Microsoft ADCS - How to Redirect the HTTP URLs for CDP and AIA from old CA to new CA

http://sysadmin-e.com/microsoft-adcs-cdp-aia/ March 1, 2013

I didn't find this documented clearly anywhere, so I figured it out on my own. Testing in the lab showed that this works correctly. I used the certutil command below to test.

certutil -URL http://corp-ca-01.mycorp.ad/CertEnroll/MyCorp-CA.crl

IIS does the redirection on the backend so clients don't know that they're being redirected since they only see the old CA name in the URL.

IIS 6.0 Redirection

Certs that were issued prior to the migration will all reference the old server URL (*http://corp-ca-01.mycorp.ad* /*CertEnroll*...) so we need to redirect that to the new server (*http://corp-ca-02.mycorp.ad* /*CertEnroll*...). Since the old server will still be up and running we need to do the following from it:



^ Under the Default Web Site, create new virtual directory named CertEnroll.

Virtual Directory Creation Wizard	×
Virtual Directory Alias Specify a short name, or alias, for this virtual	directory.
Type the alias you want to use to gain acces same naming conventions that you would for Alias: CertEnroll	ss to this Web virtual directory. Use the naming a directory.

Virtual Directory Creation Wizard	×
Web Site Content Directory Where is the content you want to publish on the Web site?	
Enter the path to the directory that contains the content for this Web site	
Path:	
C:\WINDOWS\system32\certsrv	Browse

^ There's nothing in this path, but we just need to select something so use this.

Virtual Directory Creation Wizard	×
Virtual Directory Access Permissions Set the access permissions for this virtual directory.	Cando de la como
Allow the following permissions:	
✓ Read ■ Run scripts (such as ASP)	
Execute (such as ISAPI applications or CGI)	
☐ <u>W</u> rite	
Browse	

CertEnroll Properties		<u>? ×</u>		
	·	1		
HTTP Headers	Custom Errors	ASP.NET		
Virtual Directory	Documents	Directory Security		
The content for this resource should come from:				
C A directory located on this computer				
C A share located on another computer				
A redirection to a URL				
Redirect to: /uditional moore tenrol				
The client will be sent to:				
The exact URL entered above				
A directory below URL entered				
A permanent redirection for this resource				

^ The redirection URL is http://corp-ca-02.mycorp.ad/CertEnroll (the new CA)

Copy CRT File for AIA

This needs to be done because the new server names its AIA root certificate file after itself. We just need to make a copy of that file and add the old server name to the file name.

- 1. On the new CA, corp-ca-02.mycorp.ad, go to C:\WINDOWS\system32\certsrv\CertEnroll\.
- 2. Copy the file named *corp-ca-0<u>2</u>.mycorp.ad_MyCorp-CA.crt* and name it *corp-ca-0<u>1</u>.mycorp.ad_MyCorp-CA.crt*.

-End of Document-