



# Netzwerktechnik und Verteile Systeme

Sebastian Simon



The background image shows a server room with rows of server racks. The lighting is a deep blue, creating a high-tech atmosphere. A semi-transparent white rectangular box is overlaid on the left side of the image, containing the text 'Teil 5: Monitoring'.

# **Teil 5: Monitoring**

# Monitoring



- ist die Überwachung von Vorgängen
- systematischen Erfassungen (Protokollierungen), Messungen oder Beobachtungen eines Vorgangs
- dabei werden technischer Hilfsmittel oder anderer Beobachtungssysteme eingesetzt

# Monitoring (2)

- Es gibt viele Einsatzmöglichkeiten
  - Wildtiermonitoring
  - Monitoring von Industrieanlagen
  - Beobachtung von Himmelskörpern
  - Telemonitoring (Vitaldaten von Patienten)
  - Gewässermonitoring

# Monitoring (3)

- Wird gemacht um festzustellen, dass ein Prozess einen gewünschten Verlauf nimmt
  - zB ob der Meteorit wie vorhergesagt kollidiert
- Es können Schwellwerte definiert werden, die nicht überschritten werden dürfen
  - Gewässer werden ab Wasserstand x gefährlich
  - Fuchsbestand darf in Region y nicht unterschreiten



# Monitoring in der Informatik

- Service-Monitoring
  - Zur Überwachung des Server-Status
  - Läuft der Server?
  - Wie viele User sind aktuell eingeloggt?
  - ...
- Netzwerk-Monitoring
  - Überwachung von Netzwerk, Hardware, Diensten
  - Wie viel Datenvolumen geht über die Leitung?
  - Gibt es Störungen?

# Taskmanager ist auch Monitoring

The screenshot shows the Windows Task Manager window with the 'Prozesse' tab selected. The window has a blue title bar with the text 'Task-Manager' and standard window controls. Below the title bar is a menu bar with 'Datei', 'Optionen', and 'Ansicht'. Under 'Optionen', there are sub-tabs: 'Prozesse' (selected), 'Leistung', 'App-Verlauf', 'Autostart', 'Benutzer', 'Details', and 'Dienste'. The main area displays a table of running processes.

Name	Status	1% CPU	26% Arbeitss...	0% Datenträ...	0% Netzwerk
<b>Apps (2)</b>					
Task-Manager		0%	7.0 MB	0 MB/s	0 MBit/s
Windows-Explorer		0%	22.3 MB	0 MB/s	0 MBit/s
<b>Hintergrundprozesse (14)</b>					
COM Surrogate		0%	0.6 MB	0 MB/s	0 MBit/s
COM Surrogate		0%	1.8 MB	0 MB/s	0 MBit/s
Device Association Framework ...		0%	2.5 MB	0 MB/s	0 MBit/s
Hostprozess für Windows-Aufg...		0%	3.5 MB	0 MB/s	0 MBit/s
Microsoft Distributed Transacti...		0%	0.8 MB	0 MB/s	0 MBit/s
Microsoft Windows Search-Inde...		0%	6.0 MB	0 MB/s	0 MBit/s
Spoolersubsystem-Anwendung		0%	1.9 MB	0 MB/s	0 MBit/s
ThinPrint AutoConnect compo...		0%	1.1 MB	0 MB/s	0 MBit/s

At the bottom left, there is a button labeled 'Weniger Details' with an upward arrow icon. At the bottom right, there is a button labeled 'Task beenden'.

# Überblick über aktuelle Metriken

## Right Now



Running Process Instances



Open Incidents



Open Human Tasks

## Deployed

Process Definitions

31

Decision Definitions

7

Case Definitions

6

Deployments

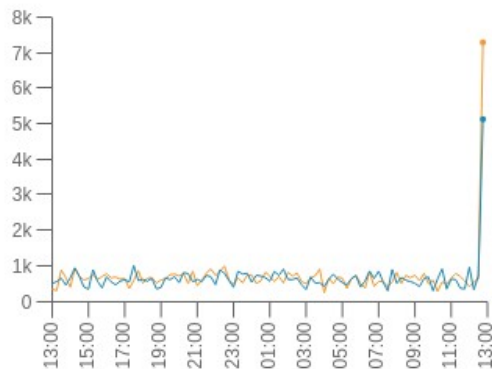
9

## Metrics

Today This week This month

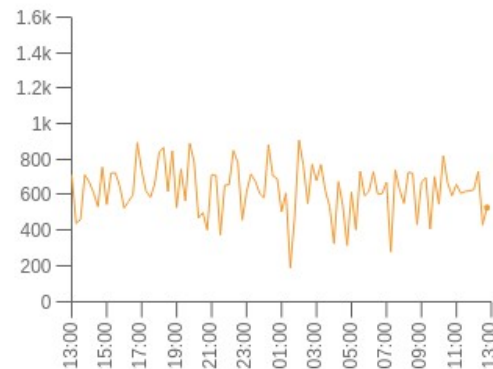
### Executed Activity Instances

Started ● Ended ●  
69.1k ↑ 65k ↑



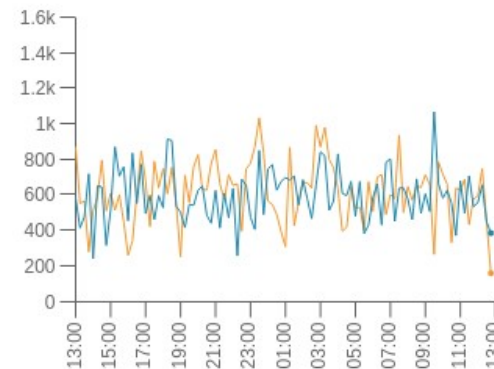
### Evaluated Decision Instances

Evaluated ●  
61.1k ↑



### Executed Jobs

Successful ● Failed ●  
60k ↑ 58.2k ↑





# Durchsuchen der Logdateien

**FILTERS: (3)** Level Alert ☒ Debug ☒ Error ☒ Clear All

**FILTERS** <<

- Log Type (1)
- Level (9)
  - ☒ Alert 11
  - ☒ Debug 9
  - ☐ Emergency 9
  - ☒ Error 12
  - [+ Show more](#)
- Node Name (1)
- IP Address (1)
- Machine Type (1)
- Vendor (1)

↓ DateTime

**failure** ☒ 🔍

4/16/2018 9:05:42 PM	dev-aus-rmat-01	SyslogGen %ASA-3-613004: Internal error: memory allocation failure	error	>
4/16/2018 9:05:42 PM	dev-aus-rmat-01	SyslogGen %ASA-6-613001: Checksum Failure in database in area string Link State Id IP_address Old	alert	>
4/16/2018 9:05:42 PM	dev-aus-rmat-01	SyslogGen %ASA-3-602306: IPSEC: SA change peer IP error, SPI: IPsec SPI, (src {original src IP address   or	debug	>
4/16/2018 9:05:32 PM	dev-aus-rmat-01	SyslogGen %ASA-3-444303: %SMART_LIC-3-COMM_FAILED: Communications failure with Cisco licensing	alert	>
4/16/2018 9:05:02 PM	dev-aus-rmat-01	SyslogGen %ASA-3-342003: REST API Agent failure notification received. Agent will be restarted	alert	>
4/16/2018 9:05:02 PM	dev-aus-rmat-01	SyslogGen %ASA-6-337001: Terminated BFD session with local discriminator <id> on <real_interface>	debug	>
4/16/2018 9:04:52 PM	dev-aus-rmat-01	SyslogGen %ASA-4-335005: NAC Downloaded ACL parse failure - host-address	error	>
4/16/2018 9:04:52 PM	dev-aus-rmat-01	SyslogGen %ASA-1-323006: Module ips experienced a data channel communication failure, data channel	error	>
4/16/2018 9:04:22 PM	dev-aus-rmat-01	SyslogGen %ASA-6-113005: AAA user authentication Rejected: reason = AAA failure: server = ip_addr	error	>
4/16/2018 9:04:12 PM	dev-aus-rmat-01	SyslogGen %ASA-2-105538: (Primary  Secondary) Failure reading response to route state request for	debug	>
4/16/2018 9:04:02 PM	dev-aus-rmat-01	SyslogGen %ASA-2-105533: (Primary  Secondary) Failure reading response to route-table change request	debug	>

# Microsoft Network Monitor

The screenshot displays the Microsoft Network Monitor 3.1 application window. The interface includes a menu bar (File, Edit, View, Frames, Capture, Filter, Tools, Help), a toolbar, and a sidebar with 'Network Conversations' (All Traffic, My Traffic, Other Traffic). The main area is divided into 'Frame Summary' and 'Frame Details' sections.

**Frame Summary Table:**

Frame Number	Time Offset	Conv Id	Source	Destination	Protocol Name	Description
50	2.907166		[Netgear Inc. 90F2E2]	[*BROADCAST]	WiFi	WiFi: [ ManagementBeacon] ....., (I), SSID = wlrgs0, Channel = 11
51	2.996171		192.168.2.115	192.168.2.20	RDP	RDP
52	2.997171		192.168.2.20	192.168.2.115	TCP	TCP: Flags=...A..., SrcPort=49206, DstPort=MS WBT Server(3389), Len=...
53	3.009172		[Netgear Inc. 90F2E2]	[*BROADCAST]	WiFi	WiFi: [ ManagementBeacon] ....., (I), SSID = wlrgs0, Channel = 11
54	3.097177		192.168.2.115	192.168.2.20	RDP	RDP
55	3.112178		[Netgear Inc. 90F2E2]	[*BROADCAST]	WiFi	WiFi: [ ManagementBeacon] ....., (I), SSID = wlrgs0, Channel = 11
56	3.214183		[Netgear Inc. 90F2E2]	[*BROADCAST]	WiFi	WiFi: [ ManagementBeacon] ....., (I), SSID = wlrgs0, Channel = 11
57	3.289188		192.168.2.20	192.168.2.115	TCP	TCP: Flags=...A..., SrcPort=49206, DstPort=MS WBT Server(3389), Len=...
58	3.316189		[Netgear Inc. 90F2E2]	[*BROADCAST]	WiFi	WiFi: [ ManagementBeacon] ....., (I), SSID = wlrgs0, Channel = 11
59	3.318189		192.168.2.22	192.168.2.121	ARP	ARP: Request, 192.168.2.22 asks for 192.168.2.121
60	3.332190		192.168.2.20	192.168.2.108	ARP	ARP: Request, 192.168.2.20 asks for 192.168.2.108
61	3.333190		192.168.2.108	192.168.2.20	ARP	ARP: Response, 192.168.2.108 at 00-0C-29-EC-F5-42
62	3.419195		[Netgear Inc. 90F2E2]	[*BROADCAST]	WiFi	WiFi: [ ManagementBeacon] ....., (I), SSID = wlrgs0, Channel = 11
63	3.521201		[Netgear Inc. 90F2E2]	[*BROADCAST]	WiFi	WiFi: [ ManagementBeacon] ....., (I), SSID = wlrgs0, Channel = 11
64	3.624207		[Netgear Inc. 90F2E2]	[*BROADCAST]	WiFi	WiFi: [ ManagementBeacon] ....., (I), SSID = wlrgs0, Channel = 11
65	3.660209		192.168.2.115	192.168.2.20	RDP	RDP
66	3.726213		[Netgear Inc. 90F2E2]	[*BROADCAST]	WiFi	WiFi: [ ManagementBeacon] ....., (I), SSID = wlrgs0, Channel = 11
67	3.828219		[Netgear Inc. 90F2E2]	[*BROADCAST]	WiFi	WiFi: [ ManagementBeacon] ....., (I), SSID = wlrgs0, Channel = 11
68	3.859220		192.168.2.20	192.168.2.115	TCP	TCP: Flags=...A..., SrcPort=49206, DstPort=MS WBT Server(3389), Len=...
69	3.894222		192.168.2.115	192.168.2.20	RDP	RDP
70	3.931224		[Netgear Inc. 90F2E2]	[*BROADCAST]	WiFi	WiFi: [ ManagementBeacon] ....., (I), SSID = wlrgs0, Channel = 11

**Frame Details (Frame 59):**

- WiFi: [Encrypted Data] F...E, (I)
- LLC: Unnumbered(U) Frame, Command Frame, SSAP = SN
- Snap: EtherType = ARP, OrgCode = XEROX CORPORATION
- Arp: Request, 192.168.2.22 asks for 192.168.2.121
  - HardwareType: Ethernet
  - ProtocolType: Internet IP (IPv4)
  - HardwareAddressLen: 6 (0x6)
  - ProtocolAddressLen: 4 (0x4)
  - OpCode: Request, 1(0x1)
  - SendersMacAddress: 00-0C-29-52-15-4C

**Hex Details:**

Offset	Hex	ASCII
0000	02 20 00 04 00 00 00 00 00 00	. . . . .
0009	00 00 05 00 00 00 00 9E 09 00	. . . . .
0012	00 28 00 00 00 02 49 DE 97	. ( . . . ID
001B	A8 C8 CF C8 01 08 42 00 00	" E I E . B .
0024	FF FF FF FF FF FF 00 14 6C	ÿÿÿÿÿÿ. 1
002D	90 F2 E2 00 0C 29 52 15 4C	ó á . . ) R L
0036	D0 29 AA AA 03 00 00 00 08	D) * . . . .
003F	06 00 01 08 00 06 04 00 01	. . . . .
0048	00 0C 29 52 15 4C C0 A8 02	. . ) R L A .
0051	16 00 00 00 00 00 00 C0 A8	. . . . . A
005A	02 79 00 00 00 00 00 00 00	. y . . . . .
0063	00 00 00 00 00 00 00 00 00	. . . . .
006C	00 00 00 00 00 00 00 00 00	. . . . .

Version 3.1.512.0      Displayed: 156      Captured: 156      Sel Frame: 59 (Tot: 1)      Prot Off: 14 (0x0E)      Frame Off: 78 (0x4E)      Sel Bytes: 4

# Microsoft Network Monitor (2)

- Ermöglicht den Netzwerkverkehr des Servers aufzuzeichnen
- Einschränkung was aufgezeichnet werden soll kann konfiguriert werden (zB nur DNS-Pakete)
- Traffic kann analysiert werden
- Inhalt einzelner Pakete einsehbar
  - Ähnlich wie in Wireshark



# Proaktiv vs. Reaktiv

- Reaktiv: Bei Auftritt eines Problems werden die Metriken aus dem Monitoring analysiert
  - User können sich nicht einloggen, Systemmonitor zeigt Überlastung der Server, Admin weist dem Server weitere Ressourcen zu
- Proaktiv: Ich prüfe laufend die verschiedenen Metriken des Systems und versuche rechtzeitig gegenzusteuern bevor Problem auftreten
  - Monitoring zeigt, dass Server > 90% ausgelastet sind, Tendenz steigend. Admin weist weitere Ressourcen zu

# Proaktiv vs. Reaktiv (2)

- Wartungskosten bei proaktiven Ansatz höher
- Wahrscheinlichkeit und Dauer von Systemausfällen sind bei reaktivem Ansatz höher
- Ausfall des Systems kann auch viel Geld kosten (zB 1000 Mitarbeiter können einen Vormittag nicht arbeiten)
- Welcher Ansatz gewählt wird muss im Einzelfall entschieden werden
- Große Systeme sollten aktiv überwacht werden