

Intel Xeon E-2336 processor



Artikel	127065
Herstellernummer	CM8070804495816
EAN	8592978334604
Intel	

Intel® Trusted-Execution-Technik

Die Intel® Trusted-Execution-Technik erhöht die Sicherheit von PCs. Sie umfasst eine Reihe von Hardware-Erweiterungen für Intel® Prozessoren und Chipsätze, die zusätzliche Sicherheitsfunktionen für die digitale Büroplattform bereitstellen, wie das sichere Starten von Systemprogrammen und des Betriebssystems und das Ausführen von Anwendungen in einem geschützten Bereich. Dies ermöglicht eine Umgebung, in der Anwendungen auf einem eigenen, von aller anderen Software des Systems abgeschotteten Bereich ausgeführt 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® 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® 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.

Cache

Der CPU-Cache ist ein Bereich des schnellen Speichers, der sich im Prozessor befindet. Intel® Smart-Cache bezieht sich auf die Architektur, die ermöglicht, dass alle Kerne den Zugriff auf den Last-Level-Cache dynamisch teilen.

Intel® AES New Instructions

Intel® AES New Instructions (Intel® AES-NI) ist eine Zusammenstellung von Anweisungen zur schnellen und sicheren Verschlüsselung und Entschlüsselung von Daten. AES-NI sind wertvolle Komponenten für kryptografische Anwendungen, z. B. für: Anwendungen zur Massenverschlüsselung/-entschlüsselung, Authentifizierung, Generierung von zufälligen Nummern und Authentifizierungsverschlüsselung.

Ruhezustände

Ruhezustände (C-Zustände) werden genutzt, um Energie zu sparen, wenn der Prozessor sich im Leerlauf befindet. C0 ist der Betriebszustand, d. h. die CPU führt sinnvolle Aufgaben aus. C1 ist der erste Leerlaufzustand, C2 der zweite usw., wobei für höhere Nummern des C-Zustands mehr Energiesparmaßnahmen durchgeführt werden.

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.

Max. Turbo-Taktfrequenz

Die max. Turbo-Taktfrequenz ist die maximale Taktfrequenz eines einzelnen Prozessorkerns, mit der der Prozessor unter Verwendung der Intel® Turbo-Boost-Technik und, falls vorhanden, der Intel® Turbo-Boost-Max-Technik 3.0 und des Intel® Thermal Velocity Boost arbeiten kann. Die Frequenz wird gewöhnlich in Gigahertz (GHz) gemessen bzw. in Milliarden von Taktzyklen pro Sekunde.

Execute-Disable-Bit

Die Execute-Disable-Bit ist eine hardwarebasierte Sicherheitsfunktion, die das Risiko von Vireninfectionen verringert und verhindern kann, dass bösartige Software auf dem Server bzw. im Netzwerk ausgeführt wird.

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.

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.

Intel® vPro™ Plattformqualifizierung

Die Intel vPro® Plattform ist eine Reihe von Hardware- und Technologien, die zum Erstellen von Business-Computing-Endpunkten mit erstklassiger Leistung, integrierter Sicherheit, moderner Verwaltbarkeit und Plattformstabilität verwendet werden.

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.

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.

Secure Key

Intel® Secure Key basiert auf einem digitalen Zufallszahlengenerator, der vollkommen zufällige Zahlen generiert und so Verschlüsselungsalgorithmen stärkt.

Intel® Turbo-Boost-Technik 2.0 Taktfrequenz

Die Taktfrequenz von Intel® Turbo-Boost-Technik 2.0 ist die maximale Taktfrequenz eines einzelnen Prozessorkerns, mit der der Prozessor mit Intel® Turbo-Boost-Technik betrieben werden kann. Die Frequenz wird gewöhnlich in Gigahertz (GHz) gemessen bzw. in Milliarden von Taktzyklen pro Sekunde.

Intel® Software Guard Extensions (Intel® SGX)

Die Intel® Software Guard Extensions (Intel® SGX) geben Anwendungen die Möglichkeit, einen per Hardware durchgesetzten Trusted-Execution-Schutz für deren sensible Routinen und Daten einzurichten. Intel® SGX bietet Entwicklern eine Möglichkeit, Code und Daten in von der CPU gesicherten vertrauenswürdigen Umgebungen für die Programmausführung (Trusted Execution Environments, TEEs) zu partitionieren.

Befehlssatzerweiterungen

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.

Thermal-Monitoring-Technologien

Thermal-Monitoring-Technologien schützen das Prozessorkern und das System über Temperaturverwaltungsfunktionen vor temperaturbedingten Ausfällen. Ein digitaler Temperatursensor auf dem Chip erkennt die Temperatur des Kerns, und die Temperaturverwaltungsfunktionen senken bei Bedarf den Energieverbrauch des Pakets und damit die Temperatur, um die Grenzwerte für den normalen Betrieb einzuhalten.

Persistenter Intel® Optane™ DC Speicher unterstützt

Der persistente Intel® Optane™ DC Speicher stellt eine revolutionäre Ebene von nichtflüchtigem Speicher dar, der zwischen dem

Arbeits- und Datenspeicher angesiedelt ist, um eine große und kostengünstige Speicherkapazität zu liefern, die mit DRAM-Leistung vergleichbar ist. Dank der großen Speicherkapazität auf Systemebene bei Kombination mit traditionellem DRAM unterstützt der persistente Intel Optane DC Speicher die Wandlung von Workloads mit beschränktem Speicher: Cloud, Datenbanken, In-Memory-Analysen, Virtualisierung und CDN-Anwendungen (Netzwerke zur Inhaltsbereitstellung).

Intel® Memory Protection Extensions (Intel® MPX)

Intel® Memory Protection Extensions (Intel® MPX) bieten eine Ansammlung von Hardwarefunktionen, die zusammen mit Compiler-änderungen von der Software zur Überprüfung verwendet werden können, dass Speicherreferenzen, die bei der Kompilierung eingesetzt werden, während der Laufzeit nicht aufgrund eines Pufferüberlaufs oder -unterlaufs unsicher werden.

Intel® Boot Guard

Die Intel® Device Protection Technology mit Boot Guard trägt zum Schutz der Umgebung vor Viren und böartigen Softwareangriffen vor der Aktivierung des Betriebssystems bei.

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.

Zusammenfassung

Intel® Trusted-Execution-Technik

Die Intel® Trusted-Execution-Technik erhöht die Sicherheit von PCs. Sie umfasst eine Reihe von Hardware-Erweiterungen für Intel® Prozessoren und Chipsätze, die zusätzliche Sicherheitsfunktionen für die digitale Büroplattform bereitstellen, wie das sichere Starten von Systemprogrammen und des Betriebssystems und das Ausführen von Anwendungen in einem geschützten Bereich. Dies ermöglicht eine Umgebung, in der Anwendungen auf einem eigenen, von aller anderen Software des Systems abgeschotteten Bereich ausgeführt 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® 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 Rechengvorgänge in separate Partitionen verschoben werden.

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.

Cache

Der CPU-Cache ist ein Bereich des schnellen Speichers, der sich im Prozessor befindet. Intel® Smart-Cache bezieht sich auf die Architektur, die ermöglicht, dass alle Kerne den Zugriff auf den Last-Level-Cache dynamisch teilen.

Intel® AES New Instructions

Intel® AES New Instructions (Intel® AES-NI) ist eine Zusammenstellung von Anweisungen zur schnellen und sicheren Verschlüsselung und Entschlüsselung von Daten. AES-NI sind wertvolle Komponenten für kryptografische Anwendungen, z. B. für: Anwendungen zur Massenverschlüsselung/-entschlüsselung, Authentifizierung, Generierung von zufälligen Nummern und Authentifizierungsverschlüsselung.

Ruhezustände

Ruhezustände (C-Zustände) werden genutzt, um Energie zu sparen, wenn der Prozessor sich im Leerlauf befindet. C0 ist der Betriebszustand, d. h. die CPU führt sinnvolle Aufgaben aus. C1 ist der erste Leerlaufzustand, C2 der zweite usw., wobei für höhere Nummern des C-Zustands mehr Energiesparmaßnahmen durchgeführt werden.

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.

Max. Turbo-Taktfrequenz

Die max. Turbo-Taktfrequenz ist die maximale Taktfrequenz eines einzelnen Prozessorkerns, mit der der Prozessor unter Verwendung der Intel® Turbo-Boost-Technik und, falls vorhanden, der Intel® Turbo-Boost-Max-Technik 3.0 und des Intel® Thermal Velocity Boost arbeiten kann. Die Frequenz wird gewöhnlich in Gigahertz (GHz) gemessen bzw. in Milliarden von Taktzyklen pro Sekunde.

Execute-Disable-Bit

Die Execute-Disable-Bit ist eine hardwarebasierte Sicherheitsfunktion, die das Risiko von Vireneinfektionen verringert und verhindern kann, dass bösartige Software auf dem Server bzw. im Netzwerk ausgeführt wird.

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.

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.

Intel® vPro™ Plattformqualifizierung

Die Intel vPro® Plattform ist eine Reihe von Hardware- und Technologien, die zum Erstellen von Business-Computing-Endpunkten mit erstklassiger Leistung, integrierter Sicherheit, moderner Verwaltbarkeit und Plattformstabilität verwendet werden.

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.

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.

Secure Key

Intel® Secure Key basiert auf einem digitalen Zufallszahlengenerator, der vollkommen zufällige Zahlen generiert und so Verschlüsselungsalgorithmen stärkt.

Intel® Turbo-Boost-Technik 2.0 Taktfrequenz

Die Taktfrequenz von Intel® Turbo-Boost-Technik 2.0 ist die maximale Taktfrequenz eines einzelnen Prozessorkerns, mit der der Prozessor mit Intel® Turbo-Boost-Technik betrieben werden kann. Die Frequenz wird gewöhnlich in Gigahertz (GHz) gemessen bzw. in Milliarden von Taktzyklen pro Sekunde.

Intel® Software Guard Extensions (Intel®SGX)

Die Intel® Software Guard Extensions (Intel® SGX) geben Anwendungen die Möglichkeit, einen per Hardware durchgesetzten Trusted-Execution-Schutz für deren sensible Routinen und Daten einzurichten. Intel® SGX bietet Entwicklern eine Möglichkeit, Code und Daten in von der CPU gesicherten vertrauenswürdigen Umgebungen für die Programmausführung (Trusted Execution Environments, TEEs) zu partitionieren.

Befehlssatzerweiterungen

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.

Thermal-Monitoring-Technologien

Thermal-Monitoring-Technologien schützen das Prozessorpaket und das System über Temperaturverwaltungsfunktionen vor temperaturbedingten Ausfällen. Ein digitaler Temperatursensor auf dem Chip erkennt die Temperatur des Kerns, und die Temperaturverwaltungsfunktionen senken bei Bedarf den Energieverbrauch des Pakets und damit die Temperatur, um die Grenzwerte für den normalen Betrieb einzuhalten.

Persistenter Intel® Optane™ DC Speicher unterstützt

Der persistente Intel® Optane™ DC Speicher stellt eine revolutionäre Ebene von nichtflüchtigem Speicher dar, der zwischen dem Arbeits- und Datenspeicher angesiedelt ist, um eine große und kostengünstige Speicherkapazität zu liefern, die mit DRAM-Leistung vergleichbar ist. Dank der großen Speicherkapazität auf Systemebene bei Kombination mit traditionellem DRAM unterstützt der persistente Intel Optane DC Speicher die Wandlung von Workloads mit beschränktem Speicher: Cloud, Datenbanken, In-Memory-Analysen, Virtualisierung und CDN-Anwendungen (Netzwerke zur Inhaltsbereitstellung).

Intel® Memory Protection Extensions (Intel® MPX)

Intel® Memory Protection Extensions (Intel® MPX) bieten eine Ansammlung von Hardwarefunktionen, die zusammen mit Compiler-änderungen von der Software zur Überprüfung verwendet werden können, dass Speicherreferenzen, die bei der Kompilierung eingesetzt werden, während der Laufzeit nicht aufgrund eines Pufferüberlaufs oder -unterlaufs unsicher werden.

Intel® Boot Guard

Die Intel® Device Protection Technology mit Boot Guard trägt zum Schutz der Umgebung vor Viren und böswilligen Softwareangriffen vor der Aktivierung des Betriebssystems bei.

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 Xeon® E-2336 Prozessor (12 MB Cache, 2,90 GHz), Intel Xeon E, LGA 1200 (Socket H5), 14 nm, Intel, E-2336, 2,9 GHz

Intel Xeon® E-2336 Prozessor (12 MB Cache, 2,90 GHz). Prozessorfamilie: Intel Xeon E, Prozessorsockel: LGA 1200 (Socket H5), Prozessor Lithografie: 14 nm. Speicherkanäle: Zweikanalig, Maximaler interner Speicher, vom Prozessor unterstützt: 128 GB, Speichertypen, vom Prozessor unterstützt: DDR4-SDRAM. Marktsegment: Server, PCI Express Konfigurationen: 1x16+1x4, 2x8+1x4, 1x8+3x4, Unterstützte Befehlssätze: SSE4.1, SSE4.2, AVX 2.0, AVX-512. Intel® Turbo Boost Technology 2.0 frequency: 4,8 GHz, Unterstützung der maximalen Enklavengröße für Intel® SGX: 0,5 GB. Verpackungsart: Einzelhandels-Box

Merkmale

Betriebsbedingungen

Tjunction 100 °C

Gewicht und Abmessungen

Prozessor-Paketgröße 37.5 x 37.5 mm

Logistikdaten

Warentarifnummer (HS) 85423119

Sonstige Funktionen

RAM-Speicher maximal 128 GB

Verpackungsdaten

Verpackungsart Einzelhandels-Box

Grafik

Eingebaute Grafikkartenadapter Nein
Separater Grafikkartenadapter Nein
Separates Grafikkartenmodell Nicht verfügbar

Speicher

Maximaler interner Speicher, vom Prozessor unterstützt 128 GB
Speichertypen, vom Prozessor unterstützt DDR4-SDRAM
Speicherkanäle Zweikanalig
ECC Ja

Technische Details

Startdatum Q3'21
Status Launched
Unterstützte Arbeitsspeicher DDR4-SDRAM
Instandhaltungszustand Baseline Servicing

Merkmale

Execute Disable Bit Ja
Leerlauf Zustände Ja
Thermal-Überwachungstechnologien Ja
Marktsegment Server
Maximale Anzahl der PCI-Express-Lanes 20
PCI-Express-Slots-Version 4.0
PCI Express Konfigurationen 1x16+1x4, 2x8+1x4, 1x8+3x4
Unterstützte Befehlssätze SSE4.1, SSE4.2, AVX 2.0, AVX-512
Skalierbarkeit 1S
CPU Konfiguration (max) 1
Exportkontrollnummer 5A992CN3
Klassifizierungsnummer (ECCN)
Warenklassifizierungssystem zur automatisierten Nachverfolgung (CCATS) G167599

Prozessor

Prozessorhersteller	Intel
Prozessor	E-2336
Grundfrequenz des Prozessors	2,9 GHz
Prozessorfamilie	Intel Xeon E
Anzahl Prozessorkerne	6
Prozessorsockel	LGA 1200 (Socket H5)
Komponente für	Server/Arbeitsstation
Prozessor Lithografie	14 nm
Prozessor-Threads	12
Systembus-Rate	8 GT/s
Prozessorbetriebsmodi	64-Bit
Prozessor Boost-Frequenz	4,8 GHz
Prozessor-Cache	12 MB
Prozessor Cache Typ	Smart Cache
Thermal Design Power (TDP)	65 W
Box	Nein
Kühler enthalten	Nein
ARK Prozessorerkennung	212253

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® Schutz	Ja
Speichererweiterungen (Intel® MPX)	
Intel® Turbo Boost Technology 2.0 frequency	4,8 GHz
Intel® Transactional Synchronization Extensions	Nein
Unterstützung der maximalen Enklavengröße für Intel® SGX	0,5 GB
Intel® VT-x mit Extended Page Tables (EPT)	Ja
Intel® Sicherer Schlüssel	Ja
Intel® OS Guard	Ja
Intel® Software Guard Extensions (Intel® SGX)	Ja
Intel® 64	Ja
Intel® Virtualization Technologie (VT-X)	Ja
Intel® Virtualisierungstechnik für direkte I/O (VT-d)	Ja
Intel® Boot Guard	Ja
Intel® Optane™ DC Persistent Memory unterstützt	Nein
Intel® vPro™ Platform Eligibility	Ja