Proximus support – automatic CRL update on F5

A step-by-step guideline to automatically update the Certificate Revocation List on a daily basis on the F5, using a script executed on 3th party host

|  |  |
| --- | --- |
| Author | Tom Vanwesemael |
| Owner | Tom Vanwesemael |
| Organization | Proximus |
| Approver | Guillermo Merguia Morales |
| Document Type | / |
| Document ID | / |
| Document location | / |
|  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Change History | | | | | | | | | |
| Version | Status | Date | Author | Owner | Reviewed by | Reviewed date | Approver | Approval date | Description of changes | |
| 1.0 | Approved | 01-04-2019 | Tom Vanwesemael | Tom Vanwesemael | Guillermo Merguia Morales | 01-04-2019 | Guillermo Merguia Morales | 01-04-2019 | First Release | |
| 1.1 | Approved | 24-04-2019 | Tom Vanwesemael | Tom Vanwesemael | Guillermo Merguia Morales | 23-04-2019 | Guillermo Merguia Morales | 23-04-2019 | Update 1.1 | |

Solution

High level layout and approach



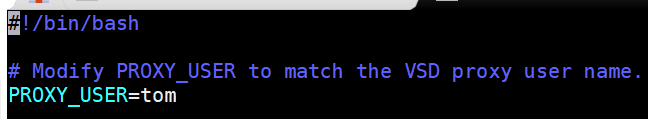
The idea is that the script first retrieves the CRL from the VSD, then copies it to the F5 with SCP into the /tmp/ directory and finally executes it on the F5 remotely from the host using TMSH.

1. Getting the script and required adjustments

The script can be downloaded from github and uploaded to the 3th party host:

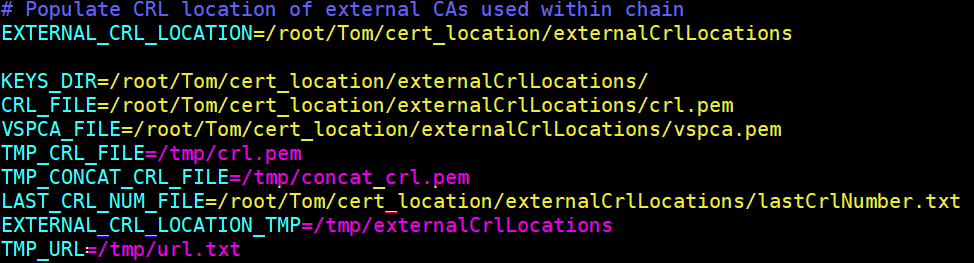
<https://github.com/tvanwese/crlreloader>

The following points need to be adjusted by the user.

* Right from the start **edit the PROXY\_USER** to the user name used for the user in the vsd.

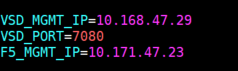
Note: Make sure that the user is created in the VSD and is attached to the **root** group. More info on this can be found in the VNS User Guide.

* Next, find or create a directory to store the certificates. In our example case we created one new directory (yellow) and used the /tmp/ directory for the according /tmp/ files (pink).



Note: Make sure that the CRL file name in the F5 = vspca.pem. If a different name is desired, be sure to replace vspca.pem everywhere by this name. 

* Lastly, change the following addresses.



1. For a standalone VSD

* VSD\_MGMT\_IP = **Management IP address** or XMPP of the standalone vsd
* VSD\_PORT = Port of the standalone VSD
* F5\_MGMT\_IP = Management IP address of the F5

1. For a VSD cluster setup

* VSD\_MGMT\_IP = **XMPP** of the VSD cluster or IP address of the **loadbalancer**
* VSD\_PORT = Port of the VSD cluster or port of the **loadbalancer**
* F5\_MGMT\_IP = Management IP address of the F5

1. For a VSD geo-redundant cluster setup

* VSD\_MGMT\_IP = IP address of the **Loadbalancer**
* VSD\_PORT = Port of the **loadbalancer**
* F5\_MGMT\_IP = Management IP address of the F5

1. Add a Cron Job on the 3th party host

Enter the following commands:

***crontab -l > /tmp/cron 2>/dev/null***

***echo "\* \* \* \* \* /path/to/the/script/crlreloader.sh" >> /tmp/cron***

***crontab /tmp/cron***

***rm /tmp/cron***

Check if the cron job is applied:

***crontab -l***

******

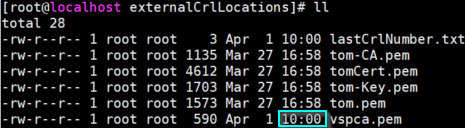
1. Monitor if script and cron job are working correctly

Verify CRL retrieval:

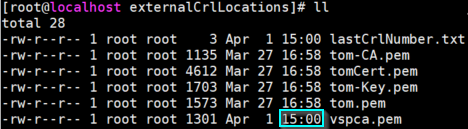
* Compare, in the location where the certifications are saved, the files before and after the cron job configured time.

Example: cronjob of the script set for 10:00 and 15:00

Before 15:00  

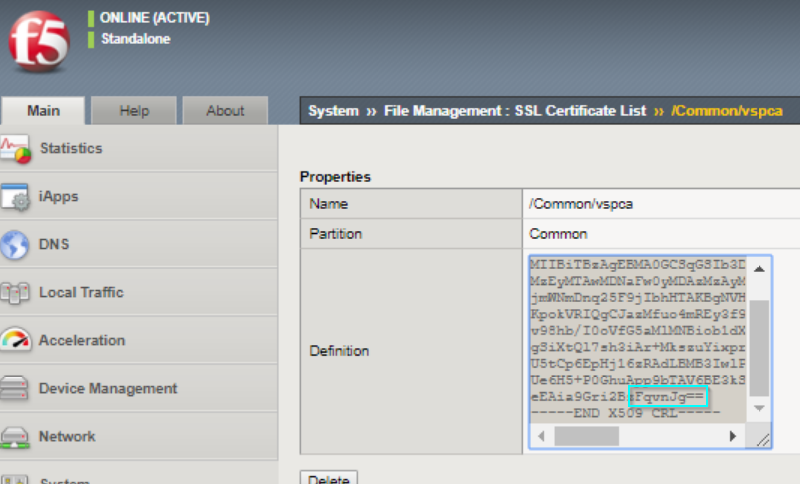



After 15:00

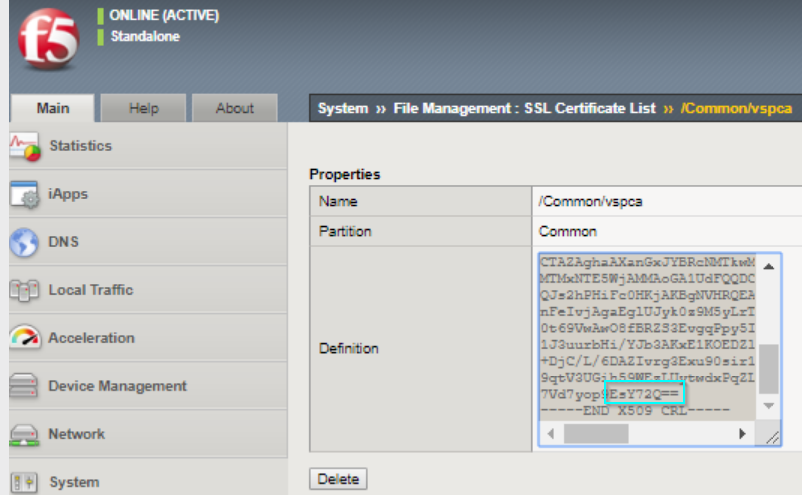


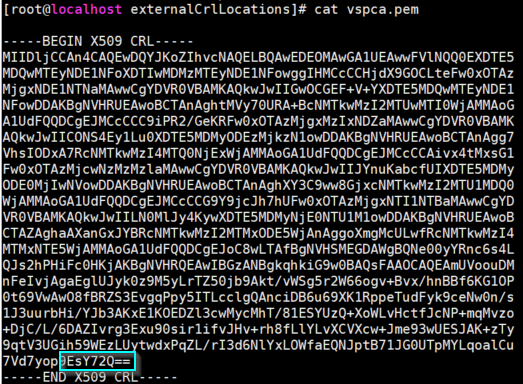
Verify SCP/Remote TMSH working:

* Check on the F5 before and after if the definition of the certificate changed. Also compare after the cron job configured time the certificate on the 3th party host with the value of the certificate in the F5 if they match.

Before – F5 

After – F5



After – Certificate

When these checks are correct, the setup is correctly working, and the CRL file will be updated automatically as configured with the cron job.