



Inventarisierung – Discovery-Windows

Skriptbasierte Inventarisierung für Windows

TITEL	Inventarisierung – Discovery-Windows
AUTOR	Docusnap Consulting
DATUM	13.03.2025
VERSION	5.2 gültig ab 13.03.2025

Die Weitergabe, sowie Vervielfältigung dieser Unterlage, auch von Teilen, Verwertung und Mitteilung ihres Inhaltes ist nicht gestattet, soweit nicht ausdrücklich durch die itelio GmbH zugestanden. Zuwiderhandlung verpflichtet zu Schadenersatz. Alle Rechte vorbehalten.

This document contains proprietary information and may not be reproduced in any form or parts whatsoever, nor may be used by or its contents divulged to third parties without written permission of itelio GmbH. All rights reserved.

INHALTSVERZEICHNIS

1.	Einleitung	4
2.	Grundlagen	5
2.1	Benötigte Rechte	5
2.2	Parameter	5
2.3	Docusnap Skript Legacy	5
3.	Skriptbasierte Windows Inventarisierung	6
3.1	Skriptbasierte Windows Inventarisierung durchführen	6
3.2	Inventarisierung importieren	6
3.3	Skriptausführung automatisieren	7
3.4	Verwendete Skriptdateien aktuell halten	8
4.	Nennenswerte Parameter	9
4.1	Software- und Dateisuche -S	9
4.1.1	Dateisuche	10
4.1.2	Softwaresuche	11
4.2	Zusatzprogramme -Y	12
4.3	Auswahl der Scankomponenten -Z	13
4.4	Dateinamen anonymisieren -ANO	14

1. Einleitung

Neben der remote Inventarisierung von Windows Systemen besteht in Docusnap auch die Möglichkeit einer skriptbasierten Inventarisierung der Windows Systeme.

Die Skriptdatei finden Sie im Installationsverzeichnis von Docusnap – im Standard:

- %Docusnap-Installationsverzeichnis%\Tools\Discovery-Windows.exe

Bei Aufruf der Discovery-Windows.exe wird eine lokale Inventarisierung durchgeführt. Alle inventarisierten Informationen werden in einer XML-Datei gespeichert, die anschließend in Docusnap importiert wird.

Auch für Linux-Systeme, Mac-Systeme, SharePoint, Exchange, DNS, DHCP, Veeam, DFS und das Active Directory existieren entsprechende Skripte, welche in eigenen Support-Dokumenten und innerhalb des Benutzerhandbuchs behandelt werden.

2. Grundlagen

2.1 Benötigte Rechte

Für den Aufruf der Discovery-Windows.exe zur Inventarisierung des lokalen Systems sind Benutzerrechte ausreichend.

Bitte beachten Sie, dass für die Inventarisierung von

- **BitLocker Status und Wiederherstellungsschlüssel**
- **Anti-Virus und Anti-Spyware Informationen**
- **Energieoptionen**
- **Bios Typ (UEFI, Legacy BIOS)**
- **Bios Startoptionen - sicherer Start / Secure Boot aktiv oder inaktiv**
- **Vorhandensein von Sicherheitsmodulen (TPM)**
- **Benutzerprofile**

die Discovery-Windows.exe mit administrativen Rechten ausgeführt werden muss.

2.2 Parameter

Die möglichen Übergabeparameter können über den Aufruf von Discovery-Windows.exe -? aufgerufen werden.

Folgendes Beispiel inventarisiert das System und legt die XML-Datei auf der zentralen Netzwerk-Freigabe \\SMDC0001\DC-Share ab:

```
Discovery-Windows.exe -O \\SMDC0001\DC-Share\
```

2.3 Discovery-Windows-Legacy

Die Discovery-Windows.exe kann nicht genutzt werden, um Windows Systeme mit folgenden Betriebssystemen manuell zu inventarisieren:

- Windows XP
- Windows Server 2000
- Windows Server 2003

Damit Windows Systeme mit den zuvor aufgeführten Betriebssystemen manuell inventarisiert werden können, muss die DocusnapScriptLegacy.exe genutzt werden.

Die Discovery-Windows-Legacy.exe ist ebenfalls im Programmverzeichnis von Docusnap - Unterordner Tools zu finden:

- %Docusnap-Installationsverzeichnis%\Tools

3. Skriptbasierte Windows Inventarisierung

3.1 Skriptbasierte Windows Inventarisierung durchführen

Die Skriptdatei finden Sie im Installationsverzeichnis von Docusnap:

- %Docusnap-Installationsverzeichnis%\Tools\Discovery-Windows.exe

Im einfachsten Fall führen Sie die Discovery-Windows.exe auf dem Zielsystem aus. Daraufhin wird die Inventarisierung des Windows Systems durchgeführt.

3.2 Inventarisierung importieren

Die Inventarisierung ist abgeschlossen, wenn die Ergebnisdatei erzeugt wurde. Die Ergebnisdatei wird standardmäßig an dem Ort erstellt, an dem der Aufruf der Discovery-Windows.exe durchgeführt wurde.

- Hostname_Benutzer_Zeitstempel.xml

Diese Daten können Sie mit Hilfe des Assistenten Skript Import nach Docusnap importieren:

- Discovery – Alle Assistenten – Dateiimport
- Inventar – Alle Assistenten – Dateiimport
- Alle Aufträge – Alle Assistenten – Dateiimport

In Schritt 1 wählen Sie Ihre Firma oder die Firma Ihres Kunden aus.

In Schritt 2 wählen Sie den Discovery Service aus, über den Sie die Inventarisierung durchführen möchten.

Für eine zeitgesteuerte Inventarisierung wählen Sie hier den Docusnap Server Discovery oder einen von Ihnen konfigurierten Discovery Service.

Beachten Sie hierbei, dass der Benutzer, der einen der Dienste ausführt, Änderungsrechte, auf den im nächsten Schritt ausgewählten Pfad besitzen muss.

Lokales System = Ablageverzeichnis kann nur lokal liegen

In Schritt 3 wählen Sie das Verzeichnis aus, in dem Sie die erzeugte XML-Datei abgelegt haben.

Dieses Verzeichnis kann auch ein Netzlaufwerk sein. Beachten Sie die Freigabeberechtigungen.

In Schritt 4 können Sie nun nach validen Skriptdateien suchen.

Sind in dem von Ihnen ausgewählten Ordner Dateien von weiteren Skriptinventarisierungen (DNS, DHCP, Active Directory etc.) vorhanden, werden auch diese berücksichtigt.

3.3 Skriptausführung automatisieren

Der große Vorteil von Docusnap besteht darin, dass regelmäßig und automatisch Daten inventarisiert werden und somit aktuell sind. Dies kann auch mit Skriptinventarisierungen erreicht werden.

Im ersten Schritt muss die Ausführung des Skripts automatisiert werden. Dies kann unter anderem mit einer Softwareverteilung erfolgen. Weiterhin besteht die Möglichkeit, dies mittels der Windows Aufgabenplanung und Gruppenrichtlinien durchzuführen – diese Variante wird folgend beschrieben.

Erstellen oder passen Sie eine Gruppenrichtlinie an und wechseln Sie in

- Computer Konfiguration – Einstellungen – Systemsteuerungseinstellungen – Geplante Aufgaben

Im Tab **Allgemein** hinterlegen Sie einen Namen / Aktion und wählen die Sicherheitsoptionen:

Folgendes Benutzerkonto verwenden: Benutzer mit lokalen Administrationsberechtigungen / lokales Systemkonto "NT-AUTORITÄT\SYSTEM" (empfohlen)

Unabhängig von der Benutzeranmeldung ausführen

Mit höchsten Privilegien ausführen

Konfigurieren für: Das passende Betriebssystem auswählen

Im Tab **Trigger** können Sie den Zeitplan der Skriptausführung konfigurieren – beispielsweise:

Aufgabe starten: Nach einem Zeitplan

Start: XX.XX.XXXX, 10:00:00

Wöchentlich, jede 1 Woche wiederholen am: Montag

Möchten Sie mehrfach in der Woche aktuelle Daten Ihrer Windows-Systeme inventarisieren, lassen Sie die Ausführung entsprechend häufiger durchführen.

Im Tab **Aktionen** definieren Sie die Ausführung der Discovery-Windows.exe

Wir empfehlen die Erstellung einer versteckten Freigabe auf dem Docusnap Server / System, dass den Docusnap Discovery Service ausführt.

In dieser Freigabe werden 2 Ordner benötigt:

Zum Ablegen der Discovery-Windows.exe – hier werden lesende Berechtigungen benötigt.

z. B. \\SRV-Docu\DocusnapScript\$\Scripts

Zum Ablegen der Ergebnisdateien– hier werden Änderungsrechte benötigt.

z. B. \\SRV-Docu\DocusnapScript\$\Firma#Domain.FQDN

Wir empfehlen für die Verwendung der Berechtigungen das Microsoft Best Practice, sodass die Gruppe **Jeder Vollzugriff** erhält und über NTFS-Berechtigungen nur die Gruppen **Domänencomputer** und **Domänencontroller** **Ändern** Rechte erhalten. Zusätzliche Härtingsmaßnahmen sind kundenspezifisch zu treffen.

Aktion: Programm starten

Programm / Skript: \\SRV-Docu\DocusnapScript\$\Scripts\Discovery-Windows.exe

Argumente: -O "\\SRV-Docu\DocusnapScript\$\Firma#Domain.FQDN"

Der -O Parameter leitet die Ergebnisdateien auf den angegebenen Pfad um. Der Benutzer bzw. die Systemkonten, welche die Inventarisierungen durchführen, müssen auf diesem Pfad Schreibrechte besitzen.

Im Tab **Einstellungen** aktivieren Sie die Optionen:

- Ausführung der Aufgabe bei Bedarf zulassen
- Aufgabe so schnell wie möglich nach einem verpassten Start ausführen
- Aufgabe beenden, falls Ausführung länger als: 1 Tag

Sollten Sie unterschiedliche Sprachen auf den Domänencontroller einsetzen, müssen Sie die SID des lokalen Systemkontos verwenden -> bearbeiten Sie hierzu die Gruppenrichtlinie nach dem Erstellen unter folgendem Pfad:

`\\IhreDomäne\SYSVOL\IhreDomäne\Policies\{IhreGPOGUID}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml`

Suchen Sie in der XML-Datei an allen Stellen nach dem String `runAs="NT AUTORITÄT\SYSTEM"` und ersetzen `NT AUTORITÄT\SYSTEM` durch die SID `S-1-8-15`.

3.4 Verwendete Skriptdateien aktuell halten

Wir empfehlen bei der Verwendung einer / der Skriptvarianten grundsätzlich die Installation eines Docusnap Discovery Services (DDS) mindestens auf dem System, auf dem auch der Docusnap Server konfiguriert wurde. Weitere DDS können in den dezentralen Netzwerken (Standorte, VLANs etc.) platziert werden.

In den Einstellungen des DDS können Sie ein zusätzliches Verzeichnis für die Ablage der Inventarisierungsmodule (Skriptdateien) angeben. Dies bewirkt, dass die Skriptdateien bei einem Update von Docusnap automatisch ausgetauscht werden und somit immer aktuell sind.

Installieren und konfigurieren Sie den DDS – ein HowTo finden Sie in unserer Knowledge Base.

Nach der Konfiguration wechseln Sie in den Reiter Einstellungen und setzen das Ablageverzeichnis:

- `C:\DocusnapScript\Scripts`

Geben Sie den Ordner im Anschluss über das Netzwerk frei: `\\SRV-Docu\DocusnapScript$`.

Diese Freigabe können Sie wieder zum Aufruf der Skriptdatei

- `\\SRV-Docu\DocusnapScript$\Scripts\Discovery-Windows.exe`

und zur Ablage der JSON-Dateien verwenden:

- `\\SRV-Docu\DocusnapScript$\Firma#Domain.FQDN`

4. Nennenswerte Parameter

Bei den folgenden Parametern ist eine kurze Erklärung notwendig.

4.1 Software- und Dateisuche -S

Die Software- und Dateisuche dient dem Suchen spezifischer Dateien auf dem Filesystem, bzw. dem Suchen von Anwendungen, die ohne Registrierung auf dem Zielsystem „installiert“ wurden.

Wie die Software- und Dateisuche innerhalb der remote-Inventarisierung durchgeführt werden kann, wird in folgendem HowTo beschrieben: Inventarisierung - Software- und Dateisuche

Die Nutzung der Software- und Dateisuche bei der Inventarisierung mittels der Discovery-Windows.exe setzt eine XML-Datei voraus. Die XML-Blöcke für die Software- und Dateisuche unterscheiden sich, können jedoch in einer XML-Datei zusammengefasst werden.

Über den Parameter -H filesearch können Sie die Hilfe mit Syntax öffnen:

```
"%Docusnap-Installationsverzeichnis%\Tools\Discovery-Windows.exe" -H filesearch
```

Die Verwendung der Software- und Dateisuche im Zuge der Skriptinventarisierung aktivieren Sie mittels des Parameters -S und dem Pfad zur XML-Datei:

```
\\SRV-Docu\DocusnapScript$\Scripts\Discovery-Windows.exe -S \\SRV-Docu\DocusnapScript$\Scripts\SoftwareAndFileSearch.xml
```

Neben dem Aufbau der XML-Datei unterscheiden sich auch die Auswertungsmöglichkeiten. Eine detaillierte Beschreibung finden Sie ebenfalls im HowTo: Inventarisierung - Software- und Dateisuche.

4.1.1 Dateisuche

Folgend eine beispielhafte XML-Datei für die Dateisuche:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Search>
  <SearchItem>
    <Category>1</Category>      <!-- DATEISUCHE-->
    <Name>Test log4j</Name>
    <FileName>*log4j*</FileName>
    <FileSize>0</FileSize>
    <IncludeExcludeList>
      <SearchPath>
        <IncludePath>C:\Temp</IncludePath>
        <ExcludePath></ExcludePath>
      </SearchPath>
      <SearchPath>
        <IncludePath>C:\ProgramData</IncludePath>
        <ExcludePath></ExcludePath>
      </SearchPath>
    </IncludeExcludeList>
    <OnlyFirstMatch>true</OnlyFirstMatch>
    <UseSystemDrive>>false</UseSystemDrive>
  </SearchItem>
</Search>
```

OPTION	ERKLÄRUNG
CATEGORY	1= Dateisuche
NAME	Bezeichnet die Suche im Allgemeinen
FILENAME	Angabe der zu suchenden Datei – Wildcards (*) können verwendet werden
FILESIZE	Optional – stimmt die Größe nicht überein, ist kein Treffer verfügbar
SEARCHPATH	Ein- ODER Ausschließende Suchpfade Ein- und Ausschluss können nicht kombiniert werden!
ONLYFIRSTMATCH	Bestimmt, ob nur das erste gefundene Ergebnis angezeigt werden soll (true) Bei false werden alle gefundenen Ergebnisse erfasst
USESYSERMDRIVE	Bestimmt, ob nur die Systempartition durchsucht werden soll (true) oder alle Partitionen auf dem System (false)

4.1.2 Softwaresuche

Folgend der Aufbau der XML-Datei für die Softwaresuche:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Search>
  <SearchItem>
    <Category>0</Category>      <!-- SOFTWARESUCHE-->
    <Name>Test log4j</Name>
    <Version />
    <Publisher>Hersteller</Publisher>
    <FileName>*log4j*.jar</FileName>
    <FileSize />
    <ModifyDate />
    <SearchPath>C:\ProgramFiles</SearchPath>
  </SearchItem>
</Search>
```

OPTION	ERKLÄRUNG
CATEGORY	0= Softwaresuche
NAME	Bezeichnet die Suche im Allgemeinen
VERSION	Optionale Angabe der Softwareversion
PUBLISHER	Hersteller der Software
FILENAME	Angabe der zu suchenden Datei – Wildcards (*) können verwendet werden
FILESIZE	Optional – stimmt die Größe nicht überein, ist kein Treffer verfügbar
MODIFYDATE	Optionale Angabe eines Änderungsdatum
SEARCHPATH	Einschließender Suchpfad

4.2 Zusatzprogramme -Y

Durch die Verwendung von Zusatzprogrammen können bei der Inventarisierung zusätzliche Informationen zu einem Windows-System erfasst werden. Die Ausführung der Zusatzprogramme kann auch im Rahmen des Docusnap-Skriptes gestartet werden. Um die Zusatzprogramme auszuführen, muss eine XML-Datei mit den benötigten Informationen erstellt werden. Die XML-Datei hat folgenden Aufbau:

```
<ToolInfo>
  <Url>systeminfo.exe</Url>
  <Parameters></Parameters>
  <ResultFile>systeminfo.txt</ResultFile>
  <OpenWith>notepad.exe</OpenWith>
  <Description>Systeminfo</Description>
  <ToolType>0</ToolType>
  <Timeout>10000</Timeout>
  <ExecuteRemote>>false</ExecuteRemote>
</ToolInfo>
```

Der Aufruf der Zusatzprogramme in Docusnap Script erfolgt mit folgendem Aufruf:

Discovery-Windows.exe -Y <Pfad\> <Dateiname.xml>

Discovery-Windows.exe -Y C:\DocusnapScript\ToolInfo.xml

Daten, die bei der Ausführung der Zusatzprogramme im Zuge des Scripts gesammelt werden, werden in der Ergebnis XML-Datei gespeichert und beim Import dieser Datei in Docusnap ausgegeben.

Weitere Informationen für die Nutzung der Zusatzprogramme erhalten Sie durch den Aufruf:

```
"%Docusnap-Installationsverzeichnis%\Tools\Discovery-Windows.exe" -H tools
```

4.3 Auswahl der Scankomponenten -Z

Docusnap liefert die Möglichkeit, die zu inventarisierenden Komponenten bei den Windows Systemen auszuwählen (Software, Hotfixe, Dienste etc.). Diese Auswahl der Komponenten können Sie auch bei Nutzung der Discovery-Windows.exe durchführen.

Der Aufruf erfolgt über den Parameter -Z <Zahl>.

Die notwendige Zahl erhalten Sie auf zwei Wegen:

1. Windows Scan Assistenten

Wechseln Sie in einen der Windows Scan Assistenten (AD oder IP). In Schritt 3 finden Sie die Schaltfläche **Komponenten Auswählen**. Wählen Sie die Komponenten aus, die inventarisiert werden sollen und notieren Sie sich den DS Skript Parameter.

2. Manuelles Aufzählen

Starten Sie die Hilfe der Discovery-Windows.exe spezifisch für die Scankomponenten:

```
"%Docusnap-Installationsverzeichnis%\Tools\Discovery-Windows.exe" -H scan
```

Nun können Sie die entsprechenden Komponenten festlegen, indem Sie die dahinter befindlichen Zahlen addieren.

4.4 Dateinamen anonymisieren -ANO

Die .XML-Dateien, die von der Discovery-Windows.exe erstellt werden, werden wie folgt benannt.

- Computername
- Benutzer oder System, der die Ausführung der Discovery-Windows.exe durchgeführt hat
- Datum und Uhrzeit der Ausführung

Beispiel:

VPC-SDA_VPC-SDA_admin_20221011090358.xml

Durch die Ausführung der Discovery-Windows.exe mit dem Parameter -ANO wird der Dateiname anonymisiert.

Beispiel:

383ee2d1-46ae-4cbc-b2f9-b4dc437bf911.xml

Durch die Verwendung des -ano Parameters kann Docusnap nicht mehr anhand des Dateinamens erkennen, ob im Zielordner bereits Dateien vom gleichen System vorhanden sind und diese in den Archiv Ordner verschieben. Das bedeutet, dass sich im Ordner mehrere Dateien eines Systems befinden können, die im Anschluss importiert werden. Dabei ist die Reihenfolge des Imports zufällig. Dadurch ist nicht sichergestellt, dass der Stand der aktuellsten Datei in Docusnap verfügbar ist.

VERSIONSHISTORIE

Datum	Beschreibung
25.04.2017	Version 1.0 fertiggestellt
24.10.2018	Version 1.1 – Austausch veralteter Screenshots, Erweiterung um Punkte Softwaresuche und Zusatzprogramme, Links aktualisiert
28.02.2020	Version 1.2 – Erweiterung um Windows 10 Schnellstart im Bereich zentrale Ausführung
09.06.2020	Version 2.0 - Überarbeitung des HowTos für Docusnap 11
23.03.2021	Version 2.1 – Erweiterung des HowTos um die Beschreibung des -ANO Parameters
03.09.2021	Version 2.2 – Benötigte Rechte bearbeitet
27.09.2022	Version 2.3 – Überarbeitung der Software- und Dateisuche
13.10.2022	Version 2.4 - Allgemeine Anpassung des HowTos
22.12.2022	Version 3.0 – Überarbeitung für Docusnap 12
19.07.2023	Version 3.1 – Berechtigungen für BitLocker Wiederherstellungsschlüssel hinzugefügt
23.11.2023	Version 4.0 - Überarbeitung des HowTos für Docusnap 13
11.11.2024	Version 4.1 - Überarbeitung des HowTos für Skript-Ablage
20.11.2024	Version 5.0 - Überarbeitung des HowTos für Docusnap 14
19.02.2025	Version 5.1 – XML-Syntax-Korrektur der Softwaresuche
13.03.2025	Version 5.2 – Best Practice Empfehlung für NTFS-Berechtigungen

