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 'OPENSSL_s390xcap.3ossl' command

$ man OPENSSL_s390xcap.3ossl

OPENSSL_S390XCAP(3ossl) OpenSSL OPENSSL_S390XCAP(3ossl)

NAME

OPENSSL_s390xcap - the IBM z processor capabilities vector

SYNOPSIS

env OPENSSL_s390xcap=... <application>

DESCRIPTION

libcrypto supports z/Architecture instruction set extensions. These extensions are denoted by individual bits in the capabilities vector. When libcrypto is initialized, the bits returned by the STFLE instruction and by the QUERY functions are stored in the vector.

To change the set of instructions available to an application, you can set the OPENSSL_s390xcap environment variable before you start the application. After initialization, the capability vector is ANDed bitwise with a mask which is derived from the environment variable.

The environment variable is a semicolon-separated list of tokens which is processed from left to right (whitespace is ignored):

OPENSSL_s390xcap="<tok1>;<tok2>;..."

There are three types of tokens:

<string>

The name of a processor generation. A bit in the environment variable's mask is set to one if and only if the specified processor generation implements the corresponding instruction set extension. Possible values are z900, z990, z9, z10, z196, zEC12, z13, z14 and z15.

<string>:<mask>:<mask>

The name of an instruction followed by two 64-bit masks. The part of the environment variable's mask corresponding to the specified instruction is set to the specified 128-bit mask. Possible values are kimd, klmd, km, kmc, kmac, kmctr, kmo, kmf, prno, kma, pcc and kdsa.

stfle:<mask>:<mask>:<mask>

Store-facility-list-extended (stfle) followed by three 64-bit masks. The part of the environment variable's mask corresponding to the stfle instruction is set to the specified 192-bit mask.

The 64-bit masks are specified in hexadecimal notation. The 0x prefix is optional. Prefix a mask with a tilde, "~", to denote a bitwise NOT operation.

The following is a list of significant bits for each instruction. Colon rows separate the individual 64-bit masks. The bit numbers in the first column are consistent with [1], that is, 0 denotes the leftmost bit and the numbering is continuous across 64-bit mask boundaries.

Bit Mask Facility/Function

stfle:

17 1<<46 message-security assist

25 1<<38 store-clock-fast facility

:

76 1<<51 message-security assist extension 3

77 1<<50 message-security assist extension 4

:

#129 1<<62 vector facility

#134 1<<57 vector packed decimal facility

#135 1<<56 vector enhancements facility 1

#146 1<<45 message-security assist extension 8

#155 1<<36 message-security assist extension 9

kimd :

1 1<<62 KIMD-SHA-1

2 1<<61 KIMD-SHA-256

3 1<<60 KIMD-SHA-512

32 1<<31 KIMD-SHA3-224

33 1<<30 KIMD-SHA3-256

34 1<<29 KIMD-SHA3-384

35 1<<28 KIMD-SHA3-512

36 1<<27 KIMD-SHAKE-128

37 1<<26 KIMD-SHAKE-256

:

65 1<<62 KIMD-GHASH

klmd :

32 1<<31 KLMD-SHA3-224

33 1<<30 KLMD-SHA3-256

34 1<<29 KLMD-SHA3-384

35 1<<28 KLMD-SHA3-512

36 1<<27 KLMD-SHAKE-128

37 1<<26 KLMD-SHAKE-256

:

km :

18 1<<45 KM-AES-128

19 1<<44 KM-AES-192

20 1<<43 KM-AES-256

50 1<<13 KM-XTS-AES-128

52 1<<11 KM-XTS-AES-256

:

kmc :

18 1<<45 KMC-AES-128

19 1<<44 KMC-AES-192

20 1<<43 KMC-AES-256

:

kmac :

18 1<<45 KMAC-AES-128

19 1<<44 KMAC-AES-192

20 1<<43 KMAC-AES-256

:

kmctr:

:

kmo :

18 1<<45 KMO-AES-128

19 1<<44 KMO-AES-192

20 1<<43 KMO-AES-256

:

kmf :

18 1<<45 KMF-AES-128

```
    # 19    1<<44    KMF-AES-192
    # 20    1<<43    KMF-AES-256
    :

prno :
    :

kma  :
    # 18    1<<45    KMA-GCM-AES-128
    # 19    1<<44    KMA-GCM-AES-192
    # 20    1<<43    KMA-GCM-AES-256
    :

pcc  :
    :
    # 64    1<<63    PCC-Scalar-Multiply-P256
    # 65    1<<62    PCC-Scalar-Multiply-P384
    # 66    1<<61    PCC-Scalar-Multiply-P521
    # 72    1<<55    PCC-Scalar-Multiply-Ed25519
    # 73    1<<54    PCC-Scalar-Multiply-Ed448
    # 80    1<<47    PCC-Scalar-Multiply-X25519
    # 81    1<<46    PCC-Scalar-Multiply-X448

kdsa :
    #  1    1<<62    KDSA-ECDSA-Verify-P256
    #  2    1<<61    KDSA-ECDSA-Verify-P384
    #  3    1<<60    KDSA-ECDSA-Verify-P521
    #  9    1<<54    KDSA-ECDSA-Sign-P256
    # 10    1<<53    KDSA-ECDSA-Sign-P384
    # 11    1<<52    KDSA-ECDSA-Sign-P521
    # 32    1<<31    KDSA-EdDSA-Verify-Ed25519
    # 36    1<<27    KDSA-EdDSA-Verify-Ed448
    # 40    1<<23    KDSA-EdDSA-Sign-Ed25519
```

44 1<<19 KDSA-EdDSA-Sign-Ed448

:

RETURN VALUES

Not available.

EXAMPLES

Disables all instruction set extensions which the z196 processor does not implement:

```
OPENSSL_s390xcap="z196"
```

Disables the vector facility:

```
OPENSSL_s390xcap="stfle:~0:~0:~0x4000000000000000"
```

Disables the KM-XTS-AES and the KIMD-SHAKE function codes:

```
OPENSSL_s390xcap="km:~0x2800:~0;kimd:~0xc000000:~0"
```

SEE ALSO

[1] z/Architecture Principles of Operation, SA22-7832-12

COPYRIGHT