Intel Xeon Platinum 8358P processor

Artikel	131200
Herstellernummer	CD8068904599101
EAN	8592978314422

Intel

Intel® Trusted Execution Technology
Intel® Trusted Execution Technology for safer computing is a versatile set of hardware extensions to Intel® processors and chipsets that enhance the digital office platform with security capabilities such as measured launch and protected execution. It enables an environment where applications can run within their own space, protected from all other software on the system.

Intel® Virtualization Technology for Directed I/O (VT-d)
Intel® Virtualization Technology for Directed I/O (VT-d) continues from the existing support for IA-32 (VT-x) and Itanium® processor (VT-i) virtualization adding new support for I/O-device virtualization. Intel VT-d can help end users improve security and reliability of the systems and also improve performance of I/O devices in virtualized environments.

Intel® Virtualization Technology (VT-x)
Intel® Virtualization Technology (VT-x) allows one hardware platform to function as multiple “virtual” platforms. It offers improved manageability by limiting downtime and maintaining productivity by isolating computing activities into separate partitions.

Intel® 64
Intel® 64 architecture delivers 64-bit computing on server, workstation, desktop and mobile platforms when combined with supporting software.[1] Intel 64 architecture improves performance by allowing systems to address more than 4 GB of both virtual and physical memory.

Cache
CPU Cache is an area of fast memory located on the processor. Intel® Smart Cache refers to the architecture that allows all cores to dynamically share access to the last level cache.

Intel® AES New Instructions
Intel® AES New Instructions (Intel® AES-NI) are a set of instructions that enable fast and secure data encryption and decryption. AES-NI are valuable for a wide range of cryptographic applications, for example: applications that perform bulk encryption/decryption, authentication, random number generation, and authenticated encryption.

Intel® Turbo Boost Technology
Intel® Turbo Boost Technology dynamically increases the processor's frequency as needed by taking advantage of thermal and power headroom to give you a burst of speed when you need it, and increased energy efficiency when you don’t.

Max Turbo Frequency
Max Turbo Frequency is the maximum single-core frequency at which the processor is capable of operating using Intel® Turbo Boost Technology and, if present, Intel® Turbo Boost Max Technology 3.0 and Intel® Thermal Velocity Boost. Frequency is typically measured in gigahertz (GHz), or billion cycles per second.

Execute Disable Bit
Execute Disable Bit is a hardware-based security feature that can reduce exposure to viruses and malicious-code attacks and

prevent harmful software from executing and propagating on the server or network.

Intel® Hyper-Threading Technology
Intel® Hyper-Threading Technology (Intel® HT Technology) delivers two processing threads per physical core. Highly threaded applications can get more work done in parallel, completing tasks sooner.

Intel® VT-x with Extended Page Tables (EPT)
Intel® VT-x with Extended Page Tables (EPT), also known as Second Level Address Translation (SLAT), provides acceleration for memory intensive virtualized applications. Extended Page Tables in Intel® Virtualization Technology platforms reduces the memory and power overhead costs and increases battery life through hardware optimization of page table management.

Intel® Speed Shift Technology
Intel® Speed Shift Technology uses hardware-controlled P-states to deliver dramatically quicker responsiveness with single-threaded, transient (short duration) workloads, such as web browsing, by allowing the processor to more quickly select its best operating frequency and voltage for optimal performance and power efficiency.

Intel® Crypto Acceleration
Intel® Crypto Acceleration reduces the performance impact of pervasive encryption and increases the performance of encryption-intensive workloads including SSL web serving, 5G infrastructure, and VPN/firewalls.

Intel® Software Guard Extensions (Intel® SGX)
Intel® Software Guard Extensions (Intel® SGX) provide applications the ability to create hardware enforced trusted execution protection for their applications' sensitive routines and data. Intel® SGX provides developers a way to partition their code and data into CPU hardened trusted execution environments (TEE's).

Intel® Speed Select Technology – Core Power
Enables flexibility for workloads that benefit from higher base frequency on a subset of the processor's cores. While the max turbo frequency across the cores remain constant across the cores, a subset of the cores can be assigned as to run at a higher base frequency than specified, while the other cores run at lower base frequency.

Intel® Speed Select Technology – Turbo Frequency
Enables flexibility for workloads that benefit from higher turbo frequency on a subset of the processor's cores. While the base frequency remains constant across the cores, a subset of the cores can be assigned to run at a higher turbo frequency than specified, while the other cores run at lower turbo frequency.

Intel® Deep Learning Boost (Intel® DL Boost) on CPU
A new set of embedded processor technologies designed to accelerate AI deep learning use cases. It extends Intel AVX-512 with a new Vector Neural Network Instruction (VNNI) that significantly increases deep learning inference performance over previous generations.

Instruction Set Extensions
Instruction Set Extensions are additional instructions which can increase performance when the same operations are performed on multiple data objects. These can include SSE (Streaming SIMD Extensions) and AVX (Advanced Vector Extensions).

Intel® Run Sure Technology
Intel® Run Sure Technology, includes advanced RAS (reliability, availability and serviceability) features that deliver high reliability and platform resiliency, to maximize uptime of servers running mission-critical workloads.

Intel® Total Memory Encryption
TME – Total Memory Encryption (TME) helps protect data against exposure via physical attack on memory, such as cold-boot attacks.

Max # of UPI Links
Intel® Ultra Path Interconnect (UPI) links are a high speed, point-to-point interconnect bus between the processors, delivering increased bandwidth and performance over Intel® QPI.

# of AVX-512 FMA Units
Intel® Advanced Vector Extensions 512 (AVX-512), new instruction set extensions, delivering ultra-wide (512-bit) vector operations capabilities, with up to 2 FMAs (Fused Multiply Add instructions), to accelerate performance for your most demanding computational tasks.

Intel® Resource Director Technology (Intel® RDT)
Intel® RDT brings new levels of visibility and control over how shared resources such as last-level cache (LLC) and memory bandwidth are used by applications, virtual machines (VMs) and containers.

Intel® Volume Management Device (VMD)

Intel® Volume Management Device (VMD) provides a common, robust method of hot plug and LED management for NVMe-based solid state drives.

Intel® Optane™ Persistent Memory Supported
Intel® Optane™ persistent memory is a revolutionary tier of non-volatile memory that sits between memory and storage to provide large, affordable memory capacity that is comparable to DRAM performance. Delivering large system-level memory capacity when combined with traditional DRAM, Intel Optane persistent memory is helping transform critical memory constrained workloads – from cloud, databases, in-memory analytics, virtualization, and content delivery networks.

Mode-based Execute Control (MBEC)
Mode-based Execute Control can more reliably verify and enforce the integrity of kernel level code.

Intel® Transactional Synchronization Extensions
Intel® Transactional Synchronization Extensions (Intel® TSX) are a set of instructions that add hardware transactional memory support to improve performance of multi-threaded software.

Zusammenfassung

Intel® Trusted Execution Technology
Intel® Trusted Execution Technology for safer computing is a versatile set of hardware extensions to Intel® processors and chipsets that enhance the digital office platform with security capabilities such as measured launch and protected execution. It enables an environment where applications can run within their own space, protected from all other software on the system.

Intel® Virtualization Technology for Directed I/O (VT-d)
Intel® Virtualization Technology for Directed I/O (VT-d) continues from the existing support for IA-32 (VT-x) and Itanium® processor (VT-i) virtualization adding new support for I/O-device virtualization. Intel VT-d can help end users improve security and reliability of the systems and also improve performance of I/O devices in virtualized environments.

Intel® Virtualization Technology (VT-x)
Intel® Virtualization Technology (VT-x) allows one hardware platform to function as multiple “virtual” platforms. It offers improved manageability by limiting downtime and maintaining productivity by isolating computing activities into separate partitions.

Intel® 64
Intel® 64 architecture delivers 64-bit computing on server, workstation, desktop and mobile platforms when combined with supporting software.[1] Intel 64 architecture improves performance by allowing systems to address more than 4 GB of both virtual and physical memory.

Cache
CPU Cache is an area of fast memory located on the processor. Intel® Smart Cache refers to the architecture that allows all cores to dynamically share access to the last level cache.

Intel® AES New Instructions
Intel® AES New Instructions (Intel® AES-NI) are a set of instructions that enable fast and secure data encryption and decryption. AES-NI are valuable for a wide range of cryptographic applications, for example: applications that perform bulk encryption/decryption, authentication, random number generation, and authenticated encryption.

Intel® Turbo Boost Technology
Intel® Turbo Boost Technology dynamically increases the processor's frequency as needed by taking advantage of thermal and power headroom to give you a burst of speed when you need it, and increased energy efficiency when you don’t.

Max Turbo Frequency
Max Turbo Frequency is the maximum single-core frequency at which the processor is capable of operating using Intel® Turbo Boost Technology and, if present, Intel® Turbo Boost Max Technology 3.0 and Intel® Thermal Velocity Boost. Frequency is typically measured in gigahertz (GHz), or billion cycles per second.

Execute Disable Bit
Execute Disable Bit is a hardware-based security feature that can reduce exposure to viruses and malicious-code attacks and prevent harmful software from executing and propagating on the server or network.

Intel® Hyper-Threading Technology
Intel® Hyper-Threading Technology (Intel® HT Technology) delivers two processing threads per physical core. Highly threaded applications can get more work done in parallel, completing tasks sooner.

Intel® VT-x with Extended Page Tables (EPT)
Intel® VT-x with Extended Page Tables (EPT), also known as Second Level Address Translation (SLAT), provides acceleration for memory intensive virtualized applications. Extended Page Tables in Intel® Virtualization Technology platforms reduces the memory and power overhead costs and increases battery life through hardware optimization of page table management.

Intel® Speed Shift Technology
Intel® Speed Shift Technology uses hardware-controlled P-states to deliver dramatically quicker responsiveness with single-threaded, transient (short duration) workloads, such as web browsing, by allowing the processor to more quickly select its best operating frequency and voltage for optimal performance and power efficiency.

Intel® Crypto Acceleration
Intel® Crypto Acceleration reduces the performance impact of pervasive encryption and increases the performance of encryption-intensive workloads including SSL web serving, 5G infrastructure, and VPN/firewalls.

Intel® Software Guard Extensions (Intel® SGX)
Intel® Software Guard Extensions (Intel® SGX) provide applications the ability to create hardware enforced trusted execution protection for their applications' sensitive routines and data. Intel® SGX provides developers a way to partition their code and data into CPU hardened trusted execution environments (TEE's).

Intel® Speed Select Technology – Core Power
Enables flexibility for workloads that benefit from higher base frequency on a subset of the processor's cores. While the max turbo frequency across the cores remain constant across the cores, a subset of the cores can be assigned as to run at a higher base frequency than specified, while the other cores run at lower base frequency.

Intel® Speed Select Technology – Turbo Frequency
Enables flexibility for workloads that benefit from higher turbo frequency on a subset of the processor's cores. While the base frequency remains constant across the cores, a subset of the cores can be assigned to run at a higher turbo frequency than specified, while the other cores run at lower turbo frequency.

Intel® Deep Learning Boost (Intel® DL Boost) on CPU
A new set of embedded processor technologies designed to accelerate AI deep learning use cases. It extends Intel AVX-512 with a new Vector Neural Network Instruction (VNNI) that significantly increases deep learning inference performance over previous generations.

Instruction Set Extensions
Instruction Set Extensions are additional instructions which can increase performance when the same operations are performed on multiple data objects. These can include SSE (Streaming SIMD Extensions) and AVX (Advanced Vector Extensions).

Intel® Run Sure Technology
Intel® Run Sure Technology, includes advanced RAS (reliability, availability and serviceability) features that deliver high reliability and platform resiliency, to maximize uptime of servers running mission-critical workloads.

Intel® Total Memory Encryption
TME – Total Memory Encryption (TME) helps protect data against exposure via physical attack on memory, such as cold-boot attacks.

Max # of UPI Links
Intel® Ultra Path Interconnect (UPI) links are a high speed, point-to-point interconnect bus between the processors, delivering increased bandwidth and performance over Intel® QPI.

# of AVX-512 FMA Units
Intel® Advanced Vector Extensions 512 (AVX-512), new instruction set extensions, delivering ultra-wide (512-bit) vector operations capabilities, with up to 2 FMAs (Fused Multiply Add instructions), to accelerate performance for your most demanding computational tasks.

Intel® Resource Director Technology (Intel® RDT)
Intel® RDT brings new levels of visibility and control over how shared resources such as last-level cache (LLC) and memory bandwidth are used by applications, virtual machines (VMs) and containers.

Intel® Volume Management Device (VMD)
Intel® Volume Management Device (VMD) provides a common, robust method of hot plug and LED management for NVMe-based solid state drives.

Intel® Optane™ Persistent Memory Supported
Intel® Optane™ persistent memory is a revolutionary tier of non-volatile memory that sits between memory and storage to provide large, affordable memory capacity that is comparable to DRAM performance. Delivering large system-level memory capacity when combined with traditional DRAM, Intel Optane persistent memory is helping transform critical memory constrained workloads – from cloud,

databases, in-memory analytics, virtualization, and content delivery networks.

Mode-based Execute Control (MBEC)
Mode-based Execute Control can more reliably verify and enforce the integrity of kernel level code.

Intel® Transactional Synchronization Extensions
Intel® Transactional Synchronization Extensions (Intel® TSX) are a set of instructions that add hardware transactional memory support to improve performance of multi-threaded software.

Intel Xeon Platinum 8358P, Intel® Xeon® Platinum, LGA 4189, 10 nm, Intel, 8358P, 2.6 GHz

Intel Xeon Platinum 8358P. Processor family: Intel® Xeon® Platinum, Processor socket: LGA 4189, Processor lithography: 10 nm. Memory channels: Octa-channel, Maximum internal memory supported by processor: 6.14 TB, Memory types supported by processor: DDR4-SDRAM. Market segment: Server, Supported instruction sets: SSE4.2, AVX, AVX 2.0, AVX-512, Scalability: 2S. Maximum Enclave Size Support for Intel® SGX: 8 GB. Processor package size: 77.5 x 56.5 mm

Merkmale

Logistics data

Harmonized System (HS) code	85423119

Operational conditions

Tcase	80 °C

Other features

Maximum internal memory	6 TB

Weight & dimensions

Processor package size	77.5 x 56.5 mm

Graphics

On-board graphics card	No
Discrete graphics card	No
On-board graphics card model	Not available
Discrete graphics card model	Not available

Memory

Maximum internal memory supported by processor	6.14 TB
Memory types supported by processor	DDR4-SDRAM
Memory clock speeds supported by processor	3200 MHz
Memory channels	Octa-channel
ECC	Yes

Technical details

Target market	Cloud Computing
Launch date	Q2'21
Status	Launched
Supported memory types	DDR4-SDRAM
Memory speed (max)	3200 MHz
Number of UPI links	3
Servicing status	Baseline Servicing

Features

Execute Disable Bit	Yes
Market segment	Server
Maximum number of PCI Express lanes	64
PCI Express slots version	4.0
Supported instruction sets	SSE4.2, AVX, AVX 2.0, AVX-512
Scalability	2S
Embedded options available	No
Export Control Classification Number (ECCN)	5A992CN3
Commodity Classification Automated Tracking System (CCATS)	G178966

Processor

Processor manufacturer	Intel
Processor generation	3rd Generation Intel® Xeon® Scalable

Processor model	8358P
Processor base frequency	2.6 GHz
Processor family	Intel® Xeon® Platinum
Processor cores	32
Processor socket	LGA 4189
Component for	Server/workstation
Processor lithography	10 nm
Processor threads	64
System bus rate	11.2 GT/s
Processor operating modes	64-bit
Processor boost frequency	3.4 GHz
Processor cache	48 MB
Thermal Design Power (TDP)	240 W
Box	No
Cooler included	No
Processor codename	Ice Lake
Processor ARK ID	212308

Processor special features

Intel® Hyper Threading Technology (Intel® HT Technology)	Yes
Intel® Turbo Boost Technology	2.0
Intel® AES New Instructions (Intel® AES-NI)	Yes
Intel Trusted Execution Technology	Yes
Intel® Speed Shift Technology	Yes
Intel® Transactional Synchronization Extensions	Yes
Intel® Total Memory Encryption	Yes
Intel® Crypto Acceleration	Yes
Intel® Platform Firmware Resilience Support	Yes
Maximum Enclave Size Support for Intel® SGX	8 GB
Intel VT-x with Extended Page Tables (EPT)	Yes
Intel Software Guard Extensions (Intel SGX)	Yes
Intel 64	Yes
Intel Virtualization Technology (VT-x)	Yes
Intel Virtualization Technology for Directed I/O (VT-d)	Yes
Intel® Optane™ Memory Ready	Yes
AVX-512 Fused Multiply-Add (FMA) units	2
Intel® Deep Learning Boost (Intel® DL Boost) on CPU	Yes
Intel® Resource Director Technology (Intel® RDT)	Yes
Intel® Volume Management Device (VMD)	Yes
Intel® Run Sure Technology	Yes
Mode-based Execute Control (MBE)	Yes
Intel® Optane™ DC Persistent Memory Supported	Yes