Full credit is given to the above companies including the OS that this PDF file was generated!

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'update-ca-trust.8' command

$ man update-ca-trust.8

UPDATE-CA-TRUST(8) UPDATE-CA-TRUST(8)

NAME

update-ca-trust - manage consolidated and dynamic configuration of CA certificates and associated trust

SYNOPSIS

update-ca-trust [COMMAND]

DESCRIPTION

update-ca-trust(8) is used to manage a consolidated and dynamic configuration feature of Certificate Authority (CA) certificates and associated trust.

The feature is available for new applications that read the consolidated configuration files found in the /etc/pki/ca-trust/extracted directory or that load the PKCS#11 module p11-kit-trust.so

Parts of the new feature are also provided in a way to make it useful for legacy applications.

Many legacy applications expect CA certificates and trust configuration in a fixed location, contained in files with particular path and name, or by referring to a classic PKCS#11 trust module provided by the NSS cryptographic library.

The dynamic configuration feature provides functionally compatible replacements for classic configuration files and for the classic NSS trust module named libnssckbi.

In order to enable legacy applications, that read the classic files or access the classic module, to make use of the new consolidated and dynamic configuration feature, the classic filenames have been changed to symbolic links. The symbolic links refer to dynamically created and consolidated output stored below the /etc/pki/ca-trust/extracted directory hierarchy.

The output is produced using the update-ca-trust command (without parameters), or using the update-ca-trust extract command. In order to produce the output, a flexible set of source configuration is read, as described in section SOURCE CONFIGURATION.

In addition, the classic PKCS#11 module is replaced with a new PKCS#11 module (p11-kit-trust.so) that dynamically reads the same source configuration.

SOURCE CONFIGURATION

The dynamic configuration feature uses several source directories that will be scanned for any number of source files. It is important to select the correct subdirectory for adding files, as the subdirectory defines how contained certificates will be trusted or distrusted, and which file formats are read.

Files in subdirectories below the directory hierarchy /usr/share/pki/ca-trust-source/ contain CA certificates and trust settings in the PEM file format. The trust settings found here will be interpreted with a low priority.

Files in subdirectories below the directory hierarchy /etc/pki/ca-trust/source/ contain CA certificates and trust settings in the PEM file format. The trust settings found here will be interpreted with a high priority.

You may use the following rules of thumb to decide, whether your configuration files should be added to the /etc or rather to the /usr directory hierarchy:

? If you are manually adding a configuration file to a system, you probably want it to override any other default configuration, and you most likely should add it to the respective subdirectory in the

/etc hierarchy.

? If you are creating a package that provides additional root CA certificates, that is intended for distribution to several computer systems, but you still want to allow the administrator to override your list, then your package should add your files to the respective subdirectory in the /usr hierarchy.

? If you are creating a package that is supposed to override the default system trust settings, that is intended for distribution to several computer systems, then your package should install the files to the respective subdirectory in the /etc hierarchy.

QUICK HELP 1: To add a certificate in the simple PEM or DER file formats to the list of CAs trusted on the system:

? add it as a new file to directory /etc/pki/ca-trust/source/anchors/

? run update-ca-trust extract

QUICK HELP 2: If your certificate is in the extended BEGIN TRUSTED file format (which may contain distrust/blocklist trust flags, or trust flags for usages other than TLS) then:

? add it as a new file to directory /etc/pki/ca-trust/source/

? run update-ca-trust extract

In order to offer simplicity and flexibility, the way certificate files are treated depends on the subdirectory they are installed to.

? simple trust anchors subdirectory: /usr/share/pki/ca-trust-source/anchors/ or /etc/pki/ca-trust/source/anchors/

? simple blocklist (distrust) subdirectory: /usr/share/pki/ca-trust-source/blocklist/ or /etc/pki/ca-trust/source/blocklist/

? extended format directory: /usr/share/pki/ca-trust-source/ or /etc/pki/ca-trust/source/

In the main directories /usr/share/pki/ca-trust-source/ or /etc/pki/ca-trust/source/ you may install one or multiple files in the following file formats:

? certificate files that include trust flags, in the BEGIN/END

TRUSTED CERTIFICATE file format (any file name), which have been created using the openssl x509 tool and the -addreject -addtrust options. Bundle files with multiple certificates are supported.

? files in the p11-kit file format using the .p11-kit file name extension, which can (e.g.) be used to distrust certificates based on serial number and issuer name, without having the full certificate available. (This is currently an undocumented format, to be extended later. For examples of the supported formats, see the files shipped with the ca-certificates package.)

? certificate files without trust flags in either the DER file format or in the PEM (BEGIN/END CERTIFICATE) file format (any file name). Such files will be added with neutral trust, neither trusted nor distrusted. They will simply be known to the system, which might be helpful to assist cryptographic software in constructing chains of certificates. (If you want a CA certificate in these file formats to be trusted, you should remove it from this directory and move it to the ./anchors subdirectory instead.)

In the anchors subdirectories /usr/share/pki/ca-trust-source/anchors/ or /etc/pki/ca-trust/source/anchors/ you may install one or multiple certificates in either the DER file format or in the PEM (BEGIN/END CERTIFICATE) file format. Each certificate will be treated as trusted for all purposes.

In the blocklist subdirectories /usr/share/pki/ca-trust-source/blocklist/ or /etc/pki/ca-trust/source/blocklist/ you may install one or multiple certificates in either the DER file format or in the PEM (BEGIN/END CERTIFICATE) file format. Each certificate will be treated as distrusted for all purposes.

Please refer to the x509(1) manual page for the documentation of the BEGIN/END CERTIFICATE and BEGIN/END TRUSTED CERTIFICATE file formats.

Applications that rely on a static file for a list of trusted CAs may load one of the files found in the /etc/pki/ca-trust/extracted directory. After modifying any file in the

/usr/share/pki/ca-trust-source/ or /etc/pki/ca-trust/source/
directories or in any of their subdirectories, or after adding a file,
it is necessary to run the update-ca-trust extract command, in order to
update the consolidated files in /etc/pki/ca-trust/extracted/ .
Applications that load the classic PKCS#11 module using filename
libnssckbi.so (which has been converted into a symbolic link pointing
to the new module) and any application capable of loading PKCS#11
modules and loading p11-kit-trust.so, will benefit from the dynamically
merged set of certificates and trust information stored in the
/usr/share/pki/ca-trust-source/ and /etc/pki/ca-trust/source/
directories.

EXTRACTED CONFIGURATION

The directory /etc/pki/ca-trust/extracted/ contains generated CA
certificate bundle files which are created and updated, based on the
SOURCE CONFIGURATION by running the update-ca-trust extract command.
If your application isn?t able to load the PKCS#11 module
p11-kit-trust.so, then you can use these files in your application to
load a list of global root CA certificates.
Please never manually edit the files stored in this directory, because
your changes will be lost and the files automatically overwritten, each
time the update-ca-trust extract command gets executed.
In order to install new trusted or distrusted certificates, please
rather install them in the respective subdirectory below the
/usr/share/pki/ca-trust-source/ or /etc/pki/ca-trust/source/
directories, as described in the SOURCE CONFIGURATION section.
The directory /etc/pki/ca-trust/extracted/java/ contains a CA
certificate bundle in the java keystore file format. Distrust
information cannot be represented in this file format, and distrusted
certificates are missing from these files. File cacerts contains CA
certificates trusted for TLS server authentication.
The directory /etc/pki/ca-trust/extracted/openssl/ contains CA
certificate bundle files in the extended BEGIN/END TRUSTED CERTIFICATE
file format, as described in the x509(1) manual page. File

ca-bundle.trust.crt contains the full set of all trusted or distrusted certificates, including the associated trust flags.

The directory /etc/pki/ca-trust/extracted/pem/ contains CA certificate bundle files in the simple BEGIN/END CERTIFICATE file format, as described in the x509(1) manual page. Distrust information cannot be represented in this file format, and distrusted certificates are missing from these files. File tls-ca-bundle.pem contains CA certificates trusted for TLS server authentication. File email-ca-bundle.pem contains CA certificates trusted for E-Mail protection. File objsign-ca-bundle.pem contains CA certificates trusted for code signing.

The directory /etc/pki/ca-trust/extracted/edk2/ contains a CA certificate bundle ("cacerts.bin") in the "sequence of EFI_SIGNATURE_LISTs" format, defined in the UEFI-2.7 specification, sections "31.4.1 Signature Database" and "EFI_CERT_X509_GUID". Distrust information cannot be represented in this file format, and distrusted certificates are missing from these files. File "cacerts.bin" contains CA certificates trusted for TLS server authentication.

COMMANDS

(absent/empty command)

Same as the extract command described below. (However, the command may print fewer warnings, as this command is being run during rpm package installation, where non-fatal status output is undesired.)

extract

Instruct update-ca-trust to scan the SOURCE CONFIGURATION and produce updated versions of the consolidated configuration files stored below the /etc/pki/ca-trust/extracted directory hierarchy.

FILES

/etc/pki/tls/certs/ca-bundle.crt

Classic filename, file contains a list of CA certificates trusted for TLS server authentication usage, in the simple BEGIN/END CERTIFICATE file format, without distrust information. This file is a symbolic link that refers to the consolidated output created by

the update-ca-trust command.

/etc/pki/tls/certs/ca-bundle.trust.crt

Classic filename, file contains a list of CA certificates in the extended BEGIN/END TRUSTED CERTIFICATE file format, which includes trust (and/or distrust) flags specific to certificate usage. This file is a symbolic link that refers to the consolidated output created by the update-ca-trust command.

/etc/pki/java/cacerts

Classic filename, file contains a list of CA certificates trusted for TLS server authentication usage, in the Java keystore file format, without distrust information. This file is a symbolic link that refers to the consolidated output created by the update-ca-trust command.

/usr/share/pki/ca-trust-source

Contains multiple, low priority source configuration files as explained in section SOURCE CONFIGURATION. Please pay attention to the specific meanings of the respective subdirectories.

/etc/pki/ca-trust/source

Contains multiple, high priority source configuration files as explained in section SOURCE CONFIGURATION. Please pay attention to the specific meanings of the respective subdirectories.

/etc/pki/ca-trust/extracted

Contains consolidated and automatically generated configuration files for consumption by applications, which are created using the update-ca-trust extract command. Don?t edit files in this directory, because they will be overwritten. See section EXTRACTED CONFIGURATION for additional details.

AUTHOR

Written by Kai Engert and Stef Walter.

update-ca-trust 07/28/2022 UPDATE-CA-TRUST(8)