

Re: Error issuing certificates from WS03 cert svc

## Re: Error issuing certificates from WS03 cert svc

---

*Source:*

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2007-04/msg00075.html>

---

- *From:* Brian Komar <[bkomarr@xxxxxxxxxxxxxxxxxxxx](mailto:bkomarr@xxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Fri, 20 Apr 2007 00:01:16 -0500
- 

PKIView gets its information by validating the most up to date CA Exchange certificate  
Brian

On Thu, 19 Apr 2007 22:29:00 +0200, Thomas Godsk Jørgensen wrote:

Hi Brian,

Before doing anything, PKIView shows that the AIA and CDP values are valid through the entire hierarchy. Moreover, I installed an additional issuing CA with the same configuration as the original. The new CA has no problem and is able to issue end entity certs. Next, I restored the revoked CA certs. However, no change. I still get the same error on the original issuing CA but the new can issue certs. So, I'm still not really sure what's going on and where the problem is. BTW, I'm not quite sure I understand why the removal of the revoked CA certs should be a problem since the original issuing CA has a valid trust with the new CA certs – can you elaborate on that?

Regarding PKIView, can you tell where it is retrieving its information about AIAs and CPDs?

Thanks,

Thomas

"Brian Komar" <[bkomarr@xxxxxxxxxxxxxxxxxxxx](mailto:bkomarr@xxxxxxxxxxxxxxxxxxxx)> wrote in message [news:roweefjxepj2.dnijyb3epvj4.dlg@xxxxxxxxxxxxxxxx](mailto:news:roweefjxepj2.dnijyb3epvj4.dlg@xxxxxxxxxxxxxxxx)

Your problem was the removal of the revoked certificates. By removing the certificates, you will get the message that regarding unable to determine the revocation information

When you use certutil -verify -urlfetch, do it against a leaf or end entity certificate.

Also, what does PKIView.msc show?

brian

On Tue, 17 Apr 2007 22:53:07 +0200, Thomas Godsk Jørgensen wrote:

Re: Error issuing certificates from WS03 cert svc

Hi,

I'm having trouble with issuing certificates from a Windows Server 2003 enterprise (subordinate) issuing CA. The CA rejects requests with a warning in the Windows Application Log (Event ID: 53, Source: CerSvc): "Certificate Services denied request 932 because: The revocation function was unable to check revocation because the revocation server was offline. 0x80092013 (-2146885613). The request was for <here comes specific cert subject info>. Additional information: Error Constructing or Publishing Certificate"

The setup is a three-level hierarchy with offline policy and root CAs set-up according to Microsoft's best practice PKI white paper and Brian Komar's MSPress PKI book. All CAs' CRLs are published on a web server (http) and in AD (ldap). The policy CA has a revoked CA cert superseded by a renewed valid CA cert. The issuing CA has one revoked CA cert superseded by two renewed valid CA certs. All certs are likewise published on the web server and in AD, but revoked certs have been removed from the web server. Validity of cert and trust chain of issuing CA's valid certs has been successfully verified with certutil -verify -urlfetch <CA\_certs>.

Trouble began after root and policy CA CRLs expired and were renewed too late. Now, all CRLs are current/valid as verified using certutil. Still, the issuing CA denies requests with the above error message - except in a very

Re: Error issuing certificates from WS03 cert svc

few apparent random cases.

Anybody experienced this or has any ideas?

Thanks very much.

Best regards,  
Thomas Godsk Joergensen  
thomas@xxxxxxxxx