Open Infrastructure - Task #6071

[user request] Checkout how to enable AES-NI or PCLMULQDQ CPU features

11/16/2018 11:21 AM - Nico Schottelius

Status:	Rejected	**Start date:**	11/16/2018
Priority:	Normal	**Due date:**	
Assignee:	Jin-Guk Kwon	**% Done:**	30%
Category:		**Estimated time:**	0.00 hour
Target version:			
PM Check date:			

Description

- A customer requested support for this feature(s).
- Currently we emulate a Qemu virtual cpu, which allows us to migrate even between different CPUs on the hosts

Research, which CPU flags we can easily pass through or enable, by keeping the possibility to migrate between different hosts.

Alternatively:

- Make a list of hosts that have compatible CPU features and cluster them (3+ per cluster)

Also keep in mind that native CPU support might benefit customers in terms of performance in general.

History

#1 - 11/16/2018 11:25 AM - Nico Schottelius

- Description updated

#2 - 11/19/2018 11:33 AM - Jin-Guk Kwon

- Status changed from New to In Progress

CPU which support AES-NI

<Intel>
The following Intel processors support the AES-NI instruction set

Westmere based processors, specifically:
Westmere-EP (Xeon 56xx) (a.k.a. Gulftown Xeon 5600-series DP server model) processors.
Clarkdale processors (except Core i3, Pentium and Celeron).
Arrandale processors (except Celeron, Pentium, Core i3, Core i5-4XXM).
Sandy Bridge processors:
Desktop: all except Pentium, Celeron, Core i3.
Mobile: all Core i7 and Core i5. Several vendors have shipped BIOS configurations with the extension disabled; a BIOS update is required to enable them.
Ivy Bridge processors.
All i5, i7, Xeon and i3-2115C only.
Haswell processors (all except i3-4000m, Pentium and Celeron).
Broadwell processors (all except Pentium and Celeron).
Silvermont/Airmont processors (all except Bay Trail-D and Bay Trail-M).
Goldmont processors.
Skylake processors.
Kaby Lake processors.
Coffee Lake processors.

<AMD>
Several AMD processors support AES instructions:

Jaguar-based processors and newer
Puma-based processors and newer
"Heavy Equipment" processors
Bulldozer-based processors
Piledriver-based processors
Steamroller-based processors
Excavator-based processors and newer

Zen based processors
Zen+ based processors

#3 - 11/19/2018 11:33 AM - Jin-Guk Kwon

- % Done changed from 0 to 30

#5 - 12/29/2018 12:53 PM - Nico Schottelius

- Subject changed from Checkout how to enable AES-NI or PCLMULQDQ CPU features to [user request] Checkout how to enable AES-NI or PCLMULQDQ CPU features

#6 - 01/02/2024 12:55 PM - Nico Schottelius

- Status changed from In Progress to Rejected