Boot Fedora 33 with CET Enabled on Tiger Lake

Enable CET in an Application

- For C/C++/FORTRAN sources, just compile with -fcf-protection.
  - This has been done by default on Fedora.
- For JIT:
  - Add ENDBR at indirect branch targets.
  - Adjust shadow stack when stack frames are changed.
- For assembly sources:
  - Place ENDBR at all indirect branch targets in assembly codes.
  - Mark all assembly codes as CET enabled.
    - Include the header file, <cet.h>, to automatically generate CET marker in assembly codes.

Enforce CET Marker on an Application

- A program/library is CET enabled only if all its components are CET enabled.
- Build the program/library with the linker switch, -z cet-report=error, identifies input objects with missing CET marker:

```
$ gcc -Wl,-z,cet-report=error x.o
/usr/bin/ld: x.o: error: missing IBT and SHSTK properties
collect2: error: ld returned 1 exit status
```

Check CET Status on a Application

- All CET enabled binaries should have be marked:

  $ readelf -n /bin/ls 2>&1 | grep SHSTK

  Properties: x86 feature: IBT, SHSTK

  Missing the CET marker means the binary is not CET enabled.

Enable CET in Fedora 33 on Tiger Lake

Boot into Fedora in GUI mode with CET enabled on Tiger Lake.

- Make a list of failures due to missing CET support in:
  - Assembly codes.
  - JITs.
  - Other high level languages.
- For each CET failure, open a Fedora rawhide bug blocking
  - https://bugzilla.redhat.com/show_bug.cgi?id=1802674
  - Add missing ENDBR and CET marker.

Milestones

Tasks	Timeline	Linux kernel	Fedora
Install Fedora 31 on Tiger Lake SDVs	March 6		
List of packages missing CET support for GUI mode boot	April 3		
Open bug reports against all failed packages	April 10	XSAVES supervisor states in v5.6	
Move to Fedora 32	July 3	Shadow Stack in v5.7?	Fedora 32 GA
Patches created for each open bug	July 24		Fedora 33 requirement freeze
	Aug 28	IBT in v5.8?	Fedora 33 development end
	Oct 4		Fedora 33 GA