|  |
| --- |
| Setting up Hyper-V 2012 Replication on Workgroup Servers |
| A Guide |
|  |

5/10/2013

|  |
| --- |
| **Metadata** |
| Author(s) | The Arizona Geological Survey |
| Current Version | 1.0 |
| Initial Publication Date | 5/10/2013 |

# Introduction

This document provides instructions regarding the use of Hyper-V 2012 to virtualize and replicate servers on x86 and x64 workgroup servers. This process makes it easy to back up entire servers and their contents.

Hyper-V is a *Windows Server Role* that can be installed on Windows Server 2012 platforms.

# Prerequisites

1. A minimum of two **Windows Server 2012** Hyper-V host servers
   1. One host server will act as the *primary* server, of which copies will be made
   2. Another host server will act as a *replica* server used to receive replica copies of virtual machines from the primary host server

# Installation and Setup

Step 1). Set up a Windows Server 2012 instance in a workgroup; do not join the server to a domain

Step 2). To install the **Windows 2012 Hyper-V role** on a Windows Server 2012 host server, open the **Windows Server 2012 Server Manager**

Step 3). Select **Local Server** (Figure 1); click **Manage**, then select **Add Roles and Features**; this will open the **Before you Begin** page of the **Add Roles and Features** wizard (Figure 2). Click **Next** to continue.

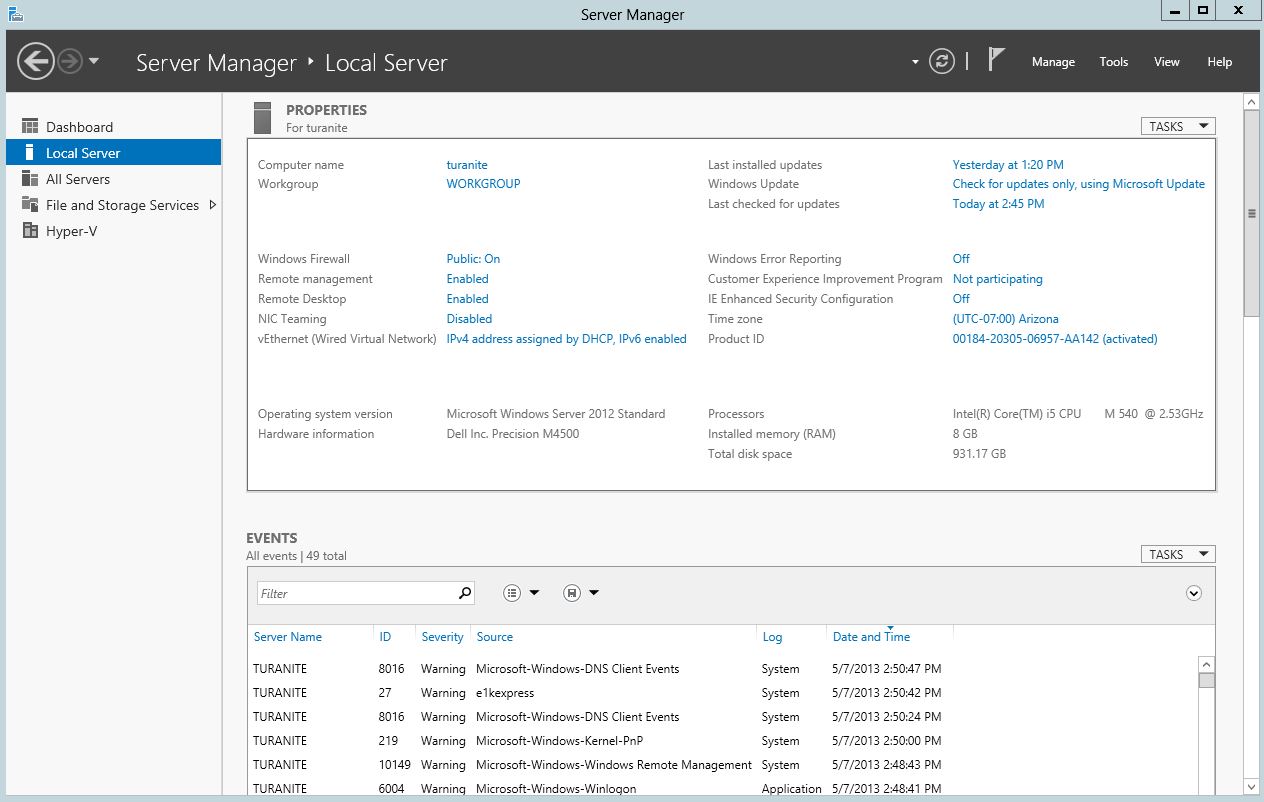


Figure 1: The Local Server window

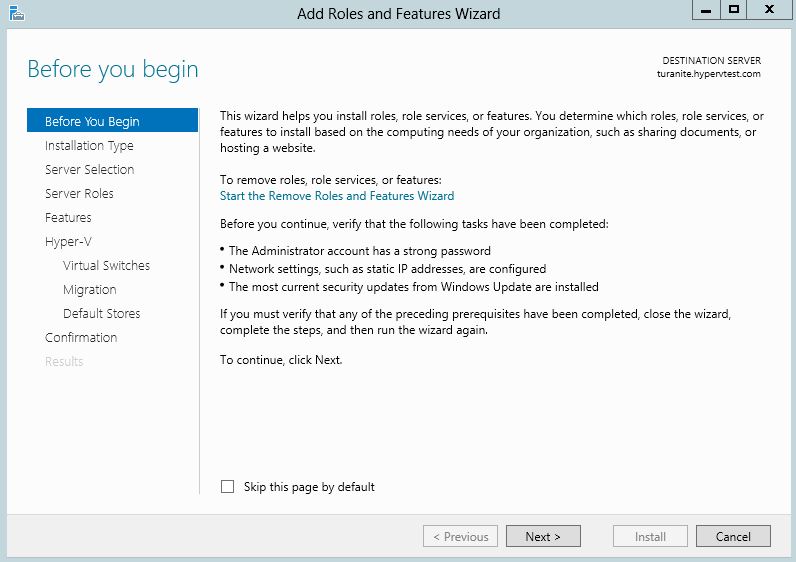


Figure 2: Before you Begin

Step 4). On the **Installation Type** page of the **Add Roles and Features** Wizard (Figure 3), click the Role-based or feature-based installation radio button; click **Next** to continue.

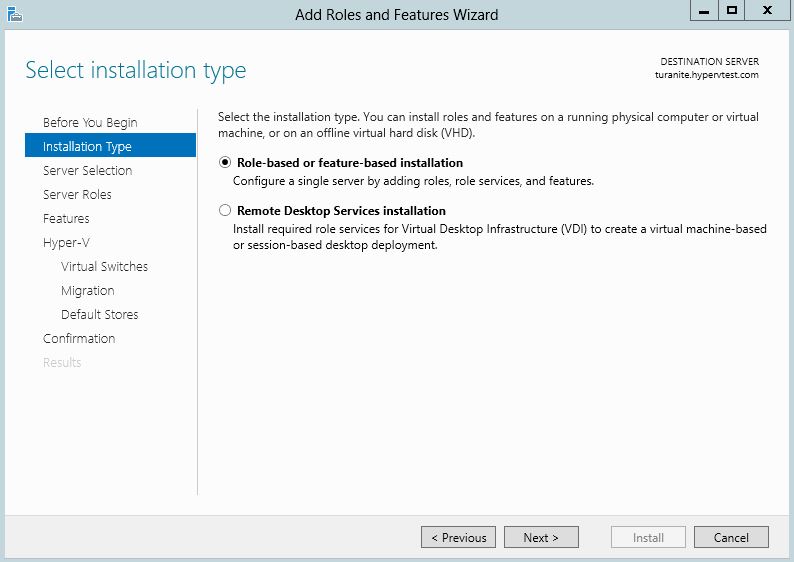


Figure 3: The Installation Type page of the Add Roles and Features Wizard

Step 5). On the **Server Selection** page of the **Add Roles and Features** Wizard (Figure 4), select the destination server to which you wish to install Hyper-V and click **Next** to continue.

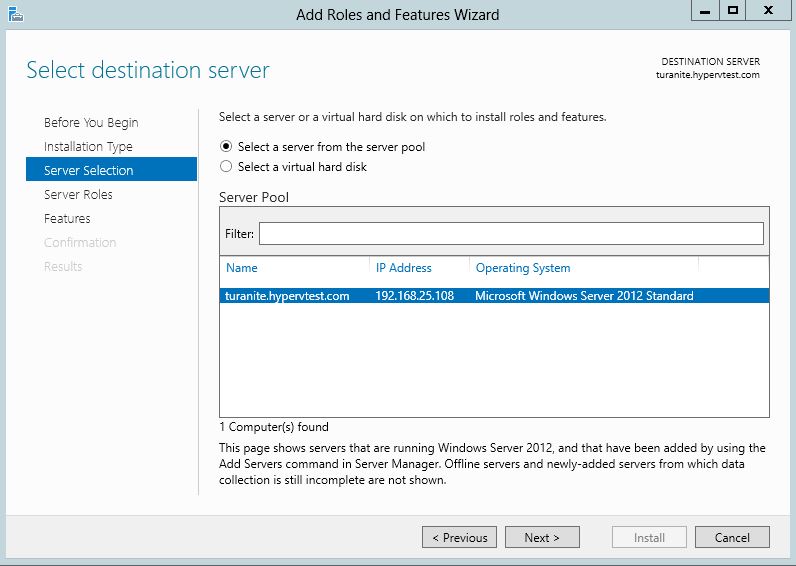


Figure 4: Server Selection

Step 6). On the **Server Roles** page of the **Add Roles and Features** Wizard (Figure 5), select the Hyper-V server role and click **Next** to continue.

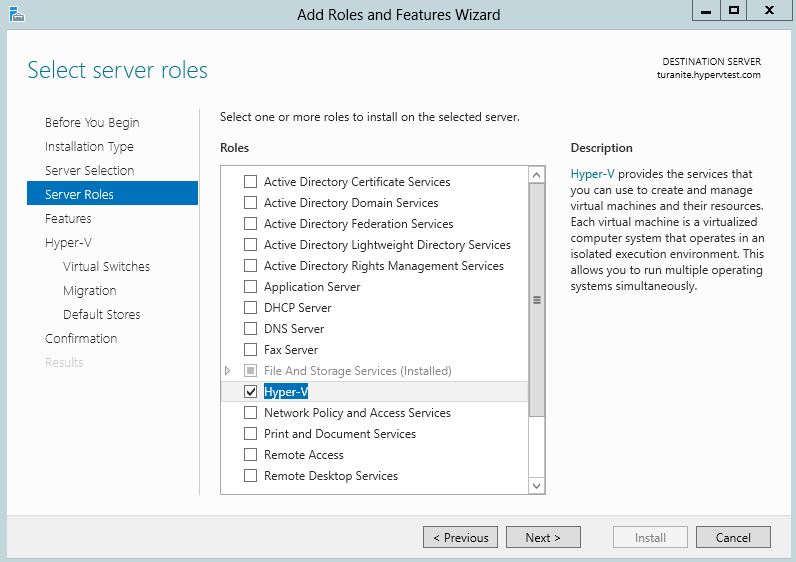


Figure 5: Server Roles

Step 7). On the **Features** page of the **Add Roles and Features** Wizard (Figure 6), select any desired features to be installed; note that for the purposes of this tutorial, the default features are sufficient. When finished, click **Next** to continue.

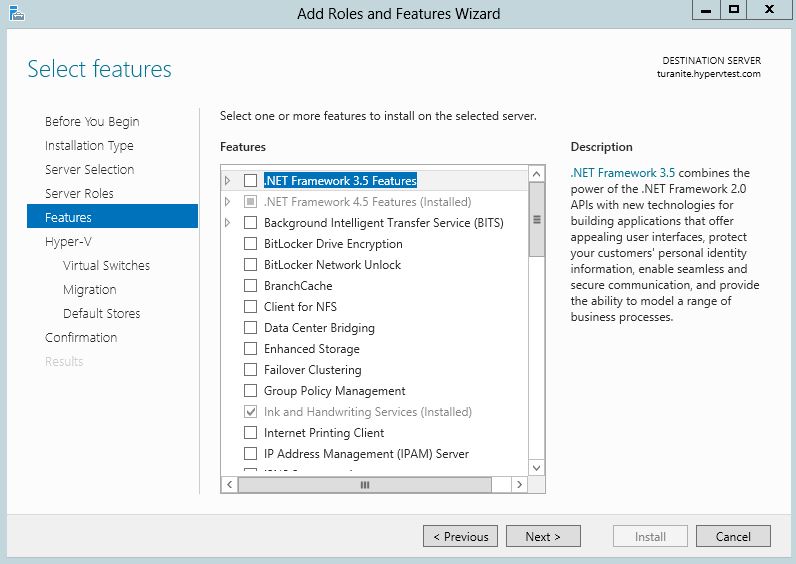


Figure 6: Features

Step 8). On the **Hyper-V** page of the **Add Roles and Features** Wizard (Figure 7), peruse information about Hyper-V; when you are finished, click **Next** to continue.

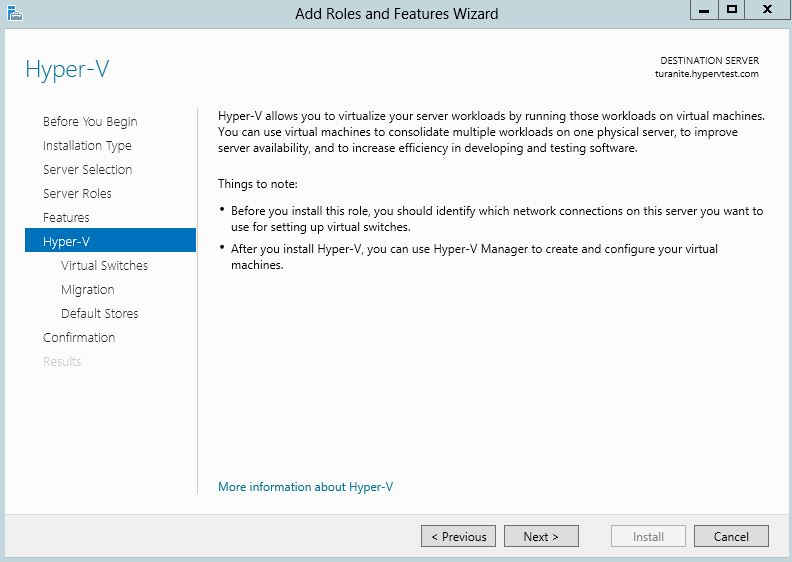


Figure 7: Information about Hyper-V

Step 9). In the **Virtual Switches** page of the **Add Roles and Features** wizard (Figure 8), create a virtual switch for your Hyper-V installation by clicking the checkbox that corresponds with the network adaptor you wish to emulate. When you have made your selection, click **Next** to continue.

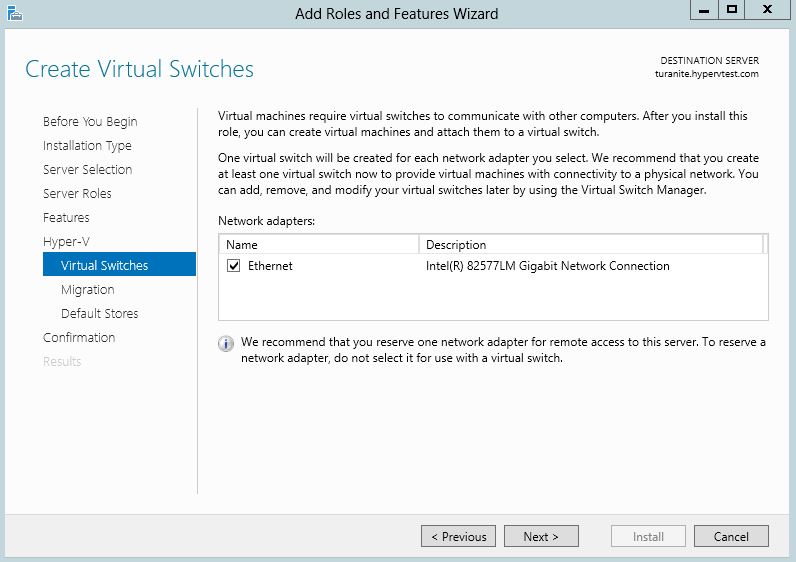


Figure 8: Virtual Switches

Step 10). On the **Migration** page of the **Add Roles and Features** Wizard (Figure 9), *do not* check the box enabling your Hyper-V installation to be able to send and receive live migrations of virtualized machines. Click **Next** to continue.

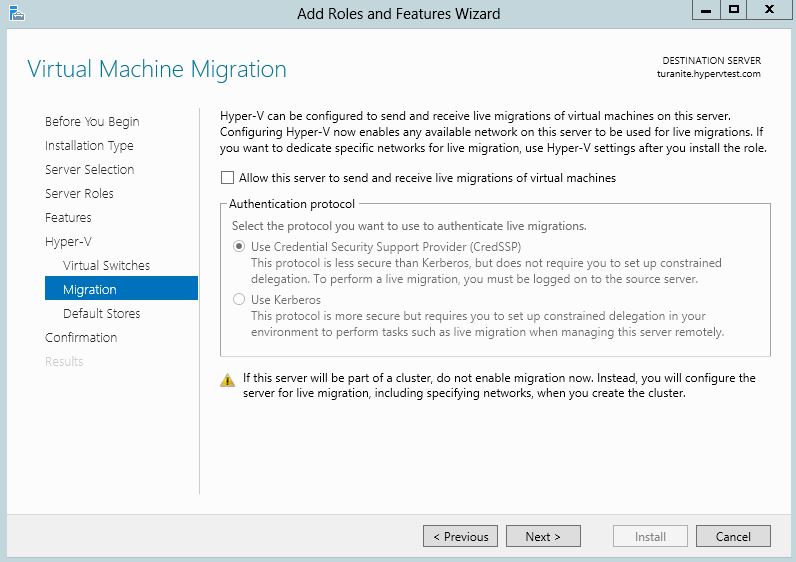


Figure 9: Virtual Machine Migration

Step 11). On the **Default Stores** page of the **Add Roles and Features** Wizard (Figure 10), click **Browse** to navigate to the location on which you wish to store virtualized hard disks and configuration files. Click **Next** to continue.

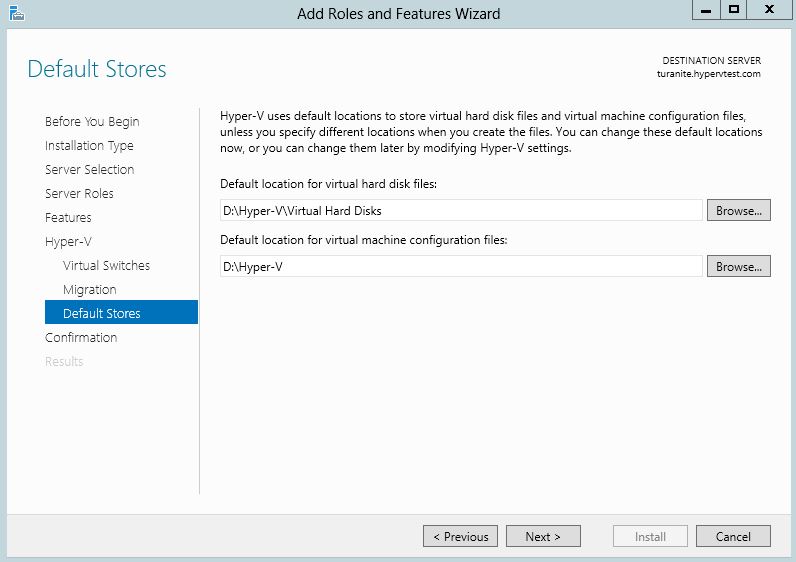


Figure 10: Default Stores

Step 12). On the **Confirmation** page of the **Add Roles and Features** wizard (Figure 11), review the roles, role services, and features you wish to install; when you are finished, click **Install** to begin the installation process.

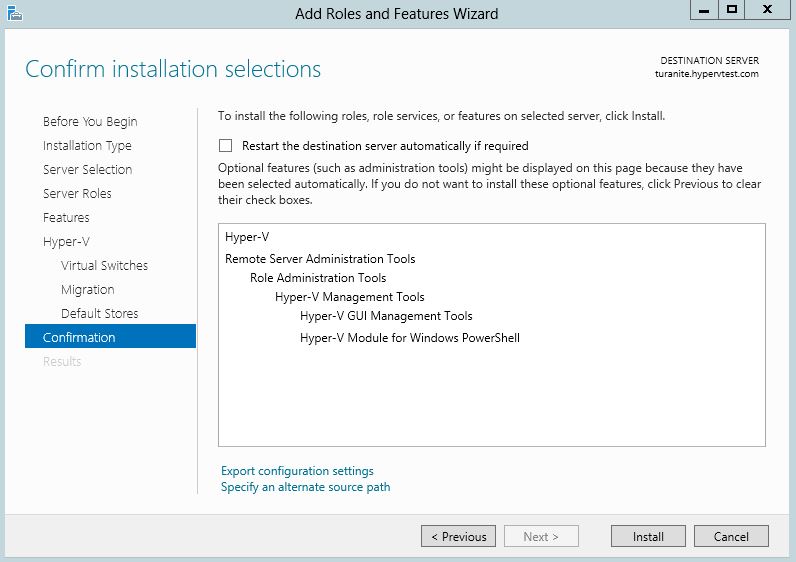


Figure 11: Confirmation

Step 13). After the installation is complete, restart the server on which the **Hyper-V** role has been installed.

Step 14). After the server has restarted, access the **Control Panel**. Open **Administrative Tools** and right-click **Hyper-V Manager**; in the context menu that appears, select **Send to Desktop** to create a desktop shortcut that will simplify access to the **Hyper-V Manager**.

Step 15). Provide each Windows Server 2012 instance with a Fully Qualified Domain Name (FQDN)

This step furnishes each Hyper-V host server with a domain name *without* joining a domain or registering a domain with a domain name server on the Internet.

1. Open the **hosts** file[[1]](#footnote-1) on each Hyper-V host server:
   1. Locate the **hosts** file
   2. Right-click the **hosts** file; in the context menu that appears, click **Open**
   3. In the **Open with** window that appears, select **Notepad** (or an equivalent text editor) and click **OK**
2. In each **hosts** file, map each IP address on the network to the appropriate domain name by appending entries[[2]](#footnote-2) to the **hosts** file. For example:

192.168.25.108 turanite.hypervtest.com   
192.168.25.100 scottyite.hypervtest.com

1. Append the primary and replica server IP addresses; map them to FQDNs of your choice
2. Save your edits
3. Remove any file extensions appended by the act of saving the **hosts** file[[3]](#footnote-3)

Step 16). Open the **Windows Server 2012 Server Manager** and select **Local Server** (Figure 12); click on the name of the server in the **Computer name** field to access the **System Properties** window (Figure 13).

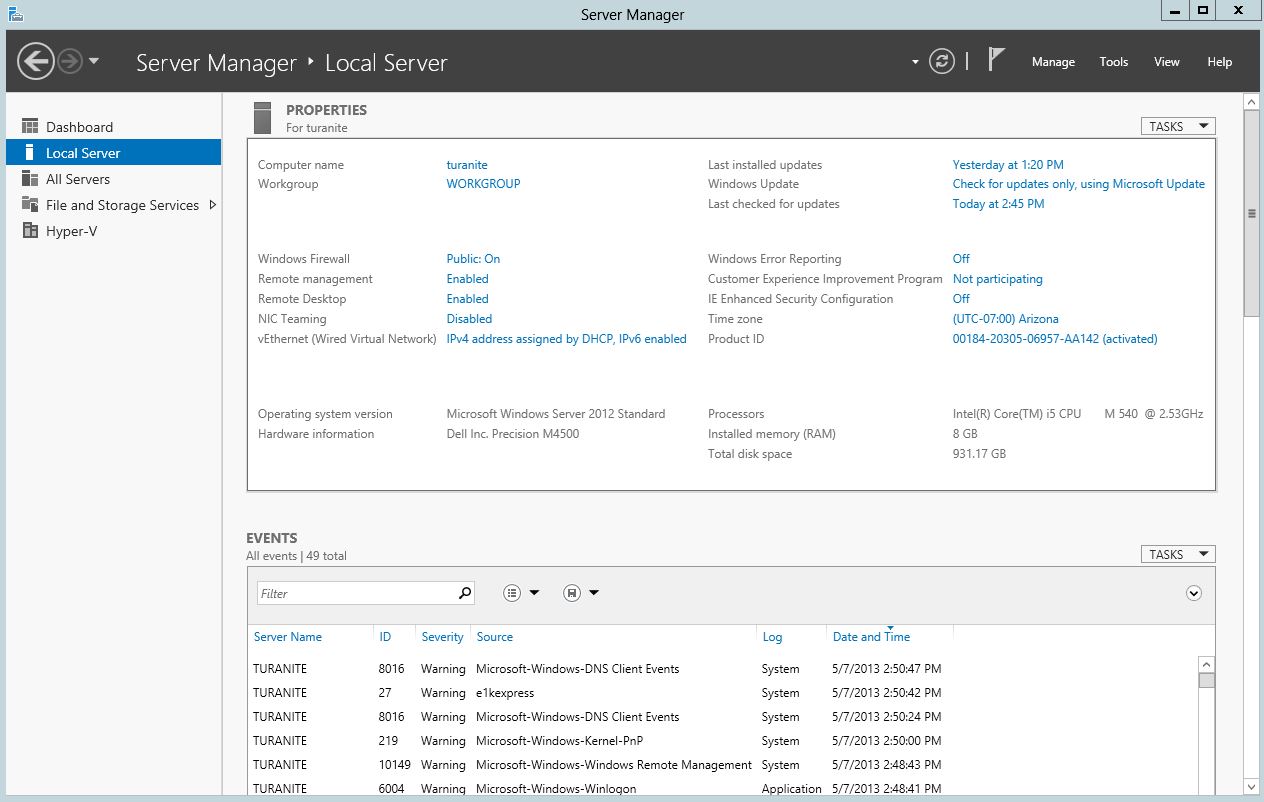


Figure 12: The Windows Server 2012 Server Manager

Step 17). In the **System Properties** Window (Figure 13), click **Change…** to bring up the **Computer Name/Domain Changes** window (Figure 14). Here, click **More…** to bring up the **DNS Suffix and NetBIOS Computer Name** window (Figure 15).

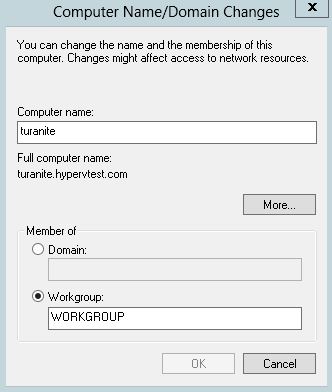


Figure 14: The Computer Name/ Domain Changes window

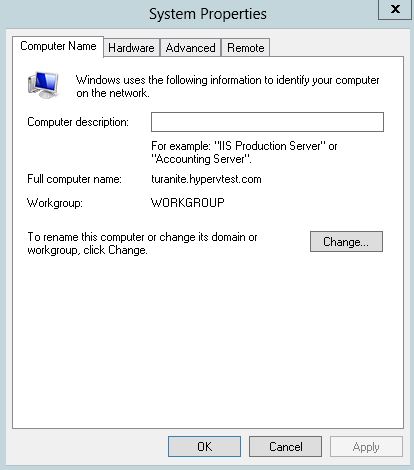


Figure 13: The System Properties window

Step 18). In the **DNS Suffix and NetBIOS Computer Name** window (Figure 15), enter the domain name you established in [Step 15](#step15) into the **Primary DNS suffix of this computer** field. Click **OK** on all three preceding windows (Figures 15-13).

Step 19). Restart the server. After the server is restarted, the server name will include the FQDN.

Step 20). Install the **Windows SDK for Windows 7** on each server

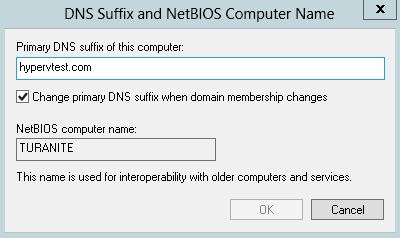


Figure 14: The DNS Suffix and NetBIOS Computer Name window

1. Download the **Windows SDK for Windows 7 ISO** (<http://www.microsoft.com/en-us/download/details.aspx?id=8442>)
2. Install **Windows SDK for Windows 7**

Step 21). Create a directory in which you will store certificate files; this directory will be used later in this tutorial

Step 22). Install SSL certificates for both the primary server and the replica server

1. Open a command prompt
2. On the taskbar, right-click the icon representing the command prompt you just opened; in the context menu that appears, right-click **Command Prompt**; click **Run as administrator**
3. In the elevated command prompt you just established, run a series of MS-DOS commands; make the substitutions listed below:
   1. Substitutions:
      1. Replace **primaryhostname** with the **FQDN** of the primary server created in [Step 15](#step15)
      2. Replace **replicahostname** with the **FQDN** of the replica server created in [Step 15](#step15)
   2. On the replica server, navigate to the directory you created in [Step 21](#step21) and run the following commands:

makecert -pe -n "CN=ReplicaTestRootCA" -ss root -sr LocalMachine -sky signature -r "ReplicaTestRootCA.cer"

makecert -pe -n "CN=**replicahostname**" -ss my -sr LocalMachine -sky exchange -eku 1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2 -in "ReplicaTestRootCA" -is root -ir LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider" -sy 12 PrimaryTestCert.cer

* 1. On the primary server, navigate to the directory you created in [Step 21](#step21) and run the following commands:

makecert -pe -n "CN=PrimaryTestRootCA" -ss root -sr LocalMachine -sky signature -r "PrimaryTestRootCA.cer"

makecert -pe -n "CN=**primaryhostname**" -ss my -sr LocalMachine -sky exchange -eku 1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2 -in "PrimaryTestRootCA" -is root -ir LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider" -sy 12 PrimaryTestCert.cer

1. On both the primary and replica servers, use the **Run** command to run **mmc** (the *Microsoft Management Console*); once in the console, click **File > Add/Remove Snap-in…**
   1. In the **Add or Remove Snap-ins** window, select **Certificates** from the **Available Snap-ins** list
   2. Click **Add >**; the **Certificates snap-in** window will appear
   3. In the **Certificates snap-in** window, click the **Computer account** radio button; click **Next** to continue
   4. In the **Select Computer** window, make sure the **Local computer** radio button is clicked; then click **Finish**
   5. In the **Add or Remove Snap-ins** window, click **OK**
2. In the Microsoft Management Console on the primary server, expose the contents of *Certificates (Local Computer),* which can be found under the **Console Root**directory
   1. Expose the contents of the **Personal** directory; click the **Certificates** directory
   2. Right-click *ReplicaTestRootCA.cer*; in the context menu that appears, mouse over **All Tasks >**; in the submenu that appears, click **Export…**
   3. In the **Certificate Export Wizard** that appears, click the **Yes, Export the private key** radio button and click **Next**
   4. On the next page of the **Certificate Export Wizard**, click **Finish**
3. Copy the **PrimaryTestRootCA.cer** file and the **RecoveryServer.pfx** file you just created from the primary server to the directory you created in [Step 21](#step21) on the replica server, and run the following command in an elevated command prompt on the replica server:

certutil -addstore -f Root "PrimaryTestRootCA.cer"

1. In the Microsoft Management Console on the replica server, expose the contents of *Certificates (Local Computer),* which can be found under the **Console Root** directory
   1. Expose the contents of the **Personal** directory
   2. Right-click on the **Certificates** directory; in the context menu that appears, mouse over **All Tasks >**; in the submenu that appears, click **Import**…
   3. Locate the **RecoveryServer.pfx** file
2. Copy the **ReplicaTestRootCA.cer** file from the replica server to the directory you created on the primary server in [Step 21](#step21), in an elevated command prompt, navigate to the directory you created on the primary server in [Step 21](#step21) and run the following command:

certutil -addstore -f Root "ReplicaTestRootCA.cer"

1. On both the primary and the replica servers, run an elevated command prompt, navigate to the directory you created in [Step 21](#step21), and run the following commands:

reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Virtualization\FailoverReplication" /v DisableCertRevocationCheck /d 1 /t REG\_DWORD /f

reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Virtualization\Replication" /v DisableCertRevocationCheck /d 1 /t REG\_DWORD /f

Step 22). Enable replication on the Primary and Replica servers

1. Open the Hyper-**V Manager** (Figure 16)

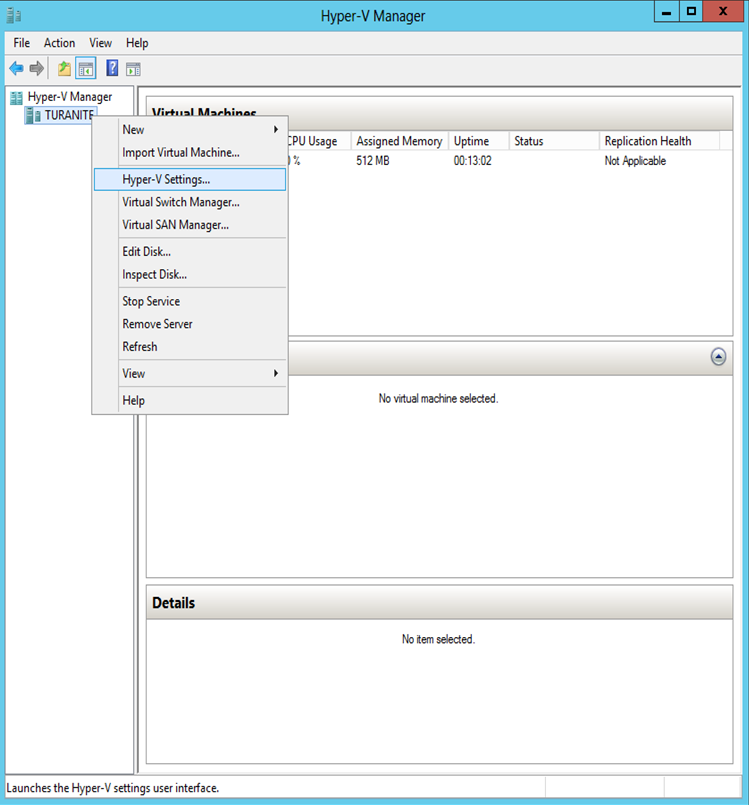


Figure 16: The Hyper-V Manager

1. In the **Hyper-V Manager** (Figure 16), right-click the primary server; in the context menu that appears, click **Hyper-V Settings…**
2. In the **Hyper-V Settings** window (Figure 17), click **Replication Configuration**
   1. Click the **Enable this computer as a Replica server** checkbox
   2. Click the **Use certificate-based Authentication (HTTPS)** checkbox
   3. Click the **Select Certificate…** button; specify the SSL certificate you installed in Step X.
   4. Click **Apply**; a dialogue box will appear prompting you to open **Port 443** in your local fire wall; *do so*
3. Repeat Steps 21-2 through 21-3 for each Hyper-V host server that you want to enable replication on

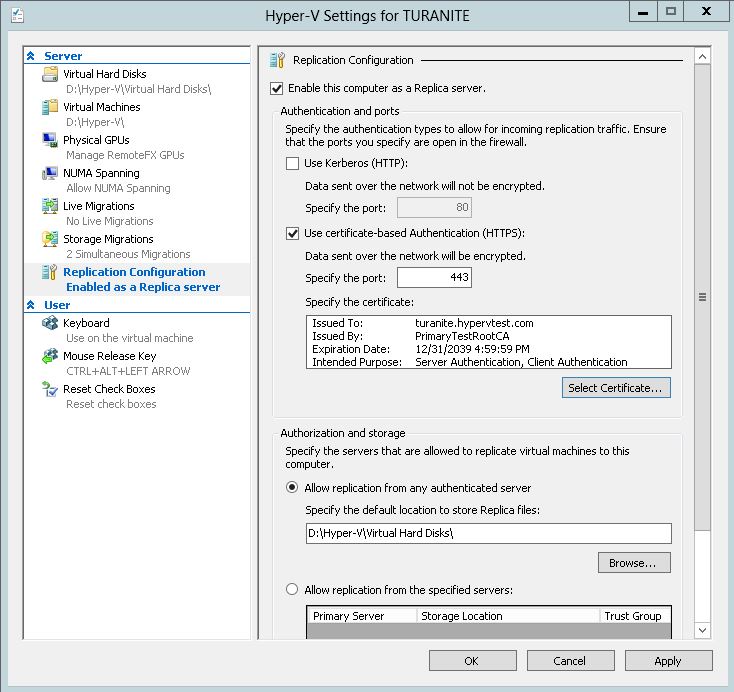


Figure 17: The Hyper-V Settings window

Step 23). Enable replication

1. In **Hyper-V Manager**, right-click the virtual machine that you wish to replicate; in the context menu that appears, click **Enable Replication**. This will bring up the **Enable Replication** Wizard.
2. Read the **Before You Begin** page of the **Enable Replication** wizard (Figure 18); when you are ready, click **Next** to continue

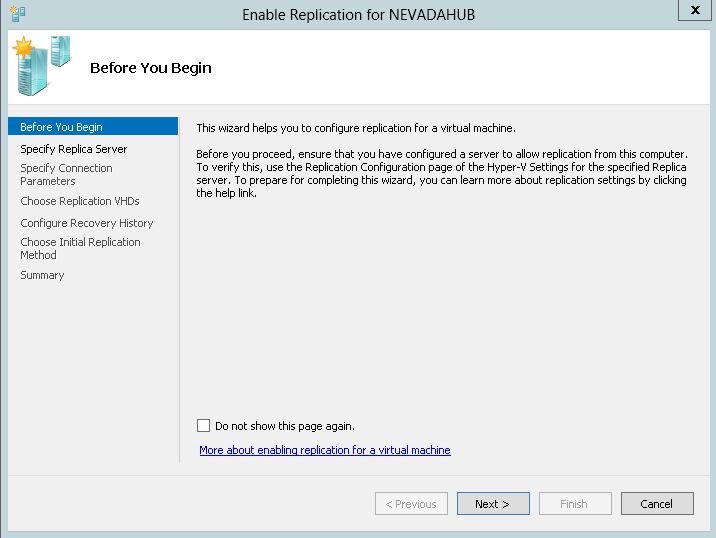


Figure 18: Before You Begin

1. On the **Specify Replica Server** page of the **Enable Replication** Wizard (Figure 19), enter the host name and FQDN of the replica server, as specified in [Step 15](#step15) and [Step 22](#step22); click **Next** to continue

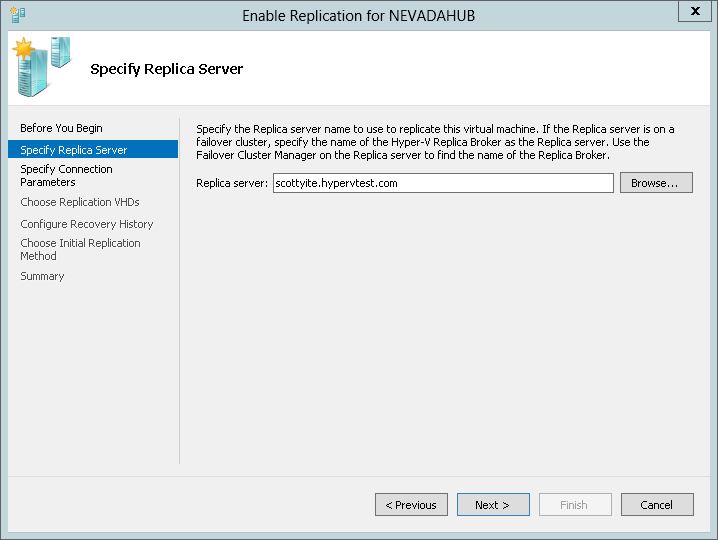


Figure 19: Specify Replica Server

1. On the **Specify Connection Parameters** page of the **Enable Replication** Wizard (Figure 20), click **Select Certificate…** to locate the SSL certificate you created in [Step 22](#step22); click **Next** to continue

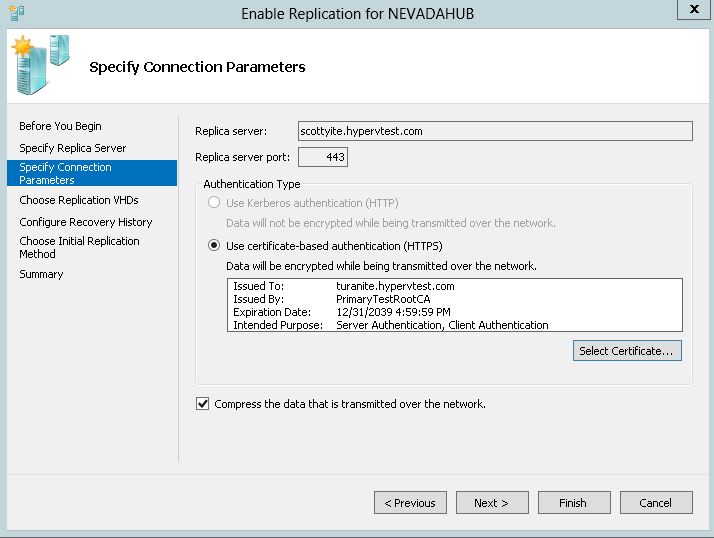


Figure 20: Specify Connection Parameters

1. On the **Choose Replication VHDs** page of the **Enable Replication** Wizard (Figure 21), click the checkboxes indicating the virtual hard disks (VHDs) you wish to replicate; typically, all VHDs are selected. Click **Next** to continue.



Figure 21: Choose Replication VHDs

1. On the **Configure Recovery History** page of the **Enable Replication** Wizard (Figure 22), specify the recovery points you wish to replicate. In this example, only the latest recovery point will be replicated, but it is possible to specify the replication of additional recovery points. Click **Next** to continue.

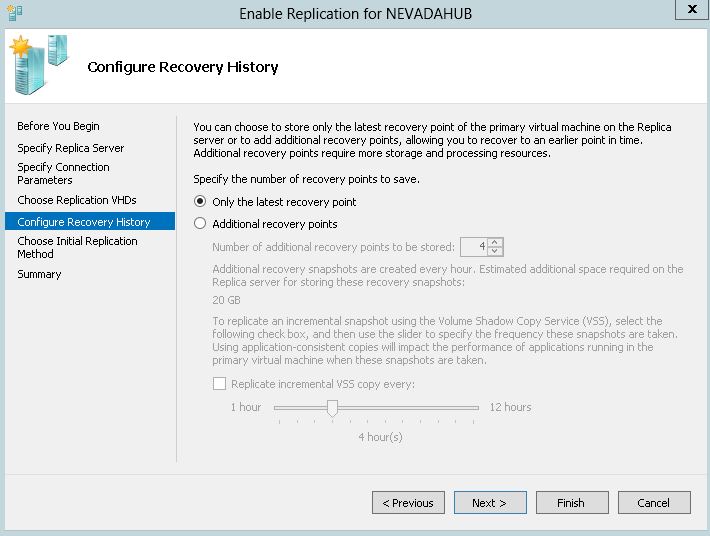


Figure 22: Configure Recovery History

1. On the **Choose Initial Replication Method** page of the **Enable Replication** Wizard (Figure 23), click the **Send initial copy over the network** radio button. If the virtual machine being replicated is very large, you might want to consider using external media to seed the initial copy.   
     
   In addition, specify the date and time at which the initial replication will occur. If you elect to start replication immediately, replication will begin as soon as this wizard is finished. Click **Next** to continue.



Figure 25: Choose Initial Replication Method

1. On the **Summary** page of the **Enable Replication** Wizard, review your settings and click **Finish**.

1. The **hosts** file is typically found at the following location:

   C:\Windows\System32\drivers\etc [↑](#footnote-ref-1)
2. Entries should not be commented out (there should be no # signs in front of them) and should use the following syntax:

   NNN.NNN.NNN.NNN hostname.domainname.com [↑](#footnote-ref-2)
3. Note: The act of editing the **hosts** file using a text editor can be problematic because saving your edits will prompt the text editor to assign a *file extension* to the **hosts** file; but the **hosts** file *should not have a file extension;* consequently, if you plan to edit the **hosts** file using a text editor, you will need to *remove* any file extensions assigned to the **hosts** file after editing it. To do so:

   In the Windows Explorer menu bar, click **Tools > Folder options…**

   In the **Folder Options** window, click the **View** tab

   In the **View** tab, *uncheck* the **Hide extensions for known file types** checkbox and click **OK**

   Rename the **hosts** file; delete the file extension (such as “.txt”)

   In the **Rename** dialogue box that appears, click **Yes** [↑](#footnote-ref-3)