IBM ECM System Monitor
Field Guides

Usage of Keystores and Truststores

August 29th, 2023
CENIT AG
Michael Wohland

Content

Introduction

Overview

This guide describes in detail how Keystores and Truststores are used in ESM.

Disclaimer

The content of this document is based on ESM Version 5.5.7.x. The descriptions and guidelines in this document are for informational purposes only. Up-to-dateness, content completeness, appropriateness and validity for all possible scenarios cannot be guaranteed. All information is provided on an as-is basis. The author is not liable for any errors or omissions in this document or any losses, injuries and damages arising from its use.

If you are planning to setup or configure ESM or to adjust an existing installation, it is absolutely necessary to take into account current security whitepapers, release notes and announcements from the official IBM ECM System Monitor product documentation website.

Purpose of this guide and Definition

Keystore is an umbrella term. Often only the term keystore is used but a truststore is meant. I am trying to use the correct wording in this guide so hopefully it is easier to distinguish between keystore and truststore in ESM.

Difference between keystore and truststore: There are various description of keystores and truststores in the World Wide Web. Basically you can find the following information.

Truststore: Is used to store the certificates for trusted entities – meaning whenever a client needs to trust something that is encrypted, it needs to have the correct certificate(s) in a truststore. I am writing certificate(s) here because you need the full path building chain of the certificates. That can include additional certificates like root and intermediate certificates.

Keystore: Is used to store the server keys (that includes the public and private key) along with the (signed) certificate that is used for the encryption.

There are several keystores and truststores in ESM that are used for different tasks. This guide will list all of them and describe their task.

ESM Server keystore for providing the https access in the webconsole

Keystore file: <ESM_Server_Install_Dir>/karaf/etc/ssl/keystore.

Keystore type: jks

Password of the keystore and keys: password

This keystore contains by default a self signed certificate of the buildserver of the ESM software and the key(s) for it. This certificate will not fit for any installation and therefore the https URL for the Webconsole will always be shown as untrusted by default in a browser. This keystore file can be replaced by a new file that contains a (self) signed certificate and the keys for the host where the ESM Server is running. Best is if the new file uses the same name, type and password. Otherwise adjustments in some files are necessary. The Server must be restarted after the file has been exchanged.

Note: The ESM Agents do have this keystore file as well but it is not in use there!

ESM Server and Agent JRE Truststore

Truststore file: <ESM_Install_Dir>/jre/lib/security/cacerts.

Truststore type: jks

Password of the truststore: changeit

By default this truststore contains multiple signer certificates to ensure that all certificates that were signed by these signers can be trusted. In some circumstances this truststore is also used in ESM and therefore sometimes certificates must be imported to this truststore.

Usage of this truststore on the ESM Server:

If the ESM Server connects to a secured system e.g. smtp over ssl or ldaps for login to ESM using LDAP accounts, the required (root, intermediate and host) certificates must be imported here.

Usage of this truststore on the ESM Agents:

On the ESM Agents this truststore is used when connections to the FileNet API (CPE) via FNCEWS40MTOM URL are established that are secured. This is the case for some of the CPE probes. Usually you will find an information about that in the probe description. Again, import the required (root, intermediate and host) certificates in this case.

ESM Agent global Keystore and Truststore

Truststore file: <ESM_Agent_Install_Dir>/karaf/data/ssl/truststore.jks

Truststore type: jks

Keystore file: <ESM_Agent_Install_Dir>/karaf/data/ssl/keystore.jks

Keystore type: jks

The password for both files is not declared because both of the files are automatically fed with the information for “keystores” that are specified in a keystore subsystem that is valid for this agent. So no manual import is needed. The agent will read the information of the subsystem and then load the certificates from the specified folder or truststore in the global truststore. If a folder or keystore is specified that also contains keys for a certificate, this will also be loaded into the global keystore.

The global truststore is used for all secure connections that are established when executing a probe, e.g. to connect to a secured webpage.

The global keystore is currently not used in ESM.

Note: Probes that establish a connection to the FileNet API do not use this truststore! – See previous chapter!

Useful tools for orchestration

Java offers a command line based tool (keytool) in the bin directory of the jre. This tool can be used to import information into a “keystore”.

Example:

```
..\..\bin\keytool -import -trustcacerts -keystore cacerts -storepass
changeit -noprompt -alias yourAliasName -file
path\to\certificate.cer
```

Alternatively you can use the open source tool keystore explorer: https://keystore-explorer.org/

Contact Information

If you have any questions, please contact us at ECM.SystemMonitor@cenit.com.

CENIT AG
Phone: +49 711 7825 30
Email: ECM.SystemMonitor@cenit.com