10.1 Ziele und Grundlagen des Monitoring and Event Management

> **Kurz erklärt**
>
> Monitoring and Event Management sorgt dafür, dass der Zustand von IT-Services und IT-Systemen kontinuierlich überwacht wird.
>
> Ziel ist es, Abweichungen möglichst früh zu erkennen, bevor daraus Incidents oder Serviceunterbrechungen entstehen.
>
> Ereignisse (Events) werden gesammelt, bewertet und – je nach Bedeutung – automatisch verarbeitet oder an die zuständigen Teams weitergeleitet.

Was ist Monitoring and Event Management?

Monitoring and Event Management ist eine ITIL Practice zur kontinuierlichen Überwachung von Services, Systemen und Infrastruktur.

Dabei werden Informationen über den aktuellen Zustand gesammelt und ausgewertet.

Beispiele:

- Server erreichbar?
- CPU-Auslastung zu hoch?
- Festplatte fast voll?
- Backup erfolgreich?
- Zertifikat läuft bald ab?
- Datenbank antwortet?
- Netzwerkverbindung aktiv?
- Webservice erreichbar?
- Temperatur im Serverraum normal?

Das Ziel besteht darin, Probleme möglichst frühzeitig zu erkennen.

Warum Monitoring wichtig ist

Ohne Monitoring werden viele Probleme erst bemerkt,

wenn Benutzer sie melden.

Dadurch entstehen:

- längere Ausfallzeiten,
- mehr Incidents,
- höhere Kosten,
- unzufriedene Benutzer,
- größere Geschäftsrisiken.

Ein gutes Monitoring erkennt viele Probleme bereits,

bevor Benutzer betroffen sind.

Ziele des Monitoring and Event Management

Die wichtigsten Ziele sind:

- frühzeitige Fehlererkennung,
- schnelle Reaktion,
- Verfügbarkeit erhöhen,
- Ausfälle vermeiden,
- automatische Benachrichtigung,
- Automatisierung unterstützen,
- Servicequalität verbessern,
- Trends erkennen,
- Ursachenanalyse erleichtern.

Monitoring ersetzt dabei keine Fehlerbehebung.

Es liefert die notwendigen Informationen.

Monitoring und Event Management unterscheiden

Diese beiden Begriffe werden häufig gemeinsam verwendet,

beschreiben jedoch unterschiedliche Aufgaben.

Monitoring	Event Management
sammelt Messwerte	bewertet Ereignisse
überwacht Systeme	entscheidet über Reaktionen
erkennt Veränderungen	verarbeitet Events
liefert Daten	löst Aktionen aus

Monitoring erzeugt Events.

Event Management verarbeitet diese.

Was ist ein Event?

Ein Event ist jede erkennbare Veränderung des Zustands eines Services oder Configuration Items.

Ein Event kann beispielsweise entstehen durch:

- Anmeldung,
- Fehler,
- Neustart,
- Backup,
- Alarm,
- Warnung,
- Hardwareausfall,
- erfolgreiche Aktualisierung,
- Zertifikatsablauf,
- Überschreiten eines Grenzwerts.

Nicht jedes Event bedeutet automatisch ein Problem.

Event ist nicht gleich Incident

Ein häufiger Irrtum:

> Jedes Event ist ein Incident.

Das stimmt nicht.

Beispiel:

Ein Server startet nach einer geplanten Wartung neu.

Das Monitoring erzeugt ein Event.

Da die Änderung geplant war,

liegt kein Incident vor.

Beispiel eines echten Incidents

Das Monitoring erkennt:

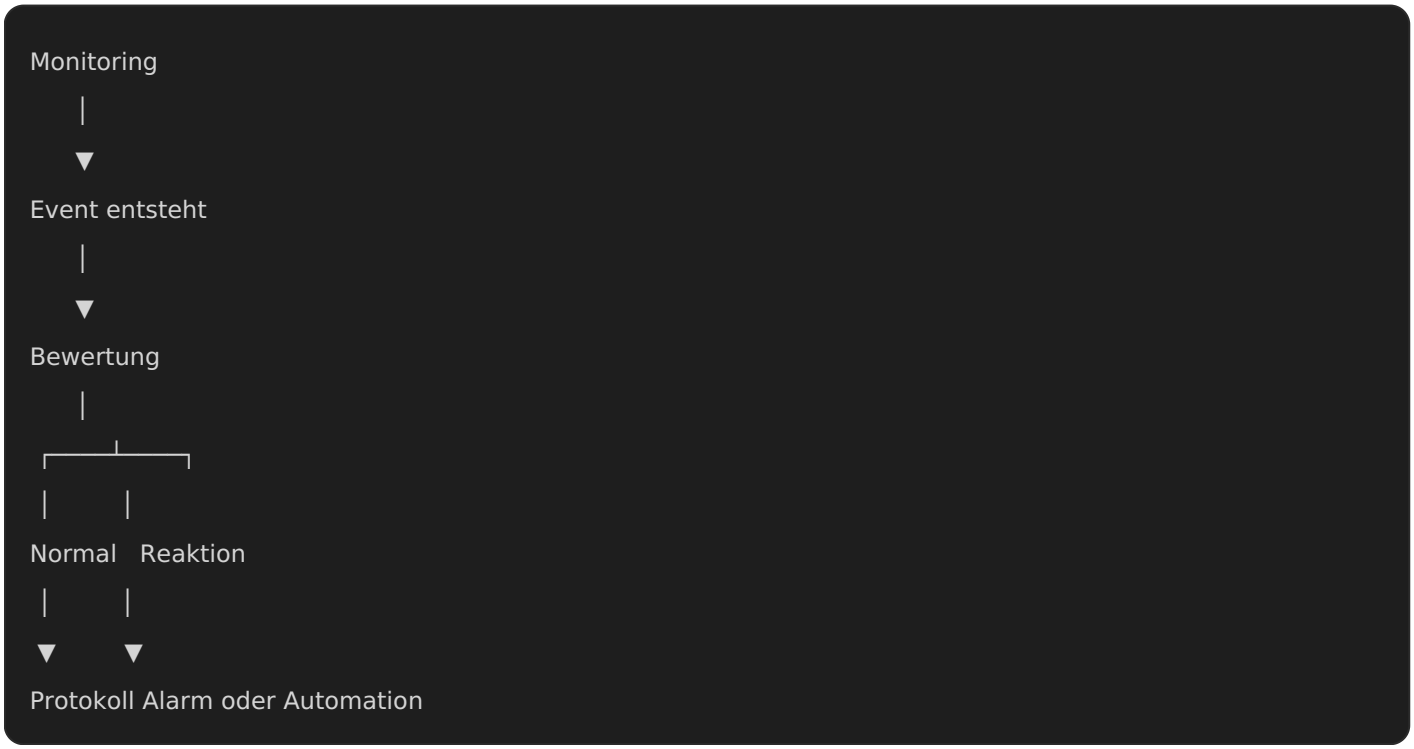
- Webserver nicht erreichbar.

Es existiert:

- keine geplante Wartung,
- kein geplanter Change.

Jetzt entsteht aus dem Event möglicherweise ein Incident.

Informationsfluss



Nicht jedes Event benötigt menschliches Eingreifen.

Arten von Monitoring

Typische Bereiche:

- Server
- Netzwerk
- Cloud
- Datenbanken
- Anwendungen
- Container
- virtuelle Maschinen
- Speicher
- Backup
- Sicherheit

- Zertifikate
- Hardware
- Umgebungsbedingungen

Je nach Service kommen unterschiedliche Überwachungen zum Einsatz.

Technisches Monitoring

Technisches Monitoring überwacht einzelne Komponenten.

Beispiele:

- CPU-Auslastung,
- RAM-Auslastung,
- Festplattenbelegung,
- Netzwerkverkehr,
- Temperatur,
- Lüfter,
- Spannungsversorgung,
- Hardwarefehler.

Es beantwortet die Frage:

> “ Funktioniert das System technisch?

Service Monitoring

Service Monitoring betrachtet den Service aus Benutzersicht.

Beispiele:

- Anmeldung möglich?
- Website erreichbar?
- E-Mail versendbar?
- Datenbankabfrage erfolgreich?
- VPN-Anmeldung funktioniert?
- API antwortet korrekt?

Ein Server kann technisch erreichbar sein,

während der eigentliche Service bereits gestört ist.

Aktives Monitoring

Beim aktiven Monitoring werden Systeme regelmäßig geprüft.

Beispiele:

- Ping,
- HTTP-Aufruf,
- Datenbankanmeldung,
- DNS-Abfrage,
- SMTP-Test,
- API-Aufruf.

Die Prüfungen erfolgen automatisch in festgelegten Intervallen.

Passives Monitoring

Beim passiven Monitoring senden Systeme selbst Informationen.

Beispiele:

- Syslog,
- Windows Event Log,
- SNMP-Traps,
- Sicherheitsmeldungen,
- Container-Logs,
- Anwendungsprotokolle.

Hier wartet das Monitoring auf eintreffende Ereignisse.

Synthetisches Monitoring

Synthetisches Monitoring simuliert typische Benutzeraktionen.

Beispiele:

- Benutzer anmelden,
- Bestellung durchführen,
- Suchfunktion testen,
- Datei hochladen,
- VPN verbinden.

Dadurch wird geprüft,

ob ein Service tatsächlich nutzbar ist.

Real User Monitoring (RUM)

Beim Real User Monitoring werden echte Benutzeraktionen ausgewertet.

Beispiele:

- Ladezeiten,
- Antwortzeiten,
- Fehlermeldungen,
- Browserdaten,
- Standortinformationen.

Dadurch erhält die IT Informationen über die tatsächliche Benutzererfahrung.

Überwachungsobjekte

Monitoring kann sich beziehen auf:

- Configuration Items,
- Services,
- Anwendungen,
- Netzwerke,
- Cloud-Ressourcen,
- Container,
- Datenbanken,
- APIs,
- Sicherheitskomponenten,
- Backup-Systeme.

Nicht jedes Objekt benötigt dieselbe Überwachung.

Grenzwerte (Thresholds)

Viele Überwachungen arbeiten mit Grenzwerten.

Beispiele:

Messwert	Grenzwert
CPU	über 90 %
RAM	über 95 %
Festplatte	über 85 % belegt
Zertifikat	läuft in 30 Tagen ab
Backup	fehlgeschlagen
Antwortzeit	über 2 Sekunden

Grenzwerte sollten regelmäßig überprüft werden.

Frühwarnungen

Nicht jeder Alarm muss sofort kritisch sein.

Beispiel:

Festplatte:

- 70 % → normal
- 85 % → Warnung
- 95 % → kritisch

Dadurch bleibt genügend Zeit,

Probleme zu beheben.

Alarmmüdigkeit (Alert Fatigue)

Zu viele unnötige Alarme führen dazu,

dass wichtige Warnungen übersehen werden.

Typische Ursachen:

- falsche Grenzwerte,
- doppelte Alarme,
- bekannte Ereignisse,
- ungefilterte Meldungen,
- schlecht abgestimmtes Monitoring.

Ein gutes Monitoring erzeugt möglichst wenige,

aber relevante Alarme.

Praxisbeispiel

Das Monitoring erkennt:

- Zertifikat läuft in 30 Tagen ab.

Es entsteht:

- Warnung,

- Ticket,
- Benachrichtigung an den Administrator.

Das Zertifikat wird rechtzeitig erneuert.

Ein späterer Incident wird vermieden.

Typische Fehler

Fehler 1

Monitoring existiert nur für Server,

nicht für Services.

Fehler 2

Grenzwerte sind ungeeignet.

Fehler 3

Zu viele unnötige Alarme.

Fehler 4

Alarme werden nicht bearbeitet.

Fehler 5

Backups werden nicht überwacht.

Fehler 6

Zertifikate werden nicht überwacht.

Fehler 7

Monitoring erkennt Fehler erst nach Benutzerbeschwerden.

Fehler 8

Monitoring wird nach Änderungen nicht angepasst.

Checkliste Monitoring

- [ ] kritische Services überwacht
- [ ] wichtige Configuration Items überwacht
- [ ] sinnvolle Grenzwerte definiert
- [ ] Alarme getestet
- [ ] Benachrichtigungen funktionieren
- [ ] Zertifikate überwacht
- [ ] Backups überwacht
- [ ] Dokumentation aktuell
- [ ] Verantwortlichkeiten festgelegt
- [ ] regelmäßige Überprüfung geplant

Bedeutung für Fachinformatiker für Systemintegration

Monitoring gehört zu den täglichen Aufgaben vieler Fachinformatiker.

Typische Tätigkeiten:

- Monitoring konfigurieren,
- Alarme auswerten,
- Grenzwerte anpassen,
- Logs analysieren,
- Events bewerten,
- Incidents erkennen,
- Automatisierungen entwickeln,
- Monitoring kontinuierlich verbessern.

Ein gut aufgebautes Monitoring verhindert viele Störungen, bevor Benutzer sie überhaupt bemerken.

Zusammenfassung

> Systeme und Services überwachen
>
> ↓

> Messwerte sammeln
>
> ↓
>
> Event erzeugen
>
> ↓
>
> Event bewerten
>
> ↓
>
> Alarm oder Automatisierung
>
> ↓
>
> Incident vermeiden oder bearbeiten
>
> ↓
>
> Service stabil halten

Merksätze

> “ Monitoring sammelt Informationen – Event Management bewertet sie.

> “ Nicht jedes Event ist ein Incident.

> “ Gutes Monitoring erkennt Probleme vor den Benutzern.

> “ Service Monitoring ist wichtiger als reine Serverüberwachung.

> “ Wenige aussagekräftige Alarme sind besser als viele unnötige Warnungen.

Verwandte Seiten

- 10.2 Event-Typen, Filter und Priorisierung
- 10.3 Alarme, Eskalationen und Automatisierung
- 10.4 Monitoring-Werkzeuge, Dashboards und Kennzahlen
- 10.5 Zusammenspiel mit Incident, Problem, Change und Service Configuration Management
- Incident Management
- Service Configuration Management
- Service Level Management
- Continual Improvement

Quellen und Versionsstand

Offizielle Grundlagen

- PeopleCert – ITIL Practice Guide: Monitoring and Event Management
- ITIL Foundation – Version 5

Einordnung

Die dargestellten Monitoring-Arten, Beispiele und Grenzwerte sind herstellerneutrale Praxisempfehlungen. ITIL schreibt keine konkreten Monitoring-Werkzeuge oder festen Schwellenwerte vor. Diese richten sich nach den überwachten Services, den Geschäftsanforderungen und der technischen Umgebung.

Behandelter Framework-Stand: ITIL Version 5
Zusätzlich berücksichtigt: aktuelle ITIL-4-Practice-Guidance
Fachlicher Stand: August 2026
