

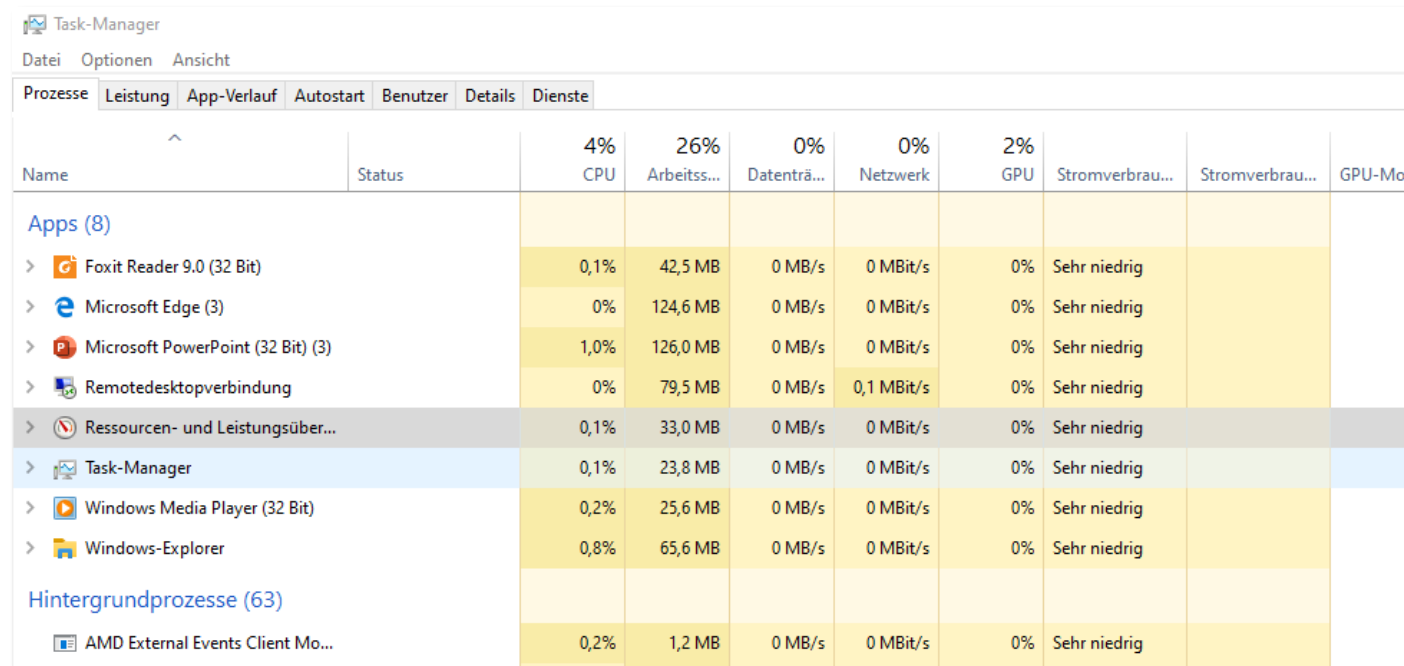
# Windows Client – Systemüberwachung

# Agenda

- Task-Manager
- Leistungsüberwachung
- Ressourcenmonitor
- Zuverlässigkeitsüberwachung
- Ereignisanzeige

# Task-Manager - Prozesse

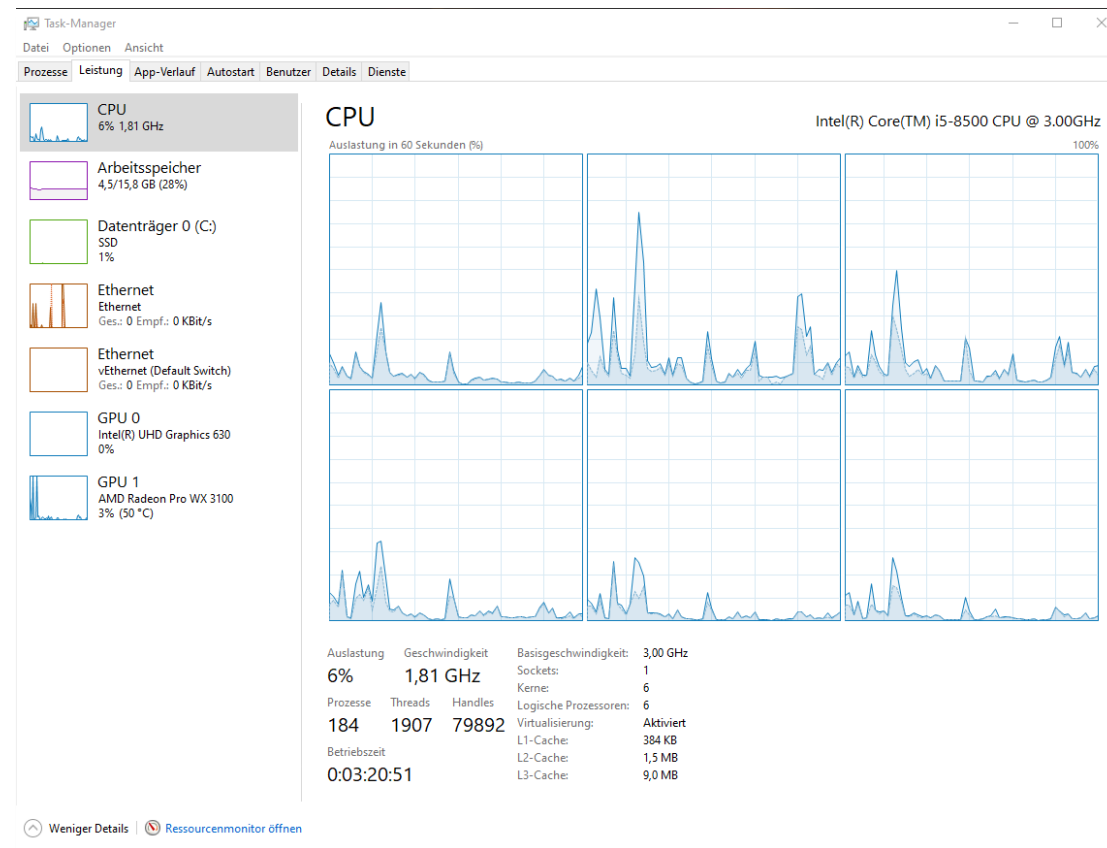
- Task-Manager hilft leistungsbezogene Probleme in Windows zu identifizieren und zu beheben



Task-Manager									
Datei Optionen Ansicht									
Prozesse Leistung App-Verlauf Autostart Benutzer Details Dienste									
Name	Status	4% CPU	26% Arbeitss...	0% Datenträ...	0% Netzwerk	2% GPU	Stromverbrau...	Stromverbrau...	GPU-Mod
Apps (8)									
> Foxit Reader 9.0 (32 Bit)		0,1%	42,5 MB	0 MB/s	0 MBit/s	0%	Sehr niedrig		
> Microsoft Edge (3)		0%	124,6 MB	0 MB/s	0 MBit/s	0%	Sehr niedrig		
> Microsoft PowerPoint (32 Bit) (3)		1,0%	126,0 MB	0 MB/s	0 MBit/s	0%	Sehr niedrig		
> Remotedesktopverbindung		0%	79,5 MB	0 MB/s	0,1 MBit/s	0%	Sehr niedrig		
> Ressourcen- und Leistungsüber...		0,1%	33,0 MB	0 MB/s	0 MBit/s	0%	Sehr niedrig		
> Task-Manager		0,1%	23,8 MB	0 MB/s	0 MBit/s	0%	Sehr niedrig		
> Windows Media Player (32 Bit)		0,2%	25,6 MB	0 MB/s	0 MBit/s	0%	Sehr niedrig		
> Windows-Explorer		0,8%	65,6 MB	0 MB/s	0 MBit/s	0%	Sehr niedrig		
Hintergrundprozesse (63)									
AMD External Events Client Mo...		0,2%	1,2 MB	0 MB/s	0 MBit/s	0%	Sehr niedrig		

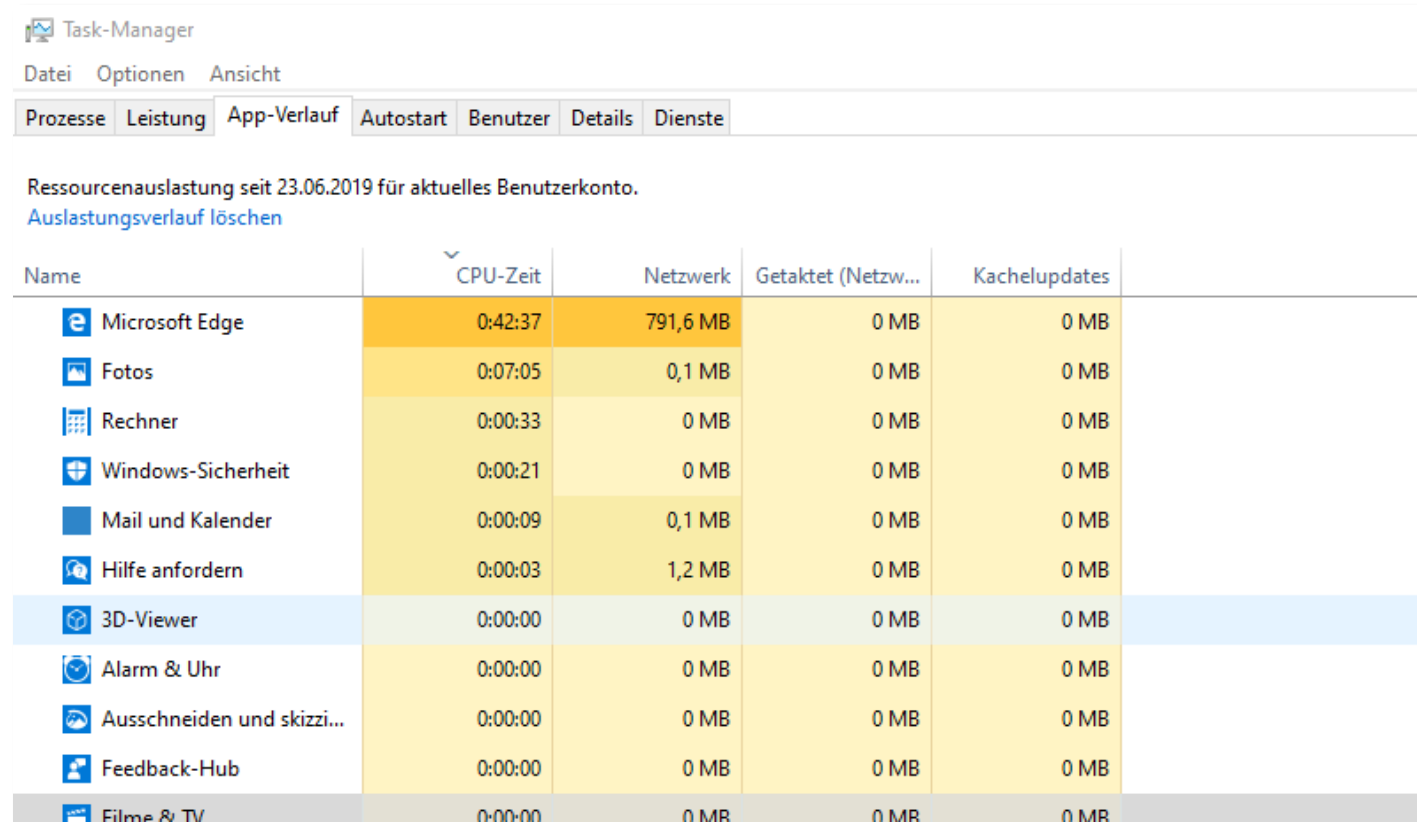
# Task-Manager - Leistung

- zeigt eine Übersicht der aktuellen Auslastung der Hardware



# Task-Manager - App-Verlauf

- zeigt den Ressourcenverbrauch der ausgeführten Apps



Task-Manager

Datei Optionen Ansicht

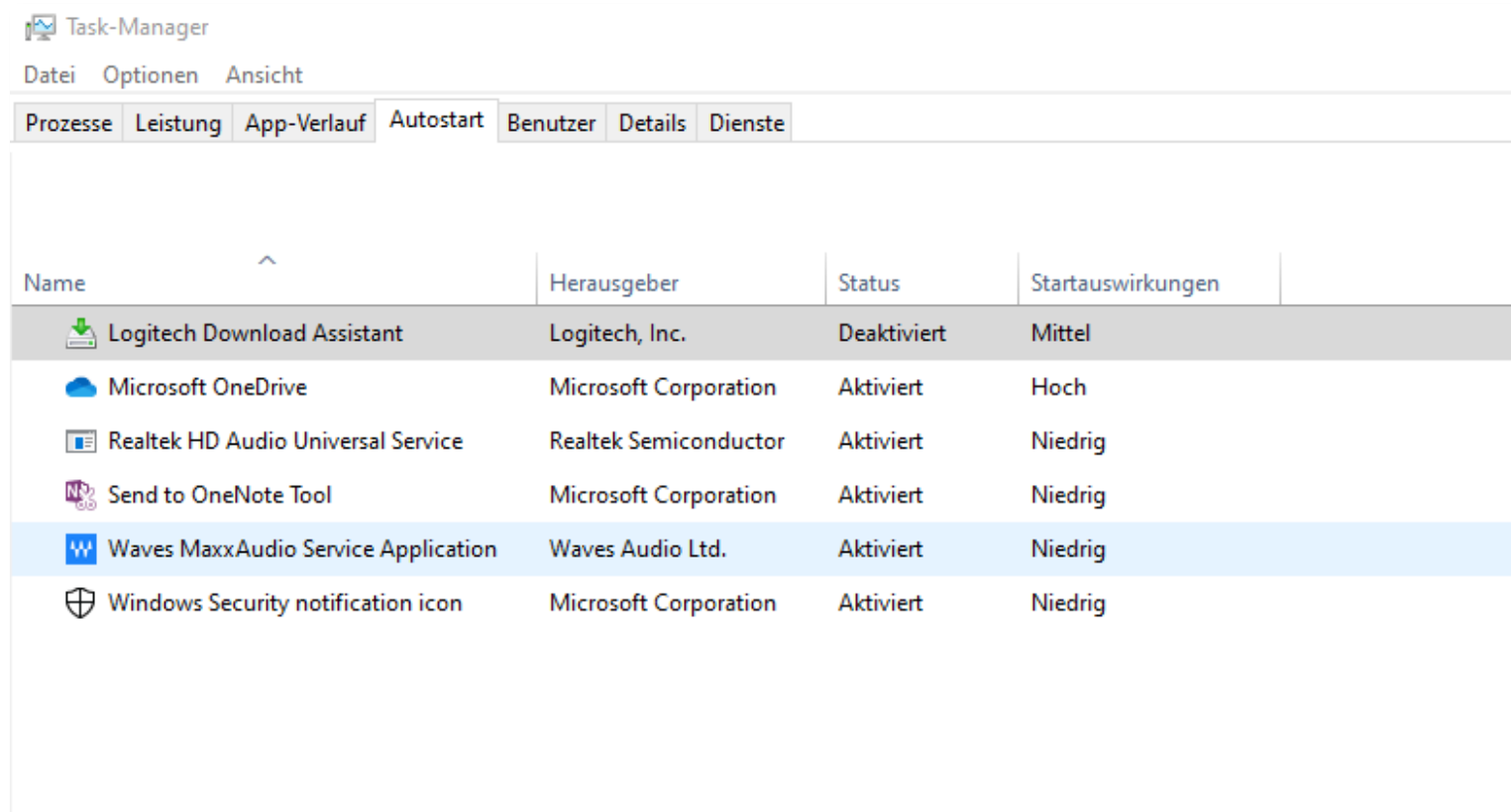
Prozesse Leistung App-Verlauf Autostart Benutzer Details Dienste

Ressourcenauslastung seit 23.06.2019 für aktuelles Benutzerkonto.  
[Auslastungsverlauf löschen](#)







Name	CPU-Zeit	Netzwerk	Getaktet (Netz...	Kachelupdates
Microsoft Edge	0:42:37	791,6 MB	0 MB	0 MB
Fotos	0:07:05	0,1 MB	0 MB	0 MB
Rechner	0:00:33	0 MB	0 MB	0 MB
Windows-Sicherheit	0:00:21	0 MB	0 MB	0 MB
Mail und Kalender	0:00:09	0,1 MB	0 MB	0 MB
Hilfe anfordern	0:00:03	1,2 MB	0 MB	0 MB
3D-Viewer	0:00:00	0 MB	0 MB	0 MB
Alarm & Uhr	0:00:00	0 MB	0 MB	0 MB
Ausschneiden und skizzi...	0:00:00	0 MB	0 MB	0 MB
Feedback-Hub	0:00:00	0 MB	0 MB	0 MB
Filme & TV	0:00:00	0 MB	0 MB	0 MB

# Task-Manager - Autostart

- zeigt die automatisch startenden Anwendungen und erlaubt deren Verwaltung

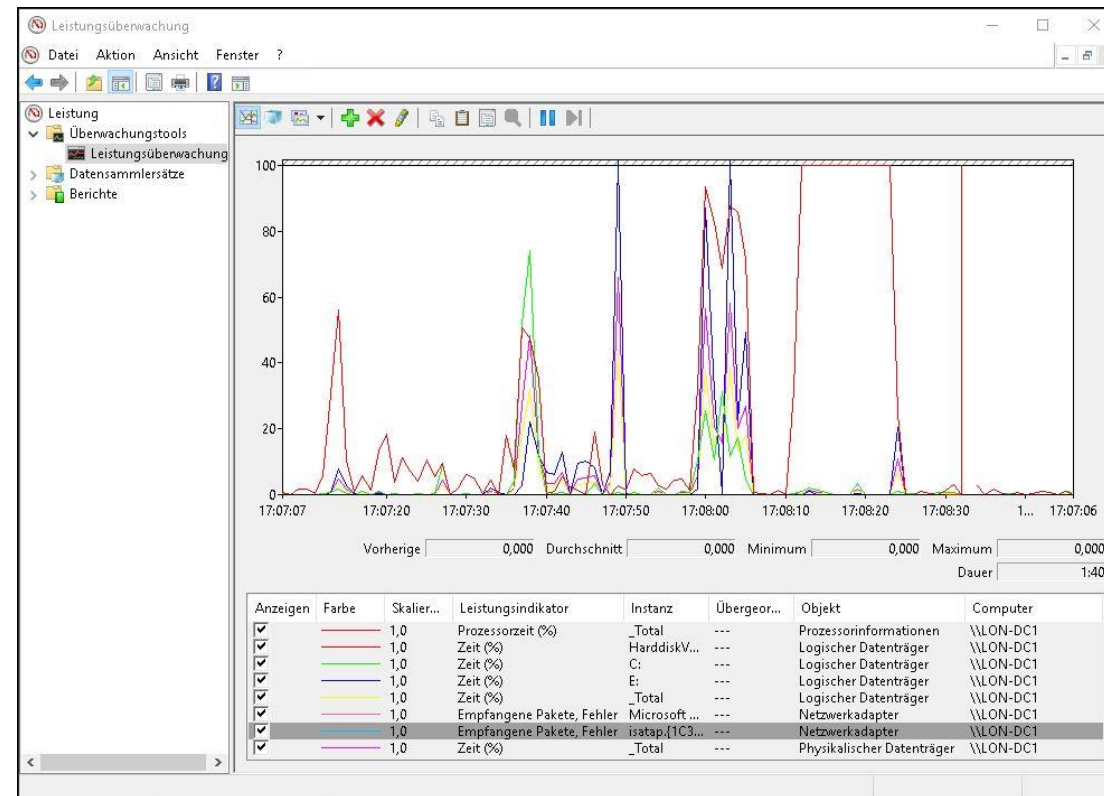


The screenshot shows the Windows Task Manager application with the 'Autostart' tab selected. The window title is 'Task-Manager'. The menu bar includes 'Datei', 'Optionen', and 'Ansicht'. The tab bar at the top contains 'Prozesse', 'Leistung', 'App-Verlauf', 'Autostart' (selected), 'Benutzer', 'Details', and 'Dienste'. The main area displays a table of autostart applications.

Name	Herausgeber	Status	Startauswirkungen
 Logitech Download Assistant	Logitech, Inc.	Deaktiviert	Mittel
 Microsoft OneDrive	Microsoft Corporation	Aktiviert	Hoch
 Realtek HD Audio Universal Service	Realtek Semiconductor	Aktiviert	Niedrig
 Send to OneNote Tool	Microsoft Corporation	Aktiviert	Niedrig
 Waves MaxxAudio Service Application	Waves Audio Ltd.	Aktiviert	Niedrig
 Windows Security notification icon	Microsoft Corporation	Aktiviert	Niedrig

# Leistungsüberwachung

- ermöglicht aktuelle Leistungsstatistiken oder historische Daten anzuzeigen, die von Datensammlersätzen gesammelt wurden



# Leistungsüberwachung

- diese vier zentralen Hardwarekomponenten sollten auf einem Windows 10-Gerät überwacht werden:
  - Prozessor
  - Festplatte
  - Arbeitsspeicher
  - Netzwerk
- ein Leistungsengpass tritt dann auf, wenn ein Computer die aktuellen Anfragen nach einer spezifischen Ressource nicht bedienen kann



# Leistungsüberwachung

## Primäre Prozessorindikatoren:

- Prozessor > % Prozessor-Zeit
- Prozessor > Interrupts/s
- System > Prozessor-Warteschlangenlänge

## Primäre Datenträgerindikatoren:

- Physikalischer Datenträger > % Zeit
- Physikalischer Datenträger > Durchschnittl. Länge der Datenträgerwarteschlange

## Primäre Netzwerkindikatoren:

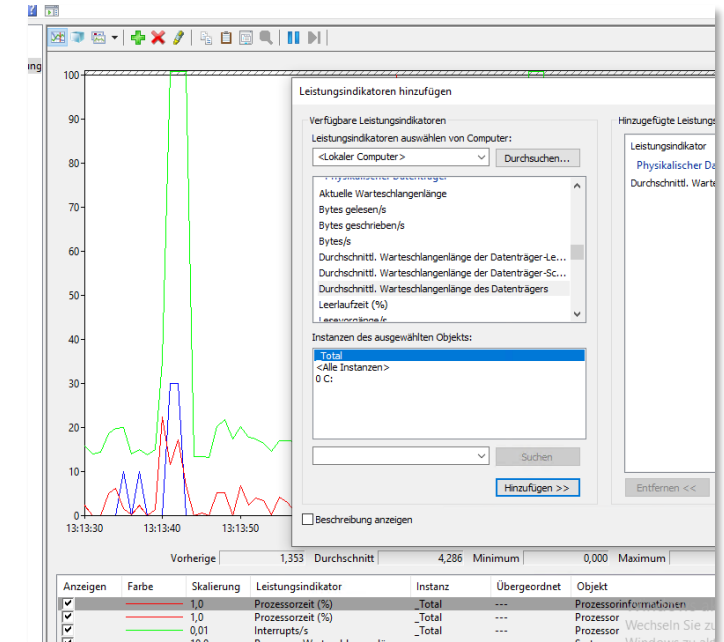
- Netzwerkschnittstelle > Aktuelle Bandbreite
- Netzwerkschnittstelle > Ausgabewarteschlangenlänge
- Netzwerkschnittstelle > Gesamtanzahl Bytes/s

## Primäre Arbeitsspeicherindikatoren:

- Speicher > Seiten/s

# Leistungsüberwachung - Leistungsmonitor

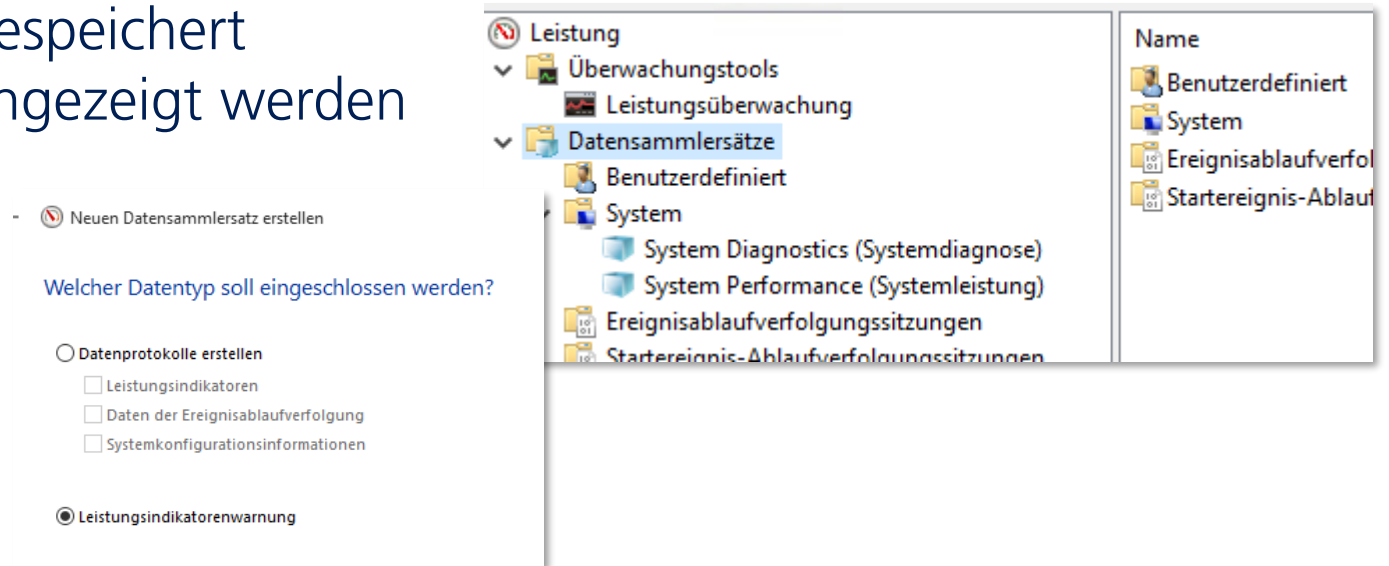
- Indikatoren müssen hinzugefügt werden
- Daten können in Echtzeit oder in Datensammlersätzen dargestellt werden
- Datensammlersätzen können leistungsbezogene und andere Systemstatistikdaten zur Analyse sammeln
- Datensammlersätze können die folgenden Datensammlertypen umfassen:
  - Leistungsindikatoren
  - Daten der Ereignisablaufverfolgung
  - Systemkonfigurationsinformationen



Leistung	Name	Typ
Überwachungstools	NT Kernel	Ab
Leistungsüberwachung	Operating System	Ko
Datensammlersätze	Processor	Ko
Benutzerdefiniert	System Services	Ko
System	Logical Disk Dirty Test	Ko
System Diagnostics (Systemdiagnose)	SMART Disk Check	Ko
System Performance (Systemleistung)	AntiSpywareProduct	Ko
Ereignisablaufverfolgungssitzungen	FirewallProduct	Ko
Startereignis-Ablaufverfolgungssitzungen	AntiVirusProduct	Ko
Berichte	UAC Settings	Ko

# Leistungsüberwachung - Datensammlersatz

- ist ein benutzerdefinierter Satz von Leistungsindikatoren, Ereignisablaufverfolgung, Systemkonfigurationsdaten oder Leistungsindikatorwarnungen
- kann nach Zeitplan, für eine bestimmte Dauer oder nach Erreichen eines Schwellenwertes erstellt werden
- Daten werden in Protokollen gespeichert
- können im Leistungsmonitor angezeigt werden
- vorkonfigurierte
  - System Diagnostics
  - System Performance
- Benutzerdefiniert



# Leistungsüberwachung - Baseline

Baseline ist ein definierter Datensammlersatz als Referenz für spätere Analysen

eine Baseline für die Leistung kann mit folgendem Zweck eingerichtet werden:

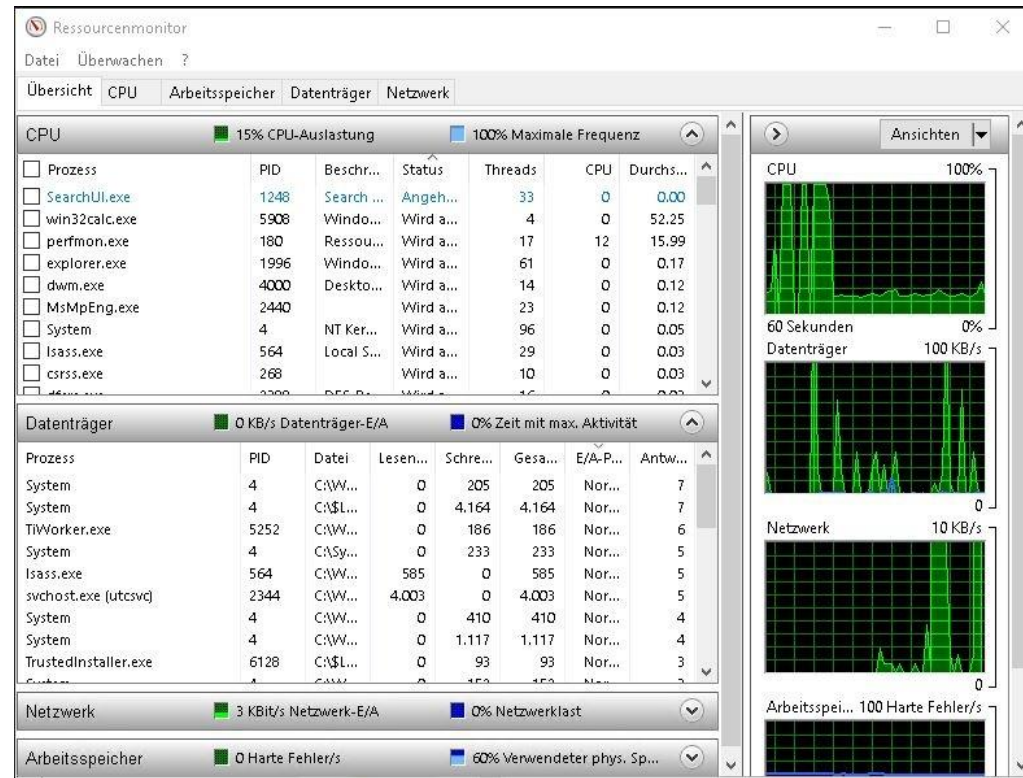
- Auswertung der Computerauslastung
- Überwachung der Systemressourcen
- Feststellung von Veränderungen und Trends in der Ressourcenauslastung
- Testen von Konfigurationsveränderungen
- Problemdiagnose

# Basislinie, Trends und Kapazitätsplanung

- durch Berechnung der leistungsbezogenen Baseline für die Umgebung können echtzeitbasierte Überwachungsdaten präziser interpretiert werden
- Einrichten einer Baseline ermöglicht:
  - Leistungstrends interpretieren
  - Kapazitätsplanung durchführen
  - Engpässe identifizieren
- Leistungstrends analysieren, um vorhersagen, zu welchem Zeitpunkt die vorhandenen Kapazitäten sehr wahrscheinlich ausgeschöpft sein werden
- Die Kapazitäten für die wichtigsten Hardwarekomponenten einplanen: Prozessor, Datenträger, Arbeitsspeicher und Netzwerk

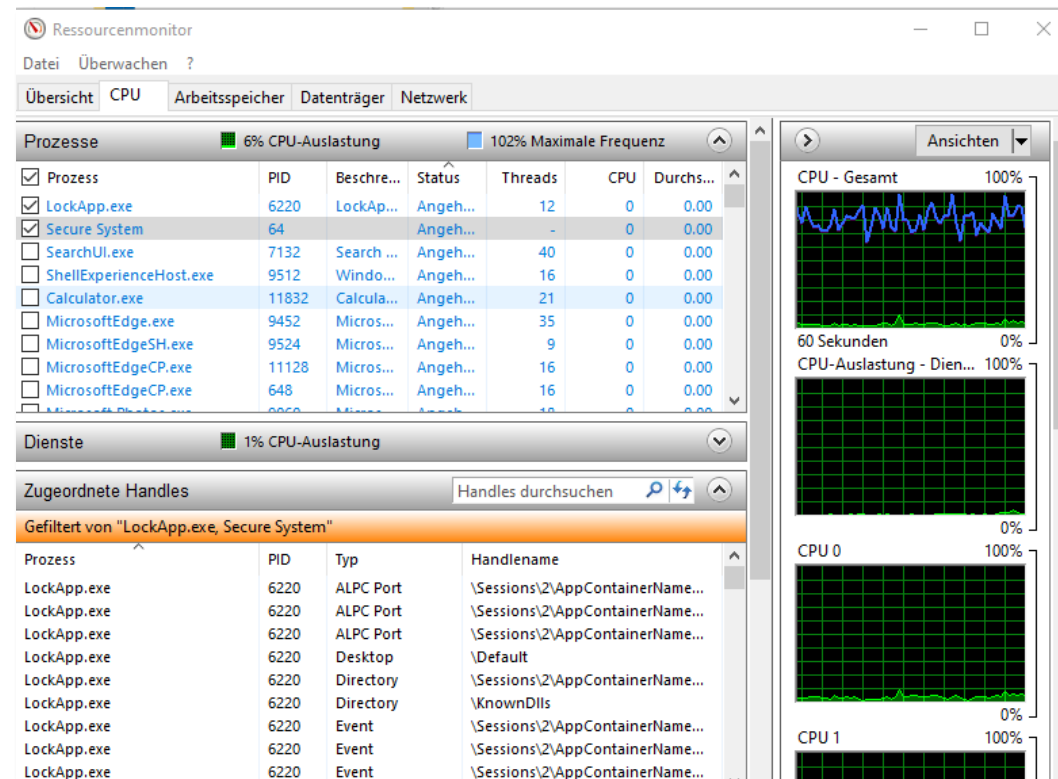
# Ressourcenmonitor

- bietet einen detaillierten Einblick in die Echtzeitleistung des Computers als der Task-Manager



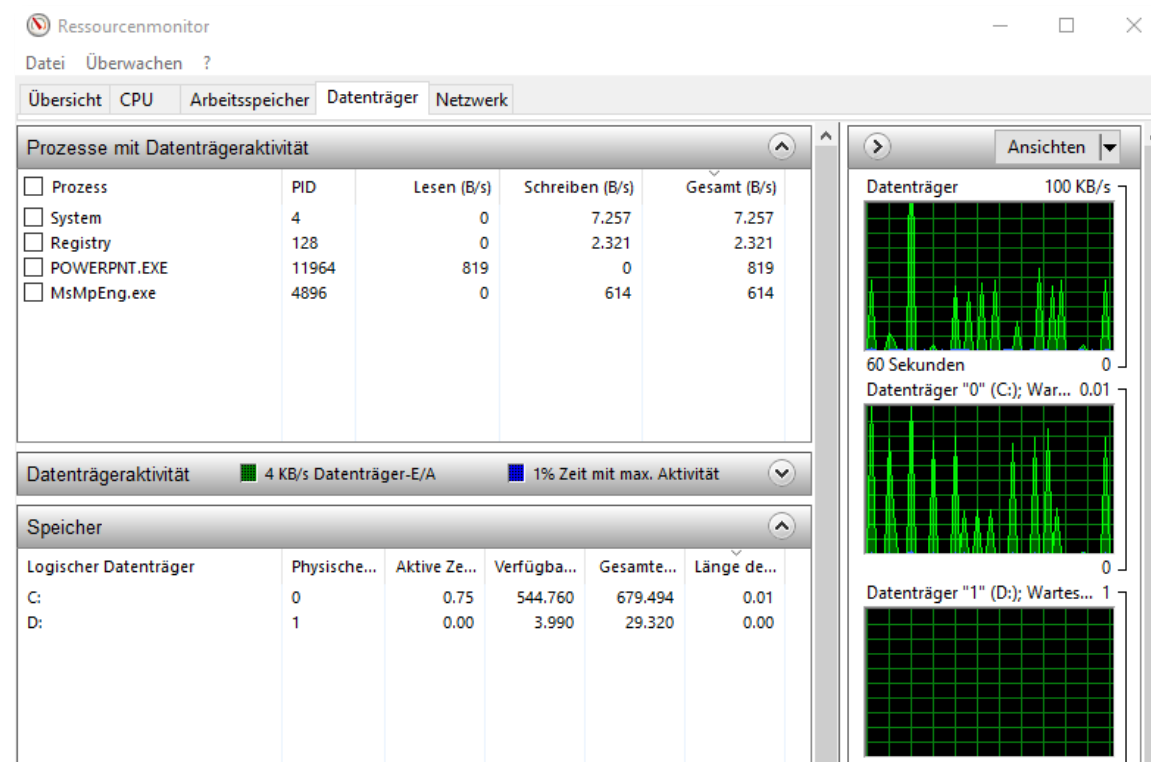
# Ressourcenmonitor - CPU

- Auslastung einzelner Kerne wird angezeigt
- Zugeordnete Handles und Module können analysiert werden



# Ressourcenmonitor - Datenträger

- Auslastung der Datenträger durch Prozesse wird angezeigt



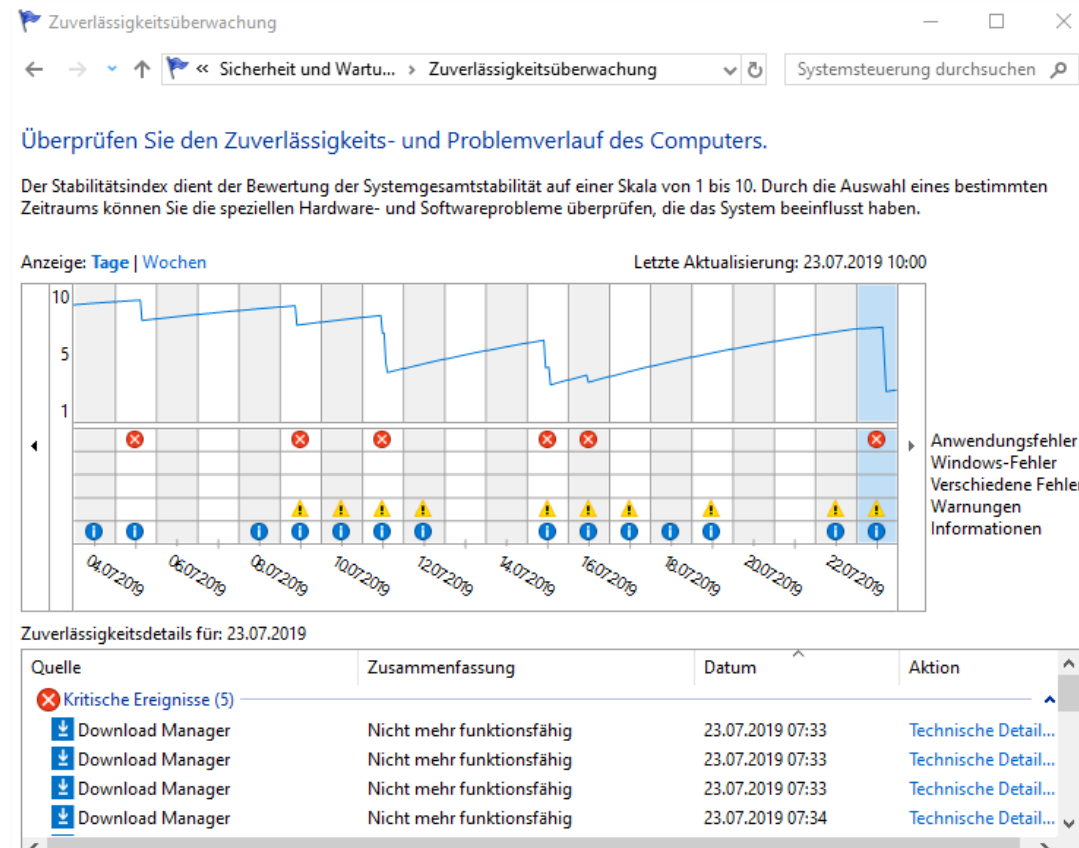


# Zuverlässigkeitsüberwachung

- Überwacht Hardware- und Softwareprobleme
- Stellt Stabilitätsindexzahl zur Verfügung (1 bis 10):
  - 1 stellt geringste Stabilität dar
  - 10 stellt höchste Stabilität dar
- Konsole Zuverlässigkeitsüberwachung enthält:
  - Historische Berichte zum Stabilitätsindex
  - Zuverlässigkeitsdetails
- Durchzuführende Aktion: speichert historische Daten, startet die Konsole Problembereiche, sucht online nach einer Lösung für ein spezifisches Problem

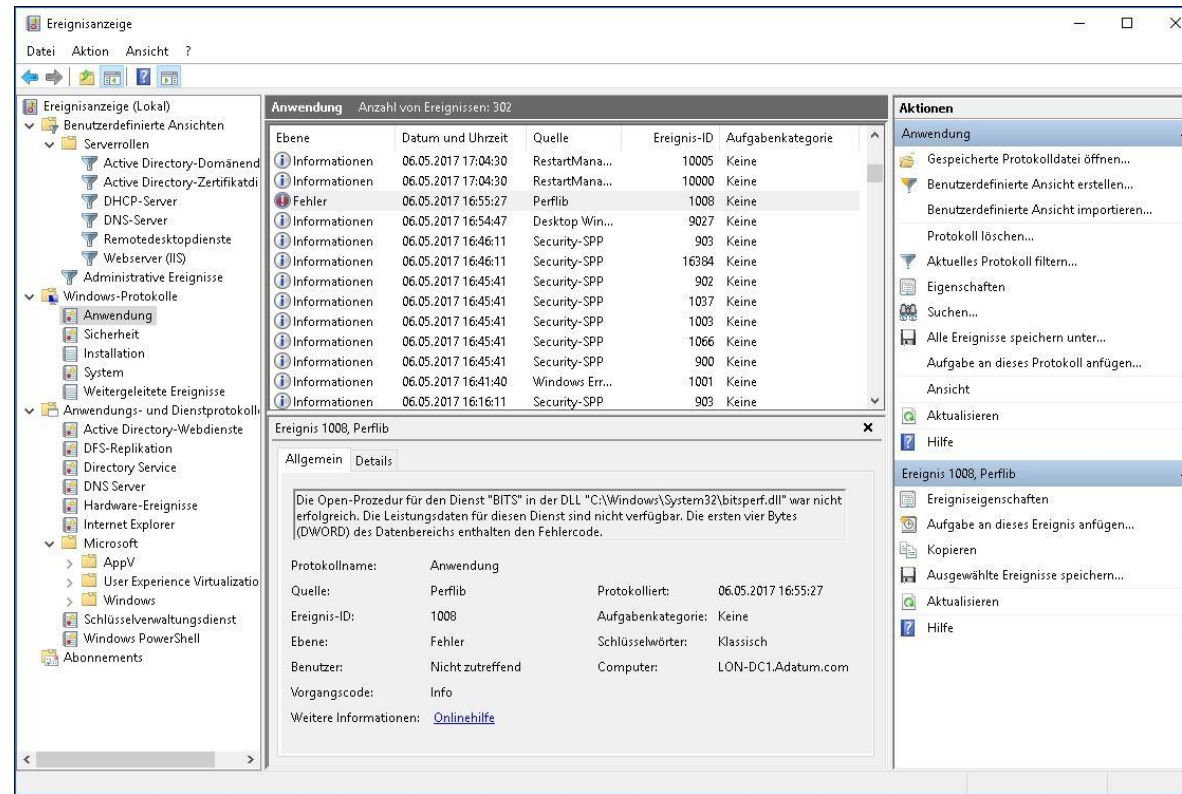
# Zuverlässigkeitsüberwachung

- verfolgt Hardware- und Softwareprobleme, die sich auf das System ausgewirkt haben



# Ereignisanzeige

- stellt kategorisierte Listen mit essenziellen Windows-Protokollereignissen für einzelne installierte Anwendungen und spezifische Windows-Komponentenkategorien bereit



# Ereignisanzeige

- mit der Ereignisanzeige können:
  - Mehrere Protokolle angezeigt werden
  - Benutzerdefinierte Ansichten erstellt werden
  - Aufgaben konfigurieren, die als Reaktion auf Ereignisse ausgeführt werden
  - Ereignisabonnements erstellt und verwaltet werden
- Die Ereignisanzeige verfügt über viele integrierte Protokolle wie:
  - Anwendungsprotokoll
  - Sicherheitsprotokoll
  - Installationsprotokoll
  - Systemprotokoll
  - Weitergeleitete Ereignisse



**VIELEN DANK  
FÜR IHRE  
AUFMERKSAMKEIT!**