vSphere 5.5 Install Pt. 6: Certificate Template

derekseaman.com/2013/10/vsphere-5-5-install-pt-6-minting-ssl-certs.html

Derek Seaman October 7, 2013

Now that you understand what type of SSL certificates you need and how many vCenter 5.5 requires, we need to create a Certificate Authority template that will mint proper certificates. You may very well be able to get away with the Microsoft “Web server” template, but it is missing a few properties that VMware still lists as a requirement. So to ensure you don’t run into any problems, this installment shows you how to setup those properties.

I’m assuming you are using a Microsoft CA for this exercise. Technically you can use any CA, so don’t think that you are just limited to Microsoft’s implementation. Certificates are standardized in the X.509 format. In a real enterprise environment CAs should be heavily locked down and you probably won’t have permissions to change anything on the CA. Find your CA administrator and have them complete this section. If you aren’t using a Microsoft CA, then the steps below won’t exactly apply to you. But research how to configure your CA for the “required” properties.

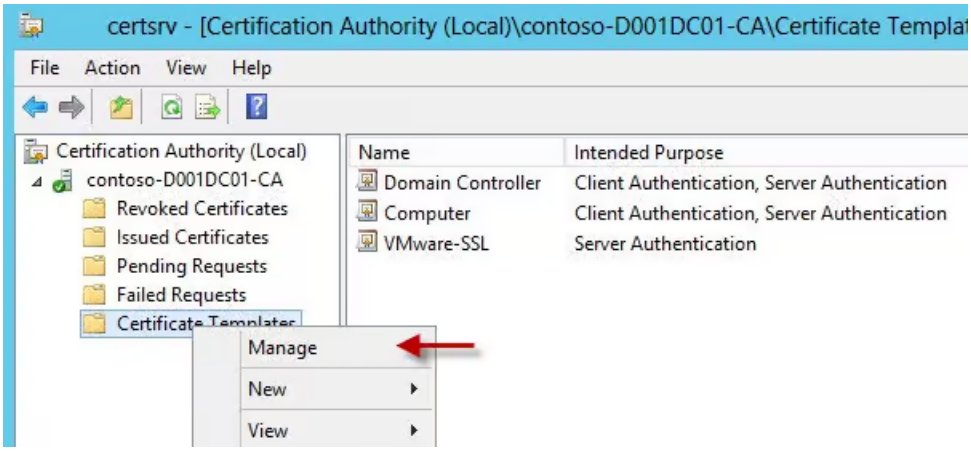
Blog Series

[vSphere 5.5 Install Pt. 17: Install VUM]
[vSphere 5.5 Install Pt. 18: VUM SSL]
[vSphere 5.5 Install Pt. 19: ESXi SSL Certificate]

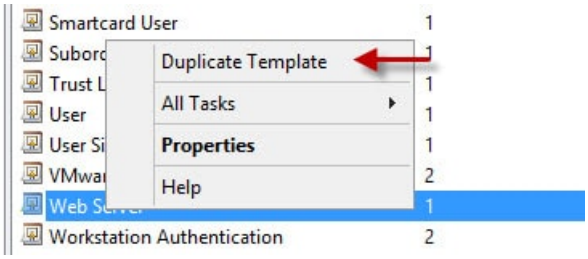
Permalink to this series: [vexpert.me/Derek55]
Permalink to the Toolkit script: [vexpert.me/toolkit55]

Certificate Template

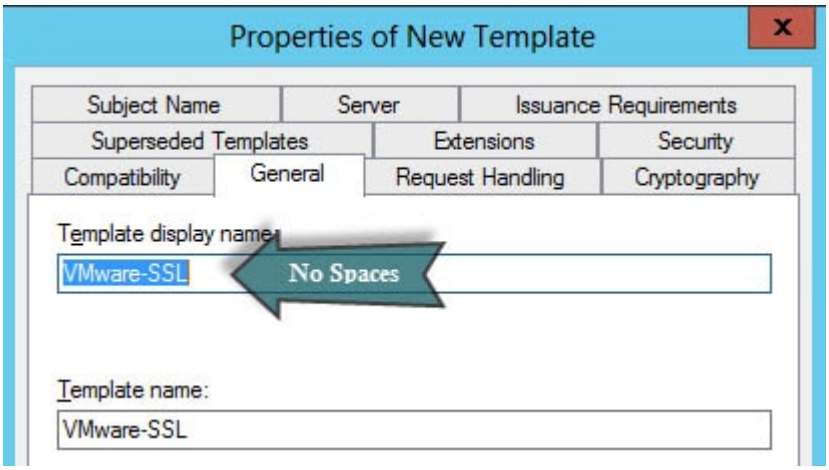
1. Logon to your Microsoft root CA. In this case I'm using Windows Server 2012. Launch the **Certification Authority** console. I've already created a custom template, VMware-SSL. But ignore that for now (just like a cooking show I have my template already done in the oven) and locate the Certificate Template container. Right click and select **Manage**.



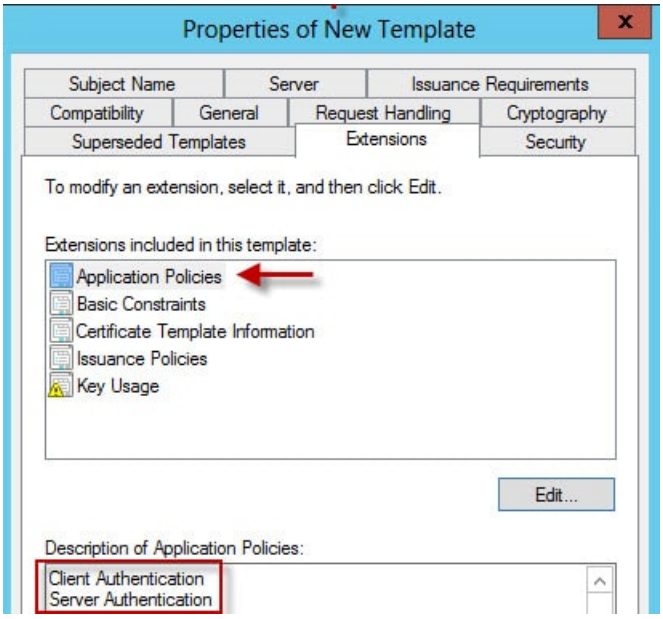
2. Locate the **Web Server** template, right click and duplicate it.



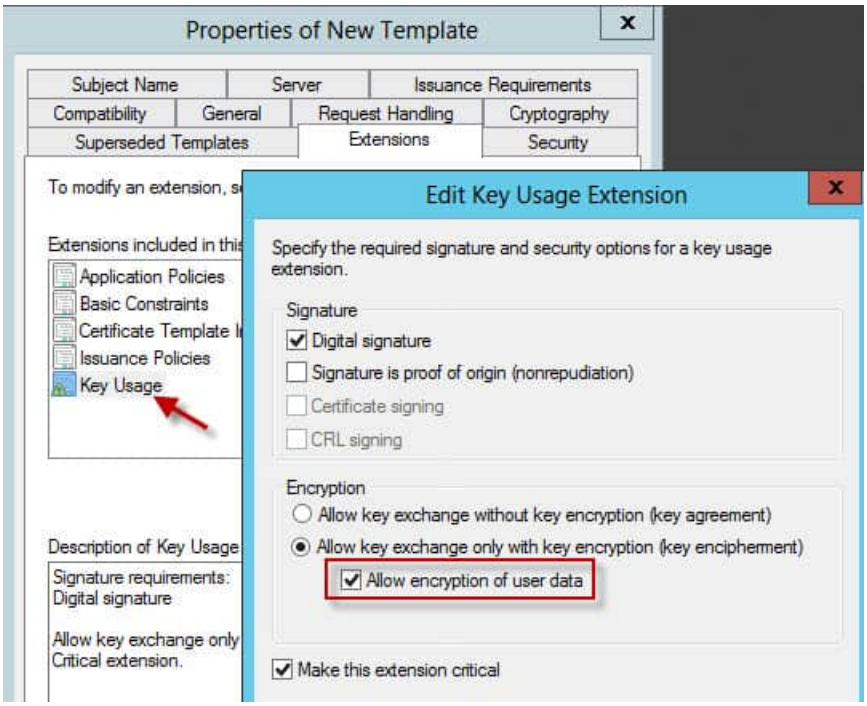
3. Don't change anything on the compatibility tab. Don't think you are clever and try changing the default value to something like Windows Server 2012. #Fail. On the General tab rename the template. I like using **VMware-SSL** because it has no spaces, so the template name and display name are the same. This avoids confusion down the road where a script requires the template name as a parameter. Spaces are allowed, but let's not confuse the situation anymore than needed…we are already confused enough.



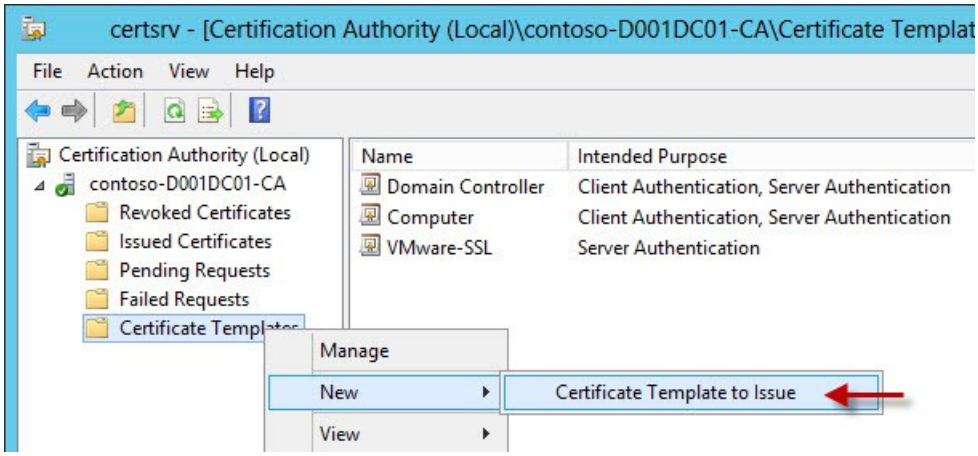
4. Click on the **Extensions** tab then highlight **Application Policies**. Click **Edit** and add **Client Authentication**.



5. Click on **Key Usage** and check the box to **allow encryption of user data**. Close out of all the certificate properties windows.



6. Back in the CA window issue the new **VMware-SSL** template, by selecting the menu item shown below. A list of available templates will appear, and just click on **VMware-SSL**. It should now appear in the right pane, as you can see below. Sometimes CAs can be slow, and it could take a couple of minutes to appear. Do not panic; be patient. Once it appears you now have a good template to use for VMware certificates (vCenter, ESXi hosts, etc.).



Summary

Creating a certificate template is not tricky and only takes a couple of minutes. It may take a few minutes for the new certificate type to replicate in AD. So don't be too surprised if you can't immediately see it. The steps are pretty much the same on Windows Server 2008 and later, so don't worry if you aren't yet using Windows Server 2012.

In Part 7 we (finally) get to mount the vCenter 5.5 ISO and install the SSO service. So yes, this install series is finally getting to the point were we can install something. But hopefully you are better educated about vCenter 5.5 than you were before you stumbled

on this series. Impress your friends at your next cocktail party about SSL OU values and PEM files.