IBM Technology Expert Labs

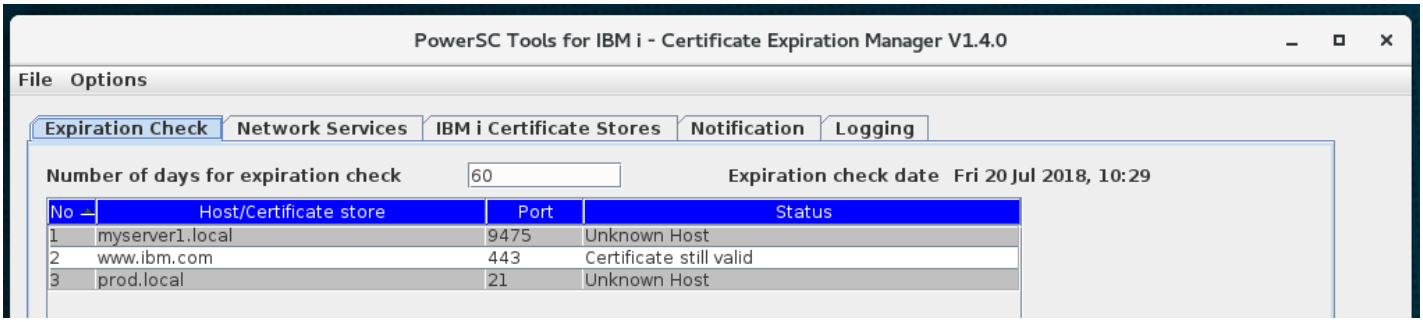
Certificate Expiration Manager

Ensure your critical certificates do not expire without notice

IBM Technology Expert Labs Power Delivery Practice is proud to provide the Certificate Expiration Manager. The primary purpose of this tool is to provide a simple way to get notified about upcoming certificate expirations. In a modern network, TLS encryption is crucial to provide encrypted communications. But this encryption only works when the certificates are in their valid date period. Expired certificates can lead to outages in an otherwise healthy network. Because of this, staying on top of certificates is a key item. Using the Certificate Expiration Manager will notify you well in advance of your certificate expiration to allow you the time needed to ensure uninterrupted service.

Certificate Expiration Notification
Using the Certificate Expiration Manager, you can be notified about upcoming TLS certificate expirations. The date range in which a certificate is determined to expire is defined by adding a number of days to the current date (program run date). If a certificate's notAfterDate is between the current date and the calculated expiration checking date, the certificate is reported as a candidate for expiration. These notifications can be sent via email or via Syslog to a central SIEM. The tool is written in Java and is designed to run on any platform that supports Java, including Windows, Mac, Linux, AIX, and even natively on the IBM i. Designed with both a GUI and non-GUI interface, it can truly run in any environment. Or use the GUI to define the parameters, save to an XML based configuration file, and then run headless on the IBM i!

Type of Certificates
The Certificate Expiration Manager is the one tool you need for checking all your TLS certificates. When run, it can be configured to check the TLS certificate on a wide variety of services including HTTPS, TELNETS, FTPS, and SMTPS on any platform, not just IBM i! Use the Certificate Expiration Manager to check you web, email, gateway, file, and any other service that is accessible. This can include both intranet and public internet facing sites as well. Don’t yet your internal or external uses get blocked by expired certificates. When run within IBM i, the utility can also check for expiring certificates in the*SYSTEM, *OBJECTSIGNING, *SIGNATUREVERIFICATION, and custom IBM i certificate stores.



Sample Syslog Message: Apr 21 17:11:51 :::1.2.3.4 local0:warn|warning| CertExpirationTag: CEF:0|IBM|CERTEXPMGR| 1.4|100|CertificateExpirationCheck|7|result= CERT_WILL_EXPIRE|

Service_name=Our secure Telnet server|Host_name=myibmi.ihost.com Port=992

NotAfterDate=Thu Dec 14 12:27:56 CET 2017 ExpCheckDate=Sun Dec 17 17:11:51 CET 2017| Result_text=Certificate will expire before check date(1)

Implementation Services

Need help securing your IBM i system? Our Expert Labs team is highly trained in the proper way to handle complex security configurations. We can guide you all the way from design to implementation. You don't have to undertake security yourself – allow IBM Expert Labs to be your trusted consultants to ensure a successful project!

Interested in a Quote or Learning More?

If you are interested in purchasing this asset or discussing it further with one of our consultants, please contact Ron Bibby at ronbibby@us.ibm.com! Or visit our website at https://ibm.biz/IBMiSecurity.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.