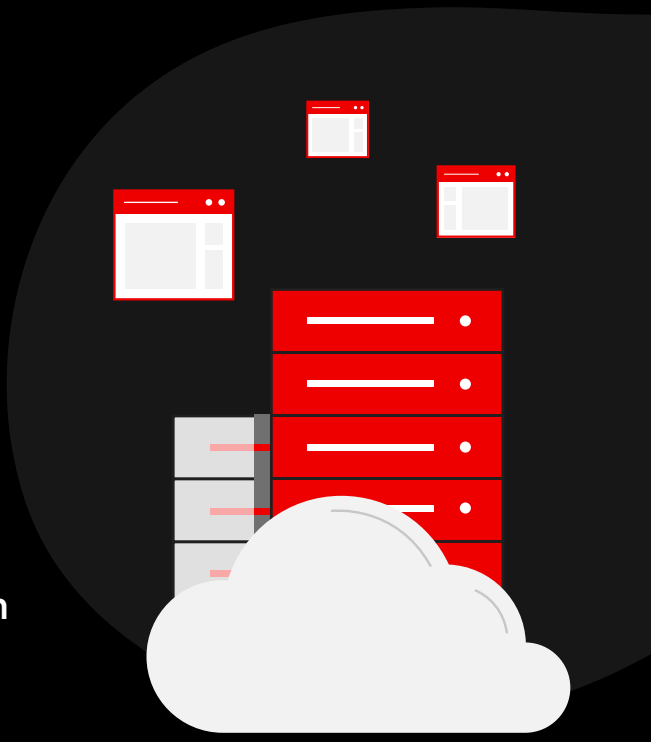
Warum Ihr Betriebssystem immer noch wichtig ist

8 Möglichkeiten, wie Linux moderne IT- und Unternehmensziele unterstützt

Red Hat

Inhalt

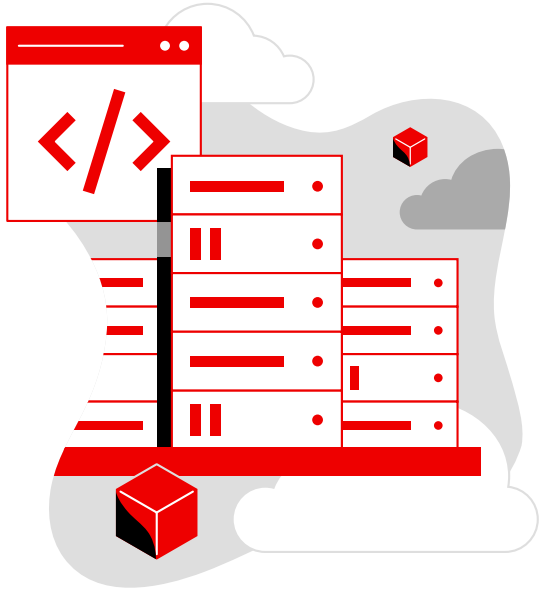


Ihr Betriebssystem ist ein zentraler Bestandteil moderner IT

Betriebssysteme haben in IT-Umgebungen schon immer eine zentrale Rolle gespielt.

Seit ihrer Entwicklung in den 1950er Jahren haben sich die Betriebssysteme ständig weiterentwickelt, um den sich ändernden Anforderungen gerecht zu werden. Die ersten Betriebssysteme konzentrierten sich in erster Linie auf die Batch-Verarbeitung und einfache Aufgabenplanung, bei der immer nur ein Job ausgeführt wurde. Mit der Einführung von Time-Sharing-Systemen in den 1960er Jahren konnten jedoch mehrere Nutzende gleichzeitig mit einem Computer interagieren. In den darauffolgenden Jahrzehnten entstanden Betriebssysteme wie UNIX, die Modularität und Portabilität in Computerumgebungen ermöglichten.

In den 1980er Jahren wurden durch den zunehmenden Verkauf und die Verbreitung von Personal Computern Betriebssysteme für die breite Öffentlichkeit eingeführt. Die Erfindung der grafischen Benutzeroberfläche (GUI) revolutionierte die Interaktion der Nutzenden mit dem Computer und machte die Datenverarbeitung für eine breitere Zielgruppe zugänglich.



Mit der wachsenden Nachfrage nach Server-based Computing entwickelte sich **Linux®** zu einem leistungsstarken, skalierbaren Betriebssystem für unternehmensgerechte Rechenzentren weltweit. Der Linux-Kernel wurde erstmals 1991 veröffentlicht und bot eine kostenlose, quelloffene Alternative zu UNIX, die von verschiedenen Personen ausgeführt, getestet, weitergegeben und modifiziert werden konnte. Linux gehört heute zu den beliebtesten Betriebssystemen weltweit und bietet eine ideale Plattform für moderne, innovative IT.

Die 2000er Jahre brachten **Virtualisierungstechnologien** und später **Container** hervor, die zu einer effizienteren Nutzung von Hardwareressourcen und einer Verlagerung zum **Cloud Computing** führten. Infolgedessen übernahmen die Betriebssysteme neue Managementfunktionen und unterstützten flexible Anwendungs-Deployments und Ressourcenoptimierung.

Der Einfluss von Betriebssystemen geht heute über die zentralen Rechenzentren hinaus und umfasst neue Technologien wie **Edge-Geräte** und das **Internet of Things (IoT)**. Betriebssysteme sorgen für eine effiziente Datenverarbeitung am Netzwerkrand und können so die Latenzzeit verringern und die Performance in Use Cases optimieren, die von Smart Cities bis hin zu autonomen Fahrzeugen reichen.

Dieses E-Book vermittelt einen Überblick darüber, wie wichtig das Betriebssystem – und insbesondere das Linux-Betriebssystem – immer noch ist und wie es modernen IT- und Geschäftsanforderungen gerecht wird.

8 Gründe, warum Ihr Betriebssystem immer noch wichtig ist

Da Unternehmen zunehmend verteilte, cloudbasierte IT-Umgebungen einsetzen, gewinnt das Betriebssystem weiter an Bedeutung.

87 % der Unternehmen verfügen über eine Multi Cloud-Strategie, und 50 % der Unternehmens-Workloads werden heute in einer Public Cloud ausgeführt.[1] Ihr Betriebssystem kann als einheitliche Basis für die Onsite- und Cloud-Infrastruktur, verschiedene Hardware und Software sowie traditionelle und cloudfähige Anwendungen dienen. Sicherheit, Management, Portierbarkeit sowie die Planung des Lifecycles beginnen mit Ihrem Betriebssystem. Die Standardisierung auf eine einheitliche Betriebssystembasis für Ihre Rechenzentrums- und Cloud-Umgebungen kann Ihre IT-Operationen vereinfachen, die Flexibilität erhöhen, die Sicherheit verbessern und Innovationen unterstützen.

Als eines der weltweit beliebtesten Betriebssysteme wählen viele Unternehmen Linux für ihre IT-Basis. Tatsächlich hatte Linux im Jahr 2022 einen Anteil von 65,6 % an neuen physischen Deployments und einen Anteil von 82,8 % an neuen virtualisierten Deployments auf dem weltweiten Markt für Serverbetriebssysteme.[2]

Unternehmen führen eine Vielzahl von Produktions- und Entwicklungs-Workloads auf Linux-Betriebssystemen aus, darunter IT- und Web-Infrastrukturen, Customer Relationship Management und Enterprise Resource Management.[3] Dieses Kapitel beschreibt, wie Ihr Linux-Betriebssystem Ihre Anwendungen, Prozesse und IT-Umgebung unterstützt, um einen Mehrwert für Ihr gesamtes Unternehmen zu schaffen.

In diesem Kapitel:

1 *Flexera: „**Flexera 2023 State of the Cloud Report**“. März 2023.*

2 *IDC Market Share: „Worldwide Server Operating System Environments Market Shares, 2022: Steady Growth Persists“. Dokument Nr. US51038623. Juli 2023.*

3 *IDC-Whitepaper, gesponsert von Red Hat: „**Red Hat Enterprise Linux: $1.7 Trillion a Year Boost for Customers**“. Dokument Nr. US48931522. März 2022.*

1 Betriebssysteme verbinden Hardware, Anwendungen und Nutzende.

Als Basisschicht in Ihrem Software-Stack unterstützt Ihr Betriebssystem Interaktionen zwischen Hardware und Anwendungen und stellt wichtige Services und Ressourcen bereit.

Ihr Betriebssystem abstrahiert die zugrunde liegenden Hardwarekomponenten, damit Anwendungen auf verschiedenen Infrastrukturen ohne Änderungen für bestimmte Systeme ausgeführt werden können. Darüber hinaus verwaltet es Ressourcen wie CPUs (Central Processing Units), Speicher, Storage und Netzwerke, um die Systemleistung zu optimieren und Konflikte zwischen mehreren aktiven Anwendungen zu vermeiden. CLIs und GUIs des Betriebssystems ermöglichen einen intuitiveren Umgang mit dem Computer und seinen Anwendungen. Sicherheitsfunktionen wie Benutzerauthentifizierung, Zugriffskontrolle und Verschlüsselung schützen Daten und Ressourcen vor unbefugtem Zugriff. Die Funktionen zur Fehler- und Ausnahmebehandlung verhindern Systemabstürze und verbessern die Zuverlässigkeit des Systems und das allgemeine Benutzererlebnis.

Moderne Betriebssysteme wie Linux implementieren in der Regel 2 Modi, den Kernelmodus und den Benutzermodus, um festzulegen, welche Berechtigungen für welche Anwendungen, Komponenten und Nutzenden verfügbar sind. Im Kernelmodus können vertrauenswürdige Kernsoftwarekomponenten – wie der **Betriebssystemkernel** und einige Gerätetreiber – privilegierte Operationen durchführen, Hardwareressourcen direkt nutzen und auf eingeschränkten Systemspeicher zugreifen.

Sämtliche andere Software – einschließlich Benutzeranwendungen, Libraries und Tools – wird im Benutzermodus mit begrenztem Zugriff auf die Systemressourcen ausgeführt. Diese Anwendungen können nur auf den Benutzerbereich zugreifen, d. h., auf isolierte Speicherbereiche, die verhindern, dass Anwendungen kritische Komponenten des Betriebssystems beeinträchtigen.

Aufbau Ihrer IT-Basis auf bewährtem Fachwissen

Linux kann einerseits als stabile Betriebsbasis für Ihre verschiedenen IT-Workloads dienen, andererseits sind viele verschiedene Linux-Distributionen verfügbar, die jeweils unterschiedliche Tools, Services und Supportrichtlinien bieten. Da sich Ihr Unternehmen auf Ihre IT-Basis stützt, ist die Wahl des Linux-Anbieters eine wichtige und strategische Entscheidung.

Wählen Sie einen vertrauenswürdigen Linux-Anbieter, der über die nötige Erfahrung und Kompetenz verfügt, um Ihr Unternehmen zu unterstützen. Dazu gehören die folgenden zentralen Aspekte:

- Eine produktionsreife Linux-Distribution, die sich an den Kundenanforderungen orientiert
- Kontinuierliche Beiträge zum und Führungsrolle innerhalb des Linux-Kernels
- Eine kollaborative Community von Kunden, Partnern und Fachleuten
- Nachgewiesene kommerzielle Unterstützung mit langen Lifecycles und Sicherheitswartung

2 Betriebssysteme gewährleisten die Kompatibilität von Hardware und Software.

Betriebssysteme verwalten Hardwareressourcen wie Storage, Netzwerke und Peripheriegeräte, um die Systemstabilität und die Kompatibilität von Hardware und Software zu erhöhen.

Anwendungen und Hardwareressourcen kommunizieren über Gerätetreiber. Betriebssysteme verwalten diese Treiber und sorgen für die korrekte Installation, das richtige Laden und den ordnungsgemäßen Betrieb, um die Systemstabilität und die Kompatibilität zwischen Anwendungen und den zugrunde liegenden Hardwarekomponenten zu erhöhen. Während der Systeminitialisierung erkennt Ihr Linux-Betriebssystem beispielsweise neu angeschlossene oder integrierte Ressourcen, identifiziert bekannte Geräte und sucht und lädt die entsprechenden Treiber. Betriebssysteme bieten auch Hardwareabstraktionsschichten, die es Anwendungen ermöglichen, mit Hardwaregeräten zu interagieren, ohne die Details der zugrunde liegenden Hardware zu kennen. Diese standardisierten Schnittstellen vereinfachen das Anwendungs-Deployment und verbessern die Portierbarkeit in unterschiedlichen Hardware-Konfigurationen.

Chipsätze, Storage und Netzwerke sind Bereiche, in denen Gerätetreiber und die Verwaltung des Betriebssystems unerlässlich sind. Viele rechenintensive Workloads wie KI/ML (Künstliche Intelligenz/ Maschinelles Lernen) können von der Hardwarebeschleunigung in Chipsätzen profitieren. Betriebssysteme können die Funktionen und die Beschleunigung von GPUs (Graphics Processing Units), SoCs (Systems on Chips) und FPGAs (Field-Programmable Gate Arrays) für diese Workloads verfügbar machen.

Außerdem ermöglichen Betriebssysteme einen stabilen und zuverlässigen Zugriff auf die auf Festplatten **gespeicherten Daten**. Sie verwalten die Dateiorganisation und -speicherung mit optimierten Methoden, um die Datenfragmentierung zu minimieren, Namenskonflikte zu vermeiden und für Konsistenz zwischen Anwendungen zu sorgen.

Darüber hinaus koordinieren Betriebssysteme netzwerkbezogene Funktionen, um zuverlässige Verbindungen und einen effizienten Datenaustausch zwischen den Systemen innerhalb eines Netzwerks zu ermöglichen. Mithilfe eines Netzwerk-Stacks verwalten Betriebssysteme die Integration von Netzwerkprotokollen, um eine End-to-End-Kommunikation in verschiedenen Netzwerken zu bieten. Sie konfigurieren und verwalten Netzwerkgeräte wie NICs (Network Interface Cards) und Wireless-Adapter, um die Datenübertragung zwischen Anwendungen zu unterstützen und zu beschleunigen. Zusätzlich implementieren sie Maßnahmen zur Netzwerksicherheit, darunter Firewalls und Verschlüsselungsprotokolle, um vor unbefugtem Zugriff und Datenpannen zu schützen.

Mehr Auswahl durch ein zertifiziertes Partnernetzwerk

Tests und Zertifizierungen stellen sicher, dass Produkte von Drittanbietern zuverlässig mit Ihrem Betriebssystem zusammenarbeiten. Wählen Sie einen Linux-Anbieter, der mit branchenführenden Hardware-, Software- und Cloud-Anbietern zusammenarbeitet, um Ihnen mehr Auswahl, Innovation und Stabilität zu bieten. Vergewissern Sie sich, dass das Partnernetzwerk des von Ihnen gewählten Anbieters die Produkte und Services umfasst, die Sie derzeit nutzen und zukünftig nutzen möchten.

3 Betriebssysteme verbessern die Zuverlässigkeit und Stabilität von Plattformen.

Betriebssysteme erkennen und behandeln Software- und Hardwarefehler, um eine stabile, zuverlässige Plattform für Anwendungen und Nutzende bereitzustellen.

Anwendungen sind für viele digitale Unternehmen von zentraler Bedeutung, und Ausfallzeiten sind oft inakzeptabel. Viele Betriebssysteme enthalten fortschrittliche Fehlererkennungsmechanismen, die Runtime-Fehler während der Anwendungsausführung erfassen und verwalten. Diese Mechanismen tragen dazu bei, systemweite Abstürze, Unterbrechungen und Datenbeschädigungen zu verhindern. Außerdem überwachen Betriebssysteme kritische Anwendungen und Systemdateien durch Dateiintegritätsprüfungen, Prüfsummen und digitale Signaturen, um sicherzustellen, dass nur autorisierter und unveränderter Code ausgeführt wird.

Hardwarefehler sind ebenfalls ein Problem. Durch das Erkennen und Verwalten von Hardwarefehlern wie Speicherfehlern, Festplattenfehlern und Prozessorfehlfunktionen können Betriebssysteme die Systemstabilität erhöhen und katastrophale Ausfälle verhindern. In Verbindung mit dem Fehlerkorrekturverfahren (ECC) und der zyklischen Redundanzprüfung (CRC), die in Speicher und Storage-Geräte integriert sind, können Betriebssysteme fehlerhafte Hardware erkennen und verwalten, um die Zuverlässigkeit der gespeicherten und von Anwendungen verwendeten Daten zu verbessern. Fehlererkennungs- und -korrekturmechanismen wie Journaling oder Prüfsummen helfen Betriebssystemen, Daten für Anwendungen und Nutzende schnell und genau abzurufen.

Wichtig ist auch, Probleme auf Systemebene zu erkennen und zu beheben. Betriebssysteme bieten Protokollierungs- und Diagnosetools, die Informationen zu Fehlern und System-Events aufzeichnen, um die Fehlerbehebung und proaktive Wartungsmaßnahmen zu unterstützen. Mithilfe dieser Tools können Systemadministrationsteams Fehlermuster analysieren, potenzielle Schwachstellen erkennen und Korrekturmaßnahmen ergreifen und so die allgemeine Stabilität und Zuverlässigkeit des Systems aufrechterhalten.

Verbesserte Stabilität durch Tools für prädiktive Analysen und proaktive Fehlerbehebung

Die Verwaltung komplexer IT-Umgebungen kann kompliziert und zeitaufwendig sein. Wählen Sie eine Linux-Distribution, die fortschrittliche Management- und Automatisierungstools bietet, damit Sie Ihre gesamte IT-Umgebung proaktiv verwalten können. Mit einheitlichen Tools, die infrastrukturübergreifend einsetzbar sind und die einzelnen Systeme in Ihrer Umgebung überwachen, können Sie Probleme erkennen, bevor sie sich auf die Geschäftsabläufe auswirken. Tools, die sich auf Operationen, Sicherheit und Geschäftsergebnisse konzentrieren, bieten Ihnen zudem die Möglichkeit, die organisatorischen Auswirkungen von Problemen und Änderungen zu erkennen und Abhilfemaßnahmen zu priorisieren.

4 Betriebssysteme sorgen für mehr Effizienz im IT-Betrieb.

Ein konsistentes Betriebssystem kann als einheitliche Basis für die verschiedenen IT-Umgebungen dienen. So können Sie Ihre Abläufe standardisieren und optimieren, die Effizienz steigern und die IT-Sicherheit verbessern.

Moderne IT-Umgebungen bestehen oft aus mehreren Infrastrukturen und Architekturen. Tatsächlich nutzen 85 % der Unternehmen mehrere Deployment-Umgebungen, und 31 % stellen Anwendungen in 5 oder mehr Umgebungen bereit.[4] Sie können beispielsweise sowohl Onsite-Rechenzentren als auch Public Cloud-Anbieter nutzen und Workloads auf Servern, Workstations und Edge-Geräten bereitstellen, die auf einer Vielzahl von Hardwarearchitekturen wie x86, Arm und IBM Power basieren.

In diesen unterschiedlichen Umgebungen ist Konsistenz von entscheidender Bedeutung. Mit standardisierten Betriebsumgebungen können Sie gemeinsame Verfahren, Richtlinien und Konfigurationen entwickeln, die die täglichen Operationen und Verwaltungsaufgaben vereinfachen. Dies bietet viele Vorteile für IT-Organisationen:

- **Interoperabilität:** Ein einheitliches Betriebssystem fördert die Interoperabilität und Integration verschiedener Infrastrukturen. Sie können verteilte Anwendungen in umfangreichen Umgebungen mit weniger Komplexität bereitstellen, verwalten und Fehler beheben.
- **Skalierbarkeit:** Einheitliche Betriebssystem-Deployments vereinfachen die Skalierung von IT-Services und -Umgebungen, da neue Infrastrukturen bestehende, validierte Konfigurationen replizieren können.
- **Sicherheit:** Standardisierte Betriebsumgebungen erleichtern die konsistente Durchsetzung von Sicherheitsrichtlinien – einschließlich regelmäßiger Patches, Aktualisierungen und Compliance-Audits – in den verschiedenen Umgebungen, sodass das Risiko von Sicherheitsschwachstellen verringert wird.
- **Verfügbarkeit:** Die Nutzung eines konsistenten Betriebssystems in Hybrid Cloud-Umgebungen vereinfacht die Problemlösung und verkürzt die Systemausfallzeiten.

Effizienz durch Standardisierung

Ihr Betriebssystem kann als konsistente, standardisierte Basis für sämtliche Infrastrukturen und Architekturen dienen. Entscheiden Sie sich für einen Linux-Anbieter, der mehrere Betriebssystemvarianten anbietet, die für unterschiedliche Deployment-Umgebungen optimiert sind und gleichzeitig die allgemeine Konsistenz wahren. Stellen Sie sicher, dass die integrierten und zugehörigen Management- und Automatisierungstools in den verschiedenen Varianten auf die gleiche Weise funktionieren. Durch die Standardisierung auf eine dieser Distributionen können Sie kohärente, einheitliche Betriebsumgebungen schaffen, die das Infrastrukturmanagement optimieren, die IT-Effizienz und -Produktivität steigern und die Sicherheit verbessern.

4 F5 Networks: „2023 State of Application Strategy Report." März 2023.

5 Betriebssysteme schützen Ihre Infrastruktur, Anwendungen und Daten.

Betriebssysteme schützen vor Bedrohungen, die die Integrität, Vertraulichkeit und Verfügbarkeit Ihrer Infrastruktur, Anwendungen und Daten gefährden können.

Der Linux-Kernel enthält zahlreiche Sicherheitsfunktionen, die zum Schutz Ihrer Infrastruktur, Anwendungen und Daten beitragen. Linux-Betriebssysteme enthalten beispielsweise die Authentifizierungs- und Autorisierungstools, die für die Implementierung von Zero-Trust-Architekturen erforderlich sind. Die Authentifizierung über Benutzernamen, Passwörter, biometrische Daten oder Sicherheits-Tokens identifiziert die Personen oder Anwendungen, die auf IT-Systeme und -Assets zugreifen möchten. Autorisierungs- und Zugriffskontrollmechanismen wie Security-Enhanced Linux (SELinux) definieren die Berechtigungen und Privilegien, die diesen Nutzenden, Gruppen oder Anwendungen gewährt werden. Mit diesen Tools lässt sich unbefugter Zugriff auf sensible Ressourcen und Systemkonfigurationen verhindern.

Weitere wichtige Sicherheitsfunktionen des Betriebssystems:

- **Verschlüsselung:** Integrierte Verschlüsselungstechnologien können vertrauliche Dateien und sensible Daten sowohl im Ruhezustand als auch bei der Übertragung in verschiedenen Netzwerken schützen. Red Hat® Enterprise Linux beispielsweise verwendet systemweite kryptografische Richtlinien, um vordefinierte kryptografische Kontrollen automatisch zu konfigurieren und auf Systeme und Anwendungen anzuwenden. Außerdem unterstützt die Lösung die CPU-gestützte Verschlüsselung von Workloads virtueller Maschinen für eine sichere Datenverarbeitung.
- **Zulassungslisten für Anwendungen:** Mit dieser Funktion wird ein Index genehmigter Anwendungen und ausführbarer Dateien erstellt, die von einer bestimmten Person auf einem System ausgeführt werden dürfen.
- **Hardware Root of Trust:** Hardwarebasierte Root-of-Trust-, Remote-Bestätigungs- und Measured-Boot-Technologien überprüfen die Systemintegrität und stellen sicher, dass die Systeme nicht verändert oder manipuliert wurden.
- **Sicherheits-Scans:** Tools zum Scannen von Compliance und Schwachstellen wie Open Security Content Automation Protocol (OpenSCAP) können Audits vereinfachen, falsch konfigurierte Systeme erkennen und beheben sowie das Einhalten der Compliance unterstützen.
- **Systemprotokollierung:** Auditing- und Protokollierungsfunktionen können Events und Aktivitäten innerhalb eines Systems aufzeichnen. Administrationsteams können diese Events dann überprüfen und analysieren, Quellen von Sicherheitsverletzungen identifizieren und Korrekturmaßnahmen implementieren.

Aufbau einer Zero-Trust- Basis

Zero-Trust-Architekturen wenden die Sicherheit auf die einzelnen Ressourcen an, anstatt die Sicherheit ausschließlich am Netzwerkrand zu verwalten. Während Linux selbst die Kernfunktionen enthält, die für die Entwicklung von Zero-Trust-Architekturen erforderlich sind, bieten einige Distributionen Funktionen und Tools, die das Einführen von Zero Trust vereinfachen. Achten Sie auf eine Linux-Distribution, die über eine vertrauenswürdige Softwarelieferkette angeboten wird und systemweite Verschlüsselungseinstellungen, Hardware-Root-of-Trust-Funktionen, integrierte Compliance-Scans und richtlinienbasierte Identitätsmanagementtools umfasst.

In diesem **Überblick** erhalten Sie weitere Informationen.

6 Betriebssysteme verwalten die Performance von Anwendungen und Workloads.

Betriebssysteme managen die CPU- und Speichernutzung, um die Hardware-Performance zu maximieren und so für ein optimiertes Anwendungs-, Workload- und Benutzererlebnis zu sorgen.

Mithilfe von Prozessplanungstechnologien optimieren Betriebssysteme die CPU- und Speichernutzung, verteilen die Workloads auf die Ressourcen und halten die Reaktionsfähigkeit des Systems aufrecht. So sorgen beispielsweise Prozessplanungsalgorithmen und Load Balancing-Mechanismen für eine effiziente Nutzung und gerechte Verteilung der CPU-Zeit. Mit Planungsalgorithmen können auch mehrere Prozesse gleichzeitig durchgeführt werden, da die CPUs schnell zwischen mehreren Prozessen umgeschaltet werden.

Durch die Priorisierung interaktiver Prozesse können Betriebssysteme reaktionsschnelle Erlebnisse schaffen, bei denen die Nutzenden nur minimale oder gar keine Verzögerungen wahrnehmen. Mit Funktionen zur Prozessplanung in Echtzeit können zudem Prozesse mit strengen Zeitvorgaben – wie etwa eingebettete oder industrielle Steuerungssysteme – bestimmte Fristen einhalten und umgehend auf externe Events reagieren.

Linux verfügt außerdem über Speicherverwaltungsfunktionen, mit denen ausreichend Speicher für Anwendungen sichergestellt, potenzielle Konflikte vermieden und die System-Performance optimiert werden können. Durch die dynamische Zuweisung und Freigabe von Speicher wird den Prozessen der für eine maximale Performance erforderliche Speicher zur Verfügung gestellt. Wenn ein Prozess den Speicher nicht mehr benötigt, stellt das Betriebssystem ihn für andere Prozesse zur Verfügung.

Optimierte Workload-Performance

Entscheiden Sie sich für eine Linux-Distribution, die Tools und Schnittstellen für das Tuning, Monitoring und Management von Performance-Merkmalen nach Anwendung, Workload oder Use Case enthält. Einige Anbieter bieten beispielsweise Tools und Services an, mit denen Sie Performance-Probleme erkennen, Profile für die Anwendungs-Performance erstellen und Daten analysieren können, um Probleme schnell zu beheben oder sogar ganz zu vermeiden.

Betriebssysteme verbessern die Speicherleistung auch durch Caching- und Puffermechanismen, die häufig abgerufene Daten in schnelleren, teureren Caches und andere Daten in größeren, langsameren Arbeitsspeichern (RAM) und Storage-Geräten speichern. Durch den Austausch von Daten zwischen Arbeitsspeicher und Festplatten ermöglicht der virtuelle Speicher den Betriebssystemen, den Prozessen einen größeren Adressbereich zur Verfügung zu stellen, als tatsächlich physisch vorhanden ist. Virtueller Speicher erhöht die Multitasking-Effizienz und ermöglicht das Ausführen größerer Anwendungen auf Systemen mit geringerem Speicherplatzbedarf.

7 Betriebssysteme verbessern die Ressourcennutzung mit virtuellen Maschinen.

Als wichtiger Bestandteil von Technologien für virtuelle Maschinen optimieren Betriebssysteme die Ressourcennutzung, isolieren Workloads und erhöhen die Skalierbarkeit in verschiedenen Umgebungen.

Virtuelle Maschinen sind isolierte Umgebungen, in denen eigene Guest-Betriebssysteme ausgeführt werden, die von Nutzenden und Anwendungen als separate Hardwareressourcen wahrgenommen werden, auch wenn sie sich die tatsächlichen physischen Ressourcen mit anderen virtuellen Maschinen teilen können. Hypervisoren sind spezialisierte Software zum Erstellen und Managen virtueller Maschinen auf einem einzelnen physischen Server. Betriebssysteme und Hypervisoren erfüllen viele identische Funktionen. Dadurch können sie viele Komponenten gemeinsam nutzen, darunter Prozessplaner, Speichermanager, Gerätetreiber, Sicherheitsfunktionen und Netzwerk-Stacks.

Erweiterte Virtualisierung

Mit der **Kernel-based Virtual Machine (KVM)** in Linux können Sie Linux als Hypervisor verwenden. Wählen Sie eine kommerzielle Linux-Distribution, die die Möglichkeiten von KVM für ein effizienteres Management erweitert.

Hypervisoren erfüllen viele Funktionen bei der Unterstützung von IT-Operationen:

- **Ressourcenzuweisung:** Hypervisoren weisen virtuellen Maschinen Ressourcen wie CPU-Zeit und Arbeitsspeicher zu, sodass mehrere virtuelle Maschinen mit einer garantierten Servicequalität auf derselben physischen Hardware ausgeführt werden können. Sie stellen den Guest-Betriebssystemen auch physische Hardware wie Netzwerkadapter, Speichercontroller und Grafikkarten als virtuelle Geräte zur Verfügung, damit mehrere virtuelle Maschinen dieselben Ressourcen nutzen können, ohne dass es zu Konflikten kommt.
- **Snapshots und Klonen:** Viele Hypervisoren bieten Snapshot- und Klonfunktionen für virtuelle Maschinen, um die Flexibilität, Skalierbarkeit und Effizienz zu erhöhen. Snapshots erfassen den Zustand und die Daten virtueller Maschinen zu bestimmten Zeitpunkten. Diese können zur Wiederherstellung oder zum Rollback auf bekannte Konfigurationen verwendet werden. Klonfunktionen duplizieren vorhandene virtuelle Maschinen, um das Deployment neuer Instanzen zu beschleunigen.
- **Livemigration und Wiederherstellung:** Livemigrations- und Hochverfügbarkeitsfunktionen tragen dazu bei, Workloads auszugleichen, die Ressourcennutzung zu optimieren und die Verfügbarkeit virtueller Maschinen zu verbessern. Bei der Livemigration werden aktive virtuelle Maschinen ohne Serviceunterbrechung zwischen physischen Hosts verschoben. Die virtuellen Maschinen und die Netzwerkverbindungen bleiben dabei aktiv, und die Anwendungen werden weiterhin ausgeführt. Wenn virtuelle Maschinen aufgrund eines Host-Ausfalls unterbrochen werden, startet der Hypervisor sie automatisch neu, und zwar innerhalb von Sekunden und ohne menschliches Eingreifen.
- **Sicherheit und Isolierung:** Hypervisoren setzen strenge Grenzen durch, die verhindern, dass virtuelle Maschinen auf den Speicher oder die Ressourcen anderer virtueller Maschinen zugreifen. Diese Grenzen tragen dazu bei, die Sicherheit zu erhöhen und die Auswirkungen potenzieller Schwachstellen und Cyberangriffe einzudämmen.

8 Betriebssysteme unterstützen moderne, cloudnative Anwendungen.

Linux-Betriebssysteme unterstützen Container-Technologien für das Bereitstellen und Verwalten moderner, cloudnativer Anwendungen mit mehr Agilität, Skalierbarkeit und Konsistenz.

52 % der Unternehmen betrachten das „Containerisieren von Workloads" als einen wichtigen Teil ihrer Initiativen zur Anwendungsmodernisierung.[5] **Container** sind Technologien, die IT-Komponenten, wie Anwendungen, Runtimes, Libraries und Abhängigkeiten, in kompakte, portierbare und isolierte Umgebungen packen. Container-Technologien virtualisieren das Betriebssystem effektiv und ermöglichen es mehreren Containern, sich einen einzigen Betriebssystem-Kernel zu teilen, der die Hardwareressourcen und die Interaktionen mit dem physischen Host-System verwaltet.

Linux-Betriebssysteme partitionieren Kernel-Ressourcen in Bezug auf Prozessbereiche, Dateisysteme und Netzwerkzugriff, um jedem Container einen eigenen Satz von Ressourcen zuzuweisen. Wie bei der herkömmlichen Virtualisierung werden die einzelnen Container isoliert, um Konflikte und Interferenzen zwischen Containern zu vermeiden. Außerdem können mehrere Container – mit jeweils eigenen Benutzerbereichen und Runtime-Umgebungen – auf demselben Host ausgeführt werden. Zur gerechten und angemessenen Ressourcenzuweisung verwalten und begrenzen Betriebssysteme die Ressourcennutzung – einschließlich CPU, Arbeitsspeicher und Festplatten-Input/Output (I/O) – auf der Basis einzelner Container.

Durch das Management von Netzwerkschnittstellen und -konfigurationen in Container-Umgebungen stellen Betriebssysteme sicher, dass die Container bei Bedarf miteinander und mit externen Systemen kommunizieren können, ohne dass die Netzwerkisolierung beeinträchtigt wird. Außerdem bieten sie Containern isolierte Dateisysteme, die über Container Storage-Treiber auf gemeinsame Daten und persistenten Storage zugreifen können.

Schließlich bieten Betriebssysteme Mandatory Access Controls (MAC), um strenge und vordefinierte Richtlinien für den Ressourcenzugriff durchzusetzen. Container können nur mit bestimmten Systemressourcen interagieren, um die Isolation zu erhöhen und vor weit verbreiteten Sicherheitsbedrohungen und Schwachstellen zu schützen.

Erweiterung Ihrer IT-Umgebung und -Kompetenzen mit Containern

Der Einstieg in die Arbeit mit Containern ist bereits mit Ihrem Linux-Betriebssystem möglich. Wählen Sie eine Linux-Distribution, die Container-Tools wie **Podman**, **Skopeo** und **Buildah** enthält, die Sie beim Entwickeln, Erstellen, Ausführen und Verwalten von Containern auf Ihren Linux-Systemen unterstützen. Wenn Sie sich für einen Linux-Anbieter entscheiden, der auch eine Plattform für die Container-Orchestrierung anbietet, können Sie die Nutzung von Containern nach und nach erweitern und skalieren.

5 *Red Hat E-Book: „Der Ansatz von Unternehmen für die Modernisierung von Legacy-Anwendungen", 6. Februar 2023.*

Die Vorteile von Open Source-Software

Open Source Communities entwickeln und warten viele gängige Betriebssysteme, darunter auch Linux, sowie zugehörige Tools und Software.

Innerhalb dieser Communities können Entwicklerinnen und Entwickler neue Funktionen und Features für Betriebssysteme vorschlagen, beitragen und testen. Die Releases werden über kostenlose Community- und kostenpflichtige Enterprise-Distributionen zur Verfügung gestellt.

Enterprise-Distributionen (auch kommerzielle Distributionen genannt) werden oft in Form einer Subskription angeboten und bieten zusätzliche Funktionen, Services und Support, die auf die jeweiligen geschäftlichen Anforderungen und Belange zugeschnitten sind. So beinhalten Subskriptionen für unternehmensgerechte Betriebssysteme beispielsweise häufig einen technischen Support, der rund um die Uhr verfügbar ist, um die Fehlerbehebung zu beschleunigen und Ausfallzeiten zu reduzieren. Sie können auch Training und Tutorials anbieten, mit denen Nutzende das Betriebssystem effizient verwalten, optimieren und Probleme beheben können.

Lifecycles mit langem Support erhöhen die Stabilität in verschiedenen IT-Umgebungen. Kommerzielle Anbieter folgen in der Regel vorhersehbaren Release-Zyklen, sodass Unternehmen Updates, Upgrades und neue Funktionen planen und vorbereiten können. In-Place-Upgrade-Tools und professionelle Services können die Migration zu neuen Versionen reibungslos und effizient gestalten.

Anbieter von Unternehmenslösungen verfügen in der Regel über Sicherheitsteams, die neue Bedrohungen bewerten, überwachen und darauf reagieren, um die Sicherheit des Betriebssystems zu erhöhen. Einige kommerzielle Distributionen verfügen über Services, die Betriebssysteme überwachen und Anleitungen zur Behebung von Sicherheitsproblemen, nicht konformen Einstellungen, ungepatchten Systemen und Konfigurationsdrift geben. Die Anbieter können ihre Betriebssysteme auch nach den Sicherheitsstandards der Branche zertifizieren lassen, um die erforderliche Compliance und das erwartete Sicherheitsniveau zu gewährleisten.

Außerdem fördern viele kommerzielle Anbieter zertifizierte Partnernetzwerke für ihre Betriebssysteme, um stabile und zuverlässige Abläufe zu ermöglichen. Zu diesen IT-Ökosystemen können Hardware- und Softwareanbieter, Public Cloud-Anbieter und Serviceorganisationen gehören.

Vorteile eines kommerziellen Open Source-Betriebssystems

Im Vergleich zu Unternehmen, die kostenlose Alternativen verwenden, profitieren Nutzende kommerzieller Betriebssysteme von folgenden Vorteilen:

23 %
niedrigere Onsite-Infrastrukturkosten über 3 Jahre[6]

72 %
weniger ungeplante Ausfallzeiten[6]

17,3 Mio. USD
höherer durchschnittlicher Nettoumsatz pro Jahr und Organisation[6]

6 *IDC-Whitepaper, gesponsert von Red Hat: „**Der Geschäftswert von Red Hat Lösungen im Vergleich zu kostenlosen Open Source-Alternativen**“, Dokument #US50423523. März 2023.*

Vereinfachtes Systemmanagement

Mit Managementtools für Betriebssysteme können Sie Ihre IT-Umgebungen effektiver konfigurieren, überwachen und optimieren.

Performance-Management

Verschaffen Sie sich einen Einblick in die System-Performance, um Engpässe zu erkennen, die Auslastung zu überwachen und Performance-Probleme zu beheben.

IT-Automatisierung

Automatisieren Sie Routineaufgaben, um manuelle Eingriffe zu reduzieren, Fehler zu minimieren und für konsistente Systemkonfigurationen zu sorgen.

Sicherheits- und Zugriffsmanagement

Analysieren, verwalten und beheben Sie Sicherheitsschwachstellen, um kritische Anwendungen und Daten zu schützen. Setzen Sie Zugriffskontrollen durch, verwalten Sie Berechtigungen, und sorgen Sie dafür, dass Nutzende je nach ihrer Rolle über die entsprechenden Berechtigungen verfügen.

Konfigurationsmanagement

Führen Sie Updates und Upgrades durch, um sicherzustellen, dass die Betriebssysteme mit den aktuellsten Sicherheits-Patches und Funktionserweiterungen arbeiten. Sorgen Sie für konsistente Konfigurationen in mehreren Systemen, um Konfigurationsdrift in verschiedenen IT-Umgebungen zu reduzieren.

Auditing und Monitoring

Protokollieren und auditieren Sie System-Events, um die Fehlerbehebung, Compliance und Sicherheitsanalyse zu vereinfachen. Optimieren Sie Audittätigkeiten, um die Compliance mit Sicherheits- und Betriebsstandards zu gewährleisten. Überwachen und optimieren Sie virtuelle Ressourcen, um eine effiziente und kosteneffektive Nutzung sicherzustellen.

Backup und Wiederherstellung

Erstellen und verwalten Sie Backups, und implementieren Sie Wiederherstellungsprozesse, um Daten im Falle von Systemausfällen oder Verlusten zu schützen.

Start in eine moderne IT mit Red Hat Enterprise Linux

Ihr Betriebssystem bildet einen wichtigen Bestandteil Ihrer IT-Infrastruktur. Red Hat Enterprise Linux bietet Ihrer Organisation einen Mehrwert.

Mit Red Hat Enterprise Linux können Sie eine effiziente, sicherheitsorientierte Basis für Innovationen in Hybrid Cloud- und Multi Cloud Umgebungen erstellen, unabhängig vom Stand Ihrer IT-Entwicklung. Dieses cloudfähige Betriebssystem bietet ein konsistentes, angepasstes IT-Erlebnis für verschiedene Footprints, wie etwa physische, virtualisierte, Hybrid Cloud-, Multi-Cloud- und sogar Edge-Infrastrukturen. Eine Standardisierung auf Red Hat Enterprise Linux für Onsite-Rechenzentrums- und Cloud-Umgebungen unterstützt Sie bei Ihrem Wechsel zur Cloud, hilft bei der Anpassung an eine digitale Welt und verbessert Produktivität, Sicherheit und Abläufe.

- Konsistenz in verschiedenen Umgebungen
- Tools für prädiktive Analysen und Fehlerbehebung
- Erweiterte Sicherheitsfunktionen
- Vertrauenswürdige Softwarelieferkette
- Integrierte Automatisierungs- und Managementfunktionen
- Tools zur Performance-Optimierung
- Großes zertifiziertes Partnernetzwerk
- Varianten für mehrere Architekturen
- Integrierte Container-Technologien

Erfahren Sie mehr über Red Hat Enterprise Linux.

1051224_0324_KVM

Red Hat