Ordivis

MODUL · INFRASTRUKTUR

Infrastruktur-Dokumentation – das Verzeichnis als Stand

Active Directory, Gruppenrichtlinien, Zertifikate und Berechtigungen als Stand dokumentieren und vergleichen

Produktversion 2026.11.22 · Handbuch-Revision 2.58
Stand 22.11.2026 · Plattform .NET 10 / Windows Server

ID-24b Infrastruktur-Dokumentation

© 2026 Ordivis IT · Christian Grams. Alle Rechte vorbehalten. Vervielfältigung nur mit schriftlicher Genehmigung.

Infrastruktur-Dokumentation – das Verzeichnis als Stand

Die Infrastruktur-Dokumentation hält fest, wie Ihr Active Directory und seine Umgebung zu einem Zeitpunkt aussahen: Gesamtstruktur, Standorte, Domänencontroller, Benutzer und Gruppen, Gruppenrichtlinien, Zertifikate, Verbund und die Rechte an Freigaben und Verzeichnisobjekten. Jede Erhebung ergibt einen **Stand** mit Zeitpunkt und Quelle. Zwei Stände desselben Bereichs lassen sich vergleichen – das beantwortet die Frage „Was hat sich geändert, seit ich hinsah?“.

Dieses Kapitel fasst zusammen: wozu die Dokumentation da ist, was sie ausdrücklich **nicht** tut, wie Sie sie einrichten, welche Bereiche es gibt, wie der Vergleich arbeitet und wo die Grenzen liegen. Die Einzelheiten jeder Seite, jedes Bereichs und jeder Meldung stehen in ID-24a, Abschnitt 6.6; die Rechte in ID-44, Abschnitt 3.15d; die Schnittstelle in ID-60.

INHALT

1 Zweck: ein Abbild, kein zweiter Bestand
2 Die fünf Abgrenzungen
3 Voraussetzungen und Rechte
3.1 Rechte
3.2 Voraussetzungen am Erhebungsrechner
3.3 Zugangsdaten: das Lesekonto
4 Einrichten
4.1 Eine Erhebungsquelle anlegen und den ersten Lauf starten
4.2 Einen Zeitplan setzen
4.3 Die Reihenfolge der Ersteinrichtung
5 Die Bereiche
6 Stände lesen und vergleichen
6.1 Ist die Dokumentation aktuell?
6.2 Zwei Stände vergleichen
6.3 Meldungen bei einer Änderung
6.4 Listen als Datei ausführen
6.5 Gruppenrichtlinien-Einstellungen (GPP) lesen und vergleichen
7 Grenzen
8 Fehlerbehebung
9 Beispiele aus der Praxis
9.1 Beispiel: Die Stadtverwaltung Musterstadt richtet die Dokumentation ein
9.2 Beispiel: Wer ist seit letzter Woche Domänen-Admin geworden?
10 Häufige Fragen
Verwandte Themen

© 2026 Ordivis IT · Christian Grams. Alle Rechte vorbehalten.

1 Zweck: ein Abbild, kein zweiter Bestand

Beim Netz (ID-22) pflegen Sie einen Bestand, und der DHCP-Server wird damit abgeglichen. Hier ist es umgekehrt: **Der Verzeichnisdienst ist die Wahrheit, Ordivis hält ein Abbild.** Daraus folgen drei Eigenschaften, die überall in diesem Bereich gelten:

- **Ein Stand ist unveränderlich.** Bearbeiten lässt sich ein erhobener Wert nirgends – weder im Client noch im Portal noch über die Schnittstelle. Was sich ändert, ergibt beim nächsten Lauf einen neuen Stand.
- **Jede Seite nennt Zeitpunkt und Quelle.** Der Kopf jeder Seite sagt, wann und woraus erhoben wurde, und von welchem Collector.
- **Ein Stand ist vollständig oder ausdrücklich unvollständig.** Scheitert eine Teilabfrage, wird sie im Stand benannt. Ein unvollständiger Stand taugt nicht als Vergleichsgrundlage und löst keine Meldung aus – sonst sähe alles, was die Erhebung nicht lesen konnte, wie gelöscht aus.

Ein Lauf, dessen Inhalt sich nicht geändert hat, bestätigt den bisherigen Stand nur; er wird nicht ein zweites Mal gespeichert.

2 Die fünf Abgrenzungen

Fünf Aussagen gelten für jeden Bereich, jede Seite und jeden Lauf. Sie stehen hier wörtlich, weil sich ein Betrieb auf sie verlässt.

Ein Lesekonto genügt. Für keinen Bereich braucht es Schreibrechte im Verzeichnis, und für keinen ein Konto mit Administratorrechten im AD. Zwei Stellen verlangen mehr als ein gewöhnliches Domänenkonto; beide sind Leserechte und gehören nicht zum Verzeichnis: das Leserecht auf den *Password Settings Container* für die feingranularen Kennwortrichtlinien und, nur auf den Dateiservern, die Mitgliedschaft in *Server-Operatoren* oder den lokalen Administratoren, weil Windows die Freigabe-ACL sonst nicht herausgibt (Abschnitt 3.3).

Auf einem Domänencontroller wird weder etwas installiert noch eine Sitzung geöffnet. Am Domänencontroller stellt der Collector ausschließlich LDAP-Leseabfragen (LDAPS 636, sonst LDAP 389 mit Signierung und Verschlüsselung) und liest für die Gruppenrichtlinien das SYSVOL per SMB. Eine WinRM-Sitzung öffnet er nur auf AD-FS-Knoten und auf Rechnern mit einer AD-LDS-Instanz. Steht ein Domänencontroller unter diesen Zielen, oder lässt sich die Liste der Domänencontroller nicht lesen, führt er dort nichts aus und nennt den Grund im Stand.

Es wird nichts ins AD geschrieben. Die Infrastruktur-Dokumentation legt kein Konto an, pflegt keine Gruppe, ändert keine Gruppenrichtlinie und setzt kein Recht. Der LDAP-Zugang des Collectors kennt nur die Suche. Auch ins SYSVOL, auf die Dateiserver, an der Zertifizierungsstelle und an einer AD-FS-Farm wird nichts geändert. Selbst der *Abgleich mit Ordivis* auf der Seite *Benutzer und Gruppen* verknüpft nur – er legt weder im AD noch in Ordivis ein Konto an.

Ein dokumentierter Stand ist keine Sicherung. Aus einem Stand lässt sich nichts wiederherstellen: kein gelöschtes Konto, keine Gruppenmitgliedschaft, keine Gruppenrichtlinie. Ein Stand enthält ohnehin nicht alles, was eine Wiederherstellung braucht – Kennwörter, Kennwort-Hashes und das LAPS-Kennwort liest der Collector nie. Sichern Sie Ihr Active Directory mit den Mitteln von Windows (Systemstatus-Sicherung

© 2026 Ordivis IT · Christian Grams. Alle Rechte vorbehalten.

der Domänencontroller, AD-Papierkorb). Die Seite *Infrastruktur-Dokumentation* sagt es im Kopf ebenso: ein Abbild, keine Sicherung.

Die resultierende Richtlinie ist eine Rechnung und keine Messung. Welche Gruppenrichtlinie an einer Organisationseinheit gewinnt, rechnet der Server aus dem dokumentierten Stand. Auf keinem Rechner läuft dafür `gpresult`. WMI-Filter werden nicht ausgewertet (je betroffener GPO benannt), lokale Richtlinien und die Loopback-Verarbeitung sind nicht enthalten. Ob eine Einstellung auf einem bestimmten Rechner tatsächlich wirkt, zeigt nur eine Messung dort. Der Server gibt diesen Satz mit jeder Rechnung aus, und die Seite *Gruppenrichtlinien* zeigt ihn über der Liste.

3 Voraussetzungen und Rechte

3.1 Rechte

Recht	Erlaubt
`infradoku.read`	Übersicht, Stände, Vergleichsbericht, Diagramme, Verzeichnisdienst, Benutzer und Gruppen, Gruppenrichtlinien, Verbund und Zertifikate, Melderegeln lesen
`infradoku.manage`	Erhebungsquellen anlegen, ändern und entfernen, Zeitplan setzen, Melderegeln und erwartete Erhebung einstellen
`infradoku.collect`	einen Lauf anfordern (*Lauf starten*, *Sammellauf*); der Collector eröffnet und schließt damit seine Läufe
`infradoku.permissions.read`	Berechtigungsmatrix; Stände, Vergleiche und Ausfuhren der beiden Berechtigungsbereiche
`discovery.read`	die Auswahl des Collectors im Dialog der Erhebungsquelle
`identity.users.read`	die Registerkarte *Abgleich mit Ordivis* sehen
`identity.users.manage`	dort einen Vorschlag bestätigen oder eine Verknüpfung aufheben
`ipam.prefix.read`	die Karte *Abgleich mit dem IPAM* auf der Seite *Verzeichnisdienst*

`infradoku.collect` ist **kein** Recht, einen abgeschlossenen Stand zu ändern. Die Berechtigungsmatrix hat ein eigenes Recht, weil sie zeigt, wo sich ein Angriff lohnt; ohne `infradoku.permissions.read` fehlt der Menüpunkt. Welche Rolle welches Recht vorbelegt hat, steht in ID-44, Abschnitt 4.

Das Modul muss für den Mandanten eingeschaltet sein: *Fußbereich* ▸ *Einstellungen* ▸ *Module*, Eintrag *Infrastruktur-Dokumentation*, dazu *Discovery* für den Collector (ID-40).

3.2 Voraussetzungen am Erhebungsrechner

Erhoben wird in dieser Fassung **immer von einem Discovery-Collector** (ID-24a). Die Zentrale selbst hat für keinen Bereich einen eigenen Erheber. Der Dialog der Erhebungsquelle bietet unter *Erhoben von* zwar *Erhebungsrechner (Regelweg)* an; für jeden Bereich warnt er dann aber, dass ein Lauf nicht möglich ist. Erhebungsrechner ist also der Rechner, auf dem der Collector läuft. Er braucht:

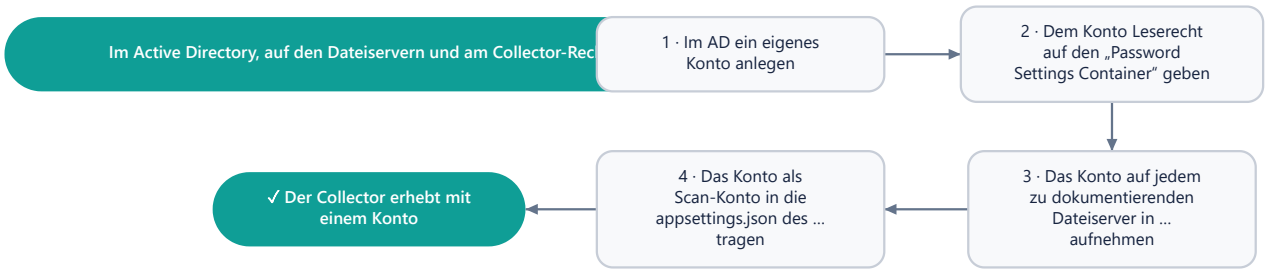
© 2026 Ordivis IT · Christian Grams. Alle Rechte vorbehalten.

- einen Mitgliedsserver oder Arbeitsplatz der Domäne, **nie einen Domänencontroller** (Installation: ID-24a, Abschnitt 4; Anmeldung: Abschnitt 5);
- einen Anmeldeschein von Oktober 2026 oder später – einem älter angemeldeten Collector fehlt das Recht `infradoku.collect` (Abschnitt 8);
- freie Wege vom Collector aus: TCP 636 (sonst 389) und 445 zu den Domänencontrollern, 445 zu den Dateiservern, für AD CS TCP 135 und den dynamischen RPC-Bereich zur Zertifizierungsstelle, für AD FS und AD LDS TCP 5985 zu den Knoten bzw. Rechnern;
- nur für die ausgestellten Zertifikate (AD CS): die Verwaltungswerkzeuge der Zertifikatdienste (RSAT) und, in der Sicherheit der Zertifizierungsstelle, das Leserecht für das **Dienstkonto** des Collectors.

3.3 Zugangsdaten: das Lesekonto

Der Collector meldet sich mit dem **Scan-Konto aus seiner eigenen** `appsettings.json` an, das Kennwort DPAPI-geschützt (ID-24a, Abschnitt 6.2). Zugangsdaten aus dem Tresor nimmt eine Quelle, die ein Collector erhebt, nicht an. Richten Sie dafür einmal je Anlage ein eigenes Lesekonto ein:

> ⚙️ **Im Active Directory, auf den Dateiservern und am Collector-Rechner** · 🔑 Domänen-Administrator für das Einrichten des Lesekontos; lokaler Administrator am Collector-Rechner



Klickweg – Zugangsdaten: das Lesekonto

1. Legen Sie im AD ein eigenes Konto an, das nur in *Domänen-Benutzer* steht.
2. Geben Sie dem Konto Leserecht auf den *Password Settings Container*, wenn Sie feingranulare Kennwortrichtlinien dokumentieren wollen.
3. Nehmen Sie das Konto auf jedem zu dokumentierenden Dateiserver in *Server-Operatoren* oder die lokalen Administratoren auf.
4. Tragen Sie das Konto als Scan-Konto in die `appsettings.json` des Collectors ein, verschlüsseln Sie das Kennwort wie in ID-24a, Abschnitt 6.2, und starten Sie den Dienst neu.

✅ **Ergebnis:** Der Collector erhebt mit einem Konto, das im Verzeichnis nichts darf außer lesen.

© 2026 Ordivis IT · Christian Grams. Alle Rechte vorbehalten.

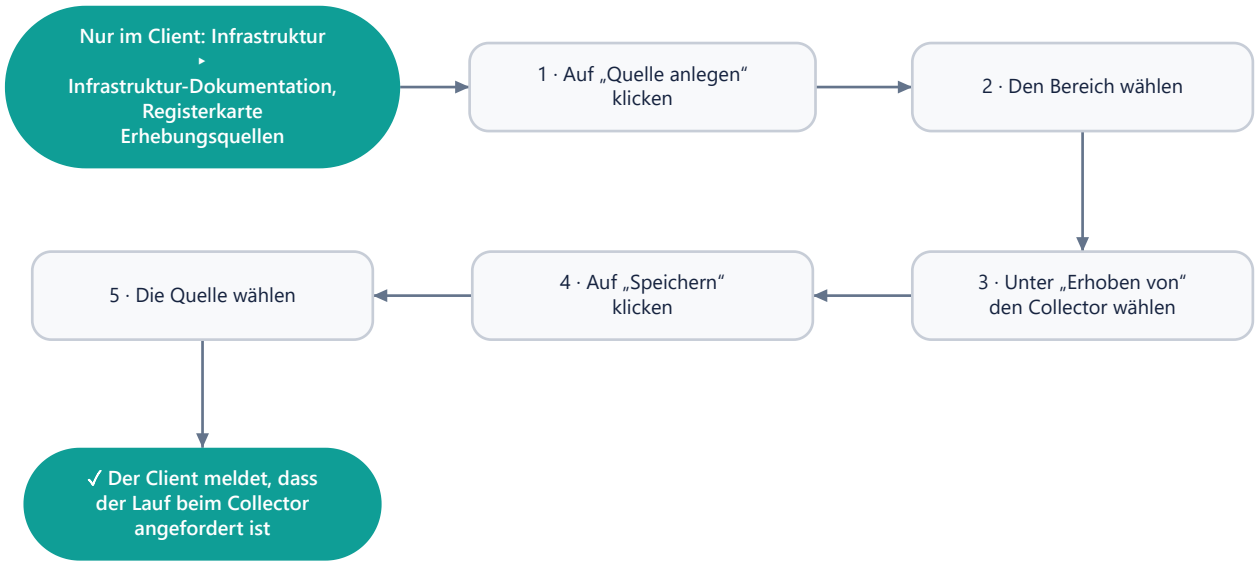
Achtung: Fehlt dem Lesekonto an einer Stelle das Leserecht, meldet das Verzeichnis keinen Fehler, sondern liefert still weniger. Der Collector prüft deshalb, ob vorhanden ist, was es in jeder Domäne gibt (eine Domäne, ein Standort, ein Domänencontroller, eine Kennwortrichtlinie, die OU *Domain Controllers*, die Domänen-Admins, *krbtgt*, die *Default Domain Policy*); fehlt davon etwas, heißt der Stand unvollständig. Eine gewöhnliche OU ohne Leserecht bemerkt diese Prüfung nicht. Vergleichen Sie beim ersten Stand die Zahl der Benutzer mit der Zahl aus der Verwaltungskonsole.

4 Einrichten

4.1 Eine Erhebungsquelle anlegen und den ersten Lauf starten

Eine **Erhebungsquelle** ist ein Bereich mit einem Ziel: etwa *Active Directory – Benutzer* für die Domäne `musterstadt.local`. Ziel ist je nach Bereich die Domäne, der Dateiserver, der Verbunddienstname der AD-FS-Farm oder der Rechner mit der AD-LDS-Instanz (Abschnitt 5).

💻 **Nur im Client:** *Infrastruktur* ▸ *Infrastruktur-Dokumentation*, Registerkarte *Erhebungsquellen* · 🔑 `infradoku.manage` zum Anlegen, `infradoku.collect` für *Lauf starten* und *Sammellauf*, `discovery.read` für die Auswahl des Collectors



Klickweg – Eine Erhebungsquelle anlegen und den ersten Lauf starten

1. Klicken Sie auf *Quelle anlegen*.
2. Wählen Sie den Bereich und tragen Sie das Ziel ein.
3. Wählen Sie unter *Erhoben von* den Collector, der das Ziel erreicht.
4. Klicken Sie auf *Speichern*.
5. Wählen Sie die Quelle und klicken Sie auf *Lauf starten* – oder auf *Sammellauf*, um alle Quellen eines Ziels zu erheben.

© 2026 Ordivis IT · Christian Grams. Alle Rechte vorbehalten.

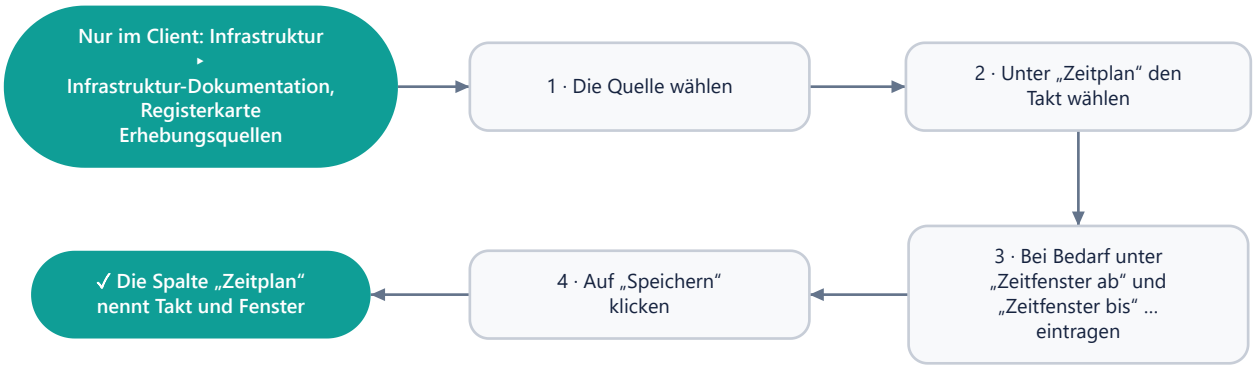
✅ **Ergebnis:** Der Client meldet, dass der Lauf beim Collector angefordert ist. Mit seinem nächsten Auftrag erhebt der Collector; danach steht der Stand auf der Registerkarte *Stände*, mit dem Rechnernamen des Collectors unter *Erhoben von*. Die bereichsabhängigen Felder (Umfang, Ordnertiefe, Vorlagen der ausgestellten Zertifikate, Knoten der Farm) erklärt ID-24a, Abschnitt 6.6.

Jede Quelle trägt zwei Grenzen: das *Zeitlimit in Sekunden* (leer: 1.800) und die *Höchstzahl der Objekte* (leer: 100.000). Keine der beiden schneidet still ab – wird eine überschritten, heißt der Stand unvollständig und nennt die Grenze. Im Feld *Grenzen* halten Sie fest, was Sie bewusst nicht erheben.

4.2 Einen Zeitplan setzen

Eine Quelle wiederholt sich auf Wunsch selbst: täglich, wöchentlich oder monatlich, wahlweise nur in einem Zeitfenster. Die geplante Aufgabe *Infrastruktur-Dokumentation (geplante Erhebung)* prüft alle 15 Minuten, welche Quelle fällig ist, und fordert den Lauf beim Collector an – genau wie *Lauf starten*.

> 💻 **Nur im Client:** *Infrastruktur* ▸ *Infrastruktur-Dokumentation*, Registerkarte *Erhebungsquellen* · 🔑 `infradoku.manage`



Klickweg – Einen Zeitplan setzen

1. Wählen Sie die Quelle und klicken Sie auf *Bearbeiten*.
2. Wählen Sie unter *Zeitplan* den Takt, etwa *Wöchentlich*.
3. Tragen Sie bei Bedarf unter *Zeitfenster ab* und *Zeitfenster bis* volle Stunden ein, etwa `22` und `4`.
4. Klicken Sie auf *Speichern*.

✅ **Ergebnis:** Die Spalte *Zeitplan* nennt Takt und Fenster. Das Fenster gilt in der Zeitzone des Mandanten.

4.3 Die Reihenfolge der Ersteinrichtung

Die erste Erhebung einer gewachsenen Domäne ist der längste Lauf. Einen Assistenten dafür gibt es nicht; gehen Sie in fünf Stufen vor, jede erst, wenn die vorige vollständige Stände hat:

1. Struktur: Gesamtstruktur, Standorte, Domänencontroller, Vertrauensstellungen, Organisationseinheiten, Kennwortrichtlinien.
2. Benutzer, Gruppen, Dienstkonten, Privilegierte Gruppen.
3. Gruppenrichtlinien.

© 2026 Ordivis IT · Christian Grams. Alle Rechte vorbehalten.

4. Berechtigungen – AD-Objekte und Berechtigungen – Freigaben, zuerst mit engem Umfang.
5. Was es nur in manchen Anlagen gibt: Zertifikate – AD CS, Verbund – AD FS, Verzeichnis – AD LDS.

Berechtigungen vor den Gruppen zu erheben ergibt keine Aussage: Die Berechtigungsmatrix rechnet dann nicht. Empfohlene Grenzen je Stufe, Richtwerte für die Dauer und die Vorbereitung je Anlage stehen in ID-24a, Abschnitt 6.6, *Ersteinrichtung: Reihenfolge, Grenzen und Dauer*. Die Dauern dort sind ausdrücklich nicht gemessen.

5 Die Bereiche

Ordivis kennt sechzehn Bereiche. Jeder wird als eigener Stand erhoben, und jeder steht auf genau einer Seite unter *Infrastruktur*.

Bereich	Ziel der Quelle	Seite
Active Directory – Gesamtstruktur, Standorte, Domänencontroller, Vertrauensstellungen, Organisationseinheiten, Kennwortrichtlinien	Domäne	*Verzeichnisdienst*
Active Directory – Benutzer, Gruppen, Dienstkonten, Privilegierte Gruppen	Domäne	*Benutzer und Gruppen*
Gruppenrichtlinien	Domäne oder ein Domänencontroller	*Gruppenrichtlinien*
Zertifikate – AD CS	Domäne	*Verbund und Zertifikate*
Verbund – AD FS	Verbunddienstname der Farm	*Verbund und Zertifikate*
Verzeichnis – AD LDS	Rechner mit der Instanz	*Verbund und Zertifikate*
Berechtigungen – AD-Objekte	Domäne	*Berechtigungsmatrix*
Berechtigungen – Freigaben	Dateiserver	*Berechtigungsmatrix*

Was jeder Bereich im Einzelnen erhebt – Felder, Befunde, die Ausnahmen für SYSVOL und Zertifizierungsstelle – steht in ID-24a, Abschnitt 6.6. Eine Quelle für einen Bereich, den es in Ihrer Anlage nicht gibt, bleibt für immer unvollständig; legen Sie sie nicht an.

6 Stände lesen und vergleichen

6.1 Ist die Dokumentation aktuell?

> 💻 **Client:** *Infrastruktur* ▸ *Übersicht* · 🌐 **Portal:** *Infrastruktur* ▸ *Übersicht* · 🔑 `infradoku.read`

Den Ausschnitt dazu zeigt Abbildung 1.

© 2026 Ordivis IT · Christian Grams. Alle Rechte vorbehalten.

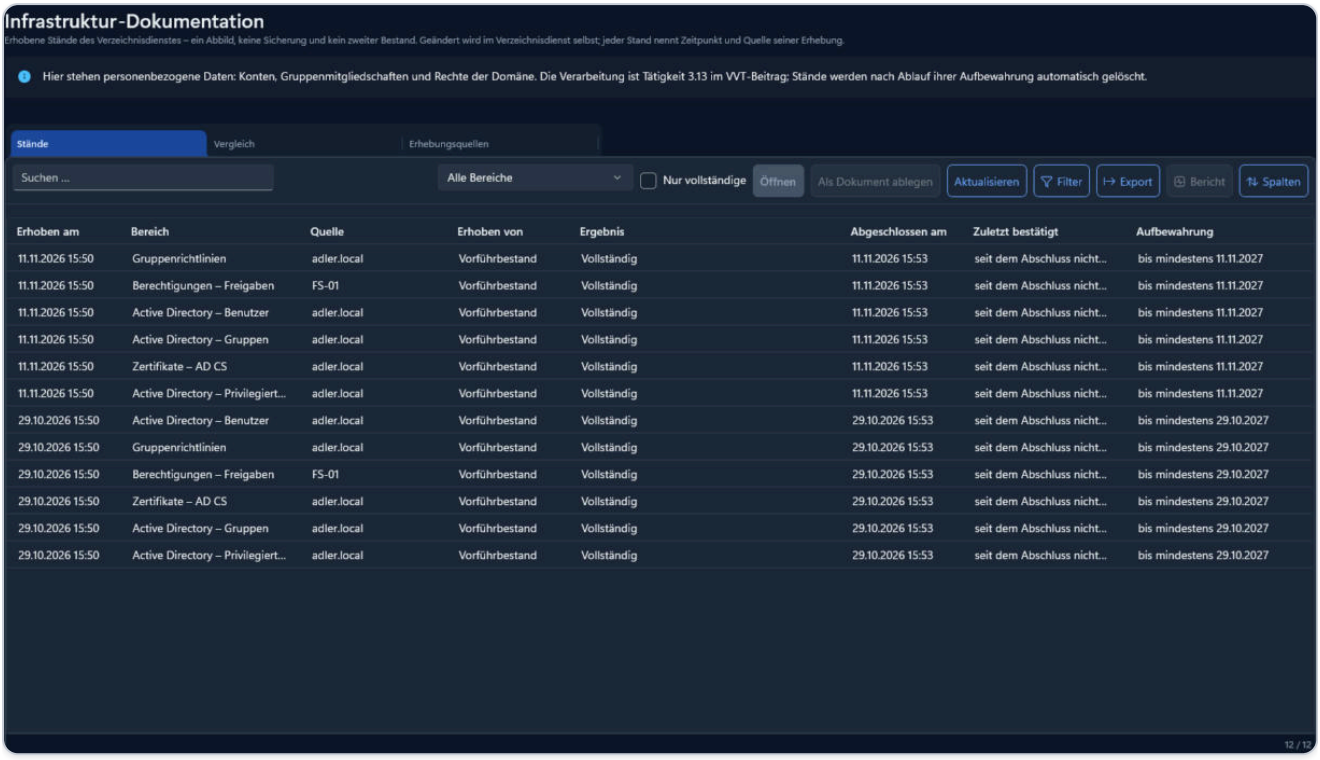
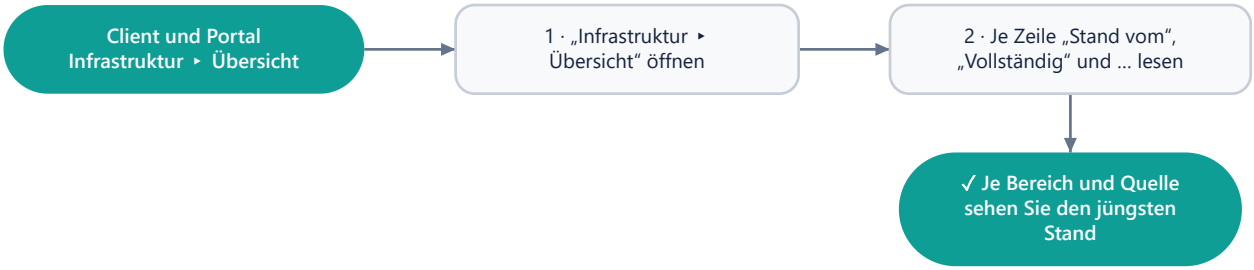


Abb. 1 – Der Reiter Stände listet jeden erhobenen Stand mit Bereich, Quelle, Ergebnis und Aufbewahrung.



Klickweg – Ist die Dokumentation aktuell?

1. Öffnen Sie *Infrastruktur ▸ Übersicht*.
2. Lesen Sie je Zeile *Stand vom*, *Vollständig* und *Änderungen zum Stand davor*.

✅ **Ergebnis:** Je Bereich und Quelle sehen Sie den jüngsten Stand. Ein Bereich ohne Quelle steht mit „kein Stand“ da – die Übersicht lässt ihn nicht weg. Sie bewertet nicht: keine Ampel, kein Prozentsatz.

6.2 Zwei Stände vergleichen

> 💻 **Client:** *Infrastruktur ▸ Infrastruktur-Dokumentation*, Registerkarte *Vergleich* · 🌐 **Portal:** *Infrastruktur ▸ Infrastruktur-Dokumentation*, Registerkarte *Vergleichsbericht* · 🔑 `infradoku.read`; für die beiden Berechtigungsbereiche zusätzlich `infradoku.permissions.read`

Den Ausschnitt dazu zeigt Abbildung 2.

© 2026 Ordivis IT · Christian Grams. Alle Rechte vorbehalten.

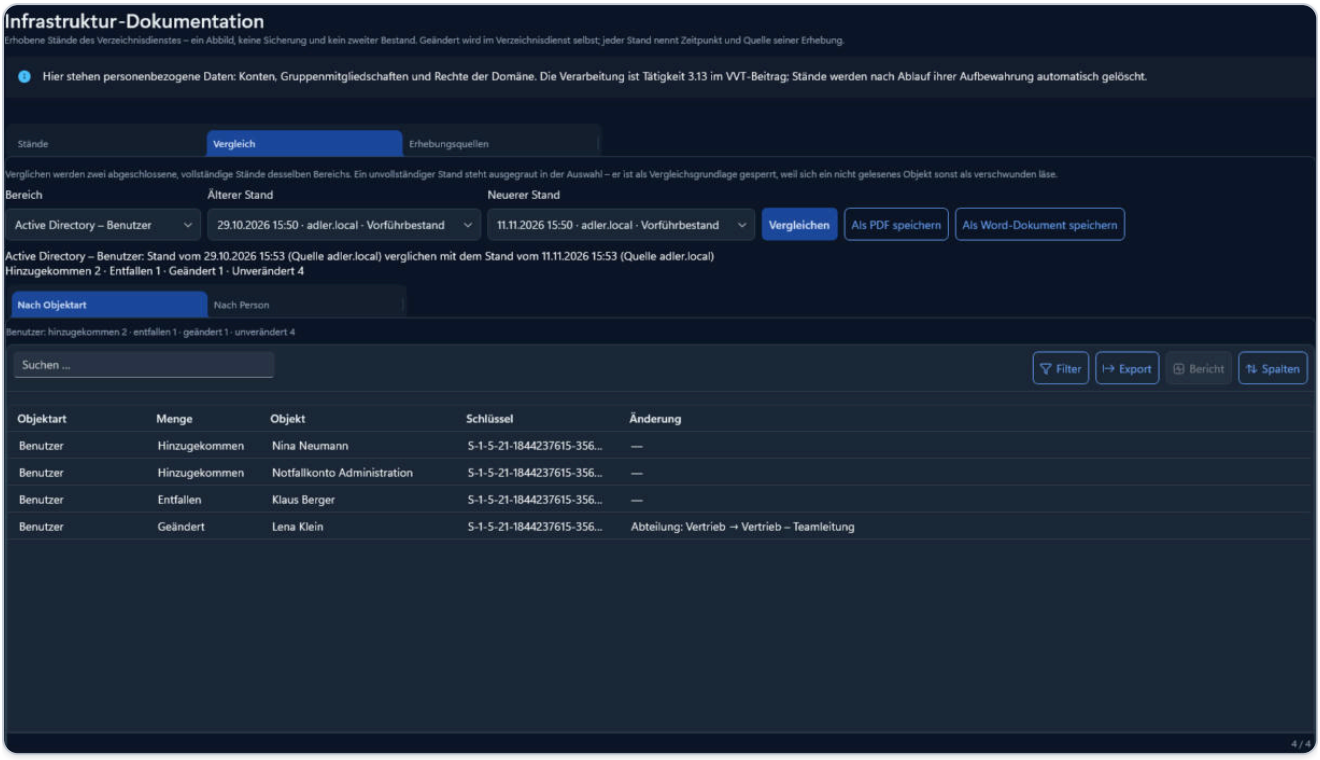


Abb. 2 – Der Vergleich zweier Benutzerstände zeigt, was hinzugekommen, entfallen oder geändert ist.



Klickweg – Zwei Stände vergleichen

1. Öffnen Sie die Registerkarte *Vergleich* (Client) oder *Vergleichsbericht* (Portal).
2. Wählen Sie den Bereich. Ordivis schlägt die beiden jüngsten vergleichbaren Stände vor.
3. Klicken Sie auf *Vergleichen* (Client) oder *Bericht anzeigen* (Portal).

✅ **Ergebnis:** Der Kopf nennt beide Stichtage und Quellen, darunter hinzugekommen, entfallen, geändert und unverändert – jede Abweichung mit altem und neuem Wert. Mit *Als PDF speichern* oder *Als Word-Dokument speichern* (Portal: *Als PDF herunterladen*, *Als Word-Dokument herunterladen*) erhalten Sie denselben Bericht als Datei. Jede solche Datei steht im Prüfprotokoll (*infradoku.exported*, mit Dateiname und Zahlen, ohne Inhalt).

Verglichen werden nur zwei abgeschlossene, vollständige Stände **desselben Bereichs**. Einen offenen oder unvollständigen Stand und zwei Stände verschiedener Bereiche lehnt der Server ab und nennt den Grund. Für die Gruppenrichtlinien gibt es zusätzlich den Vergleich je Einstellung (Registerkarte *Änderungen* der

© 2026 Ordivis IT · Christian Grams. Alle Rechte vorbehalten.

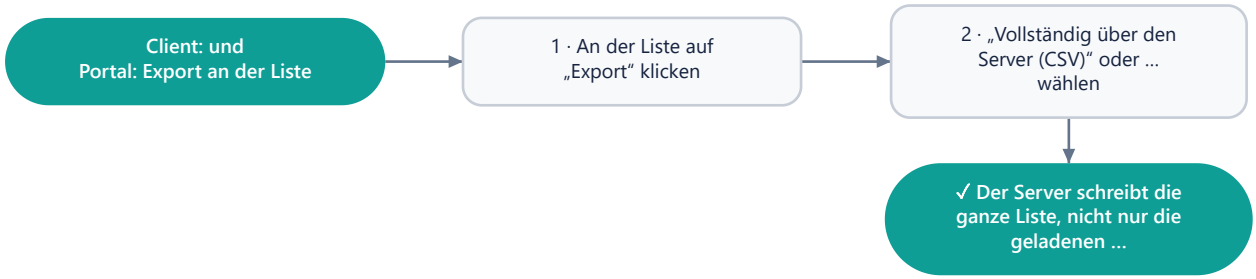
Seite *Gruppenrichtlinien*), für die Berechtigungen den Abgleich je Person (Registerkarte *Änderungen* der *Berechtigungsmatrix*). Einen Stand als PDF ablegen, Listen ausführen, die Diagramme und die Auswertung im Berichtswesen beschreibt ID-24a, Abschnitt 6.6.

6.3 Meldungen bei einer Änderung

Nach jedem Abschluss vergleicht der Server den neuen Stand mit dem vorigen derselben Quelle. Ein fester Regelkatalog – etwa „Neue Mitgliedschaft in einer privilegierten Gruppe“ oder „Neue Vertrauensstellung“ – meldet über die Alarmierung (ID-29). Der erste Stand einer Quelle meldet nie, ein unvollständiger Lauf ebenfalls nicht. Dazu rechnen eigene Aufgaben an der Uhr: die Fristen der Zertifikate und Sperrlisten und das Ausbleiben einer Erhebung. Eingestellt wird auf der Seite *Infrastruktur* ▸ *Melderegeln* im Client (Recht `infradoku.manage`); Katalog, Schwellen und Vorgaben stehen in ID-24a, Abschnitt 6.6.

6.4 Listen als Datei ausführen

> 💻 **Client** und 🌐 **Portal:** *Export* an der Liste · 🔑 dasselbe Recht wie die Liste (`infradoku.read` ; für die beiden Berechtigungsbereiche zusätzlich `infradoku.permissions.read`)



Klickweg – Listen als Datei ausführen

1. Klicken Sie an der Liste auf *Export*.
2. Wählen Sie *Vollständig über den Server (CSV)* oder *Vollständig über den Server (XLSX)*.

✅ **Ergebnis:** Der Server schreibt die **ganze** Liste, nicht nur die geladenen Zeilen. So lassen sich ausführen:

Liste	Seite	Inhalt der Datei	Dateiname (Beispiel)
Stände	*Infrastruktur-Dokumentation*, Registerkarte *Stände*	alle Stände der Auswahl (Bereich), mit Ergebnis und benannten Fehlschlägen, Bestätigung und Aufbewahrung	`staende_ad-gruppen_20261114-0915.csv`

© 2026 Ordivis IT · Christian Grams. Alle Rechte vorbehalten.

Liste	Seite	Inhalt der Datei	Dateiname (Beispiel)
Vergleich	Registerkarte *Vergleich* (Portal: *Abweichungen nach Objektart*)	je Feld einer Abweichung eine Zeile mit altem und neuem Wert; die Zahlen im Kopf	`vergleich_ad-gruppen_20261001-0600_bis_20261031-0600.csv`
Erhebungsquellen	Registerkarte *Quellen* (nur Client)	Ziel, Umfang, Anmeldung, Zeitplan und letzter Lauf	`quellen_alle_20261114-0915.csv`
Zertifikatsfristen	*Zertifikate*, Registerkarte *Fristen*	alle Zertifikate nach Restlaufzeit; fehlt eine Quelle, nennt der Kopf sie	`zertifikatsfristen_alle_20261114-0915.csv`
Meldungen	*Melderegeln*, Liste *Zuletzt gemeldet*	alle Meldungen, nicht nur die letzten 200	`meldungen_alle_20261114-0915.csv`
Gruppenrichtlinien	*Gruppenrichtlinien*, Registerkarten der Objektarten	alle Treffer der Filter oben (GPO, Teil, Art, Teiltext), nicht nur die gezeigte Seite; bei Verknüpfungen und Einstellungen vorn der Name der GPO	`gpo-einstellung_gpo_20261031-0600.xlsx`

Über der Tabelle stehen Anlage (Mandant), Auswahl oder Stand, die Vollständigkeit und der Zeitpunkt der Ausfuhr. Der Zeitstempel im Dateinamen ist bei einer Liste aus einem Stand der Stichtag des Standes, sonst der Zeitpunkt der Ausfuhr. In der XLSX-Datei sind Datum und Zeitpunkt echte Datumswerte in Ihrer Zeitzone, wie in der CSV; ein Wert, der mit `=`, `+`, `-` oder `@` beginnt, bleibt Text. Jede Ausfuhr steht im Prüfprotokoll (*infradoku.exported*, mit Liste und Zeilenzahl).

Ohne Matrixrecht fehlen in der Melderliste die Meldungen über Berechtigungen; der Kopf der Datei nennt ihre Zahl und das fehlende Recht. Zwei Stände der Berechtigungen lassen sich ohne `infradoku.permissions.read` nicht vergleichen – auch nicht als Datei.

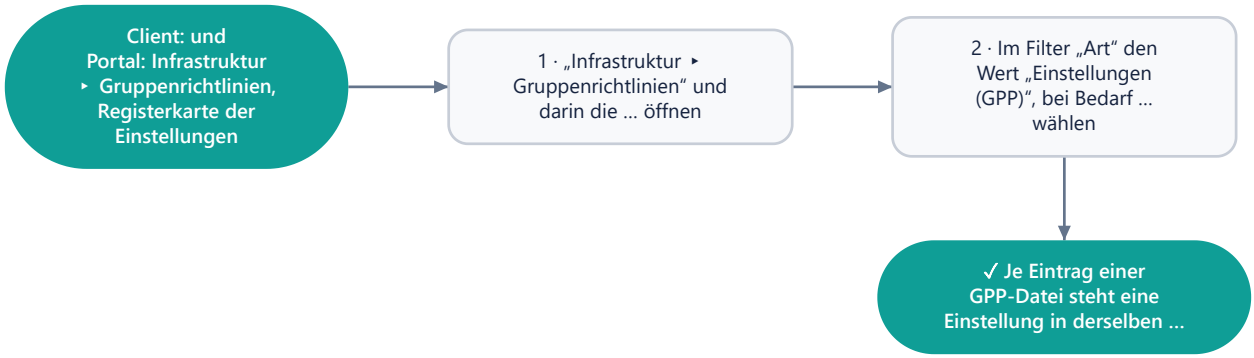
6.5 Gruppenrichtlinien-Einstellungen (GPP) lesen und vergleichen

💻 **Client** und 🌐 **Portal:** *Infrastruktur* ▸ *Gruppenrichtlinien*, Registerkarte der Einstellungen · 🔑 `infradoku.read`

Neben den administrativen Vorlagen (`Registry.pol`) zerlegt der Collector seit November 2026 auch die Gruppenrichtlinien-Einstellungen (Group Policy Preferences) – die XML-Dateien unter `Machine\Preferences` und `User\Preferences` im Ordner jeder GPO, etwa `Registry.xml`, `Groups.xml`,

© 2026 Ordivis IT · Christian Grams. Alle Rechte vorbehalten.

`Drives.xml`, `Files.xml`, `Folders.xml`, `Shortcuts.xml`, `ScheduledTasks.xml`, `Services.xml`, `Printers.xml`, `EnvironmentVariables.xml`, `IniFiles.xml`, `DataSources.xml` und `NetworkShares.xml`. Gelesen wird nur, auf demselben SMB-Weg wie die `Registry.pol`.



Klickweg – Gruppenrichtlinien-Einstellungen (GPP) lesen und vergleichen

1. Öffnen Sie *Infrastruktur* ▸ *Gruppenrichtlinien* und darin die Einstellungen.
2. Wählen Sie im Filter *Art* den Wert **Einstellungen (GPP)**, bei Bedarf dazu *Teil* (Computer oder Benutzer).

✅ **Ergebnis:** Je Eintrag einer GPP-Datei steht eine Einstellung in derselben Form wie eine aus der `Registry.pol`:

Spalte	Inhalt bei GPP
Teil	*Computer* (`Machine`) oder *Benutzer* (`User`)
Pfad	bei `Registry.xml` der Schlüssel, etwa `Registry\HKEY_LOCAL_MACHINE\SOFTWARE\…`; sonst die Art, etwa `Drives` oder `Groups`
Name	bei `Registry.xml` der Wertname, sonst der Name des Eintrags (etwa `H:`); zwei gleichnamige Einträge tragen ihre Kennung dahinter
Typ	bei `Registry.xml` der Registrierungstyp, sonst die Eintragsart (etwa `Drive`, `Group`, `NTService`)
Wert	die Eigenschaften des Eintrags als `Name=Wert`, bei Gruppen auch die Mitglieder
Zustand	die Aktion: *erstellen (C)*, *ersetzen (R)*, *aktualisieren (U)* oder *löschen (D)*
Hinweis	*deaktiviert*, die Zielgruppenadressierung kurz als Text (etwa „Zielgruppe: Gruppe BEISPIEL\Kasse UND NICHT Computer PC01“) und gegebenenfalls der Kennworthinweis

Der Vergleich zweier Stände (Registerkarte *Änderungen*), die resultierende Richtlinie und die Ausfuhr behandeln diese Einstellungen wie jede andere: Eine geänderte Aktion oder ein geänderter Pfad eines Laufwerks erscheint als *geändert*, ein neuer Eintrag als *hinzugekommen*. Eine eigene Seite gibt es dafür nicht.

⛔ **Gespeicherte Kennwörter (MS14-025).** Ältere GPP-Dateien können ein Kennwort im Attribut `cpassword` tragen. Der Schlüssel dazu ist öffentlich, und jeder Domänenbenutzer kann das SYSVOL lesen – das Kennwort gilt damit als bekannt. Ordivis übernimmt und entschlüsselt es **nie**: Der Wert erscheint

© 2026 Ordivis IT · Christian Grams. Alle Rechte vorbehalten.

weder in der Einstellung noch im Original noch im Befund. Stattdessen steht an der Einstellung „GPP enthält ein gespeichertes Kennwort (cpassword) — entfernen, MS14-025“, und je betroffener Datei steht ein Befund im Stand. Entfernen Sie den Eintrag in der Gruppenrichtlinienverwaltung und ändern Sie das Kennwort des betroffenen Kontos. Ein neuer solcher Befund meldet über die Melderegel „Gespeichertes Kennwort in einer Gruppenrichtlinie (GPP)“, Vorgabe *Kritisch* (ID-24a, Abschnitt 6.6).

Nicht zerlegt. Eine GPP-Datei unbekannter Art, eine Datei, die kein gültiges XML ist (auch eine mit DTD), und ein Eintrag ohne Eigenschaften erscheinen als *nicht zerlegt* mit Dateinamen und dem Original ohne `cpassword` – sie werden nicht still weggelassen. Ist eine solche Datei kein gültiges XML und enthält das Wort `cpassword`, fehlt das Original ganz.

Bereinigung älterer Stände. Vor November 2026 legte der Collector GPP-Dateien als Ganzes *nicht zerlegt* ab, mit dem Original samt `cpassword`. Beim ersten Start nach der Aktualisierung entfernt Ordivis deshalb einmal je Mandant aus den vorhandenen Ständen das Original jeder GPP-Datei, die ein nicht leeres `cpassword` enthält (bei einer Datei, die kein gültiges XML ist, genügt das Wort). An der Einstellung steht danach im Hinweis „Original entfernt (cpassword, MS14-025)“, und das Prüfprotokoll nennt je Mandant die Zahl der entfernten Originale, aber keine Werte. Die Stände selbst und alle übrigen Angaben bleiben unverändert, ebenso Dateien mit leerem `cpassword=""`. Der Vergleich zweier älterer Stände zeigt eine Datei weiterhin als *geändert*, wenn sie sich damals geändert hatte. Das Kennwort selbst müssen Sie trotzdem ändern: Es stand im SYSVOL und gilt als bekannt.

7 Grenzen

- **Kein Echtzeit-Abgleich.** Erhoben wird nach Plan oder auf Anforderung, nicht bei jeder Änderung im Verzeichnis. Zwischen zwei Läufen weiß Ordivis nichts.
- **Kein Entra ID, kein Exchange.** Erhoben wird das lokale Active Directory mit seinen Diensten AD CS, AD FS und AD LDS.
- **Eine Domäne je Quelle.** Verweise auf eine andere Domäne verfolgt der Collector nicht; dafür gehört eine eigene Erhebungsquelle her.
- **Keine eigenen Melderegeln.** Der Katalog ist fest; je Regel lassen sich Schalter, Dringlichkeit, Empfänger und Mengengrenze einstellen.
- **Kennwörter nie.** Weder Kennwörter noch Kennwort-Hashes, das LAPS-Kennwort oder das Kennwort eines gMSA werden gelesen.
- **Aufbewahrung.** Ein Stand bleibt 12 Monate nach seiner letzten Geltung, je Kalenderjahr bleibt ein Jahresstand unbefristet, und der jüngste Stand je Bereich und Quelle bleibt immer. Die Aufgabe *Infrastruktur-Dokumentation: Aufbewahrung* löscht den Rest täglich.
- **Begrenzte Anzeigen.** Eine Registerkarte holt höchstens 2.000 Objekte je Objektart; *Export ▸ Vollständig über den Server (CSV)* oder *(XLSX)* führt die ganze Objektart aus (Abschnitt 6.4). Diagramme zeichnen höchstens 120 Knoten.

© 2026 Ordivis IT · Christian Grams. Alle Rechte vorbehalten.

8 Fehlerbehebung

Meldung	Ursache	Abhilfe
„Für den Bereich „…“ ist am Erhebungsrechner kein Erheber vorhanden. …“	Unter *Erhoben von* steht *Erhebungsrechner (Regelweg)*.	Die Quelle bearbeiten und unter *Erhoben von* einen Collector wählen (Abschnitt 3.2).
„Eine Quelle, die ein Collector erhebt, kann keine Zugangsdaten aus dem Tresor verwenden – der Collector meldet sich mit seinem eigenen Scan-Konto an.“	Die Quelle trägt einen Tresoreintrag und einen Collector.	Den Tresoreintrag entfernen; das Scan-Konto steht in der `appsettings.json` des Collectors (Abschnitt 3.3).
„Infrastruktur-Dokumentation: Für diesen Collector sind Erhebungen angefordert, aber sein Zugang trägt das Recht „infradoku.collect“ nicht (Anmeldeschein von vor IDO-29). …“	Der Collector wurde vor Oktober 2026 angemeldet; ein ausgestelltes Recht wächst nicht nach.	Den Collector mit einem neuen Anmeldeschein neu anmelden (ID-24a, Abschnitt 13.1).
„Dieser Stand ist unvollständig und deshalb keine Vergleichsgrundlage: …“	Im Stand ist mindestens eine Teilabfrage gescheitert; sie steht hinter dem Doppelpunkt.	Die Ursache beheben (meist ein fehlendes Leserecht oder ein nicht erreichbares Ziel) und die Quelle neu erheben.
„Zwei Stände verschiedener Bereiche lassen sich nicht vergleichen.“	Die beiden gewählten Stände gehören zu verschiedenen Bereichen.	Zwei Stände desselben Bereichs wählen.
„Das Zeitlimit von … Sekunden wurde überschritten.“	Der Lauf hat das Zeitlimit der Quelle erreicht.	Das Zeitlimit der Quelle erhöhen, nach dem ersten vollständigen Lauf auf etwa das Doppelte der gemessenen Dauer.
„Es gibt noch keinen vollständigen Gruppenstand – die Berechtigungsmatrix braucht einen.“	Die Berechtigungen wurden vor den Gruppen erhoben.	Die Gruppen vollständig erheben, danach die Berechtigungen noch einmal (Abschnitt 4.3).

Weitere Meldungen, die Teilabfragen eines unvollständigen Standes und die Meldungen beim Ablegen als PDF stehen in ID-24a, Abschnitte 6.6 und 13.

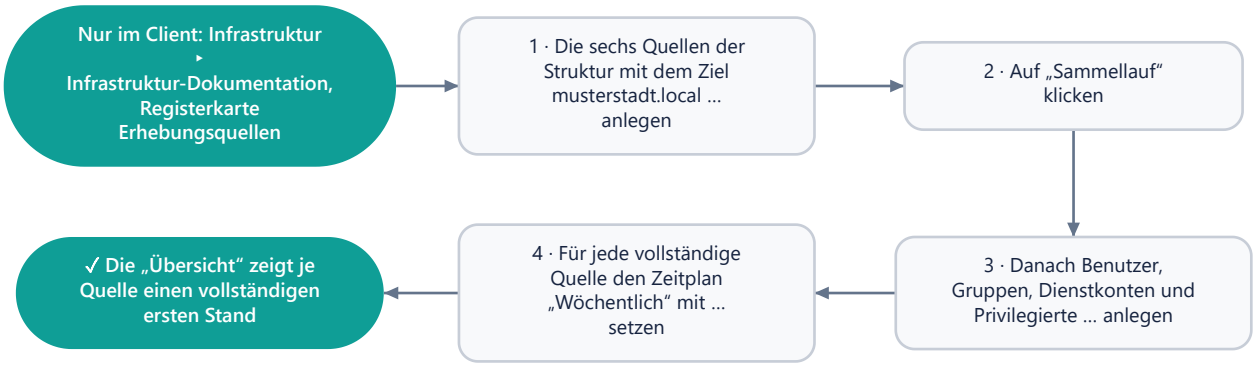
9 Beispiele aus der Praxis

9.1 Beispiel: Die Stadtverwaltung Musterstadt richtet die Dokumentation ein

Die IT der Stadtverwaltung Musterstadt will ihre Domäne `musterstadt.local` dokumentieren. Der Collector des Rathauses läuft auf einem Mitgliedsserver. Das Lesekonto `svc-doku` steht nur in *Domänen-Benutzer*, hat Leserecht auf den *Password Settings Container* und ist auf dem Dateiserver `fs01` Mitglied der *Server-Operatoren*.

© 2026 Ordivis IT · Christian Grams. Alle Rechte vorbehalten.

💻 **Nur im Client:** *Infrastruktur* ▸ *Infrastruktur-Dokumentation*, Registerkarte *Erhebungsquellen* · 🔑 `infradoku.manage` , `infradoku.collect` , `discovery.read`



Klickweg – Beispiel: Die Stadtverwaltung Musterstadt richtet die Dokumentation ein

1. Legen Sie die sechs Quellen der Struktur mit dem Ziel `musterstadt.local` und dem Collector des Rathauses an.
2. Klicken Sie auf *Sammellauf* und warten Sie, bis alle sechs Stände *Vollständig* zeigen.
3. Legen Sie danach Benutzer, Gruppen, Dienstkonten und Privilegierte Gruppen an, dann die Gruppenrichtlinien, zuletzt *Berechtigungen – Freigaben* für `fs01` mit einer einzigen Freigabe als Umfang.
4. Setzen Sie für jede vollständige Quelle den Zeitplan *Wöchentlich* mit dem Zeitfenster 22 bis 4 Uhr.

✅ **Ergebnis:** Die *Übersicht* zeigt je Quelle einen vollständigen ersten Stand. Gemeldet wurde nichts – der erste Stand meldet nie. Ab der zweiten Woche zeigt *Änderungen zum Stand davor*, was sich in der Woche getan hat.

9.2 Beispiel: Wer ist seit letzter Woche Domänen-Admin geworden?

Montags will die Leitung wissen, ob sich an den privilegierten Konten etwas geändert hat.

Den Ausschnitt dazu zeigt Abbildung 3.

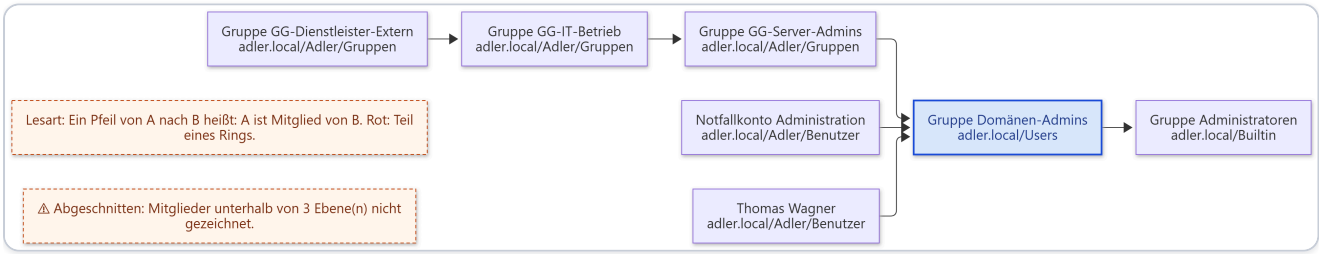
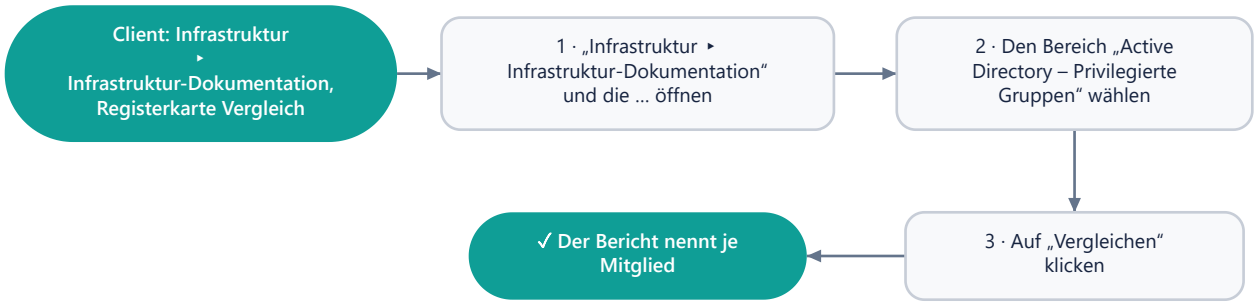


Abb. 3 – Das Diagramm zeigt, über welche Gruppen ein Konto in Domänen-Admins gelangt; die Pfeile lesen sich „ist Mitglied von“.

💻 **Client:** *Infrastruktur* ▸ *Infrastruktur-Dokumentation*, Registerkarte *Vergleich* · 🔑 `infradoku.read`

© 2026 Ordivis IT · Christian Grams. Alle Rechte vorbehalten.



Klickweg – Beispiel: Wer ist seit letzter Woche Domänen-Admin geworden?

1. Öffnen Sie *Infrastruktur* ▸ *Infrastruktur-Dokumentation* und die Registerkarte *Vergleich*.
2. Wählen Sie den Bereich *Active Directory – Privilegierte Gruppen*.
3. Klicken Sie auf *Vergleichen* und speichern Sie den Bericht als PDF.

✅ **Ergebnis:** Der Bericht nennt je Mitglied, was hinzukam oder entfiel, mit beiden Stichtagen. Ist eine Melderegel mit Empfängern eingestellt, kam die neue Mitgliedschaft schon nach dem Lauf als Alarm.

10 Häufige Fragen

Braucht Ordivis ein Konto mit Domänen-Admin-Rechten? Nein. Ein Lesekonto genügt (Abschnitt 2). Ein Konto mit Schreibrechten im Verzeichnis wäre unnötig und der größte denkbare Schaden.

Muss auf den Domänencontrollern etwas installiert werden? Nein. Der Collector läuft auf einem Mitgliedsserver oder Arbeitsplatz und liest die Domänencontroller per LDAP und SMB (Abschnitt 2).

Kann ich aus einem Stand ein gelöschtes Konto oder eine Gruppenrichtlinie zurückholen? Nein. Ein dokumentierter Stand ist keine Sicherung (Abschnitt 2). Für die Wiederherstellung brauchen Sie die Sicherung der Domänencontroller oder den AD-Papierkorb.

Warum zeigt die resultierende Richtlinie etwas anderes als `gpresult` auf dem Rechner? Weil sie eine Rechnung aus dem dokumentierten Stand ist: ohne WMI-Filter, lokale Richtlinien und Loopback, und mit dem Stand vom Zeitpunkt der Erhebung (Abschnitt 2).

Kann ich einen erhobenen Wert korrigieren? Nein. Ein Stand ist ein Abbild; geändert wird im Verzeichnisdienst, und der nächste Lauf zeigt es. Neben dem Stand pflegen lässt sich etwa die Anwendung einer AD-LDS-Instanz (ID-24a, Abschnitt 6.6).

Warum kann ich einen Stand nicht vergleichen? Er ist offen oder unvollständig, oder der andere Stand gehört zu einem anderen Bereich (Abschnitt 6.2). Der Server nennt den Grund.

Kann die Zentrale ohne Collector erheben? Nicht in dieser Fassung (Abschnitt 3.2).

Warum steht in einer Gruppe oder in der Berechtigungsmatrix eine SID statt eines Namens? Weil das Konto zu einer anderen Domäne gehört. Konten und Gruppen anderer Domänen **derselben Gesamtstruktur** schlägt der Collector im globalen Katalog nach und zeigt sie als `DOMÄNE\Name (globaler Katalog)` – in der Matrix, in der Mitgliedsauskunft und in den Spalten *Mitglied (andere Domäne)* bzw. *Treuhänder (andere Domäne)*. Dafür braucht er TCP 3269 (sonst 3268) zu einem globalen Katalog (ID-24a,

© 2026 Ordivis IT · Christian Grams. Alle Rechte vorbehalten.

Abschnitt 6.6); ist der nicht erreichbar, nennt der Stand das als Hinweis und bleibt vollständig – Matrix und Vergleich gehen weiter, nur ohne diese Namen. Eine SID mit dem Zusatz *(nicht im globalen Katalog)* gehört zu einer Domäne außerhalb der Gesamtstruktur (über eine Vertrauensstellung) oder zu einem gelöschten Konto; Ordivis rät dann keinen Namen. Die Gruppen der anderen Domäne stehen nicht im Stand – wer über sie berechtigt ist, zeigt erst eine eigene Erhebungsquelle für diese Domäne.

Wie lange bleiben die Stände? 12 Monate nach ihrer letzten Geltung, dazu ein Jahresstand je Kalenderjahr unbefristet (Abschnitt 7).

Verwandte Themen

- **ID-24a – Discovery-Collector** – Installation, Scan-Konto und Abschnitt 6.6 mit allen Einzelheiten der Bereiche und Seiten
- **ID-24 – Modul Discovery** – die Scans der Zentrale und die Anmeldedaten
- **ID-44 – Rollen und Rechte** – die Rechte `infradoku.*` und ihre Vorbelegung
- **ID-60 – API-Referenz** – die Schnittstelle unter `/api/v1/infradoku`
- **ID-29 – Modul BCM** – die Alarmierung, über die die Melderegeln zustellen
- **ID-27a – Reports und SQL-Abfragen** – die Datenquellen der Infrastruktur-Dokumentation im Berichtswesen
- **ID-57 – Verarbeitungstätigkeiten (VVT-Beitrag)** – die Verarbeitung personenbezogener Daten in den Ständen

© 2026 Ordivis IT · Christian Grams. Alle Rechte vorbehalten.