Agenda and Minutes: x86 Community Call October 2018

No new items were added to the agenda. Minutes are added in blue. Closed ACTIONS in green.

September minutes were at
https://lists.xenproject.org/archives/html/xen-devel/2018-09/msg01822.html

Attendees (right now based on past attendees - delete/add as appropriate)

Lars Kurth
Wei Liu, George Dunlap, Paul Durrant, Sergey Dyasli, Andy Cooper, Roger Monee (Citrix)
Christopher Clark (OpenXT Project)
Doug Goldstein (Rackspace)
Rich Persaud (BAE Systems)
Brian Woods, Janakarajan Natarajan (AMD)
Tamas K Lengyel (AIS)
Daniel Smith (Apertus)
Jan Beulich, Juergen Gross (Suse)
Please add your name to this list, if you were present at the call and are not on the list

Admin Items

Daylight savings: when to have winter meetings

Option 1: If we keep the meeting at 14:00 - 15:00 UTC, meetings in the US and Europe will be one hour earlier, while the China will be at the same time
Option 2: If we move the meeting to 15:00 - 16:00 UTC during winter time, meetings in the US and Europe will stay the same, while the China will be at 23:00-24:00

ACTION: Lars to kick off a call with attendees, go with Option 2 if there is no input from Chinese vendors

Open / Closed Actions from Previous calls

- [Open] Lars to bring up x86 bottleneck at next AB call – due to the Aug holidays we didn't have any of the relevant vendors on the call. On the Sept call, we had a similar issue for different reasons. I have done a little bit of Analysis, which I am willing to share.
- [Defer this for now as necessary info has been obtained] Christopher will follow up on IRC/xen-devel@ re memory scrubbing

- [Open] Lars would be happy to start a discussion on IRC, then xen-devel and start tidying the JIRA instance up - discussed on IRC, but did not have time to play with Jira

Doug: would like to start tagging patch series with JIRA tickets
Andy: Bug fixing - probably not relevant; for development often 40 to 50 patches in total to implement - this would only really work, if we required JIRA tickets for bugs
Doug: also wanted to bring up bug tracking
Andy: a large number of stuff that shouldn't be tickets (wishlist items)

- [Closed] Juergen agreed to add Argo to the work tracking list for the 4.12 release
- [Closed] Lars to give Christopher write access to JIRA
- [Closed] Christopher to create a JIRA ticket for the Argo work, see https://xenproject.atlassian.net/browse/XEN-118

New Series / Series that need attention

Decide during the call/and or add your series prior to the meeting (include a link, title and name)

Jan:
x86: more power-efficient CPU parking
Blocked on HW vendors (aka Intel and AMD) - not in HW manual. That only applies to the last patch (aka 5). Andy says he has reviewed it, Jan disagrees. Patch 4

ACTION: Andy will double checked
ACTION Janek: will take a look and ask relevant people in AMD
ACTION: Lars to escalate Intel part to Susie Li / John Ji

x86/HVM: implement memory read caching

Was on George's list: will look at it after LinuxCon
Andy has an issue with the series: aka divergent direction from how HW behaves. Fully understand the reasons, but has reservations about the approach. Jan notes that alternative approach may be too heavy weight to implement.

Main issue Andy has is to do with function naming, which is potentially confusing.

All agreed that we need to fix the underlying bug. May need to break the tie. Issue is that Andy believes that the fix makes things worse, while Jan believes it makes things better.

Need to continue on xen-devel

x86emul: fixes, improvements, and beginnings of AVX512 support

Andy points out that a series like this takes almost a day to review, because of complexity and size (also of the manual). Issues with cross-correlating manual vs. emulator code, because code uses different names than manual. Renaming helpers helped a little a bit. Would be disappointing if we missed 4.12

ACTION: Need a separate discussion to come up with a workable approach and no-one has a good solution. Between George and Andy and bring back to xen-devel

Would be interesting for someone else to have a go at this. Looks like Intel will look at the series.

Release Planning

Also see https://lists.xenproject.org/archives/html/xen-devel/2018-10/msg00620.html (latest 4.12 Update)

- Last posting date: December 14th, 2018
  [as this is just before Christmas some maintainers might ask for an earlier last posting date if their Ack is needed]
- Hard code freeze: January 11th, 2019

Maintainer Responsiveness (Paul Durrant)

I think we should discuss maintainer responsiveness, specifically w.r.t. AMD IOMMU.
If we have to ping Suravee every time, this will take a very long time
Underlying issue is higher priority work
Brian: only Suravee can do reviews right now until Brian and Janek have picked up the skills
Andy: has in the past tried to separate out IOMMU work from general clean-up work (which others can review) - affects primarily Paul. Can upstream IOMMU stuff for Intel, but then the series is blocked until AMD. Can we somehow split this, but Jan doesn't want AMD to become a second class citizen.

How easy is it to split common and vendor => relatively straight forward

Nested virtualization testing (Tamas K Lengyel)

Looking for information on what type of testing is done for nested virtualization. According to the wiki (https://wiki.xenproject.org/wiki/Nested_Virtualization_in_Xen) there is a clear regression happening with new versions of Xen. However, my tests show that the regression is actually hardware related: nested Virtualbox & KVM works on 2nd gen i7 CPUs with Xen 4.11 but not on 6th gen i7 CPUs.

Andy: this has never worked reasonably well.
George: notes that most of the time this works fine ad-hoc, but not good enough for anything production.
Older CPUs: works fine. Newer CPUs definitely crashes. New HW features that are not implemented for nested: aka emulate or squash.

NIST Security Paper
(needs responses by the community by end of week)

I was pointed by Andy Cooper / Matthew Allen to https://csrc.nist.gov/CSRC/media/Publications/nistir/8221/draft/documents/nistir-8221-draft.pdf which is looking for public responses by the end of the week. Email: NISTIR8221@nist.gov

It is full of inaccuracies and problems. Matthew is planning to reply publicly on Citrix's behalf, but I think there are some issues with the Xen Project should address independently. To start with, there is a claim that Xen has far more CVEs than KVM which simply isn't true, and could be very damaging for us if it ends up in a non-draft NIST publication. There are also descriptions of bits of architecture in Xen which I've never come across.

Have come across it very recently: Chris is going to draft a response on behalf of Citrix. Any response is a matter of public record.

Not a general NIST paper: with small audience, these papers are often referenced in the commercial community. Title of forensics: paper said a lot of wrong things.

Makes sense to write a response (e.g. a wiki page with a few paragraphs this week) which can be evolved over time. Maybe pick out a few questions. Ask a few questions, don't put to much effort in it. Ask author to reference the wiki page.

ACTION: Lars set up wiki page and add to the minutes and respond to the call for feedback
See https://wiki.xenproject.org/wiki/Characterizing_Vulnerabilities_in_Platform_Security

AOB

- Lars was wondering who will be at KVM forum. Maybe we can get a Xen group together (although this is not strictly x86 related)
  Christopher Clark, Rich Persaud, Daniel Smith and Citrix folks attending => Lars to start a thread to coordinate a face-2-face meeting
- AMD Ryzen/EPYC machines for the Xen Project test lab: any recommendations as per specific CPU skews or will any do
  ACTION: Lars to email Brian & Jon Grimm
- Bug tracking (Doug)
  ACTION: Set up cross functional call