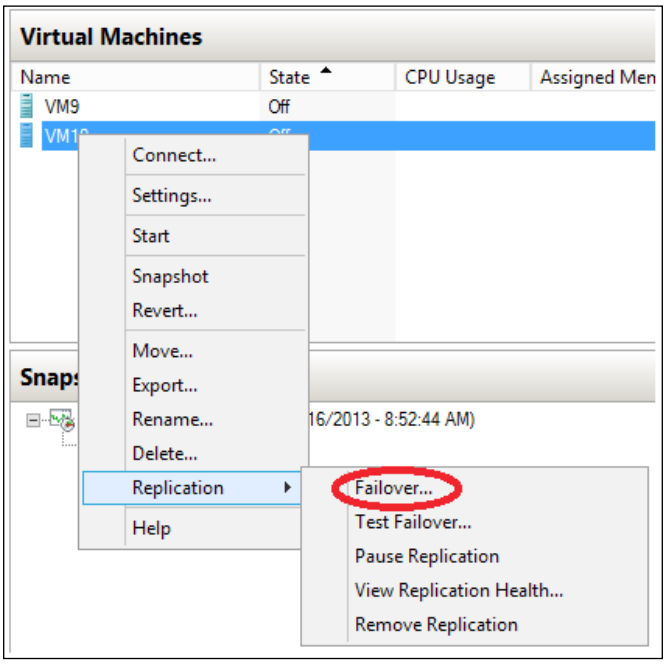
Management tasks regarding primary sites are as follows:

- **Planned failover**: You make a planned failover when you want to make some maintenance tasks on your primary server and you want all of your virtual machines to still be available. All of the primary virtual machines are turned off and their replica virtual machines are turned on. You can find more about planned failover at `http://www.virtualizationadmin.com/articles-tutorials/microsoft-hyper-v-articles/networking/working-replicas-hyper-v-30-part6.html`.
- **Pause replication**: You can halt the replication process at any time. You can use this option, for example, if your link between the two sides is down and you don't want to have your event log or information pane filled with warnings or errors. To halt a replication, right-click on the virtual machine, navigate to **Replication** | **Pause Replication**.
- **Resume replication**: When all of your problems are solved, you can resume the replication. To resume a paused replication, right-click on virtual machine, and navigate to **Replication** | **Resume Replication**.
- **Check replication in the Hyper-V Management console**: To view and test the replication health of your virtual machines, refer to the following links:
    - `http://www.virtualizationadmin.com/articles-tutorials/microsoft-hyper-v-articles/networking/working-replicas-hyper-v-30-part4.html`
    - `http://www.virtualizationadmin.com/articles-tutorials/microsoft-hyper-v-articles/networking/working-replicas-hyper-v-30-part5.html`
- **Disable replication**: If at any time you wish to stop replication on a virtual machine, just right-click on the virtual machine and navigate to **Replication** | **Remove Replication**.

Replica site management

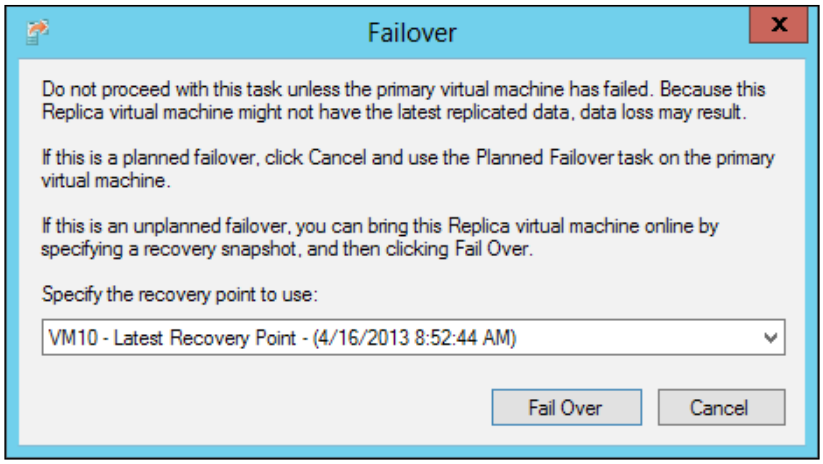
Management tasks regarding replica sites are as follows:

- **Failover**: This is an unplanned event. In case of a disaster, this is the task that must be performed. During this task the replica virtual machine in your replica site is turned on, and it becomes a primary virtual machine. The failover menu is shown in the following screenshot:



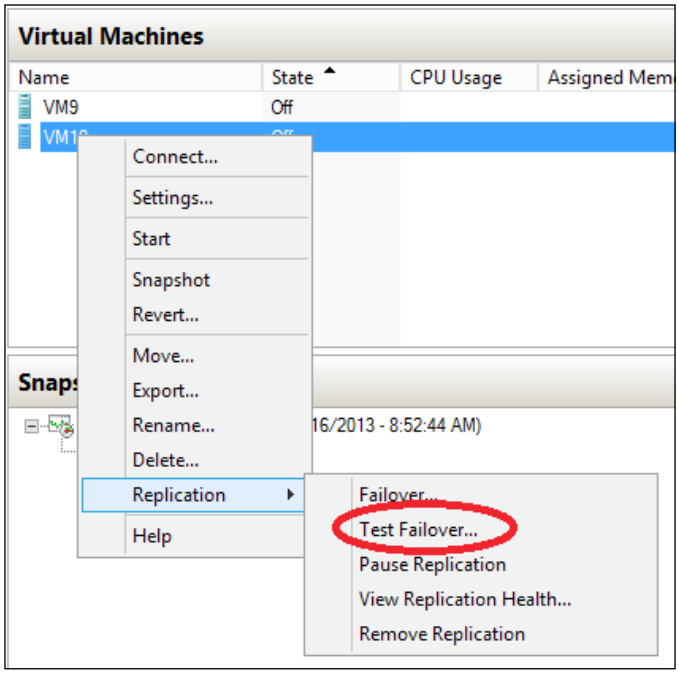
You can find more about failover at the link: `http://www.virtualizationadmin.com/articles-tutorials/microsoft-hyper-v-articles/networking/working-replicas-hyper-v-30-part6.html`.

By clicking on **Failover...** the replica virtual machine is promoted, and it becomes a primary virtual machine. If there are multiple recovery points, the wizard will ask you to select one. The recovery point selection menu is displayed in the following screenshot:



- **Reverse Replication**: When the primary server is back online, you can perform a reverse replication and thus move the virtual machine execution back to the primary server.
- **Remove Recovery Point**: This option is only available after a failover was performed. Before you can execute reverse replication, you have to remove all of the recovery points for that virtual machine. After the reverse replication is over, the replication process will make new recovery points for that virtual machine. Removing recovery points is a step in the reverse replication wizard.

- **Test Failover**: **Test failover...** is done when you want to view the virtual machine in the replica site without interfering with the virtual machine in the primary site. Test failover menu is shown in the following screenshot:



- **Cancel Test Failover**: If you are performing a test failover and you are finished with the test, you can cancel the process with a right-click on the virtual machine and by navigating to **Replication** | **Stop Test Failover**.

Administration of certificates

Certificates require more administration because they have an expiration period. After the period has expired they need to be renewed. To renew a certificate, refer to this article: `http://technet.microsoft.com/en-us/library/cc730605.aspx`.

Summary

In this chapter, we saw all the procedures that you need to do when Hyper-V Replica is not performing in the right way. We classified them in two groups: primary site and replica site management. We also looked at the steps that need to be performed when disaster occurs at the primary site, and how to perform reverse replication when the production site is functional again. In the next chapter, we will take an overview of all the chapters and give a conclusion on Hyper-V Replica.

Summary

In this book, we were introduced to Windows Server 2012, the newest edition of Windows Server, and learned what it can offer to the IT department. There are new concepts and useful features that make the IT administrators' life easier. Windows Server 2012 is designed for enterprises that want to deploy modern datacenters with state-of-the-art capabilities. The new user interface, the simplified configuration, and all of the built-in features are what that makes Windows Server 2012 appealing to the IT administrators. In this book, we concentrated on four functionalities of Windows Server 2012. Those features are: Hyper-V, Hyper-V replica, Failover Clustering, and SMB. Combining all of these in one datacenter allows the administrator: easier administration of storage space, faster provisioning of virtual machines, failover capabilities in case of malfunctions in the datacenter, and business continuity and disaster recovery mechanism. These are four very important aspects when designing a datacenter. And, when you get all of them in one product, you can see how valuable this product is. Business processes is how the enterprise works. Some of the processes are more important than others and they are called value chains. These processes are the ones that generate income for the enterprise. It can either be sales process, or manufacturing process, or supply management process, or something else. All of these processes rely on some kind of an information system. Because they are valuable to the enterprise, there must not be any disruptions to the workflow of the process. Any disruption will lead to unfulfilled goals of the enterprise.

For example, the information system goes down and the supermarket cannot sell anything, or the supply chain system goes down and the deliveries get mixed up and end at a different location. All these problems affect the enterprise income and respect. That is why information system availability is very important. It is upon the IT department to implement such a system that will allow the business to function properly in case of any disruptions. Whether it is power outage, fire hazard, earthquake, or scheduled maintenance, IT should be all about the business and it should be aligned with the business. This is what Windows Server 2012 can offer to the enterprise. With the implementation of Windows Server 2012, you get all the key factors that were explained previously. You get a state-of-the-art virtualization platform that allows you provision of virtual machines faster, a concept for easier administration of storage space mechanism, in case of disaster scenarios. All of this will ensure business continuity in your enterprise, which is your primary goal.

Index

A

Actions pane 56
Active Directory Certificate Services 34
Active Directory Domain 33
Application consistent replicas 43

B

broker manager, Hyper-V replica 11
Business Continuity and Disaster Recovery (BCDR) solution 6

C

certificate
  administration 75
  importing 64-69
  requesting 64-69
Certificate Authority (CA) 34
certificate template
  creating 58-63
Computer account 65

E

encrypted communication
  about 57
  certificate, importing 64-69
  certificate, requesting 64-69
  certificate template, creating 58-63
  certificate template, screenshot 58
  self-signed certificate, authenticating with 69
Enroll permissions 63
Enterprise Certificate Authority 55
Extensions tab 62

F

failover
  about 73
  URL 73
Failover Cluster
  about 23, 33
  creating, steps 26-28
  setting up 23-25
Failover Cluster environment
  virtual machine replication 49
Failover cluster management console 71
Failover Cluster traffic 21
failover scenarios, Hyper-V Replica
  about 51
  planned failover 52
  test failover 52
  unplanned failover 53
firewall rules
  configuring 46-49
Fully Qualified Domain Name (FQDN) 68

H

Hyper-V
  installing 7-9
  security, considerations 11
Hyper-V 3.0
  features 5, 6
Hyper-V management console 71
Hyper-V Replica
  Application consistent replicas 43
  authenticating, types 55, 56
  authorization, options 36

broker manager 11
configuring on server, in replica state 34-36
failover scenarios 51
firewall rules, configuring 46-49
functionalities 10
in standalone Hyper-V hosts environment 34
Kerberos authentication 36
managing 71
prerequisites 7
replication manager 10
replication tracker 10
requisites 33, 34
standard replicas 42
virtual machines, configuring 36-45
Hyper-V Replica authentication, types
certificate-based authentication 55
Kerberos 55
Hyper-V Replica Broker role 49, 50
Hyper-V Settings 56
Hyper-V VSS (Volume Shadow Copy Services) 43

I

installation
Hyper-V 7-9
iSCSI connections
setting up 18-21
iSCSI traffic 21

K

Kerberos
about 55, 56
configuring, steps 56, 57
Kerberos authentication 36
Kerberos configuration
screenshot 57

L

Live Migration 30
Local computer 65
Logical Unit Number (LUN) 18

N

networking
setting up 21
non-encrypted communication
about 56
using 56, 57

P

planned failover
about 52
URL 72
primary site management
disable replication 72
Hyper-V Management console, replication checking in 72
pause replication 72
planned failover 72
resume replication 72

Q

Quick Migration option 30

R

Read permissions 63
Remove Recovery Point option 74
Replica site management
about 72, 73
Cancel Test Failover 75
failover 73
Remove Recovery Point 74
reverse replication 74
Test Failover 75
replication
checking, in Hyper-V Management console 72
disable 72
pause 72
reverse 74
Replication Configuration 56
replication manager, Hyper-V replica 10
replication tracker, Hyper-V replica 10

S

security permissions
on SMB file shares, setting up 23
Security tab 63
Server Message Block. *See* **SMB**
SMB
protocol 13
SMB file shares
security permissions, setting up 23
SMB server
installing 14
iSCSI connections, setting up 18-21
networking, setting up 21-23
security permissions, setting up 23
SMB file share, creating 14-18
SMB Traffic 21
standard replicas 42
Subject Name tab 61

T

test failover
about 52, 75
cancelling 75

U

unplanned failover 53

V

virtualization 5
virtual machine replication
in Failover Cluster environment 49-51
virtual machines
configuring, for replication 36-42
Live Migrate, from one node to another 30
migration 29, 30

Thank you for buying

Hyper-V Replica Essentials

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

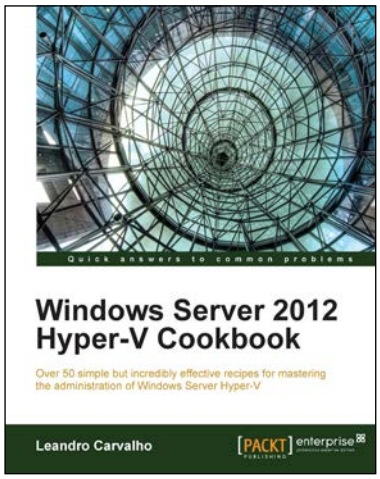
In 2010, Packt launched two new brands, Packt Enterprise and Packt Open Source, in order to continue its focus on specialization. This book is part of the Packt Enterprise brand, home to books published on enterprise software – software created by major vendors, including (but not limited to) IBM, Microsoft 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

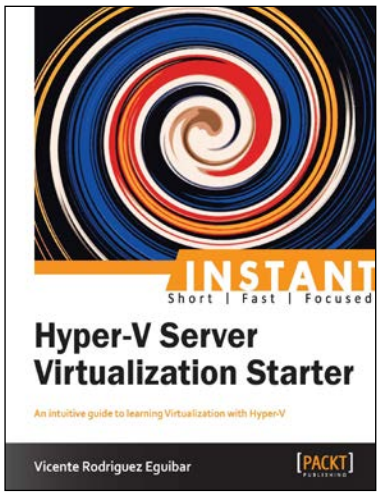


Windows Server 2012 Hyper-V Cookbook

ISBN: 978-1-84968-442-2 Paperback: 304 pages

Over 50 simple but incredibly effective recipes for mastering the administration of Windows Server Hyper-V

1. Take advantage of numerous Hyper-V best practices for administrators
2. Get to grips with migrating virtual machines between servers and old Hyper-V versions, automating tasks with PowerShell, providing a High Availability and Disaster Recovery environment, and much more
3. A practical Cookbook bursting with essential recipes



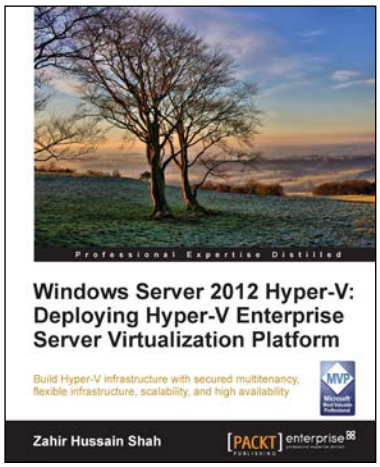
Instant Hyper-V Server Virtualization Starter

ISBN: 978-1-78217-997-9 Paperback: 58 pages

An intuitive guide to learningVirtualization with Hyper-V

1. Learn something new in an Instant! A short, fast, focused guide delivering immediate results
2. Step-by-step, practical guide to understanding and implementing virtualization for an enterprise environment
3. Learn how to create a virtual machine in three steps

[PACKT] PUBLISHING enterprise professional expertise distilled



Windows Server 2012 Hyper-V: Deploying Hyper-V Enterprise Server Virtualization Platform

ISBN: 978-1-84968-834-5 Paperback: 410 pages

Build Hyper-V infrastructure with secured multitenancy, flexible infrastructure, scalability, and high availability

1. A complete step-by-step Hyper-V deployment guide, covering all Hyper-V features for configuration and management best practices
2. Understand multi-tenancy, flexible architecture, scalability, and high availability features of new Windows Server 2012 Hyper-V

Windows Server 2012 Automation with PowerShell Cookbook

ISBN: 978-1-84968-946-5 Paperback: 372 pages

Over 110 recipes to automate Windows Server administrative tasks using PowerShell

1. Extend the capabilities of your Windows environment
2. Improve the process reliability by using well defined PowerShell scripts
3. Full of examples, scripts, and real-world best practices