(https://www.intel.com/content/www/us/en/homepage.html)

Communities

Data Center

Intel Community Blogs Tech Innovation Data Center

78 Discussions

Advancing Open-Source Firmware on Intel® Xeon® 6 Based Platforms with coreboot

Subscribe

Article Options

shuoliu0

Employee

10-10-2024 66

Co-Authors:

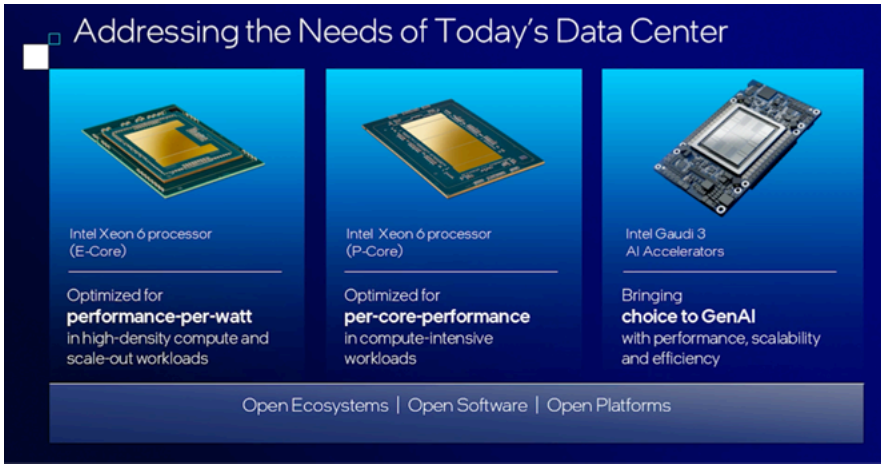
Nagendra Manickam, Director - Cloud Firmware Enabling

Vincent Zimmer, Senior Principal Engineer

Shui Liu, Firmware Architect

On September 24, 2024, Intel ushered in a new era of high-performance enterprise AI systems and solutions with the introduction of the Intel® Xeon® 6 processor. Intel's commitment to open-source innovation drives the software-defined infrastructure that has revolutionized modern data centers and powered the data-centric era. By fostering an open ecosystem, including in the firmware domain, Intel empowers customers to optimize workloads with enhanced performance, efficiency, and security. Collaboration with key industry partners remains crucial to achieving this vision.

Firmware plays a vital role in data centers by efficiently managing the interaction between Intel Xeon processors and server hardware, ensuring optimal performance and reliability. It enables precise control over system resources, power management, and security features critical for high-performance computing environments. With robust firmware, Intel Xeon processors deliver the stability and efficiency needed to support demanding workloads and maximize data center efficiency.



Addressing the Needs of Today's Data Center

Intel Xeon 6 processor (E-Core)

Optimized for **performance-per-watt** in high-density compute and scale-out workloads

Intel Xeon 6 processor (P-Core)

Optimized for **per-core-performance** in compute-intensive workloads

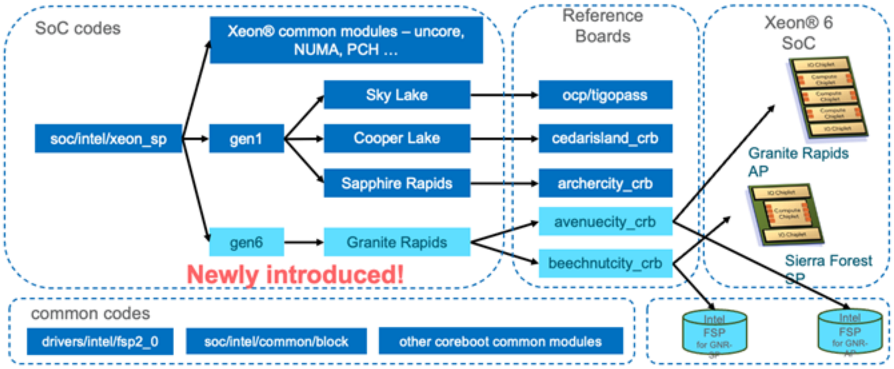
Intel Gaudi 3 AI Accelerators

Bringing **choice to GenAI** with performance, scalability and efficiency

Open Ecosystems | Open Software | Open Platforms

Partnering with 9elements to enable coreboot support on Intel Xeon 6 Processors

Intel is working with 9elements to develop an open-source firmware solution—coreboot, for platforms based on the Intel® Xeon® 6 processor using the Firmware Support Package (FSP). This collaboration significantly advances the adoption of coreboot in enterprise environments and aligns with the Open Compute Project's (OCP) Open Platform Firmware (OPF) vision. By integrating coreboot support, we aim to promote transparency, enhance security, and improve scalability in firmware development across the industry. By advancing coreboot adoption in enterprise environments, we are accelerating the transition of the x86 ecosystem toward open-source solutions. This empowers customers to optimize workloads with enhanced performance, efficiency, and security, fostering increased collaboration and innovation in the industry.



Why coreboot?

In today's dynamic enterprise environment, coreboot stands out as a solution that embraces the power of openness and collaboration—key factors in driving innovation.

coreboot - A Worthy Long-Term Investment

Community-Driven Innovation

Coreboot thrives on the power of collaboration, with over 1,000 contributors from companies like Intel, Google, and AMD. This open-source model mirrors Linux, creating a collective pool of knowledge and resources that continuously improve the firmware. The open ecosystem fosters rapid innovation, enabling enterprises to avoid vendor lock-in and benefit from shared expertise.

Streamlined Architecture for Efficient Boot

Compared to UEFI, coreboot uses a minimalist, modular architecture designed to boot systems faster by initializing only essential hardware components. Its monolithic code structure, much like Linux, allows for significant code reuse across different hardware generations, reducing complexity and maintenance overhead. By leveraging Linux as a bootloader via LinuxBoot, coreboot ensures faster boot times and improved system reliability.

Cost-Effective Scaling

The modular and open-source nature of coreboot offers enterprises the flexibility to scale without the heavy investment of proprietary firmware. Whether deploying small test systems or scaling across data centers, coreboot's adaptable framework ensures cost-effective growth, keeping capital expenditures low while maximizing efficiency.

Security and Transparency

Coreboot's transparency allows enterprises to thoroughly vet their firmware for vulnerabilities, ensuring faster patching and a smaller attack surface. Security features like measured boot, TPM, Intel® TXT, and CBnT are baked in, providing robust protection. Coreboot's response to vulnerabilities like CVE-2022-29264 showcases the open-source community's speed and effectiveness in addressing security issues.

Sustainability and Long-Term Maintainability

Coreboot promotes a sustainable approach by extending the lifespan of older hardware, reducing e-waste, and supporting a circular economy. Code enhancements often trickle down to older platforms, ensuring that legacy systems benefit from the latest developments. For example, improvements made for Granite Rapids platforms also enhance the performance and security of earlier generations like Sapphire Rapids and Skylake-SP.

Open Ecosystem and Flexibility

Coreboot's flexible open-source foundation empowers enterprises to take full control of their infrastructure. With support for multiple operating systems and payloads like U-root, businesses have the freedom to choose the best-fit solutions. This level of customization, combined with a robust ecosystem of developers, helps bridge the gap between prototypes and production, ensuring scalability and long-term growth.

Code Quality and Collaborative Standards

The benefits of upstream collaboration in coreboot extend beyond innovation. Code quality is maintained at a high standard as contributions undergo rigorous review from diverse stakeholders. For instance, the development of Granite Rapids led to a 30% reduction in code complexity, demonstrating the effectiveness of collaborative refinement (Granite Rapids example).

Intel Remains Committed to Open-Source First Strategy in Firmware Ecosystem

Intel has long championed open-source firmware, starting with the Xeon® Scalable Processor Gen 1 in partnership with Meta on the OCP Tioga Pass platform 4 years ago. This groundbreaking collaboration laid a strong foundation for open firmware systems in enterprise environments, marking the very first step toward a more transparent and controllable future for data centers (details here).

From the first Intel Xeon processor generation through the newest Intel Xeon 6 Scalable processor, Intel has steadily advanced its open-source strategy, investing a great amount of resources working together with the coreboot community, OEMs, and CSPs to drive greater adoption and innovation. While industry-wide integration takes time, Intel's collaborative approach has created a flexible, scalable firmware framework that will shape future data center infrastructure.

How to Get Started

Intel is doubling down on its commitment to open platforms and collaboration, and coreboot is a prime example of this. As detailed in our coreboot technical paper on Intel Xeon 4 and Xeon 5 platforms, coreboot simplifies the initialization process, making it easier than ever to start small and grow with your needs. It is a good starting point on leveraging its modular, open-source firmware to customize and scale based on their unique requirements.

With the introduction of Xeon-6 coreboot, we're excited to open the doors for evaluation. We invite OEMs, partners, and developers to join us in building a future where open-source firmware enables innovation and scalability. Let's shape an open, secure ecosystem—together.

You're invited to join Intel at the 2024 OCP Global Summit, October 15-17, in San Jose, CA.

Notices and Disclaimers

Performance varies by use, configuration, and other factors. Learn more on the Performance Index site.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Your costs and results may vary.

Intel technologies may require enabled hardware, software, or service activation.

Translate

0 Kudos

You must be a registered user to add a comment. If you've already registered, sign in. Otherwise, register and sign in.

Comment

Community support is provided Monday to Friday. Other contact methods are available here.

Intel does not verify all solutions, including but not limited to any file transfers that may appear in this community. Accordingly, Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

For more complete information about compiler optimizations, see our Optimization Notice.

Company Overview (https://www.intel.com/content/www/us/en/company-overview/company-overview.html)
Contact Intel (https://www.intel.com/content/www/us/en/support/contact-us.html)
Newsroom (https://www.intel.com/content/www/us/en/newsroom/home.html)
Investors (https://www.intc.com/)
Careers (https://www.intel.com/content/www/us/en/jobs/life-at-intel.html)
Corporate Responsibility (https://www.intel.com/content/www/us/en/corporate-responsibility/corporate-responsibility.html)
Diversity & Inclusion (https://www.intel.com/content/www/us/en/diversity/diversity-at-intel.html)
Public Policy (https://www.intel.com/content/www/us/en/company-overview/public-policy.html)

(https://www.facebook.com/Intel) (https://twitter.com/intel) (https://www.linkedin.com/company/intel-corporation) (https://www.youtube.co sub_confirmation=1)

Terms of Use (https://www.intel.com/content/www/us/en/legal/terms-of-use.html)
*Trademarks (https://www.intel.com/content/www/us/en/legal/trademarks.html)
Cookies (https://www.intel.com/content/www/us/en/privacy/intel-cookie-notice.html)
Privacy (https://www.intel.com/content/www/us/en/privacy/intel-privacy-notice.html)
Supply Chain Transparency (https://www.intel.com/content/www/us/en/corporate-responsibility/statement-combating-modern-slavery.html)
Site Map (https://www.intel.com/content/www/us/en/siteindex.html)
Recycling (https://www.intel.com/content/www/us/en/support/articles/000098122/services.html)
Your Privacy Choices ✓✗ (/#)
Notice at Collection (https://www.intel.com/content/www/us/en/privacy/privacy-residents-certain-states.html)

Intel technologies may require enabled hardware, software or service activation. // No product or component can be absolutely secure. // Your costs and results may vary. // Performance varies by use, configuration and other factors. // See our complete legal Notices and Disclaimers (https://edc.intel.com/content/www/us/en/products/performance/benchmarks/overview/#GUID-26B0C71C-25E9-477D-9007-52FCA56EE18C). // Intel is committed to respecting human rights and avoiding causing or contributing to adverse impacts on human rights. See Intel's Global Human Rights Principles (https://www.intel.com/content/www/us/en/policy/policy-human-rights.html). Intel's products and software are intended only to be used in applications that do not cause or contribute to adverse impacts on human rights.

intel (https://www.intel.com/content/www/us/en/homepage.html)