# Intel Xeon 4216 processor


| | |
|---|---|
| **Artikel** | 111070 |
| **Herstellernummer** | CD8069504213901 |
| **EAN** | 5054444257112 |

Intel

**Intel® Turbo-Boost-Technik**

Die Intel® Turbo-Boost-Technik erhöht dynamisch die Frequenz eines Prozessors nach Bedarf, indem die Temperatur- und Leistungsreserven ausgenutzt werden, um bei Bedarf mehr Geschwindigkeit und andernfalls mehr Energieeffizienz zu bieten.

**Intel® vPro™ Plattformqualifizierung**

Intel® vPro™-Technik ist eine Zusammenstellung von Sicherheits- und Verwaltbarkeitsfunktionen, die in den Prozessor integriert sind und vier kritische Bereiche in der IT-Sicherheit handhaben: 1) Bedrohungsverwaltung, darunter Schutz vor Rootkits, Viren und Malware, 2) Schutz von Identitäten und Website-Zugriffspunkten, 3) Schutz von vertraulichen persönlichen und geschäftlichen Daten, 4) Remote- und lokale Überwachung, Korrektur und Reparatur von PCs und Workstations.

**Intel® Hyper-Threading-Technik**

Die Intel® Hyper-Threading-Technik ermöglicht zwei Verarbeitungs-Threads pro physischem Kern. Anwendungen mit vielen Threads können mehr Aufgaben parallel erledigen und Tasks früher beenden.

**Intel® Virtualisierungstechnik (VT-x)**

Mit der Intel® Virtualisierungstechnik (VT-x) kann eine Hardwareplattform als mehrere „virtuelle“ Plattformen eingesetzt werden. Sie bietet verbesserte Verwaltbarkeit durch weniger Ausfallzeiten und eine Beibehaltung der Produktivität, indem die Rechenvorgänge in separate Partitionen verschoben werden.

**Intel® Directed-I/O-Virtualisierungstechnik (VT-d)**

Die Intel® Directed-I/O-Virtualisierungstechnik (VT-d) setzt die bestehende Unterstützung von Virtualisierungslösungen für die IA-32 (VT-x) und Systeme mit Itanium® Prozessoren (VT-i) fort und erweitert diese um neue Unterstützung für die I/O-Gerätevirtualisierung. Die Intel VT-d kann Benutzern helfen, die Sicherheit und Zuverlässigkeit von Systemen sowie die Leistung von I/O-Geräten in virtualisierten Umgebungen zu verbessern.

**Intel® VT-x mit Extended Page Tables (EPT)**

Intel® VT-x mit Extended Page Tables (EPT), auch bekannt als Second Level Address Translation (SLAT), beschleunigt speicherintensive Virtualisierungsanwendungen. Der Einsatz von Extended Page Tables bei Plattformen mit Intel® Virtualisierungstechnik reduziert die Gesamtkosten für Speicher und Stromversorgung und erhöht die Akkulaufzeit durch Hardwareoptimierung der Seitentabellenverwaltung.

**Intel® TSX-NI**

Bei den Intel® Transactional Synchronization Extensions New Instructions (Intel® TSX-NI) handelt es sich um eine Reihe von Anweisungen für die Multithread-Leistungsskalierung. Diese Technik verbessert die Effizienz bei parallelen Vorgängen durch die verbesserte Steuerung von Locks in Software.

**Intel® 64**

In Verbindung mit der entsprechenden Software ermöglicht die Intel® 64 Architektur die 64-Bit-Verarbeitung bei Servern, Workstations, PCs und Mobilplattformen.[1] Intel 64 verbessert die Leistung, da das System durch diese Prozessorerweiterung mehr als 4 GB virtuellen und physischen Speicher adressieren kann.

**Befehlssatz**

Ein Befehlssatz bezeichnet den Satz grundlegender Befehle und Anweisungen, die ein Mikroprozessor versteht und ausführen kann. Der angezeigte Wert gibt an, mit welchem Intel Befehlssatz dieser Prozessor kompatibel ist.

**Erweiterungen des Befehlssatzes**

Befehlssatzerweiterungen sind zusätzliche Anweisungen zur Erhöhung der Leistung, wenn die gleichen Vorgänge auf mehreren Datenobjekten ausgeführt werden. Diese können SSE (Streaming SIMD Extensions) und AVX (Advanced Vector Extensions) umfassen.

**Anzahl der AVX-512 FMA-Einheiten**

Intel® Advanced Vector Extensions 512 (AVX-512) sind neue Anleitungssatzerweiterungen, die Ultra-Breitband (512 Bit) Vektorbetriebsfunktionalitäten mit bis zu 2 FMAs („Fused Multiply Add“-Anweisungen) zur Beschleunigung Ihrer anspruchsvollsten rechnergestützten Aufgaben bieten.

**Erweiterte Intel SpeedStep® Technologie**

Die Erweiterte Intel SpeedStep® Technologie ist eine fortschrittliche Funktionalität für die auf Mobilgeräten benötigte Kombination von hoher Leistung bei einem möglichst niedrigen Energieverbrauch. Die herkömmliche Intel SpeedStep® Technologie schaltet die Spannung und die Frequenz je nach Prozessorauslastung gleichzeitig zwischen hohen und niedrigen Werten um. Die Erweiterte Intel SpeedStep® Technologie baut auf dieser Architektur auf und nutzt Designstrategien wie Trennung zwischen Spannungs- und Frequenzänderungen sowie Taktpartitionierung und Wiederherstellung.

**Intel® Speed Shift Technology**

Die Intel® Speed Shift Technology nutzt hardware-gesteuerte P-Stati, um mit vorübergehenden Single-Thread-Workloads von kurzer Dauer (wie beim Browsen im Internet) eine bedeutend schnellere Reaktionszeit zu erzielen. Dazu wird es dem Prozessor ermöglicht, die jeweils beste Betriebsfrequenz und Spannung zu wählen, um optimale Leistung und Energieeffizienz zu erzielen.

**Intel® Deep Learning Boost (Intel® DL Boost)**

Ein neuer Satz mit Embedded-Prozessor-Technologien zur Beschleunigung von KI-Deep-Learning-Anwendungsfällen. Damit wird Intel AVX-512 mit einer neuen VNNI (Vector Neural Network Instruction) erweitert, welche die Deep-Learning-Leistung im Vergleich zu früheren Generationen bedeutend verbessert.

**Intel® Resource Director Technology (Intel® RDT)**

Intel® Resource Director Technology (Intel® RDT) ermöglicht bessere Transparenz und Kontrolle der Verwendung gemeinsam genutzter Ressourcen durch Anwendungen, virtuelle Maschinen (VMs) und Container – zum Beispiel Last-Level-Cache (LLC) und Speicherbandbreite.

**Intel® Volume Management Device (VMD)**

Intel® Volume Management Device (VMD) bietet eine allgemeine, robuste Hot-Plug- und LED-Management-Methode für NVME-Solid-State-Laufwerke.

## Zusammenfassung

---

**Intel® Turbo-Boost-Technik**

Die Intel® Turbo-Boost-Technik erhöht dynamisch die Frequenz eines Prozessors nach Bedarf, indem die Temperatur- und

Leistungsreserven ausgenutzt werden, um bei Bedarf mehr Geschwindigkeit und andernfalls mehr Energieeffizienz zu bieten.

**Intel® vPro™ Plattformqualifizierung**

Intel® vPro™-Technik ist eine Zusammenstellung von Sicherheits- und Verwaltbarkeitsfunktionen, die in den Prozessor integriert sind und vier kritische Bereiche in der IT-Sicherheit handhaben: 1) Bedrohungsverwaltung, darunter Schutz vor Rootkits, Viren und Malware, 2) Schutz von Identitäten und Website-Zugriffspunkten, 3) Schutz von vertraulichen persönlichen und geschäftlichen Daten, 4) Remote- und lokale Überwachung, Korrektur und Reparatur von PCs und Workstations.

**Intel® Hyper-Threading-Technik**

Die Intel® Hyper-Threading-Technik ermöglicht zwei Verarbeitungs-Threads pro physischem Kern. Anwendungen mit vielen Threads können mehr Aufgaben parallel erledigen und Tasks früher beenden.

**Intel® Virtualisierungstechnik (VT-x)**

Mit der Intel® Virtualisierungstechnik (VT-x) kann eine Hardwareplattform als mehrere „virtuelle“ Plattformen eingesetzt werden. Sie bietet verbesserte Verwaltbarkeit durch weniger Ausfallzeiten und eine Beibehaltung der Produktivität, indem die Rechenvorgänge in separate Partitionen verschoben werden.

**Intel® Directed-I/O-Virtualisierungstechnik (VT-d)**

Die Intel® Directed-I/O-Virtualisierungstechnik (VT-d) setzt die bestehende Unterstützung von Virtualisierungslösungen für die IA-32 (VT-x) und Systeme mit Itanium® Prozessoren (VT-i) fort und erweitert diese um neue Unterstützung für die I/O-Gerätevirtualisierung. Die Intel VT-d kann Benutzern helfen, die Sicherheit und Zuverlässigkeit von Systemen sowie die Leistung von I/O-Geräten in virtualisierten Umgebungen zu verbessern.

**Intel® VT-x mit Extended Page Tables (EPT)**

Intel® VT-x mit Extended Page Tables (EPT), auch bekannt als Second Level Address Translation (SLAT), beschleunigt speicherintensive Virtualisierungsanwendungen. Der Einsatz von Extended Page Tables bei Plattformen mit Intel® Virtualisierungstechnik reduziert die Gesamtkosten für Speicher und Stromversorgung und erhöht die Akkulaufzeit durch Hardwareoptimierung der Seitentabellenverwaltung.

**Intel® TSX-NI**

Bei den Intel® Transactional Synchronization Extensions New Instructions (Intel® TSX-NI) handelt es sich um eine Reihe von Anweisungen für die Multithread-Leistungsskalierung. Diese Technik verbessert die Effizienz bei parallelen Vorgängen durch die verbesserte Steuerung von Locks in Software.

**Intel® 64**

In Verbindung mit der entsprechenden Software ermöglicht die Intel® 64 Architektur die 64-Bit-Verarbeitung bei Servern, Workstations, PCs und Mobilplattformen.[1] Intel 64 verbessert die Leistung, da das System durch diese Prozessorerweiterung mehr als 4 GB virtuellen und physischen Speicher adressieren kann.

**Befehlssatz**

Ein Befehlssatz bezeichnet den Satz grundlegender Befehle und Anweisungen, die ein Mikroprozessor versteht und ausführen kann. Der angezeigte Wert gibt an, mit welchem Intel Befehlssatz dieser Prozessor kompatibel ist.

**Erweiterungen des Befehlssatzes**

Befehlssatzerweiterungen sind zusätzliche Anweisungen zur Erhöhung der Leistung, wenn die gleichen Vorgänge auf mehreren Datenobjekten ausgeführt werden. Diese können SSE (Streaming SIMD Extensions) und AVX (Advanced Vector Extensions) umfassen.

**Anzahl der AVX-512 FMA-Einheiten**

Intel® Advanced Vector Extensions 512 (AVX-512) sind neue Anleitungssatzerweiterungen, die Ultra-Breitband (512 Bit) Vektorbetriebsfunktionalitäten mit bis zu 2 FMAs („Fused Multiply Add“-Anweisungen) zur Beschleunigung Ihrer anspruchsvollsten rechnergestützten Aufgaben bieten.

**Erweiterte Intel SpeedStep® Technologie**

Die Erweiterte Intel SpeedStep® Technologie ist eine fortschrittliche Funktionalität für die auf Mobilgeräten benötigte Kombination von

hoher Leistung bei einem möglichst niedrigen Energieverbrauch. Die herkömmliche Intel SpeedStep® Technologie schaltet die Spannung und die Frequenz je nach Prozessorauslastung gleichzeitig zwischen hohen und niedrigen Werten um. Die Erweiterte Intel SpeedStep® Technologie baut auf dieser Architektur auf und nutzt Designstrategien wie Trennung zwischen Spannungs- und Frequenzänderungen sowie Taktpartitionierung und Wiederherstellung.

**Intel® Speed Shift Technology**

Die Intel® Speed Shift Technology nutzt hardware-gesteuerte P-Stati, um mit vorübergehenden Single-Thread-Workloads von kurzer Dauer (wie beim Browsen im Internet) eine bedeutend schnellere Reaktionszeit zu erzielen. Dazu wird es dem Prozessor ermöglicht, die jeweils beste Betriebsfrequenz und Spannung zu wählen, um optimale Leistung und Energieeffizienz zu erzielen.

**Intel® Deep Learning Boost (Intel® DL Boost)**

Ein neuer Satz mit Embedded-Prozessor-Technologien zur Beschleunigung von KI-Deep-Learning-Anwendungsfällen. Damit wird Intel AVX-512 mit einer neuen VNNI (Vector Neural Network Instruction) erweitert, welche die Deep-Learning-Leistung im Vergleich zu früheren Generationen bedeutend verbessert.

**Intel® Resource Director Technology (Intel® RDT)**

Intel® Resource Director Technology (Intel® RDT) ermöglicht bessere Transparenz und Kontrolle der Verwendung gemeinsam genutzter Ressourcen durch Anwendungen, virtuelle Maschinen (VMs) und Container – zum Beispiel Last-Level-Cache (LLC) und Speicherbandbreite.

**Intel® Volume Management Device (VMD)**

Intel® Volume Management Device (VMD) bietet eine allgemeine, robuste Hot-Plug- und LED-Management-Methode für NVME-Solid-State-Laufwerke.

Intel Xeon 4216, Intel® Xeon Silver, LGA 3647 (Socket P), 14 nm, Intel, 2,1 GHz, 64-Bit

Intel Xeon 4216. Prozessorfamilie: Intel® Xeon Silver, Prozessorsockel: LGA 3647 (Socket P), Prozessor Lithografie: 14 nm. Speicherkanäle: Hexa-Kanal, Maximaler interner Speicher, vom Prozessor unterstützt: 1,02 TB, Speichertypen, vom Prozessor unterstützt: DDR4-SDRAM. Marktsegment: Server, Unterstützte Befehlssätze: SSE4.2, AVX, AVX 2.0, AVX-512, Skalierbarkeit: 2S. Verpackungsbreite: 43 mm, Verpackungstiefe: 137 mm, Verpackungshöhe: 112 mm. Prozessor-Paketgröße: 76mm x 56.5mm

## Merkmale

### Betriebsbedingungen

| | |
|---|---|
| Tcase | 79 °C |

### Gewicht und Abmessungen

| | |
|---|---|
| Prozessor-Paketgröße | 76mm x 56.5mm |

### Logistikdaten

| | |
|---|---|
| Warentarifnummer (HS) | 85423119 |

### Sonstige Funktionen

| | |
|---|---|
| RAM-Speicher maximal | 1 TB |

### Grafik

| | |
|---|---|
| Eingebaute Grafikadapter | Nein |
| Separater Grafikadapter | Nein |

### Verpackungsdaten

| | |
|---|---|
| Verpackungsbreite | 43 mm |
| Verpackungstiefe | 137 mm |
| Verpackungshöhe | 112 mm |
| Paketgewicht | 201 g |
| Verpackungsart | Einzelhandels-Box |

### Technische Details

| | |
|---|---|
| Startdatum | Q2'19 |
| Produkttyp | Processor |
| Status | Launched |
| Unterstützte Arbeitsspeicher | DDR4-SDRAM |
| Speichergeschwindigkeit (max.) | 2400 MHz |
| Anzahl der UPI-Links | 2 |
| Instandhaltungsstatus | Baseline Servicing |

### Merkmale

| | |
|---|---|
| Execute Disable Bit | Ja |
| Marktsegment | Server |
| Maximale Anzahl der PCI-Express-Lanes | 48 |

| | |
|---|---|
| On-Board Grafikadaptermodell | Nicht verfügbar |
| Dediziertes Grafikadaptermodell | Nicht verfügbar |

## Speicher

| | |
|---|---|
| Maximaler interner Speicher, vom Prozessor unterstützt | 1,02 TB |
| Speichertypen, vom Prozessor unterstützt | DDR4-SDRAM |
| Speichertaktraten, vom Prozessor unterstützt | 2400 MHz |
| Speicherkanäle | Hexa-Kanal |
| ECC | Ja |

| | |
|---|---|
| PCI-Express-Slots-Version | 3.0 |
| Unterstützte Befehlssätze | SSE4.2, AVX, AVX 2.0, AVX-512 |
| Skalierbarkeit | 2S |
| Eingebettete Optionen verfügbar | Ja |
| PCI Express CEM Revision | 3.0 |
| Exportkontroll-Klassifizierungsnummer (ECCN) | 5A992C |
| Warenklassifizierungssystem zur automatisierten Nachverfolgung (CCATS) | G077159 |

## Prozessor

| | |
|---|---|
| Prozessorhersteller | Intel |
| Prozessorgeneration | Skalierbare Intel® Xeon® der 2. Generation |
| Prozessor | 4216 |
| Grundfrequenz des Prozessors | 2,1 GHz |
| Prozessorfamilie | Intel® Xeon Silver |
| Anzahl Prozessorkerne | 16 |
| Prozessorsockel | LGA 3647 (Socket P) |
| Komponente für | Server/Arbeitsstation |
| Prozessor Lithografie | 14 nm |
| Prozessor-Threads | 32 |
| Prozessorbetriebsmodi | 64-Bit |
| Prozessor Boost-Frequenz | 3,2 GHz |
| Prozessor-Cache | 22 MB |
| Thermal Design Power (TDP) | 100 W |
| Box | Nein |
| Kühler enthalten | Nein |
| Prozessor Codename | Cascade Lake |
| ARK Prozessorerkennung | 193394 |

## Prozessor Besonderheiten

| | |
|---|---|
| Intel® Hyper-Threading-Technik (Intel® HT Technology) | Ja |
| Intel® Turbo-Boost-Technologie | 2.0 |
| Intel® AES New Instructions (Intel® AES-NI) | Ja |
| Verbesserte Intel SpeedStep Technologie | Ja |
| Intel® Trusted-Execution-Technik | Ja |
| Intel®-Speed-Shift-Technologie | Ja |
| Intel® Transactional Synchronization Extensions | Ja |
| Intel® VT-x mit Extended Page Tables (EPT) | Ja |
| Intel® TSX-NI | Ja |
| Intel® 64 | Ja |
| Intel® Virtualization Technologie (VT-X) | Ja |
| Intel® Virtualisierungstechnik für direkte I/O (VT-d) | Ja |
| Intel Turbo Boost Max Technology 3.0 | Nein |
| AVX-512 Abgesicherte Multiply-Add (FMA) Einheiten | 1 |
| Intel® Deep Learning Boost (Intel® DL Boost) | Ja |
| Intel® Speed Select-Technologie - Leistungsprofil (Intel® SST-PP) | Nein |
| Intel® Resource Director | Ja |

| | |
|---|---|
| Technology (Intel® RDT) | |
| Intel® Volume Management Device (VMD) | Ja |
| Intel® Run Sure Technology | Nein |
| Modusbasierte Execute Control (MBE) | Ja |
| Intel® Optane™ DC Persistent Memory unterstützt | Nein |
| Intel® vPro™ Platform Eligibility | Ja |
| Intel Speed Select Technology (SST) | Nein |
| Intel® Speed Select Technology - Base Frequency (Intel® SST-BF) | Nein |
| Intel® Optane™ DC Persistent Memory-Technologie | Nein |