Certificate Expiration Alerting

Author: Fabian Kunz

Mail: fabian@free-fsolutions.com

Product version: Windows Server 2003 CA, Windows Server 2008 CA, Windows Server 2008 R2 CA

Introduction

Today a lot of services and systems such as Microsoft Lync and Microsoft Exchange require certificates. Every administrator knows the problem with expired certificates. In case of public issued certificates from a trusted Certificate Provider most of them will inform their customers with an email before a certificate will expire.
But what happens with certificates issued from an internal Microsoft Windows Certification Authority (CA)? A lot of Microsoft Lync and Microsoft Exchange customers have no monitoring solution in place such as for example Microsoft Operations Manager (SCOM) to monitor the expiration status of their certificates.

The Certificate Expiration Alerter helps IT departments monitor the expiration status of all their certificates which are issued from an internal Windows Server Certificate Authority (CA). When a certificate is about to expire, the Certificate Expiration Alerter sends a notification email with information about the certificate.

This allows IT administrator to be proactive and take action by renewing the certificates before they expire and prevent possible service downtimes. This article explains the use of this tool.

Description

The Certificate Expiration Alerter is a command-line tool based on.NET Framework 2.0. It connects to a Windows Certification Authority (CA) specified as a command-line parameter, and detects which certificates will expire at the defined day specified as a command-line parameter. The administrator receives an email notifying which certificates will expire at the specified day. There is an optional regex parameter to filter certificates with specific Common Names. The administrator must create a Scheduled Task to run the tool once per day.

Purpose

This tool can be used to monitor internally issued certificates that are about to expire. Armed with this information, the administrator can take proactive action to renew the certificate before it expires.

Requirements

This tool runs on Windows 2003, Windows 2008 or Windows 2008 R2 Server. The Windows version supported is English and German. At least .NET Framework 2.0 is required to run this tool.

Examples

CertExpAlerter is a command-line tool that supports the following parameters. These parameters are:

```
-m = SMTP server name or ip address to relay the notification message.
-s = sender's email address in the format sender@company.com.
-r = recipient's email address in the format recipient@company.com. To
supply multiple email addresses, use the delimiter ";".
-d = number of days to check when a certificate expires.
-c = CA server path in form of "CAServerName\Common Name of the CA
certificate"
-f = regular expression to filter based on the certificate's Common
Name.
```

The common use case is scenario 4. Before you create a Scheduled Task for this tool, first run scenarios 1 and 2. Scenario 1 (Test Email Receipt) makes sure that the tool is able to send emails successfully. Scenario 2 ensures that the user account used by the Scheduled Task has sufficient privileges to connect to the Windows CA. If both tests are successful, you can create the Scheduled Task.

Scenario 1: Test Email Receipt

The following command-line sends a test email immediately. This allows the administrator to ensure that the tool is properly sending notifications of certification expiration.

```
CertExpAlerter.exe -m SMTPServerName -s sender@company.com -r
recipient@company.com
```

Scenario 2: List all issued certificates

The following command-line arguments will list all the certificates issued by this CA with their expiration information.

```
CertExpAlerter.exe -c "CAServer\Root CA"
```

Scenario 3: List all issued certificates that will expire in x days

This command lists all certificates that will expire in exactly 15 days.

```
CertExpAlerter.exe -c "CAServer\Root CA" -d 15
```

Scenario 4: Send notification emails about certificates that will expire in x days

The administrator must create a Scheduled Task and run the tool on a daily basis. An email will be sent to recipient@company.com if a certificate will expire in exactly 30 days.

```
CertExpAlerter.exe -m SMTPServerName -s sender@free-fsolutions.com -r
recipient@company.com -d 30 -c "CAServer\Root CA"
```

Scenario 5: Filter based on Certificate Common Name

To query certificates that matches a specific regular expression in the Common Name, use the parameter, '-f'. This parameter uses regular expressions (regex). This parameter is not case sensitive. This parameter can be used in any of the previous listed scenarios, except in scenario "Test Email Receipt".

This command returns all certificates with a Common Name that starts with the string 'PC'.

```
CertExpAlerter.exe -c "CAServer\Root CA" -f "^PC"
```

This command returns all certificates with Common Name that does NOT start with the string 'PC'.

```
CertExpAlerter.exe -c "CAServer\Root CA" -f "^(?!PC)"
```

Output

Figure 1 illustrates listing of all certificates with their expiration date information's (Scenario 2).

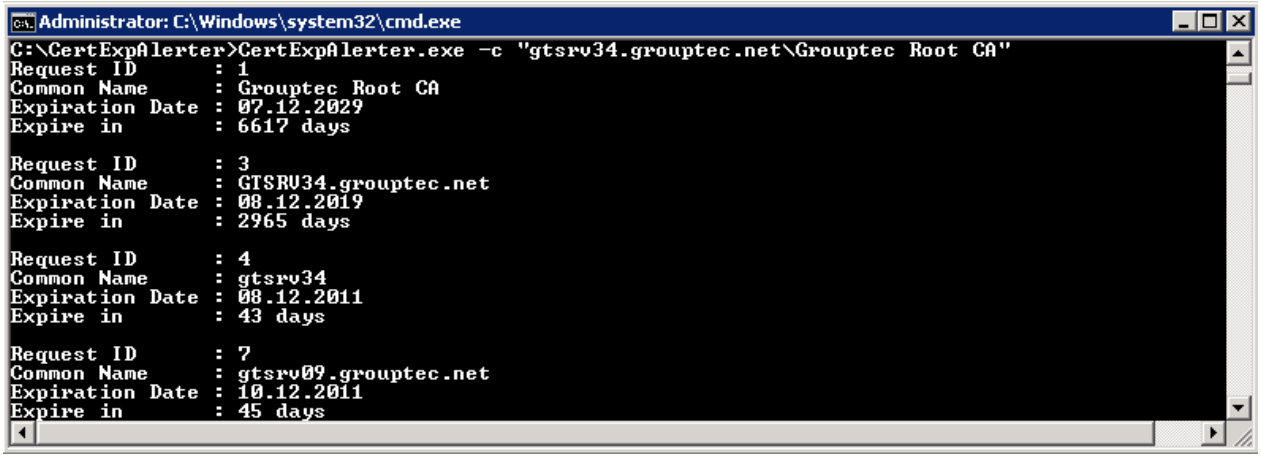

Figure 1 Querying certificates

Figure 2 illustrates querying certificates where the Common Name begins with “test” (Scenario 5).

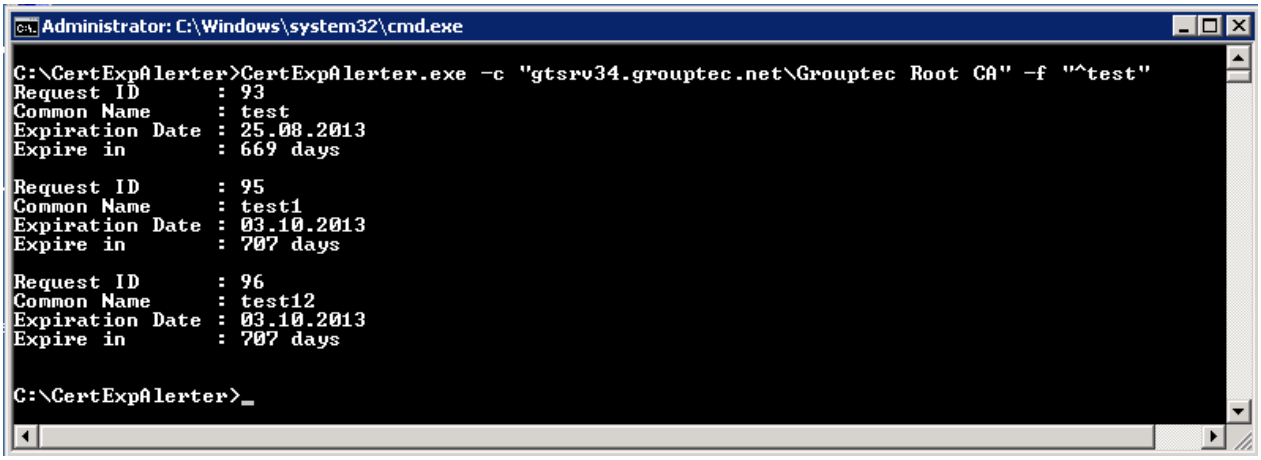

Figure 2 Querying certificates with the optional filter parameter

Figure 3 illustrates querying certificates about to expire in exactly 707 days (Scenario 3).

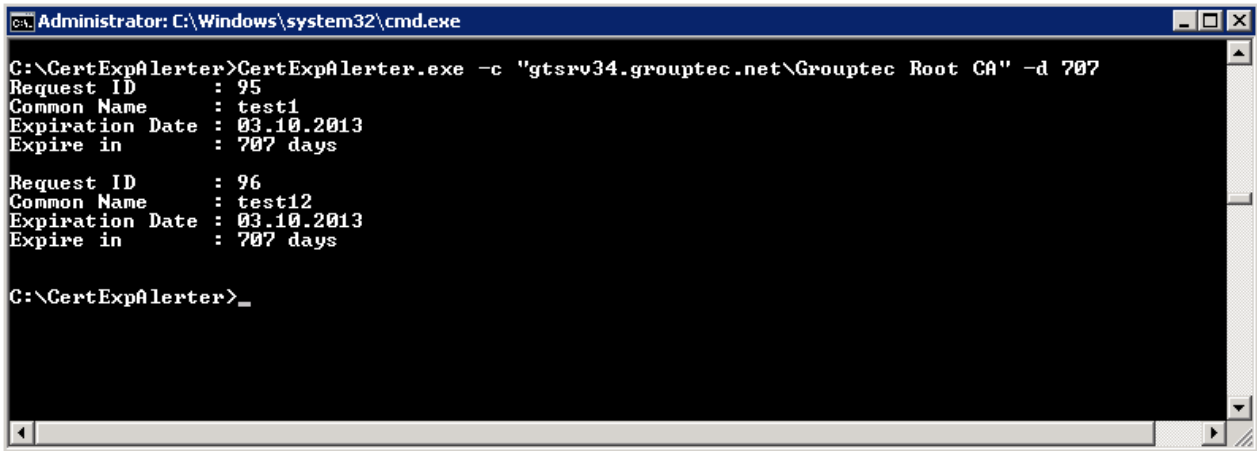

Figure 3 Querying certificates with the optional filter parameter

The email notification contains information about the certificate that matches the optional filter and the specified day criteria that are about to expire (Scenario 4). This is illustrated in Figure 4.

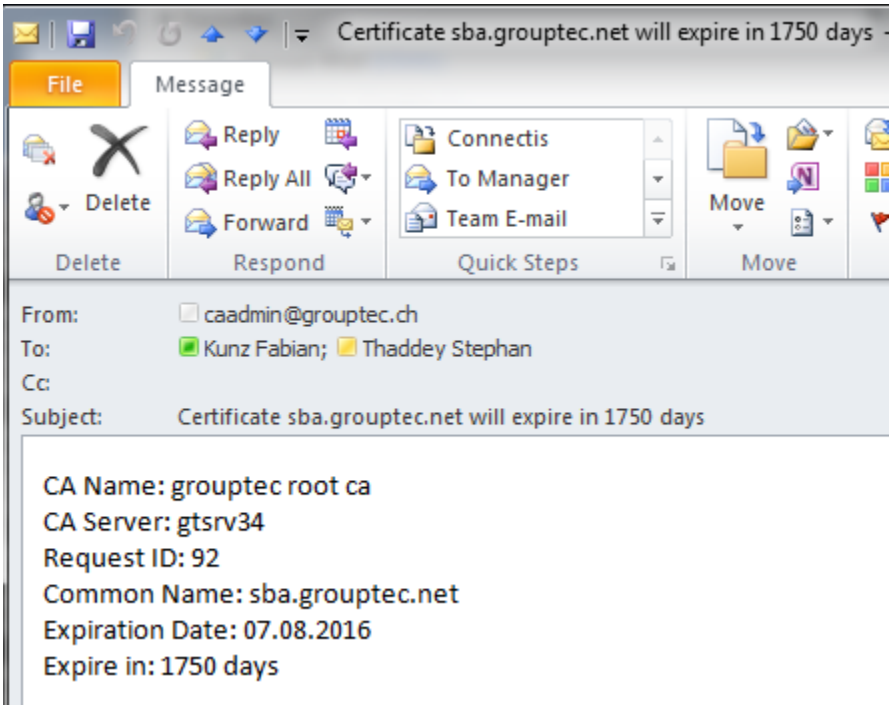

Figure 4 Email notification

Summary

Monitoring solutions such as System Center Operations Manager (SCOM) provides the ability to monitor the expiration of certificates. However, if you do not have such a monitoring solution available, CertExpAlerter offers an easy and free solution to monitor your certificates. Please feel free to reach out to me if you have further questions.

Additional Information

- http://sourceforge.net/projects/certexpalerter/
- http://blogs.technet.com/b/nexthop/archive/2011/11/18/certificate-expiration-alerting.aspx