Ordivis

MODUL · DISCOVERY

Modul Discovery (Netzwerk-Inventarisierung)

Automatische Netzwerk-Inventarisierung per WMI, SSH, SNMP und LDAP

Produktversion 2026.08.19 · Handbuch-Revision 1.0
Stand 19.08.2026 · Plattform .NET 10 / Windows Server

ID-24 Discovery

Modul Discovery (Netzwerk-Inventarisierung)

Eine CMDB ist nur so nützlich wie ihre Aktualität. Pflegt man jeden Server und jeden PC von Hand ein, hinkt der Datenbestand der Wirklichkeit fast immer hinterher: Geräte kommen dazu, verschwinden oder bekommen neue Software, ohne dass es jemand nachträgt. Auf Dauer traut niemand mehr den Einträgen.

Discovery nimmt Ihnen diese Fleißarbeit ab. „Discovery“ heißt Erkennung: Das Modul durchsucht das Netzwerk selbstständig und findet heraus, welche Geräte es gibt und was auf ihnen läuft. Ein einfacher Netzwerk-Scan prüft, welche Adressen überhaupt antworten. Der ausführlichere Deep-Scan meldet sich mit hinterlegten Zugangsdaten an einem System an und liest Details aus, bis hin zur installierten Software. Die Funde landen nicht ungefragt in der CMDB, sondern zuerst als Vorschläge (Kandidaten), die Sie prüfen und übernehmen. So bleibt die Dokumentation aktuell, ohne dass Sie die Kontrolle abgeben.

INHALT

1 Zweck & Nutzen
2 Scan-Arten
3 Anmeldedaten (Credential-Vault)
4 Einen Scan durchführen
5 Scan-Abgleich & Übernahme
6 Verteilte Discovery: Collector an entfernten Standorten
6.1 Einen Collector anlegen
6.2 Den Collector am Standort installieren
6.3 Was der Collector meldet
6.4 Betrieb und Überwachung
7 Client-Inventar: Funde prüfen und übernehmen
7.1 Übernehmen
7.2 Verwerfen
8 AD/LDAP – immer read-only
9 Action1-Anbindung (optional)
9.1 Was Action1 liefert — und was nicht
9.2 Einrichten
9.3 ⛔ Zwei harte Grenzen
9.4 Vom Befund zum Vollzug
10 Rollen & Rechte (Auszug)
Verwandte Themen

1 Zweck & Nutzen

- CMDB aktuell und vollständig halten, ohne alles manuell zu pflegen.
- Grundlage für Lizenz-Compliance (installierte Software).
- Erkennung neuer/unbekannter Geräte im Netz.

2 Scan-Arten

Scan	Liest	Protokoll
Netzwerk-Scan	erreichbare Adressen	ICMP/Port
Deep-Scan Windows	OS, Hardware, installierte Software (Registry-Uninstall)	WMI / PowerShell
Deep-Scan Linux/Unix	System- und Paketinfos (dpkg/rpm)	SSH
Deep-Scan Netzwerkgerät	Systembeschreibung/-name	SNMP (v2c)
Deep-Scan Verzeichnis	Computerobjekte aus dem AD (read-only)	LDAP/AD

3 Anmeldedaten (Credential-Vault)

Der Deep-Scan benötigt je Ziel passende Zugangsdaten:

- **Windows (WMI/PowerShell):** `DOMAIN\Benutzer` + Passwort.
- **SSH:** Benutzer + Passwort **oder** privater Schlüssel.
- **SNMP:** Community-String (v2c).
- **LDAP/AD:** Bind-DN bzw. Domänen-Benutzer + Passwort.

Zugangsdaten werden **AES-256-verschlüsselt** im **Credential-Vault** gespeichert (Klartext wird nie zurückgegeben).

So hinterlegen Sie Zugangsdaten:

> 💻 **Nur im Client:** *CMDB* ▸ *Discovery-Scan* ▸ *Anmeldedaten* · 🔑 `discovery.manage` — Im Portal gibt es den Vault nicht; er verlangt bewusst den verwalteten Arbeitsplatz.

🔒 **Pflichtreihenfolge** — ohne gesetzten Vault-Schlüssel (siehe die Karte unten) lässt sich nichts speichern. Das ist die erste Voraussetzung, nicht die letzte.

1. Öffnen Sie *CMDB* ▸ *Discovery-Scan* und wechseln Sie auf *Anmeldedaten*.
2. Legen Sie einen neuen Eintrag an und wählen Sie das Verfahren (Windows, SSH, SNMP, LDAP/AD).
3. Tragen Sie Benutzer und Kennwort bzw. den privaten Schlüssel oder den Community-String ein.
4. Vergeben Sie einen sprechenden Namen – er ist das, was Sie beim Scan auswählen.
5. Speichern Sie.

✅ **Ergebnis:** Der Zugang steht beim Scan zur Auswahl. Das Kennwort selbst bekommen Sie nie wieder zu sehen – auch nicht als Administrator.

> **Voraussetzung:** Der Vault-Schlüssel `CredentialVault:EncryptionKey` (32-Byte, Base64) muss als Umgebungs-/Secret-Variable gesetzt sein – **nicht** in `appsettings.json`.

> **Wichtig:** Die Verwaltung der Anmeldedaten erfordert das Recht `discovery.manage`.

Für **Collector an entfernten Standorten** gilt eine andere Regel: Deren Scan-Kennwort steht **nicht** in diesem Vault, sondern bleibt auf dem Standort-Rechner (Abschnitt 6.2).

4 Einen Scan durchführen

> 💻 **Client:** *CMDB* ▸ *Discovery-Scan* · 🌐 **Portal:** *Netz (IPAM)* ▸ *Discovery* · 🔑 `discovery.read` zum Lesen, `discovery.manage` zum Starten

> **Voraussetzung:** Die Anmeldedaten für das Zielsystem liegen im Credential-Vault (Abschnitt 3). Ohne sie liefert ein Scan nur, was ohne Anmeldung sichtbar ist – also fast nichts.

🔒 **Pflichtreihenfolge** — Ziel und Scan-Art bestimmen, **welche** Anmeldedaten überhaupt zur Auswahl stehen. Ein zuerst gewählter Zugang passt danach womöglich nicht zum Verfahren.

1. Öffnen Sie *CMDB* ▸ *Discovery-Scan*.
2. Wählen Sie das *Ziel* (Subnetz, Hostliste oder AD) und die *Scan-Art*.
3. Wählen Sie die passenden **Anmeldedaten** aus dem Vault.
4. Starten Sie den Scan. Die **API** führt ihn im Hintergrund aus; in einem entfernten Netz übernimmt das der dort installierte **Discovery-Collector** (Abschnitt 6).
5. Warten Sie das Ende des Laufs ab.

✅ **Ergebnis:** Die Treffer stehen im **Scan-Abgleich** als Kandidaten – noch nicht als CI. Erst das Übernehmen legt an (Abschnitt 5).

5 Scan-Abgleich & Übernahme

Im **Scan-Abgleich** vergleichen Sie Treffer mit vorhandenen CIs:

- **Neu:** legt ein neues CI an.
- **Aktualisieren:** ergänzt/aktualisiert Attribute und installierte Software.
- **Ignorieren:** blendet den Kandidaten aus.

Erst beim **Übernehmen** entstehen CIs, Software-Installationen und ein **Inventar-Snapshot**. Abbildung 1 zeigt den Weg vom Scan bis dorthin.

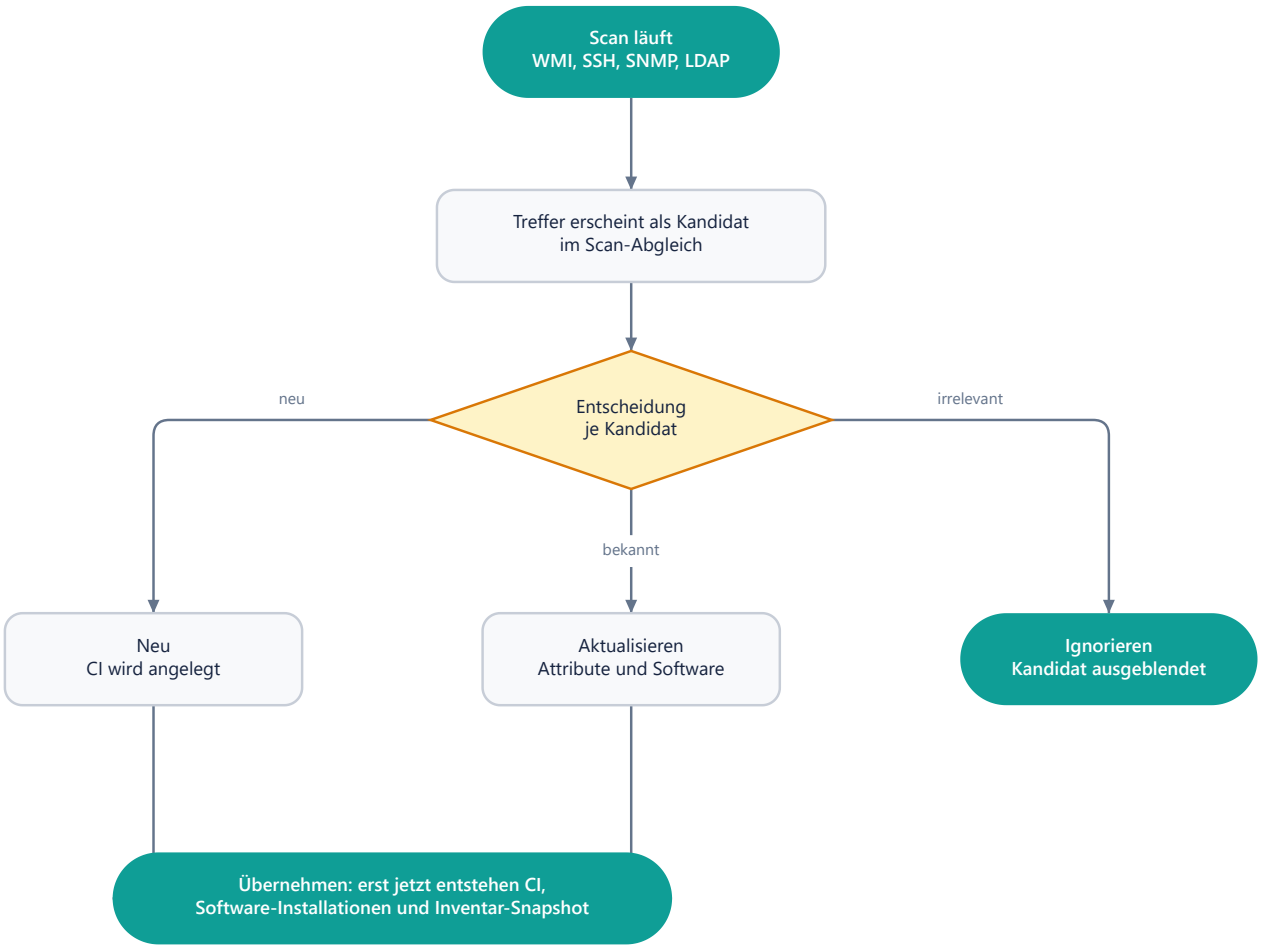

Abb. 1 – Vom Scan-Treffer zum Configuration Item. Bis zum Übernehmen ändert sich in der CMDB nichts.

6 Verteilte Discovery: Collector an entfernten Standorten

Die Scans aus Abschnitt 4 laufen **auf dem Ordivis-Server**. Damit endet ihre Reichweite an der ersten Netzgrenze: Eine Außenstelle, ein isoliertes Produktionssegment oder das Netz eines betreuten Kunden ist von dort aus nicht erreichbar – und was man nicht erreicht, kann man nicht inventarisieren.

Ein **Collector** ist ein kleiner Windows-Dienst, den Sie *im* fremden Netz installieren. Er durchsucht die Netzbereiche, die Sie ihm zuweisen, und meldet seine Funde an die Zentrale.

Die Verbindung geht immer vom Standort AUS. Der Collector ruft in der Zentrale an, nie umgekehrt. Am Remote-Standort ist deshalb **keine eingehende Firewall-Freigabe** nötig, und ein Standort hinter einem NAT-Router funktioniert genauso wie einer mit fester Adresse.

6.1 Einen Collector anlegen

> 💻 **Nur im Client:** *CMDB* ▸ *Discovery-Collector* ▸ *Collector anlegen* · 🔑 `discovery.manage` — Im Portal gibt es die Collector-Verwaltung nicht.

🔒 **Pflichtreihenfolge** — der Anmeldeschein entsteht **beim Speichern** und wird **einmal** gezeigt. Wer ihn nicht sofort kopiert, muss den Collector neu anlegen.

1. Öffnen Sie *CMDB ▸ Discovery-Collector* und wählen Sie *Collector anlegen*.
2. Tragen Sie ein: - **Bezeichnung** – wie der Standort im Alltag genannt wird (z. B. „Collector Rathaus"). - **Standort** – rein beschreibend, für die Übersicht. - **Netzbereiche** – ein oder mehrere CIDR-Netze, kommagetrennt (z. B. `10.1.0.0/24, 10.1.4.0/24`). - **Abstand der Läufe** in Minuten. `0` bedeutet: läuft nur auf Anforderung, nicht von selbst.
3. Nach dem Speichern erscheint der **Anmeldeschein** – ein einmalig einlösbarer Zugangscode. **Kopieren Sie ihn jetzt:** Er wird kein zweites Mal angezeigt.

6.2 Den Collector am Standort installieren

Verwenden Sie das eigenständige Paket **Ordivis-Collector-Setup**. Es enthält ausschließlich den Collector-Dienst – nicht Server, Datenbank oder Client. Der Installer fragt:

- **Adresse der Ordivis-API** – dieselbe URL, die auch die Clients verwenden.
- **Anmeldeschein** – der Code aus Schritt 6.1.
- **Scan-Konto** (optional) – ein **lesendes** Windows-Konto in der Form `DOMÄNE\benutzer`.

Das Scan-Kennwort wird auf dem Standort-Rechner mit dem Windows-Maschinenschlüssel verschlüsselt und **verlässt ihn nie**. Die Zentrale erfährt es nicht – sie könnte es sonst über alle Standorte hinweg verlieren. Jeder Standort haftet für sein eigenes Netz.

> **Ohne Scan-Konto** bleibt es beim Netz-Durchlauf: Der Collector meldet, welche Adressen antworten, mit Name und MAC-Adresse. Das ist deutlich weniger als ein Tiefen-Scan, aber immer noch mehr als nichts.

6.3 Was der Collector meldet

Stufe	Erhebt	Voraussetzung
Netz-Durchlauf	antwortende Adressen, Hostname, MAC-Adresse, Antwortzeit	keine
Tiefen-Scan	Betriebssystem, Hersteller, Modell, Arbeitsspeicher, installierte Anwendungen	Scan-Konto (WMI)

Die **MAC-Adresse** ist dabei wichtiger, als sie aussieht: Sie ist das einzige Merkmal, das einen Rechner über einen Adresswechsel per DHCP hinweg wiedererkennt. Deshalb steht der Collector *im* Segment – von der Zentrale aus wäre sie nicht zu bekommen.

6.4 Betrieb und Überwachung

Die Liste **Discovery-Collector** zeigt je Standort den Zustand:

Zustand	Bedeutung
Anmeldung ausstehend	angelegt, aber der Anmeldeschein ist noch nicht eingelöst
Aktiv	angemeldet, meldet sich regelmäßig
Aktiv (Läufe aus)	meldet Lebenszeichen, scannt aber nicht (in der Zentrale abgeschaltet)
Überfällig	hat sich zu lange nicht gemeldet – der Rechner ist aus, der Dienst gestoppt oder die Verbindung gestört
Gesperrt	vom Betreiber gesperrt; sein Zugang ist widerrufen

Ein Collector gilt als **überfällig**, wenn seit dem letzten Lebenszeichen mehr als das Doppelte seines Melde-Abstands verstrichen ist (mindestens eine Stunde). Ein einzelnes ausgefallenes Lebenszeichen ist noch kein Vorfall.

Sperren widerruft den Zugang sofort – der Collector ist ab dem nächsten Anruf draußen, unabhängig davon, ob der Rechner noch läuft. **Anmeldeschein erneuern** setzt einen neuen Code aus und widerruft dabei den alten Zugang; das ist der Weg, um ein Geheimnis planmäßig zu wechseln.

> **Verbindungsabriss ist kein Datenverlust.** Ist die Zentrale nicht erreichbar, legt der Collector seinen Bericht in eine lokale Warteschlange und reicht ihn beim nächsten Kontakt nach. Weil jeder Bericht eine eigene Kennung trägt, erkennt die Zentrale den Nachzügler und verbucht ihn nicht doppelt.

7 Client-Inventar: Funde prüfen und übernehmen

Alles, was Collector und angebundene Werkzeuge melden, landet unter **CMDB ▸ Client-Inventar** – und zwar als **Fund**, nicht als CI.

> **Ein Fund ist kein Configuration Item.** Was im Netz gefunden wurde, ist eine Beobachtung. Ein CI ist eine Aussage der Organisation über ihren Bestand. Erst die Bestätigung durch einen Menschen macht aus dem einen das andere – genau wie bei den unbestätigten IP-Adressen der IPAM.

Die Liste ist filter-, sortier- und exportierbar (CSV und PDF), mit zwei Sichten:

- **Clients** – eine Zeile je Rechner, mit Standort, Betriebssystem und Anzahl der Anwendungen.
- **Anwendungen** – eine Zeile je Anwendung und Version, mit der Zahl der betroffenen Clients. Das ist die Frage, die im Betrieb tatsächlich gestellt wird: „Wo läuft das überall?"

7.1 Übernehmen

> 💻 **Nur im Client:** *CMDB ▸ Client-Inventar* · 🔑 `cmdb.ci.update` — Im Portal gibt es das Client-Inventar nicht.

🔒 **Pflichtreihenfolge** — der Dublettenabgleich (Schritt 3) läuft **vor** der Entscheidung. Wer ihn übergeht und blind anlegt, hat denselben Rechner zweimal in der CMDB.

1. Öffnen Sie *CMDB ▸ Client-Inventar*.
2. Markieren Sie den Fund, den Sie übernehmen möchten.
3. Klicken Sie auf *Übernehmen*. Ordivis Platform prüft **zuerst**, ob es schon ein CI mit denselben Merkmalen gibt (gleiche MAC-Adresse, gleicher Hostname), und zeigt die Treffer an.
4. Entscheiden Sie: - **Bestehendes CI** – der Fund aktualisiert dessen Merkmale und setzt den Verifizierungsstempel. - **Neues CI anlegen** – als „Client / Notebook“; die Klasse können Sie danach jederzeit ändern.
5. Bestätigen Sie.

✅ **Ergebnis:** Aus der Beobachtung ist eine Aussage der Organisation geworden – ein CI mit Verifizierungsstempel.

In beiden Fällen werden die gemeldeten Anwendungen als **Software-Installationen** mit dem Client verknüpft – die Grundlage der Lizenzzählung.

Der Abgleich steht **vor** der Übernahme und nicht als Bereinigung danach: Wer ihn übergeht, legt Dubletten an und merkt es erst, wenn beide gepflegt werden müssen.

7.2 Verwerfen

Verwerfen nimmt einen Fund vom Tisch, ohne ein CI anzulegen – für Geräte, die dokumentiert nicht in die CMDB gehören (Gastgeräte, Fremdtechnik, Testaufbauten). Die Entscheidung hält: Beim nächsten Lauf kommt derselbe Fund nicht wieder hoch. Über **Wieder öffnen** holen Sie ihn zurück.

8 AD/LDAP – immer read-only

Der Verzeichnis-Scan liest ausschließlich. Ordivis Platform schreibt **niemals** ins Active Directory.

Ebenso gilt: **LAPS-Kennwörter und BitLocker-Wiederherstellungsschlüssel werden nie übertragen.** Sie stehen im Verzeichnis teils an denselben Objekten wie die Computerdaten; in einem Betriebsdatenbestand haben sie nichts zu suchen.

9 Action1-Anbindung (optional)

Ordivis kann **Action1** als zusätzliche Erfassungsquelle nutzen — behandelt wie die Ordivis Toolbox: Die Funde landen im **selben Staging** (§7) und werden dort geprüft und übernommen. Es entsteht kein zweiter Weg in die CMDB.

⚠️ **Durchgehend optional.** Ohne eingerichtete Verbindung tut die Anbindung nichts; ein Haus ohne Action1-Konto merkt von ihr nichts.

9.1 Was Action1 liefert — und was nicht

⚠️ **Action1 speichert kein Inventar.** Die Cloud fragt den Endpunkt bei Bedarf ab, hält das Ergebnis kurz vor und löscht es danach wieder; dauerhaft geführt werden nur Rechnername, IP-Adresse und

Verbindungsstatistik. Es gibt deshalb kein „Inventar lesen", sondern nur *Abfrage auslösen → warten → Ergebnis abholen*. Ordivis bildet das als **Auftrag** ab und führt den Bestand anschließend selbst weiter: **Action1 liefert den Augenblick, Ordivis die Geschichte.**

⚠️ **Jede Abfrage geht auf die Endgeräte los** und ist damit nicht umsonst. Der Abrufabstand ist deshalb eine Betriebsentscheidung und steht in der Verbindung (Untergrenze 15 Minuten).

⚠️ **Action1 erreicht nur Geräte mit eigenem Agenten.** Netzwerktechnik, Appliances und alles ohne Agent bleiben außen vor. Die **Abdeckungsanzeige** nennt das ausdrücklich — eine unsichtbare Lücke ist im Audit schlimmer als eine bekannte.

⚠️ **Schwachstellen löst Action1 gegen NIST NVD, MSRC und VulnCheck auf, nicht gegen CERT-Bund.** Für BSI-Nachweise bleibt der CSAF-Weg notwendig; die Anbindung ersetzt ihn nicht.

9.2 Einrichten

Einstellungen › Erkennung › Action1 — erforderlich ist das Recht `discovery.action1.admin`.

Angabe	Bedeutung
Region	NorthAmerica, NA-2, **Europe** (Vorgabe für den DACH-Raum), Australia. Sie bestimmt das Rechenzentrum.
Client-ID / Client-Secret	OAuth2-Zugangsdaten. Das Geheimnis wird verschlüsselt abgelegt und nie im Klartext zurückgegeben.
Organisation	Action1 führt eine eigene Mandantenebene. Die Zuordnung wird **ausgewählt, nie geraten** — eine falsche trüge Befunde eines fremden Kunden in Ihren Bestand.
Abrufabstand	Wie oft abgeglichen wird (Vorgabe 12 Stunden).
Anfragen je Minute	Schutz vor der Ratengrenze des Anbieters.

Die Verbindungsprüfung meldet sich an und ruft `GET /Me` — sie belegt die Erreichbarkeit, nicht die Vollständigkeit der Rechte.

9.3 ⛔ Zwei harte Grenzen

Der BitLocker-Wiederherstellungsschlüssel wird gar nicht erst abgefragt. Am CI steht ausschließlich der *Zustand*, dass eine Verschlüsselung aktiv ist. Der Schlüssel verbleibt allein im Active Directory und wird von Ordivis **niemals ausgelesen, dokumentiert oder genutzt**. Das ist strenger als „nicht speichern" und bestimmt die Bauart: Beim Abrufen und Herausfiltern liefe der Schlüssel durch Arbeitsspeicher, Zwischenspeicher und möglicherweise durch Protokolle. Die Sperre greift bei der Auswahl der Datenquellen und ist **nicht abschaltbar** — eine abschaltbare Sperre wäre keine.

Personenbeziehbare Datenquellen sind ausgeschaltet, bis jemand sie einschaltet. Angemeldete Benutzer, Anmeldestatistik, Profile, laufende Prozesse, Webbrowser, Sofortnachrichtendienste und Cloud-Speicher fallen unter die Mitbestimmung (§ 87 BetrVG bzw. die Personalvertretungsgesetze der Länder). Jede Quelle nennt ihren **Zweck**, und jedes Ein- und Ausschalten wird mit Person und Zeitpunkt protokolliert. Bei einem Behördenkunden ist das ein Projektrisiko, kein Nebenaspekt.

9.4 Vom Befund zum Vollzug

Die Rückrichtung ist bewusst schmal: Action1 ist **keine Senke für CI-Daten**. Möglich sind

- **Ausrollauftrag** aus einem Änderungsantrag — ⚠️ **erst nach Freigabe, nie automatisch**. Der Weg vom Befund zur Änderung an hunderten Arbeitsplätzen darf keine Abkürzung haben.
- **Rückmeldung je Gerät** an denselben Änderungsantrag, damit niemand in zwei Systemen nachsieht.
- **Risikoakzeptanz**: Wird ein Befund im ISMS mit Begründung akzeptiert, steht dieselbe Entscheidung auch in Action1 — eine Entscheidung, zwei Systeme konsistent. Ohne Begründung wird nichts geschrieben.
- **Wartungsfenster**: Der im Antrag geplante Termin wird übertragen, statt ihn zweimal einzutragen.

10 Rollen & Rechte (Auszug)

Recht	Erlaubt
`discovery.read`	Scan-Daten, Collector und Client-Inventar lesen
`discovery.manage`	Scans auslösen, Anmeldedaten und Anhänge verwalten
`discovery.collector.manage`	Collector anlegen, Anmeldeschein ausstellen, sperren, löschen
`discovery.result.review`	Funde prüfen, als CI übernehmen oder verwerfen
`cmdb.ci.create` / `cmdb.ci.update`	die bei der Übernahme entstehenden CIs schreiben

Die beiden Collector-Rechte sind bewusst von `discovery.manage` getrennt: Wer einen Scan auslösen darf, darf damit noch lange nicht einen Dienst in ein fremdes Netz stellen oder CIs anlegen.

Verwandte Themen

- **ID-21 – Modul CMDB** – Übernahme der Fundstücke in die CMDB
- **ID-22 – Modul IPAM** – gefundene Adressen in der IP-Verwaltung
- **ID-21b – Benutzerkonten in der CMDB** – Konten aus AD und LDAP
- **ID-50 – Betriebshandbuch – Installation & Serverbetrieb** – Netzzugang und Dienstkonten für Scans