

Re: PKI – Single Offline Root for Multiple Forest

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2008-03/msg00077.html>

- *From:* "Brian Komar \ (MVP\)" <brian.komar.nospam@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 24 Mar 2008 22:28:47 -0500
-

Inline...

"patilp" <patilp@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:2194CCDF-7C6E-49DD-AF5B-BE762837669C@xxxxxxxxxxxxxxxxxxxx

A few questions---

- a) Can i have a single PKI hierarchy spanning multiple forests ? Meaning can a single standalone root CA create certs for issuing / subordinate enterprise CA's which are located in different AD Forests ?

Yes, the key is to not use LDAP:/// paths for CDP or AIA extensions. I have deployed this model quite a few times and only use HTTP:// locations. If they did have the servers, we could have used a specific LDAP server (<ldap://ldap.example.com/OU=PKI...>)

i am looking for some official guidelines which i can't seem to find anywhere.

I am working on a new whitepaper that is going to recommend only using HTTP URLs if at all possible.

i am guessing i can do it by changing the cdp/aia parameters for every CA cert creation and keep modifying that for a new CA cert. When it s time to renew i can put it back. Will this work ?

Actually, you should not have to change anything if you go to HTTP URLs. In this type of environment, the offline CAs would not use LDAP URLs, so need to change if you use the default variable names for the certs and CRLs. For the issuing CAs, it is more of a touchy/feely decision. Where are the certificates going to be used? If they are localized to that forest, then you could use LDAP URLs for that issuingCA. If they are used between forests, I would again, use HTTP alone or as the primary URL.

- b) Also most of the docs state that LDAP CDP /AIA entry on the root CA must

Re: PKI – Single Offline Root for Multiple Forest

be prior to HTTP entry in the list – Is there any specific reason for this or it doesn't matter.

Actually, those are much older docs. I personally recommend HTTP first in all cases. It is more of a universal protocol, and the default LDAP URLs are only recognized by Windows clients (2000 or later) that are members of the forest. Unix, non-domain members, etc will fail on the LDAP URL. If it is the primary URL, this can result in excessive time-outs as it fails on the LDAP URL. Check out the latest version of the Revocation checking whitepaper at www.microsoft.com/pki

Thanks in advance for any response.

--

Patilp