In this article we will look at how to configure Hyper-V HTTPS Replica [in a domain environment](http://www.vkernel.ro/blog/configuring-hyper-v-replica-using-certificate-based-authentication-https#anchor009), [in a clustered environment](http://www.vkernel.ro/blog/configuring-hyper-v-replica-using-certificate-based-authentication-https#anchor010) and [in a workgroup environment](http://www.vkernel.ro/blog/configuring-hyper-v-replica-using-certificate-based-authentication-https#anchor011). They are all different in some way especially from a certificate perspective, and the requirements for the certificate that is being requested are as follows:

**Enhanced Key Usage** – This field in the certificate must be set up for both Client and Server authentication.

**Certificate Subject Field** –  The certificate is bound to the name of the machine.This field must be set to the FQDN of the host, or the NetBios name if the host is not part of a domain. If the server is part of a cluster, the subject field must be set to the FQDN of the Hyper-V Replica Broker (HVR Broker), and this certificate must be installed on all the nodes in the cluster.

The certificate must be a valid X.509v3 certificate that is not revoked and trusted on the machines. The root certificate must be present in the Trusted Root Certification Authorities.

With this in mind let’s start with the simplest deployment,

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

For this I presume you already have an [Active Directory Certificates Service](http://www.vkernel.ro/blog/installing-an-enterprise-certificate-authority-in-windows-server-2012) running and functional. We are going to use this internal CA to issue the certificates needed for HTTPS replication. Now log in to one of your Hyper-V hosts, go to **Run**, type **mmc.exe** and hit **Enter**. From the **File** menu choose **Add/Remove Snap-in**.



In the **Add/Remove Snap-ins** window select the **Certificates** object and hit **Add**, then on the wizard choose **Computer account** > **Local Computer**.

    

Here, expand **Certificates (Local computer)**, right-click the **Personal** folder and choose **All Tasks > Request New Certificate**.



On the **Certificate Enrollment** wizard select **Active Directory Enrollment Policy** (it should be selected by default) and click **Next**.



You get to the **Request Certificates** page. All you have to do here is check the box next to **Computer** and hit the **Enroll** button.

    

At the end you should get a certificate with a private key and a common name that corresponds to the server name.



Repeat this for all your Hyper-V hosts. And since you have an Active Directory environment why not use the Auto-Enrollment policy. All you have to do is create a GPO and link it to the appropriate OU (where your Hyper-V hosts are located). On how to configure Auto-Enroll using group policy [read this article](http://www.vkernel.ro/blog/set-up-automatic-certificate-enrollment-autoenroll).

The next step is to open the **Hyper-V Manager** and configure the hypervisor as a HTTPS replica server. Right-click the server you want to be a replica server and choose **Hyper-V Settings**; or you can use the **Actions** pane.



Once the **Hyper-V Settings** window opens, go to the **Replication Configuration** section and check the box **Enable this computer as a Replica server**. Now since we want to secure the replication traffic, we need to enable the **Use certificate-based authentication (HTTPS)** box. After this, click the **Select Certificate** button. As soon as you click it, another window with the available and compatible certificates is presented. In our case we have just one certificate. Select it then click **OK**.



If for some reason there is no certificate available, the certificate is incompatible or the certificate chain in not complete, you will get the bellow error message window:

No valid certificate found. A valid certificate for replication should have the following properties: “…”. Install a valid certificate and try again.



On the **Authorization and storage** section choose where you want to store the VMs that are replicating to this host and from where it should accept the connections. Click **OK** when done. You immediate get the following message:

Ensure the inbound TCP exception for port ‘443’ is enabled in the firewall. If you are using Windows Firewall , enable “Hyper-V Replica HTTPS Listener (TCP-In)” rule.



What actually is saying is that port 443 has to be opened on this server in order for the replication to work. If you don’t use Windows Firewall as a security measure you will need to configure this port on the product you are using. If that’s not the case, just open **Windows Firewall with Advance Security**, click **Inbound Rules** then right-click and enable **Hyper-V Replica HTTPS Listener (TCP-In)**.



Now let’s enable replication for a VM. When you do this for the first time, you will have to select a certificate during the wizard. This is done by clicking the **Select Certificate** button. After this continue the wizard and choose the options that best suit your needs. For more information about enabling replication on a VM [read this guide](http://www.vkernel.ro/blog/configuring-hyper-v-replica-in-windows-server-2012r2#anchor008).

    

Once you click **Finish** the VM starts replicating to the specified replica server.

    

And looks like is working like a charm, and without loosing any more time I will jump to the next HTTPS Replica example, and that’s