Adrian Costea's blog

- Home
- Contact

Search | Search |

- Microsoft
  - Active Directory
  - Exchange Server
    - Exchange Server 2010
    - Exchange Server 2013
  - Hyper-V
  - ISA/TMG
  - Microsoft RDS/VDI
  - PowerShell
  - SQL Server
    - SQL Server 2008/2008 R2
    - SQL Server 2012
  - System Center
    - Data Protection Manager (DPM)
      - DPM 2010
      - DPM 2012
    - Virtual Machine Manager (VMM)
      - VMM 2008
      - VMM 2012
  - WDS/MDT
  - Windows Clients
  - Windows Server
    - Windows Server 2008/2008 R2
    - Windows Server 2012
  - WSUS
- Virtualization
- VMware
  - PowerCLI
  - VMware ESX/ESXi
  - VMware vCenter
 - VMware ThinApp
  - VMware Workstation
  - VMware vSphere Replication

« Read Previous Post

Read Next Post »

Dec 27 2011

# Install Certification Authority in Windows Server 2008 R2

Yes, you can have your own Certification Authority (CA), and issue certificates for clients. The bad news is that certificates issued by your internal CA are trusted only by you internal clients, or by clients that have your root certificate imported. For internal applications, sites etc this is gold, because you don't have to by a commercial certificate, but if you have a public HTTPS site you will need a commercial certificate. Certification authorities can have multiple ramifications or levels, like Root CA, then a Subordinate CA, and the last one is the Issuing CA.Bellow I created a diagram for a better visualization.
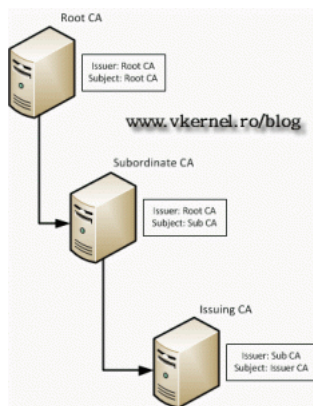
Root CA will issue certificates only for Subordinate CA, and the Subordinate CA will issue certificates only for Issuing CA. The Issuing CA is the one that will issue certificates for internal clients. You can, off course create more than three ramifications, but even those commercials Certification Authorities are not going with more than three. Now there are multiple types of Certification Authorities for Windows Domains. The first and the bigger one is Enterprise Root CA, then is Enterprise Subordinate CA. These two types are used only if you have a Windows Domain implemented in your network. The last two are Enterprise Standalone CA, and Subordinate Standalone CA. These are used if you don't have a Windows Domain implemented. Now the difference between Enterprise and Standalone is that with Enterprise you have certificate templates, and the root certificate will automatically be deployed to all clients. I will end this introduction now, and start working.

For this guide I have a Domain Controller (DC) running Windows Server 2008 R2, and another Windows Server 2008 R2 (named Server-Cert) joined to the domain, which will be our Enterprise Root CA. Yes I'm going with the Enterprise version, because is a Windows Domain, and for small business is more than sufficient a single Enterprise Root CA.

Go to *Server-Cert* and open **Server Manager**; right-click **Roles** and choose **Add Roles**.
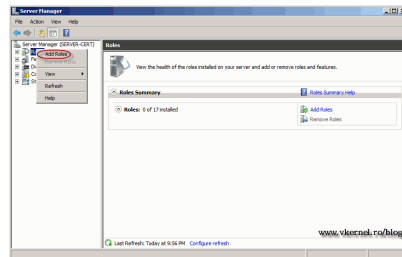

Click **Next** to skip the Welcome screen. On the Roles screen select the **Active Directory Certificate Services** and click **Next**.
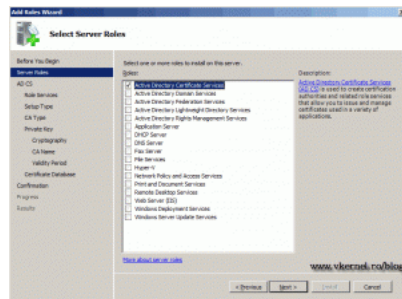

Skip the introduction of AD CS. On the **Role Services** screen we have the option to install more than just the certificate service. For this demonstration I'm going to install the **Certification Authority Web Enrollment** too. This will give us a web page to request certificates, and it's great, believe me. As soon as you click the **Certification Authority Web Enrollment** you will be asked to install some required prerequisites. And off course a web site to function needs a web server. Just click **Add Required Roles Services** and continue the wizard.
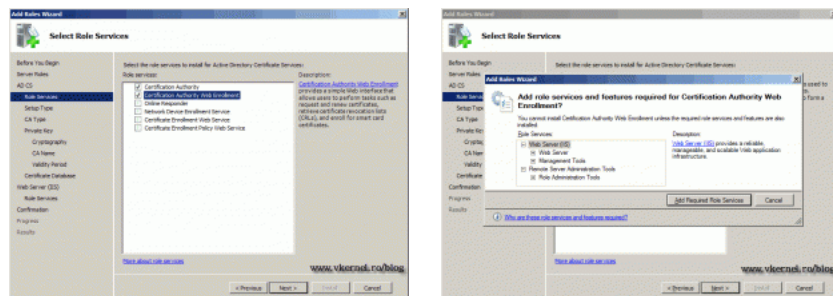
Because this is about installing Enterprise Root CA, just leave the defaults here and click **Next**.
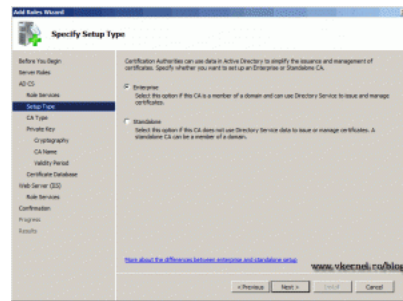
Again leave the defaults here to install a Root CA.
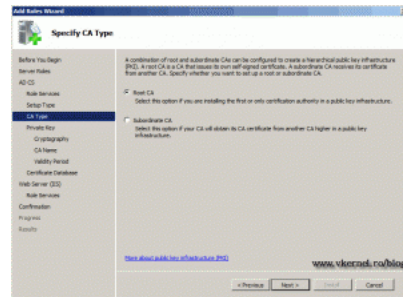
We need to create a new private key, so click **Next** to continue.
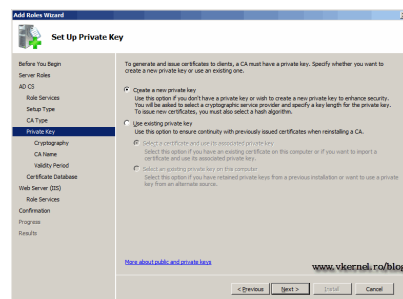
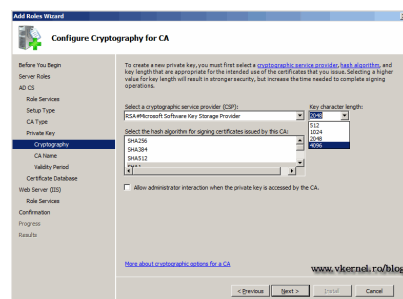For Enterprise Root CA I usually choose a length key of 4096 and leave the rest to default.
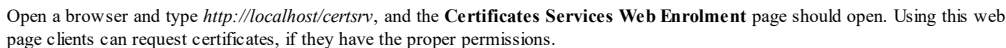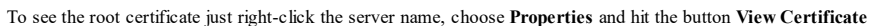

Give your Root CA a name. I always change the name, because I really hate the default one.
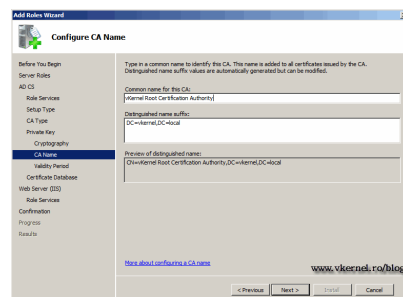
Select a validity period. For Enterprise Root CA I usually type 30 years.

If you have a reason to change the default log and database location, do it using the **Browse** buttons. Now comes the IIS installation part, just go with the defaults and finish the wizard.

The installation is done. Go to **Administrative Tools > Certification Authority** to open the Management Console for the Certificate Services. From this console you can revoke certificates and create templates.

To see the root certificate just right-click the server name, choose **Properties** and hit the button **View Certificate**

Open a browser and type *http://localhost/certsrv*, and the **Certificates Services Web Enrolment** page should open. Using this web page clients can request certificates, if they have the proper permissions.

Want content like this delivered right to your

email inbox?

More similar articles

Set Up Automatic Certificate Enrollment (Autoenroll)

How to reset forgotten Active Directory Domain Administrator password

Configuring Hyper-V Replica using Certificate-Based Authentication (HTTPS)

Backing up Domain Controllers using Windows Server Backup and DPM

Creating Active Directory Forest Trusts

Changing the Directory Services Restore Mode (DSRM) Admin Password

Tags: Active Directory, Windows Domains

6 comments

Skip to comment form ↓

1.

alex

11/08/2014 at 10:30 (UTC 2)

Reply

I have follow the step and done all the setting but when i go to Certificates Services Web Enrolment and try to create a subordinate Certification Authority" template , i dont see any options thr ,its only show Basic EFS and Users, please advice.

1.

Adrian Costea

12/08/2014 at 09:40 (UTC 2)

Reply

Hi,
It's because you are logged in with a simple domain user. You need to be logged in with a domain admin account, then your Subordinate Certification Authority will be appear in the list.

2.

Richard Buss

01/08/2014 at 23:17 (UTC 2)

Reply

Actually the server must be running AD AS services so it needs to be a DC or Exchange box in order to select the Enterprise option.

1.

Adrian Costea

03/08/2014 at 16:00 (UTC 2)

Reply

@Richard
Wrong. To install an Enterprise CA all you need is an AD environment cerid the server that is going to server as a certification authority needs to be part of that domain. It's not a must that you need to install certification services on a domain controller; you can, but it's not a must. And one other thing, it does not need to be an Exchange server. You can run certificate services without an Exchange server in your environment.
@mahin
In your case there is some problem with your AD environment, or some restrictions apply.

3. ![icon]

mahin

20/04/2013 at 11:03 (UTC 2)

Reply

hello
i follow the above senario
i have a problem with it !
when i wanna install active directory certificate servise in windows server 2008 r2 i'm not able to select enterprise because it
is disable !!! what can i do?
this server is joined to a domain.

1. ![avatar]

Adrian Costea

21/04/2013 at 13:22 (UTC 2)

Reply

Maybe you have a broken AD environment or a Certification Authority already exist. I will check the second one first
then do an AD investigation.

Leave a Reply

Your email address will not be published. Required fields are marked *

Message: *

Name: *

Email: *

Website:

![CAPTCHA image: GU2D]

CAPTCHA Code *

Submit Comment

Subscribe via Email

Your email address

Subscribe

▷ ✕

Popular Posts

- [Creating an Offline MDT Deployment Media](#)
- [Configure WSUS to deploy updates using Group Policy](#)
- [How to remove RDS CALs from a RD License Server](#)
- [Set Up Automatic Certificate Enrollment (Autoenroll)](#)
- [Configure Internal Windows CA to issue SAN certificates](#)
- [Creating and Using VMware Guest Customization Specification](#)
- [Sysprep and Capture a Windows Image with MDT 2012](#)
- [Building an Active Directory (AD) Test Lab using…](#)
- [Configuring and managing WSUS Downstream Replica Servers](#)
- [Creating/Configuring iSCSI in VMware vSphere/ESXi 5](#)

Recent Comments

- virtualization on [Add users in VMware vCenter](#)
- [Adrian Costea](#) on [How to remove RDS CALs from a RD License Server](#)
- [Adrian Costea](#) on [Creating an Offline MDT Deployment Media](#)
- [Adrian Costea](#) on [Creating RDS Session Collections in Windows Server 2012/R2](#)
- Brad Wilson on [How to remove RDS CALs from a RD License Server](#)

Copyright

© 2011-2018 Adrian Costea's blog.

- Terms and Conditions
- Privacy Policy
- Return to top

Powered by WordPress and the Graphene Theme.