

RE: renewing web certificates

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.general/2006-12/msg00026.html>

- *From:* briandel@xxxxxxxxxxxxxxxxxxxxxxxx (Brian Delaney [MSFT])
 - *Date:* Tue, 28 Nov 2006 22:52:51 GMT
-

Hi Paul,

Only a single CDP and AIA path are required in issued certificates (Exception: no paths are required in the Root CAs certificate). However, if you are going to publish this information to one path only you must consider the availability of that choice. For example if you publish to a single webserver and that webserver goes down, all certs issued by that CA are going to be invalid until the CDP path comes back up. So if you are publishing to a web server, there should be at least two web servers on the backend (Cluster or Round Robin).

Another consideration would be the users that are frequently using certificates from your CA. Are they all internal clients? In this case the default ldap path is already fault tolerant and fast as it is serviced by all DCs but not available externally.

As you mention, yes a standalone CA is outside of AD, but that does not stop you from manually publishing it's CRLs to AD for high availability using certutil -dspublish

As for the issues, try using pkiview.msc from the Windows Server 2003 Resource Kit, that will download all the CRLs in the chain and alert you of most problems.

Hope this helps,

Brian Delaney
Microsoft Canada

--

This posting is provided "AS IS" with no warranties, and confers no rights.

Thread-Topic: renewing web certificates
thread-index: AccScgrWtcmJQf7YQAmSQtNpWp/6YA==
X-WBNR-Posting-Host: 82.33.159.241
From: =?Utf-8?B?UGF1bA==?= <Paul@xxxxxxxxxxxxxxxxxxxxxxxx>
References: <E195E078-7ECF-4768-8C33-E2352C40DA55@xxxxxxxxxxxxxxxx>

RE: renewing web certificates

<48FBD978-27A8-4FCF-9891-D6771EB4C98F@xxxxxxxxxxxxxx>

Subject: RE: renewing web certificates
Date: Mon, 27 Nov 2006 14:19:02 -0800

I have been trawling the Internet to find out information about the CDP locations. There seems to be three locations where a CRL can be published

in

my scenario (offline standalone root CA and an online Sub CA). These are http, unc and a ldap path.

I have read that the unc path to a file share is not required if

publishing

to AD. This is a little confusing because I am using the standalone CA

and

thought this was outside of AD.

My basic question is, in an attempt to find out which location is offline can I safely remove some of the CDP locations say:

remove the ldap location
remove the file locaton

Just leave the http location. I would be doing this on the root CA then request a new sub ca cert hopefully installing a new cert with only the

http

location should help me diaganose why the sub ca does not issue certs

"Paul" wrote:

It turns out that the subordinate CA is also runs out next week so this

must

be the reason why I can't issue certs beyond next week. I have tried to

issue

a new sub cert but now I get a problem on the sub CA saying the

RE: renewing web certificates

revocation

server is offline and can not issue certs. Could anyone explain or

provide a

link about how to configure all them CDP settings?

"Paul" wrote:

Hi,

Just a quick question. I have a web certificate about to run out next

week.

The web cert is one that is issued by our own CA. I am wanting to

renew this

certificate but I'm not sure of the procedure.

Inside IIS server certificates I have many options from renewing to removing. I only want to renew so i chose this option but

unfortunately this

only renewed the certificate with the same expiry date of next week.

If I chose replace then the only option I have is to chose the

currently

installed cert.

Do I have to remove the existing cert before I can make a renewal.

Surely

this can't be right because what if was purchasing a cert from an

external

RE: renewing web certificates

source this could take a few days to process and leave the
web site

off line

during this period.

Any help is much appreciated