11.4 Pflege, Discovery und Datenqualität

> **Kurz erklärt**
>
> Eine Configuration Management Database (CMDB) ist nur dann hilfreich, wenn ihre Informationen aktuell und korrekt sind.
>
> Deshalb gehören die kontinuierliche Pflege, automatische Discovery-Verfahren und die regelmäßige Überprüfung der Datenqualität zu den wichtigsten Aufgaben des Service Configuration Management.
>
> Ziel ist es, jederzeit eine zuverlässige Informationsbasis für Incident Management, Problem Management, Change Enablement und andere ITIL Practices bereitzustellen.

Warum Datenqualität entscheidend ist

Eine unvollständige oder veraltete CMDB kann mehr Schaden anrichten als gar keine CMDB.

Falsche Informationen führen beispielsweise zu:

- fehlerhaften Changes,
- unnötigen Incidents,
- falschen Prioritäten,
- längeren Ausfallzeiten,
- ungenauen Auswirkungsanalysen,
- erhöhtem Arbeitsaufwand.

Eine hohe Datenqualität ist daher wichtiger als eine möglichst große Anzahl gespeicherter Configuration Items.

Was bedeutet Datenqualität?

Datenqualität beschreibt,

wie zuverlässig und nutzbar Informationen sind.

Wichtige Qualitätsmerkmale:

- vollständig,
- aktuell,
- korrekt,

- eindeutig,
- konsistent,
- nachvollziehbar,
- relevant.

Nur wenn diese Eigenschaften erfüllt sind,

können andere ITIL Practices auf die Daten vertrauen.

Vollständigkeit

Alle erforderlichen Informationen sollten vorhanden sein.

Beispiele:

- Verantwortlicher,
- Status,
- Beziehungen,
- Version,
- Servicezuordnung,
- Standort.

Fehlende Informationen erschweren spätere Entscheidungen.

Aktualität

Configuration-Daten müssen Änderungen zeitnah widerspiegeln.

Beispiele:

- neuer Server,
- neue IP-Adresse,
- Firmware-Update,
- neuer Standort,
- neue Beziehungen,
- Außerbetriebnahme.

Veraltete Informationen führen schnell zu Fehlentscheidungen.

Korrektheit

Die gespeicherten Informationen müssen der Realität entsprechen.

Beispiel:

Die CMDB enthält:

> Windows Server 2022

Tatsächlich läuft:

> Windows Server 2025

Solche Abweichungen können Fehleranalysen und Sicherheitsmaßnahmen erheblich erschweren.

Konsistenz

Informationen dürfen sich nicht widersprechen.

Beispiel:

Die CMDB nennt als Verantwortlichen das Linux-Team,

während die Dokumentation das Windows-Team aufführt.

Solche Widersprüche sollten vermieden werden.

Was ist Discovery?

Discovery bezeichnet die automatische Erkennung von Configuration Items und ihren Eigenschaften.

Discovery-Werkzeuge können beispielsweise erkennen:

- Server,
- Betriebssysteme,
- virtuelle Maschinen,
- Container,
- Netzwerkgeräte,
- installierte Software,
- IP-Adressen,
- Dienste,
- Cloud-Ressourcen.

Dadurch sinkt der manuelle Pflegeaufwand erheblich.

Wie funktioniert Discovery?

Je nach Werkzeug kommen unterschiedliche Verfahren zum Einsatz.

Beispiele:

- Netzwerk-Scans,
- SNMP,
- WMI,
- SSH,
- WinRM,
- Hypervisor-Schnittstellen,
- Cloud-APIs,
- Agenten,
- Kubernetes-APIs.

Welche Methode verwendet wird,

hängt von der jeweiligen Infrastruktur ab.

Agentenbasierte Discovery

Ein Agent wird direkt auf dem System installiert.

Vorteile:

- viele Detailinformationen,
- regelmäßige Aktualisierung,
- hohe Genauigkeit.

Nachteile:

- zusätzlicher Verwaltungsaufwand,
- Software muss installiert werden.

Agentenlose Discovery

Hier erfolgt die Erkennung über Netzwerkprotokolle oder Programmierschnittstellen.

Vorteile:

- keine zusätzliche Software auf den Zielsystemen,
- einfache Einführung.

Nachteile:

- teilweise geringerer Detailgrad,
- Zugriff auf geeignete Schnittstellen erforderlich.

Automatisch erkannte Informationen

Discovery kann beispielsweise erfassen:

- Hostname,
- IP-Adresse,
- Betriebssystem,
- CPU,
- Arbeitsspeicher,
- Festplatten,
- installierte Software,
- Netzwerkadapter,
- Dienste,
- offene Ports.

Nicht alle Informationen lassen sich automatisch erkennen.

Was Discovery nicht erkennt

Geschäftsbezogene Informationen müssen häufig manuell ergänzt werden.

Beispiele:

- Service Owner,
- Kritikalität,
- Geschäftsprozess,
- SLA,
- Kostenstelle,
- Ansprechpartner,
- interne Dokumentationen.

Diese Informationen entstehen meist außerhalb der technischen Infrastruktur.

Regelmäßige Discovery

Discovery sollte regelmäßig ausgeführt werden.

Beispiele:

- täglich,
- stündlich,
- nach Changes,

- nach Deployments.

Dadurch bleiben Änderungen möglichst aktuell.

Abgleich mit der CMDB

Nach einer Discovery werden erkannte Änderungen mit der CMDB verglichen.

Mögliche Ergebnisse:

- neues CI gefunden,
- bestehendes CI geändert,
- CI entfernt,
- Version geändert,
- neue Beziehung erkannt.

Nicht jede Änderung wird automatisch übernommen.

Je nach Organisation erfolgt zunächst eine Prüfung.

Manuelle Pflege

Auch bei umfangreicher Discovery bleibt manuelle Pflege notwendig.

Typische Aufgaben:

- Servicezuordnung,
- Verantwortlichkeiten,
- Dokumentationen,
- Beziehungen,
- Kritikalität,
- Genehmigungen.

Automatische Verfahren ersetzen diese Arbeiten nicht vollständig.

Qualitätssicherung

Configuration-Daten sollten regelmäßig überprüft werden.

Mögliche Maßnahmen:

- Stichproben,
- Audits,
- automatische Plausibilitätsprüfungen,
- Vergleich mit Inventarsystemen,

- Vergleich mit Monitoring,
- Review nach Changes.

Dadurch lassen sich Fehler früh erkennen.

Configuration Audits

Ein Configuration Audit überprüft,

ob die dokumentierten Informationen der tatsächlichen Umgebung entsprechen.

Beispielsweise wird geprüft:

- Existiert das CI noch?
- Stimmen Versionen?
- Sind Beziehungen aktuell?
- Wurde ein Change korrekt dokumentiert?
- Stimmen Verantwortlichkeiten?

Audits erhöhen die Zuverlässigkeit der CMDB.

Data Owner

Für wichtige Configuration Items sollte klar geregelt sein,

wer für die Daten verantwortlich ist.

Typische Verantwortliche:

- Windows-Team,
- Linux-Team,
- Netzwerk-Team,
- Datenbankadministration,
- Cloud-Team,
- Service Owner.

Dadurch bleibt die Pflege dauerhaft sichergestellt.

Kennzahlen zur Datenqualität

Auch Datenqualität kann gemessen werden.

Beispiele:

- Anteil vollständiger CIs,

- Anzahl veralteter Einträge,
- Discovery-Erfolgsquote,
- Anzahl widersprüchlicher Datensätze,
- Aktualisierungsdauer nach einem Change,
- Audit-Ergebnisse.

Diese Kennzahlen unterstützen Continual Improvement.

Praxisbeispiel

Ein Discovery-Werkzeug erkennt,

dass auf einem Server eine neue Version des Betriebssystems installiert wurde.

Die Änderung wird erkannt,

aber zunächst nicht automatisch übernommen.

Nach erfolgreicher Prüfung aktualisiert der Administrator die CMDB.

Dadurch bleiben Dokumentation und tatsächlicher Zustand identisch.

Typische Fehler

Fehler 1

Configuration Items werden nie überprüft.

Fehler 2

Discovery wird nicht genutzt.

Fehler 3

Discovery überschreibt ungeprüft manuelle Angaben.

Fehler 4

Verantwortlichkeiten fehlen.

Fehler 5

Veraltete Beziehungen bleiben bestehen.

Fehler 6

Audits finden nicht statt.

Fehler 7

Zu viele irrelevante Informationen werden gespeichert.

Fehler 8

Monitoring und CMDB liefern widersprüchliche Daten.

Fehler 9

Changes werden nicht in die CMDB übernommen.

Fehler 10

Niemand misst die Datenqualität.

Checkliste Datenqualität

- [ ] Configuration Items vollständig
- [ ] Informationen aktuell
- [ ] Beziehungen korrekt
- [ ] Verantwortliche gepflegt
- [ ] Versionen aktuell
- [ ] Dokumentationen verknüpft
- [ ] Audits durchgeführt
- [ ] Daten regelmäßig überprüft

Checkliste Discovery

- [ ] Discovery aktiv
- [ ] geeignete Verfahren ausgewählt
- [ ] regelmäßige Ausführung geplant
- [ ] Änderungen geprüft

- [ ] CMDB aktualisiert
- [ ] Monitoring abgestimmt
- [ ] Fehler protokolliert
- [ ] Ergebnisse dokumentiert

Bedeutung für Fachinformatiker für Systemintegration

Fachinformatiker sorgen häufig dafür,

dass Configuration-Daten korrekt und aktuell bleiben.

Typische Aufgaben:

- Discovery konfigurieren,
- neue Systeme erfassen,
- Beziehungen pflegen,
- Audits durchführen,
- Änderungen dokumentieren,
- Datenqualität verbessern,
- Monitoring mit der CMDB abstimmen.

Eine zuverlässige CMDB entsteht nicht einmalig, sondern durch kontinuierliche Pflege.

Zusammenfassung

> Configuration Items erfassen
>
> ↓
>
> Discovery durchführen
>
> ↓
>
> Änderungen erkennen
>
> ↓
>
> Daten prüfen
>
> ↓
>
> CMDB aktualisieren

> ↓
>
> Datenqualität überwachen
>
> ↓
>
> Regelmäßig auditieren

Merksätze

> Eine CMDB ist nur so gut wie ihre Daten.

> Discovery reduziert manuellen Pflegeaufwand, ersetzt ihn aber nicht vollständig.

> Geschäftsbezogene Informationen müssen häufig manuell ergänzt werden.

> Regelmäßige Audits verbessern die Datenqualität.

> Aktuelle Configuration-Daten unterstützen nahezu alle ITIL Practices.

Verwandte Seiten

- 11.1 Ziele und Grundlagen des Service Configuration Management
- 11.2 Configuration Items, Attribute und Beziehungen
- 11.3 CMDB und Configuration Management System (CMS)
- 11.5 Zusammenspiel mit Incident, Problem, Change und Monitoring
- Monitoring and Event Management
- Change Enablement
- Continual Improvement

Quellen und Versionsstand

Offizielle Grundlagen

- PeopleCert – ITIL Practice Guide: Service Configuration Management
- ITIL Foundation – Version 5

Einordnung

Die beschriebenen Discovery-Verfahren, Qualitätskriterien und Auditmaßnahmen orientieren sich an den Empfehlungen der ITIL Practice „Service Configuration Management“. Welche Discovery-Werkzeuge, Schnittstellen und Prüfmechanismen eingesetzt werden, hängt von der jeweiligen IT-Landschaft und den organisatorischen Anforderungen ab.

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