Corelan Team

:: Knowledge is not an object, it's a flow ::

Free tool : Windows 2003/2008 Certificate Authority Certificate List Utility for pending requests and about-to-expire certificates

Corelan Team (corelanc0d3r) · Friday, April 10th, 2009

In one of my earlier posts, I have talked about setting up a Windows 2008 based Certificate Authority/PKI. Once your Windows 2008 CA setup is in place and configured, you can go ahead and starting issuing certificates. But at the same time, you need to put a maintenance/management procedure in place so you can stay on top of certain tasks, such as processing pending certificate requests or identify certificates that will expire and need manual renewal. Unfortunately there is no easy way to get notified when new requests are pending, or certificates will expire somewhere in the future.

I wrote a small script that will help you putting in place this maintenance process.

This free utility requires .Net framework and requires proper permissions to connect to the CA admin interface. It uses the Windows Server 2003, 2008 or Vista version of certutil and will run against a 2003 or 2008 CA.

The tool will perform the following tasks

– list all pending certificate requests

– list all certificates that will expire in a given number of days (or have expired in the last x days)

You can configure the tool to send you an email based on the results of these 2 queries. What I usually do is run this script in 2 separate schedules :

– look for pending requests, run script every day

– look for certificates that will expire in the next x days, and run script on a weekly basis.

Of course, you are free to schedule the script the way you want.

Usage

After unpacking the zip file, you will get a single .exe file. After launching the tool without specifying any parameters, you will get this :

```
----------------------------------------
 PVE CA Cert List Utility - (c) 2009
 List pending requests and expirations
 http://www.corelan.be:8800
 Version : 1.0.0.58
----------------------------------------
  Usage :

  pvecacertlist.exe parameters

  Parameters :
    -h    Show this help text. All other options will be ignored
    -s <CAServer\CAName> optional, only used when CA is not running
                           on the local machine)
    -e <Nr of days> Show list of certificates that will expire in less
                     than <Nr of days> days
    -p    Show list of pending certificate requests
      Note : you must specify at least option -e or option -p.
             Otherwise, there won't be any output
    -i <templateName>
          Only show certificates from the specified certificate template
          defined here (max. 1 template)
    -v    Verbose - show verbose output
    -n    notify - send email with report.
          This option requires a valid config file. By default, the
          utility will search for a file called smtp.cfg.
          This file must contain the following entries :
              mailserver=<hostname or IP of mailserver>
              mailserverport=<port to connect to on mailserver
              mailfrom=<email address>
              mailto=<email address>
          You can specify multiple To: addresses by separating the
          addresses with a comma
    -c <path to custom smtp config file>   This parameter allows you
          to specify the path/filename to a custom smtp config file
    -o    Only send email when action is required. Used only with -n
    -f <path to report file>   Use this parameter to specify a path/filename
          where the utility output report needs to be written to
          If this parameter is not used, the report will be written into
          a file called report.txt in the working directory
    -b    Don't write anything to log/report files
    -u    Check for updates)
```

Let's have a look at some of the parameters :

-s : if you run the utility on the CA server itself, you don't need to specify the –s parameter. If you are running the utility from a remote machine, you need to specify the CA Servername\CA name using the –s parameter. You can get the exact CA Servername\CA name string by running "certutil" on

the CA server, look for “Config:”. This is the string you need to use. (Put the string between double quotes if it contains spaces)

-e : if you want to look for certificates that will expire in a given number of days, specify the –e parameter, followed by the number of days that you want to look ahead. You can use a negative value to look back in time (to list certificates that have expired)

-p : If you want to look for pending certificate requests, specify the –p parameter.

You can use –e and –p at the same time. The tool will perform both queries in the same run.

The –v parameter will show verbose output when running the script.

-i : only show certificates that match with the specified templatename. You can only provide one template name.

-n : Notify. If you want to send emails, you need to create a file called smtp.cfg first. This file needs to contain 4 entries (as indicated above). If you only use the –n parameter, you will get an email every time, regardless whether pending requests / certificates that will expire are found. This file needs to be in the application directory or in the working directory. In order for mail notification to work, a valid smtp configuration file must exist. You can either create a file called smtp.cfg (in the working directory), or you can specify a custom Mysmtp.cfg file (any path/name will work) by using the -c parameter.

-o : This parameter can only be used when –n is used as well. It will force the tool to only send emails when actions need to be taken (pending requests, or certificates that will expire)

-u : check for update. If you enable this option, and enable email notification (-n) as well, the report will contain a note if an updated version is detected.

By default, output will be written into a file called report.txt (in working directory). If you don’t want to write anything to a local file, use the -b parameter. If you want to specify a custom path/filename to write the report into, use the -f parameter to overrule the default local report.txt file.

If you find bugs or want to leave feedback about this tool, please use the discussion forum.

Download

Current version : **1.1.0.90**

Last update : **3 may 2010 21:41:02**

Forum : http://www.corelan.be:8800/index.php/forum/pve-ca-cert-list-utility

Show your respect for my work :

You must be logged on to download this tool. You can register/log in using the “Login/Register/Logout” link in menu bar at the top of this blog.

Please log in to download PVE CA Cert List Utility (7.9 KiB)

MD5 checksum :

0675294f06a8e624d4bf9fdb9a2fe55a *pvecacertlist.zip

Changelog :

1.1.0.90

- Added feature -si. This option only works in conjunction with -e, and will tell the utility to only search in issued certificates
- Fixed a bug with -i (filter on templates)

1.1.0.81
- Added feature -r. This option only works in conjunction with -e (check for certificates that are about to expire)
When enabled, this option will filter out all 'about to expire' certificates that have already been renewed.

1.1.0.2
- This version should now work properly with non-English operating systems

1.0.0.60
- Fixed issue with spaces in column names (for win2k3 compatibility)

1.0.0.58
- Fixed issue with non-english OS (reported at http://www.corelan.be:8800/index.php/forum/pve-ca-cert-list-utility/windows-server-2003-compatability)
- Added feature allowing to filter on template

1.0.0.23
- Added verbose logging in case email cannot be sent (error only visible when -v is used)

1.0.0.22
- Fixed issue with -u (check for update) parameter.

1.0.0.21
- Added some new features, as requested by reidca (see http://www.corelan.be:8800/index.php/forum/pve-ca-cert-list-utility/windows-server-2003-compatability) :
* ability to specify location/filename of smtp config file. If nothing is specified, application folder/working directory will be used, and the file must be called smtp.cfg.
* ability to specify multiple recipients in smtp.cfg file. (Separate recipients with comma !)
* ability to specify filename/path of report file. If nothing is specified, output will be written to report.txt
* ability to specify a negative value when looking for expired certificates, allowing to look back in time

1.0.0.5
- Added output to file (output is written to report.txt automatically)
- Fixed issue. Utility will now attempt to find and use smtp.cfg either in application folder or in working directory
- Fixed issue that prevented the utility to work on some Windows 2003 systems
Issue reported by reidca at http://www.corelan.be:8800/index.php/forum/pve-ca-cert-list-utility/windows-server-2003-compatability

1.0.0.1
- Initial version

This entry was posted
on Friday, April 10th, 2009 at 7:08 pm and is filed under 001_Security, Certificates, My Free Tools, Windows Server
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.