Inventarisierung - Software- und Dateisuche

Software- und Dateisuche für Linux, Mac und Windows
Inventarisierung

TITEL	Inventarisierung - Software- und Dateisuche
AUTOR	Docusnap Consulting
DATUM	12.12.2023
VERSION	1.1 | gültig ab 27.09.2022

INHALTSVERZEICHNIS

1. Einleitung

Die Software- und Dateisuche in Docusnap dient dem Suchen spezifischer Dateien auf dem Filesystem von Linux-, Mac- und Windows-Systemen. Hierbei werden Dateinamen definiert, die Docusnap daraufhin im Zuge der Inventarisierung auf dem Dateisystem sucht.

Die gefundenen Dateien werden je nach Kategorisierung (Dateisuche Linux, Mac und Windows oder Softwaresuche Windows) auf unterschiedlichen Wegen in Docusnap zur Auswertung bereitgestellt.

Die Softwaresuche bezeichnet hierbei Anwendungen, die ohne Registrierung auf dem Zielsystem „installiert" wurden. Werden die definierten Dateien gefunden, wird ein entsprechender Eintrag in der Liste installierter Softwareprodukte des Systems erzeugt. Daraufhin kann diese Software auch im Bereich des Lizenzmanagements analysiert werden.

Die Dateisuche bezeichnet hierbei jegliche Dateien, die Sie, beispielweise aufgrund einer Sicherheitslücke (log4j), suchen möchten. Die Dateien werden daraufhin auch mit dem Pfad, in dem diese gefunden wurden, aufgelistet. Ein neues Objekt innerhalb der Zusammenfassung sowie ein neues vordefiniertes Docusnap Connect Paket liefern die Möglichkeit zur systemübergreifenden Analyse.

Zum aktuellen Zeitpunkt (September 2022) ist es nicht möglich, eine Dateisuche mit den Skriptvarianten für Linux und Mac durchzuführen.

Eine detaillierte Beschreibung, wie die Software- und Dateisuche bei der Verwendung der Skriptvariante für Windows eingesetzt werden kann, finden Sie im HowTo: Inventarisierung – Docusnap Skript für Windows.

2. Software- und Dateisuche einrichten

Die Software- und Dateisuche wird in der Docusnap **Administration - Inventar** eingerichtet und verwaltet. Im ersten Schritt vergeben Sie einen **Namen** und wählen die **Kategorie** aus:

- Dateisuche Linux
- Dateisuche Mac
- Dateisuche Windows
- Softwaresuche Windows

Im nächsten Schritt definieren Sie den **Suchbegriff bzw. Dateiname**. Hier kann der tatsächliche Dateiname hinterlegt werden. Auch **Platzhalter** können verwendet werden, um die Suche flexibler zu gestalten (z. B. Docusnap*.exe). Ein ? ersetzt ein Zeichen, der * ersetzt mehrere Zeichen.

Die Angabe des Suchpfads unterscheidet sich, je nachdem, welche Kategorie gewählt wurde – weitere Informationen in den folgenden Abschnitten. Die übrigen Felder sind optional:

- Dateigröße (Angabe in Bytes)
- Änderungsdatum
- Hersteller
- Version

Mit Hilfe der Schaltfläche Löschen können Einträge wieder entfernt werden. Auch verwendete Einträge können gelöscht werden. Wenn ein Auftrag für eine Inventarisierung erstellt wurde, in der die Dateisuche verwendet wird, kann der Auftrag auch noch ausgeführt werden, wenn die dazugehörige Definition der Software- und Dateisuche gelöscht wurde. Wenn der Auftrag bearbeitet wird, steht allerdings die gelöschte Definition nicht mehr zur Verfügung und sobald die Bearbeitung fertiggestellt wurde, wird diese Definition bei der Inventarisierung nicht mehr berücksichtigt.

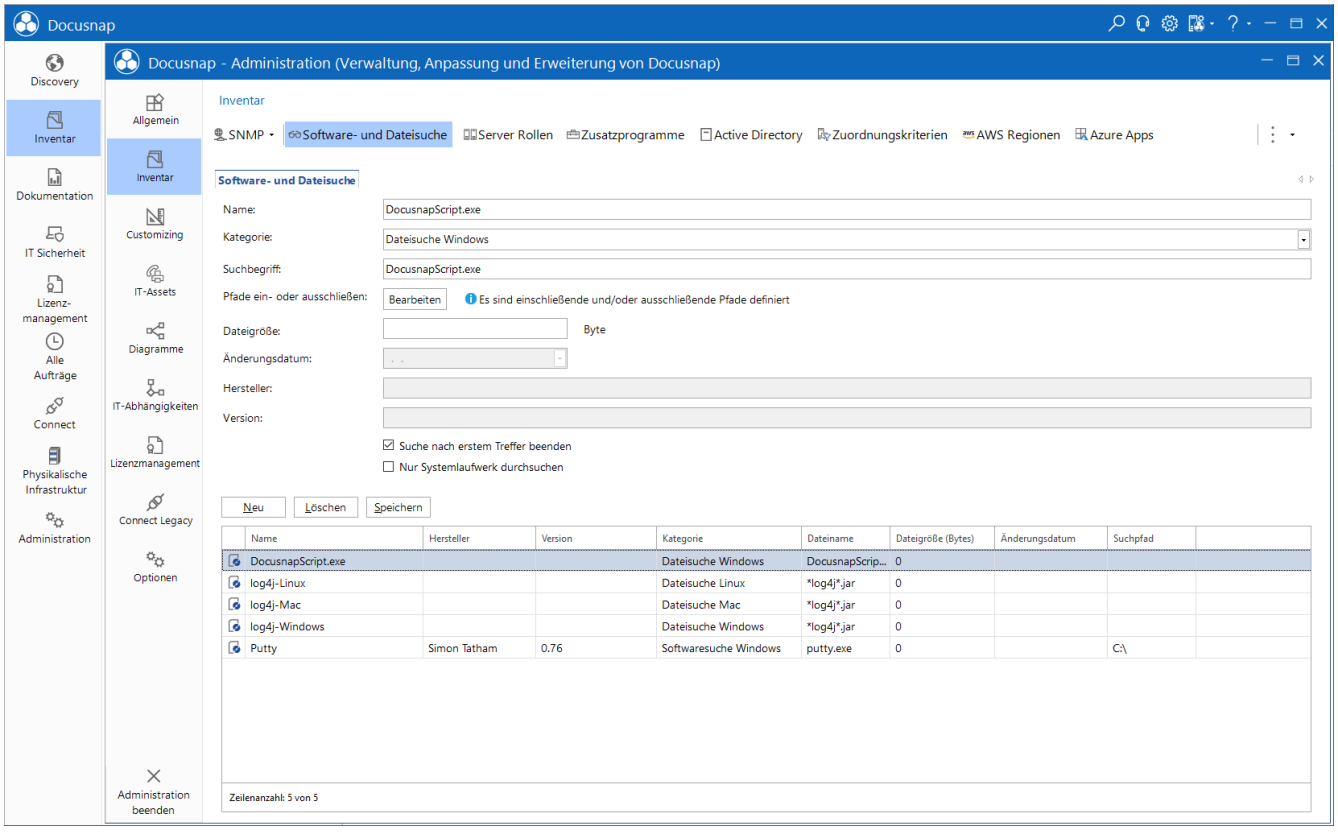

Abbildung 1 - Software- und Dateisuche verwalten

2.1 Softwaresuche Windows

Bei der Softwaresuche Windows ist der Suchpfad optional. Wird kein Suchpfad angegeben, werden alle lokalen Laufwerke durchsucht.

Die Angabe eines Suchpfads kann maßgeblich zur Ausführungszeit beitragen. Die Windows Softwaresuche kann die Scanzeiten erheblich verlängern und erfordert eine merklich höhere Auslastung auf den beteiligten Systemen. Unter anderem ist, bezüglich der Scanzeiten sowie auch der Auslastung, ebenfalls relevant, wie viele Softwaresuchen pro Scan aktiviert werden.

Die Software Suche wird beendet, sobald eine Datei mit dem entsprechenden Dateinamen gefunden wurde.

2.2 Dateisuche

Bei der Dateisuche können Sie sowohl ein- als auch ausschließende Suchpfade definieren. **Für jeden Pfad muss ein eigener Eintrag über den Button Neu erstellt werden.**

Werden keine Pfadangaben durchgeführt, werden auch hier alle lokalen Laufwerke durchsucht.

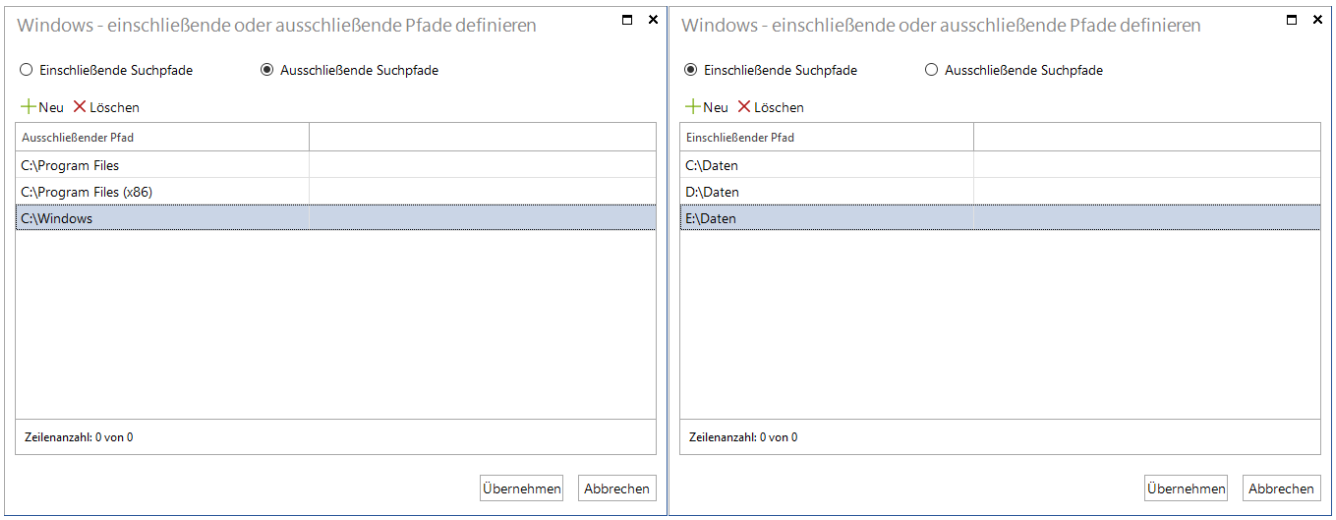

Abbildung 2 - Ein- und Ausschließende Suchpfade definieren

Bei der Dateisuche Windows gibt es im Vergleich mit der Dateisuche Linux und Mac die zusätzliche Option Suche nach erstem Treffer beenden.

Wird diese Option aktiviert, beendet Docusnap die Suche nach der angegebenen Datei, sobald diese erstmalig gefunden wurde.

Geht es Ihnen also beispielsweise darum, z. B. im Falle einer Bedrohung die evtl. betroffenen Systeme zu identifizieren, würde es ausreichen, die Suche nach erstmaligem Fund zu beenden.

Möchten Sie jedoch im Detail Informationen zu der gesuchten Datei auf dem jeweiligen System erhalten, führen Sie die Dateisuche ohne die genannte Option durch. Docusnap listet ihnen anschließend alle gefundenen Pfade der Datei auf.

Auch bei der Dateisuche Windows gilt, dass die Suche die Scanzeiten maßgeblich verlängern kann und eine höhere Auslastung auf den beteiligten Systemen erzeugt wird.

3. Software- und Dateisuche durchführen

Damit die Software- und Dateisuche im Zuge der Inventarisierung durchgeführt werden kann, müssen Sie diese in den Optionen aktivieren.

Öffnen Sie hierfür die **Optionen** (Titelleiste - Zahnrad) - **Inventarisierung**:

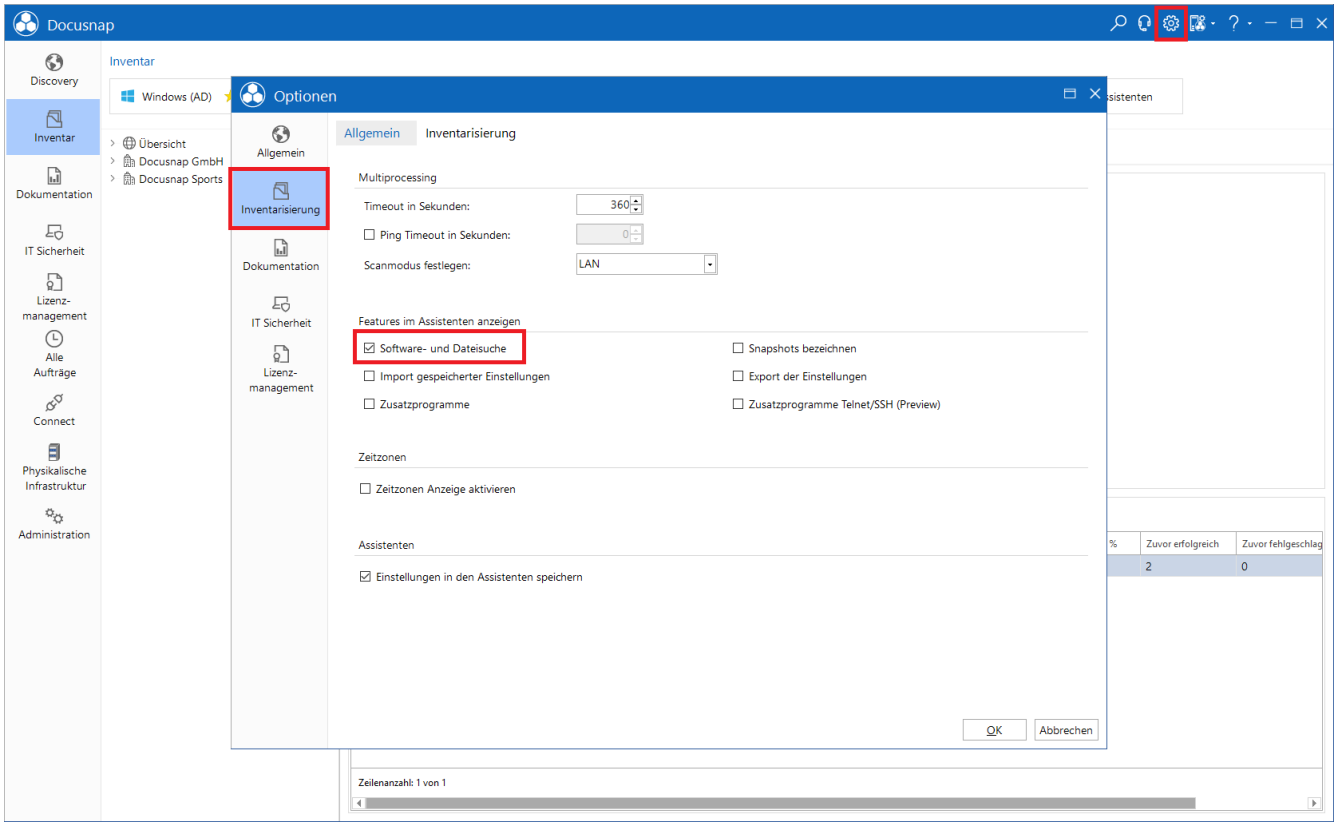

Abbildung 3 - Software- und Dateisuche aktivieren

Im Anschluss können Sie in den entsprechenden Assistenten (Linux, Mac, Windows (AD) und Windows (IP)) die zu suchende Software bzw. Dateien auswählen:

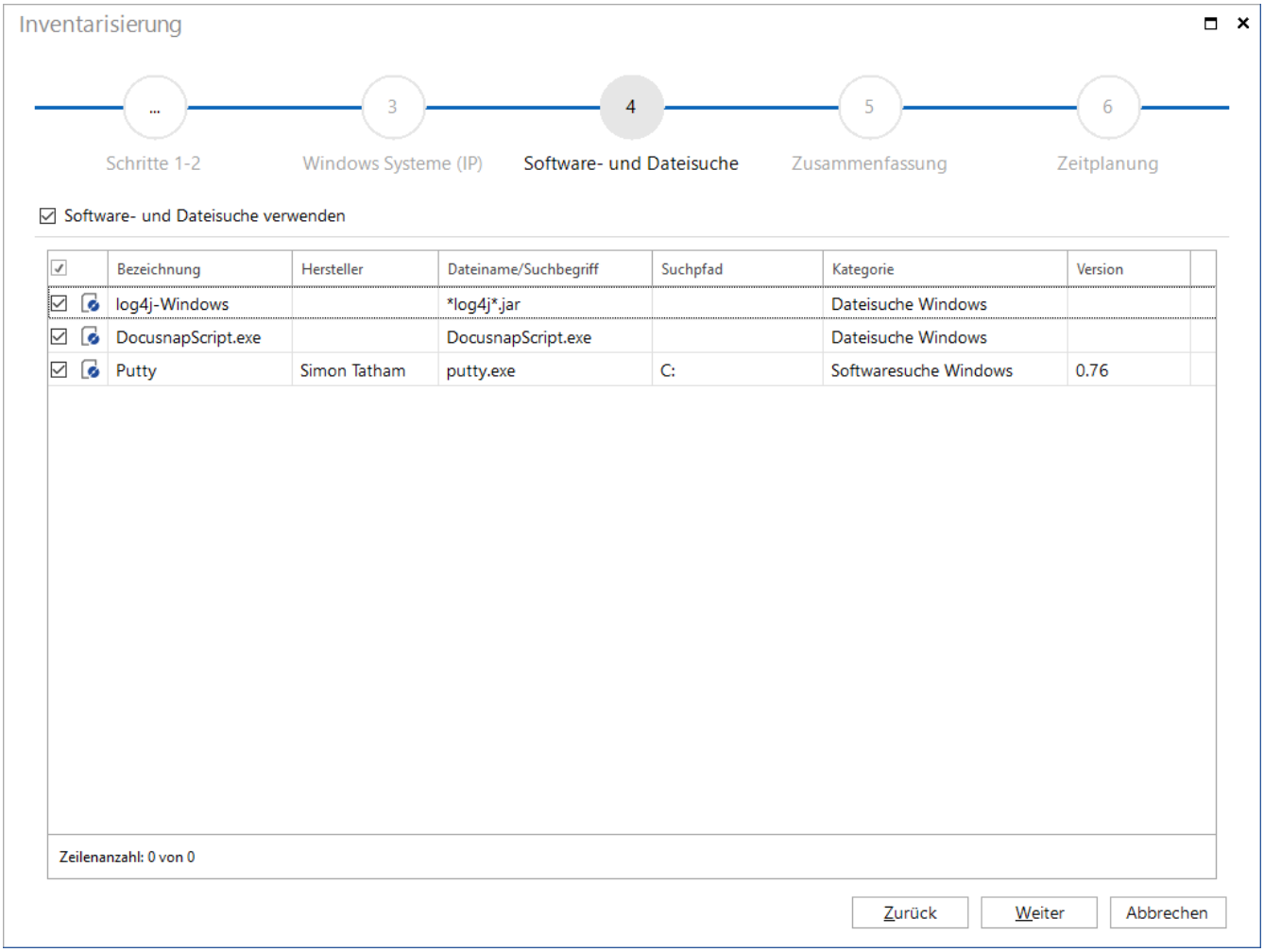

Abbildung 4 - Software- und Dateisuche in der Inventarisierung verwenden (Windows IP)

4. Analyse

4.1 Softwaresuche

Werden die definierten Dateien im Zuge der Softwaresuche gefunden, werden für diese entsprechende Einträge in der Softwareliste des Systems erzeugt. Somit wird diese Software auch in allen übrigen Auswertungen installierter Softwareprodukte aufgelistet. Dies bedeutet Beispielsweise:

- Direkt unterhalb des Systems in der Liste installierter Software
- Zusammenfassung – Software (Firma – Infrastruktur – Domäne - Zusammenfassung)
- Software-Berichte (Firma – Infrastruktur – Domäne – Berichte – Infrastruktur SW)

4.2 Dateisuche

Auch bei der Dateisuche liegt die erste Analysemöglichkeit direkt unterhalb des Systems. Im Knoten **Dateien** werden Ihnen die gefundenen Dateien aufgelistet. Neben dem Dateinamen wird Ihnen auch der Dateipfad, Version, Dateigröße, Änderungsdatum sowie das Suchkriterium angezeigt.

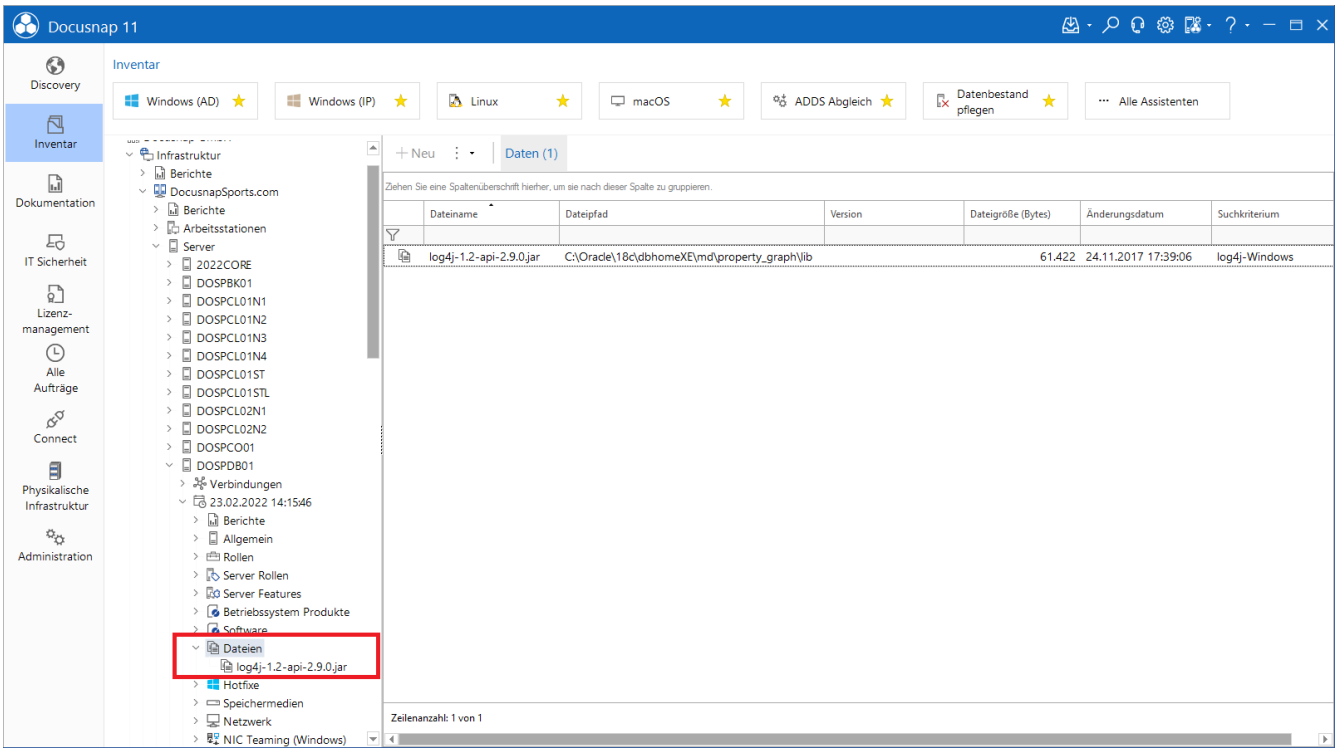

Abbildung 5 - Dateisuche - Gefundene Datei

Die nächste Möglichkeit für die Analyse der Dateisuche finden Sie im Bereich Zusammenfassung: Firma – Infrastruktur – Domäne – Zusammenfassung – Dateien.

Hier werden zunächst die in der Administration angelegten Suchbegriffe, für die Treffer vorhanden sind, angezeigt. In der nächsten Ebene werden die Systeme aufgelistet, auf den die Dateien gefunden wurden. Daraufhin können Sie sich die Detailinformationen der gesuchten Datei(en) auf dem System anzeigen lassen.

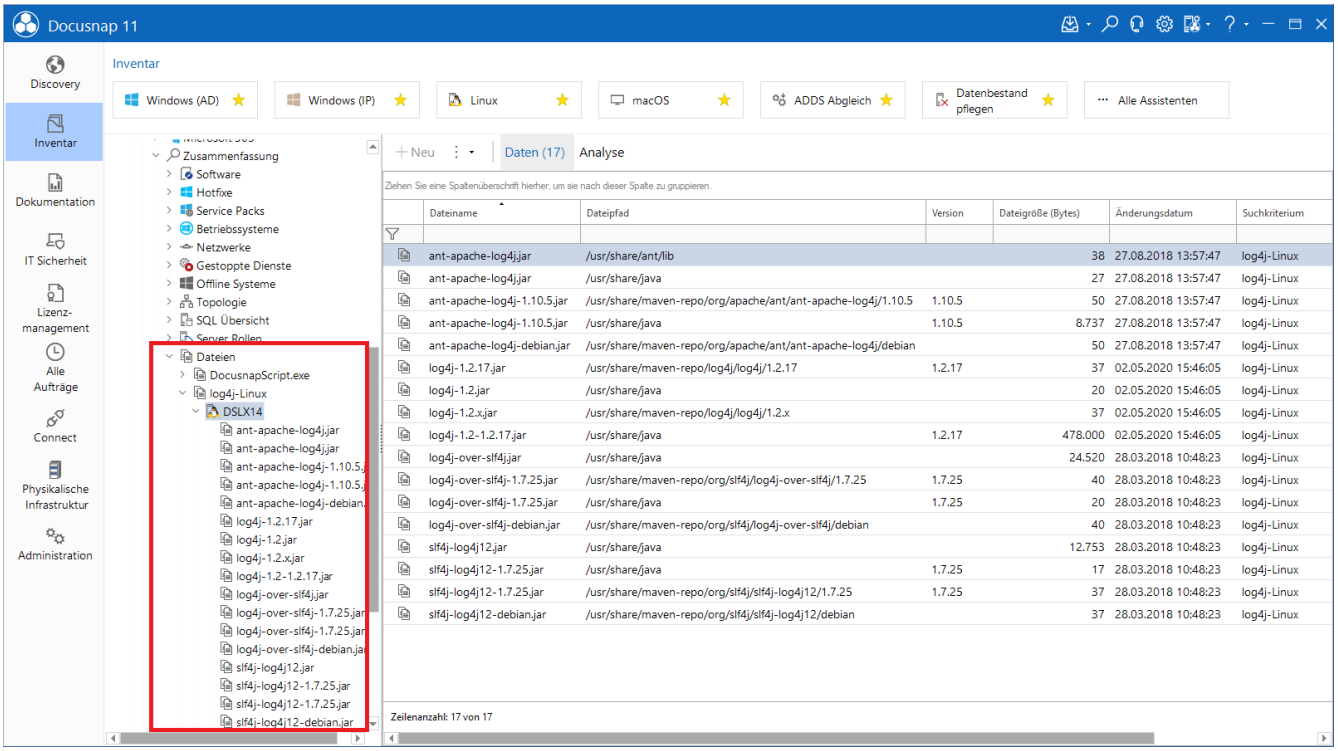

Abbildung 6 - Dateisuche in der Zusammenfassung

Für die Dateisuche ist zusätzlich ein vordefiniertes Docusnap Connect Paket verfügbar. In diesem Connect Paket können die Treffer der Dateisuche auch domänenübergreifend ausgewertet werden.

Innerhalb des Connect Paktes werden die Treffer aller eingerichteten Dateisuchen aufgelistet. Beachten Sie die Gruppierungs- (Rechtsklick – Gruppierung aktivieren – Feld, nach dem gruppiert werden soll, auswählen) und Filtermöglichkeiten.

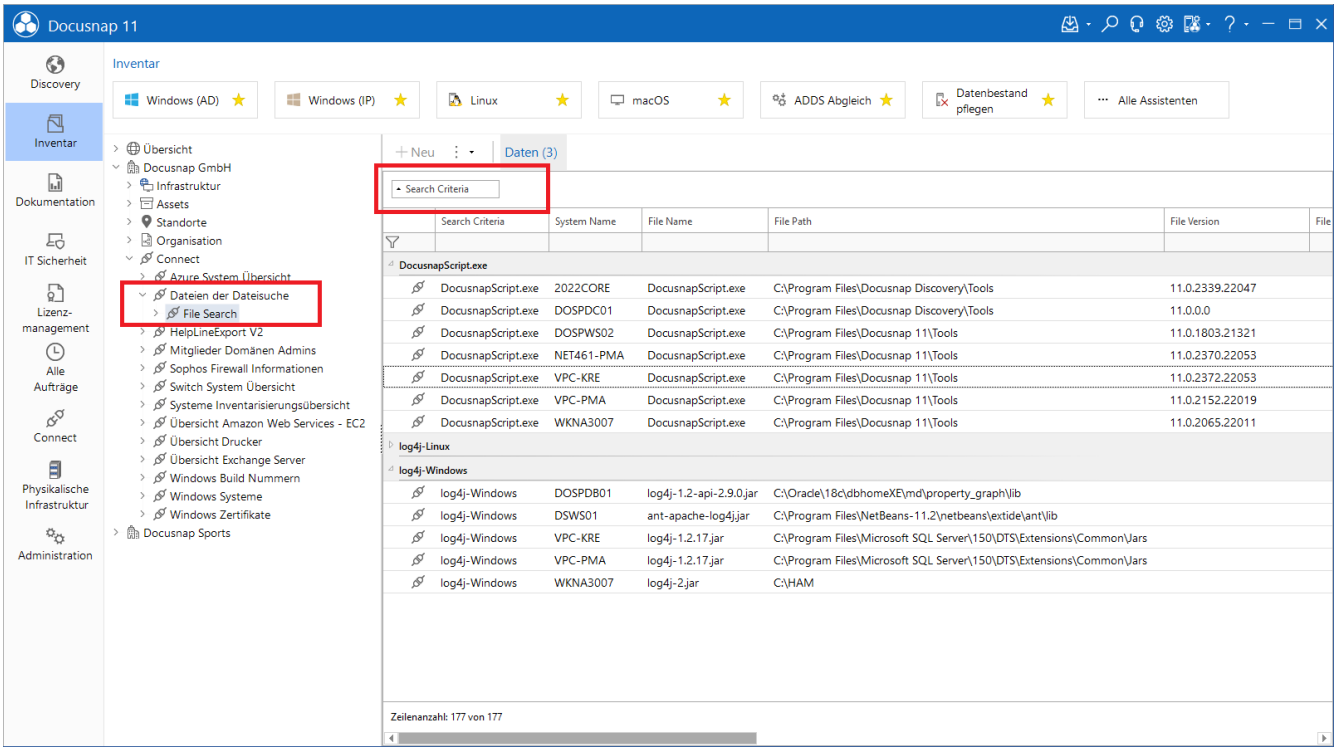

Abbildung 7 - Dateisuche - Docusnap Connect Paket

ABBILDUNGSVERZEICHNIS

VERSIONSHISTORIE

Datum	Beschreibung
24.02.2022	Erstellung des HowTos
27.09.2022	Screenshots angepasst

Docusnap