**Configure Hyper-V Certificate-Based Authentication (HTTPS) Replica in a workgroup environment**

Doing this in a workgroup environment involves more work if you don’t want to buy the certificates from a commercial CA and go with a free solution. You don’t have an internal Enterprise CA anymore either; you could, but I presume your Hyper-V servers are in a workgroup environment because the business is not mature enough for a domain. Now we will have to create a root CA certificate and import it into the certificates store on every Hyper-V server, then issues the computer certificates and import those also. For this I will use a free tool called [Makecert.exe](http://go.microsoft.com/fwlink/p/?linkid=84091), which is a command line tool from Microsoft to issue certificates. After you install the tool you can find it in *C:\Program Files\ Microsoft SDKs\Windows\v7.1\Bin*. Open an elevated command prompt to this path and issue the following command to create our root authority certificate (replace the name of the certificate in the command line with your own):

makecert -pe -n "CN=vKernel Root Certification Authority" -ss root -sr LocalMachine -sky signature -r

"vKernel Root Certification Authority.cer"



The command also installs the certificate in the root store of the local machine and saves it  as a local file in the folder where Makecert.exe is located (*C:\Program Files\ Microsoft SDKs\Windows\v7.1\Bin*.)

[](http://www.vkernel.ro/blog/wp-content/uploads/2014/09/Configure-Hyper-V-HTTPS-Replica-58.gif) 

The next step is to create our certificates for our Hyper-V hosts. As before, the command also installs the certificate in the **Personal** store of the local machine and is saved locally as a file. The certificate can be used for both Client and Server authentication. Use the following command to create our first computer certificate:

Replace *vKernel Root Certification Authority* with the name of your root certificate and Server-HV1 with the name of your Hyper-V host. In case you added a name suffix to your infrastructure you will need to type the FQDN after the CN.

makecert -pe -n "CN=Server-HV1" -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 "vKernel Root Certification Authority"

-is root -ir LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider"

-sy 12 Server-HV1.cer



Run the following command a couple of times to issue certificates to all of your Hyper-V hosts.



By now all the hosts certificates should be installed in the **Personal** machine folder store on the Hyper-V host where you used the Makecert.exe command.



Also if you open a certificate it should have a private key, and the certificate chain should be OK.

[](http://www.vkernel.ro/blog/wp-content/uploads/2014/09/Configure-Hyper-V-HTTPS-Replica-63.gif) 

The next step is to export the certificate(s) from this certificate store and import them on the right hosts. Right click one of the certificates, choose **All Tasks > Export**. The **Certificate Export Wizard** should open, and once you get to the **Export Private Key** page select the first option, **Yes, export the private key** and click **Next**.



Here check the box **Export all extended properties** and continue the wizard.



Type the password for the certificate then on the **File to Export** page provide the path where to save the certificate. Finish the wizard.

[](http://www.vkernel.ro/blog/wp-content/uploads/2014/09/Configure-Hyper-V-HTTPS-Replica-67.gif) 

Repeat this step for the rest of the certificates. When done with the computer certificates go to the **Trusted Root Certification Authorities** store, find your root certificate and export this to, following the above procedure.



Now that we have all the certificates exported we need to put them on the right host(s) in the right place. Let’s start with the root certificate. Copy this one on every Hyper-V host then open it. The **Certificate Import Wizard** will pop-up. On the **Welcome** page of the wizard select **Local Machine** and click **Next**.



Continue the wizard by providing the necessary information.

[](http://www.vkernel.ro/blog/wp-content/uploads/2014/09/Configure-Hyper-V-HTTPS-Replica-71.gif) 

When you get to the **Certificate Store** page choose the second option **Place all certificates in the following store** then hit the **Browse** button.



Select **Trusted Root Certification Authorities** and click **OK** then **Next** to import the certificate.



Repeat this on every one of your Hyper-V servers. Once you’re done, move on by importing the computer certificates on their specific hosts. Let’s say you have a certificate with a **Common Name** field of Server-HV2; you will have to import this certificate on the Hyper-V server with the same name (Server-HV2). Follow the above procedure to import the certificate, but once you get to the **Select Certificate Store** window, make sure you select the **Personal** folder this time.



Now if you look in the certificates store on one of your Hyper-V hosts you should see the root certificate and the computer certificate imported.

    

Also, the certificate has its private key and the chain looks good with no problem whatsoever.



You might think that we are done, but there is still one thing left to do before we start configuring the Replica server, and that’s the CRL (Certificate Revocation List) checking. You know that every browser when you go on a secure site checks if the certificate is revoked or not by downloading the CRL. Hyper-V does that too, but since we used a not so advanced tool to create our certification authority, our certificates don’t have the CRL field; and by Hyper-V not being able to check for the certificate CRL will trow an error when you try to enable it as an HTTPS Replica server:

*Failed to modify service settings. Failed to validate certificate in Personal certificate store of local computer. Failed to modify service settings. Could not validate certificate with thumbprint ‘…’ in the Personal certificate store of local computer. Error: The revocation function was unable to check revocation for the certificate. (0x80092012).*



To pass this, you either use commercial CA certificates or implement an [Enterprise Internal CA](http://www.vkernel.ro/blog/installing-an-enterprise-certificate-authority-in-windows-server-2012) with an [OCSP Responder](http://www.vkernel.ro/blog/installing-and-configuring-a-microsoft-online-certificate-status-protocol-ocsp-responder). Those two are valid, but remember, you are in a workgroup environment and a small business, and you can’t afford a domain, there is to much licensing cost involved. The third option is to edit the registry. Run the bellow command to disable the CRL checking on your Hyper-V servers:

reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Virtualization\Replication" /v

DisableCertRevocationCheck /d 1 /t REG\_DWORD /f



Now we can go ahead and configure a Replica server. From the **Hyper-V Manager** console, right-click the server and choose **Hyper-V Settings**.



On the **Replication Configuration** setting check the box **Enable this computer as a Replica server** then enable the HTTPS authentication from the **Use certificate-base Authentication (HTTPS)** box. Hit the **Select Certificate** button and select your certificate. On the **Authorization and storage** section choose where to put the VMs that are replicating and from which hosts to accept replication. Click **OK** when done but don’t forget to open port 443 in the host firewall so it can accept replication traffic.

    

Now from the Hyper-V server where you have your VMs running, right click the one(s) you want to replicate and choose **Enable Replication**.



On the wizard that just opened, on the **Specify Replica Server** page, type the server name you configured as a Replica Server.



Here by clicking the **Select Certificate** button you will be give a list with all the compatible certificates for Hyper-V replication. In our case we have just one. Select the certificate and click **OK**.

    

Choose which drives you want to replicate for this VM. As a best practice is better to put the guest *pagefile* on a separate virtual disk and exclude it from replication to save bandwidth, time and storage.



Select the replication interval then how many recovery points you want to have for the VM. 30 seconds is only if you have enough bandwidth to support the replication traffic, if not you should select another one.

    

If you don’t want to start the replication right away, you can schedule it for later from the **Schedule Initial Replication** section. Also you have the option to send the initial replica using an external media. In this example however I will use the default settings.



Click **Finish** to start the replication process.



Depending on the size of the VM and how fast your internet connection is (if you are doing replication over WAN) it will take a while, but at the end you should have your VM(s) replicated and in good shape. Now if there is a problem on the VM from the first site, you can just go ahead and failover to the other VM from the second site (replica VM) so users can still do what they were doing.

    

We’ve come a long way, but at the end everything is working as it should. Now you can have encryption between your Hyper-V servers during replication; and I know it’s a little bit of work on some cases, but you have to choose between costs and difficulty.