



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

Die Weitergabe, sowie Vervielfältigung dieser Unterlage, auch von Teilen, Verwertung und Mitteilung ihres Inhaltes ist nicht gestattet, soweit nicht ausdrücklich durch die Docusnap 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 Docusnap GmbH. All rights reserved.

INHALTSVERZEICHNIS

1. Einleitung	4
2. Software- und Dateisuche einrichten	5
2.1 Softwaresuche Windows	6
2.2 Dateisuche	6
3. Software- und Dateisuche durchführen	8
4. Analyse	10
4.1 Softwaresuche	10
4.2 Dateisuche	10

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, beispielsweise 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:

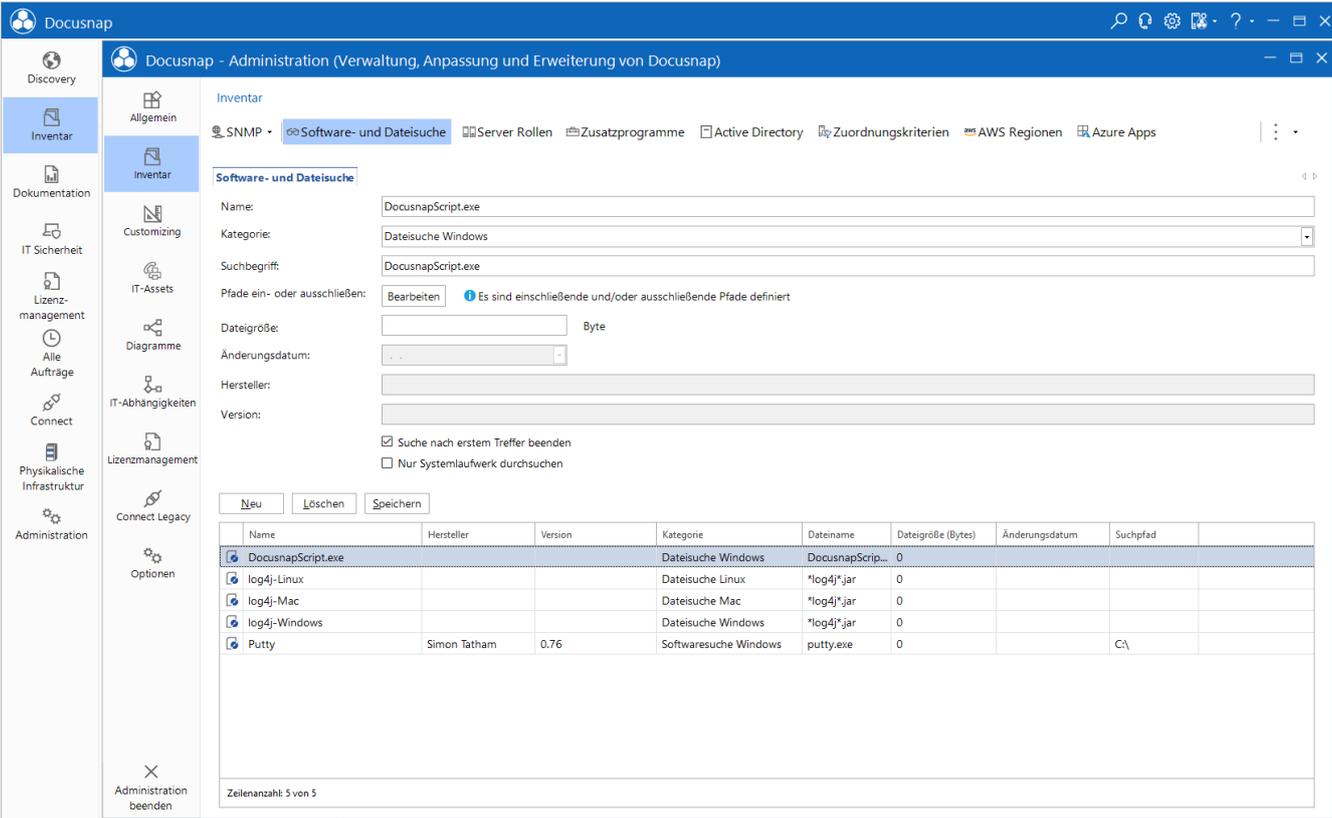
- Dateisuche Linux
- Dateisuche Mac
- Dateisuche Windows
- Softwaresuche Windows

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.



The screenshot shows the 'Software- und Dateisuche' configuration page in the Docusnap Administration interface. The configuration fields are as follows:

- Name: DocusnapScript.exe
- Kategorie: Dateisuche Windows
- Suchbegriff: DocusnapScript.exe
- Pfade ein- oder ausschließen: Bearbeiten (Es sind einschließende und/oder ausschließende Pfade definiert)
- Dateigröße: (empty) Byte
- Änderungsdatum: (empty)
- Hersteller: (empty)
- Version: (empty)
- Suche nach erstem Treffer beenden:
- Nur Systemlaufwerk durchsuchen:

Below the configuration fields is a table with the following data:

Name	Hersteller	Version	Kategorie	Dateiname	Dateigröße (Bytes)	Änderungsdatum	Suchpfad
<input checked="" type="checkbox"/> DocusnapScript.exe			Dateisuche Windows	DocusnapScript...	0		
<input checked="" type="checkbox"/> log4j-Linux			Dateisuche Linux	*log4j*.jar	0		
<input checked="" type="checkbox"/> log4j-Mac			Dateisuche Mac	*log4j*.jar	0		
<input checked="" type="checkbox"/> log4j-Windows			Dateisuche Windows	*log4j*.jar	0		
<input checked="" type="checkbox"/> Putty	Simon Tatham	0.76	Softwaresuche Windows	putty.exe	0		C:\

At the bottom of the table, it says 'Zeilenanzahl: 5 von 5'.

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.

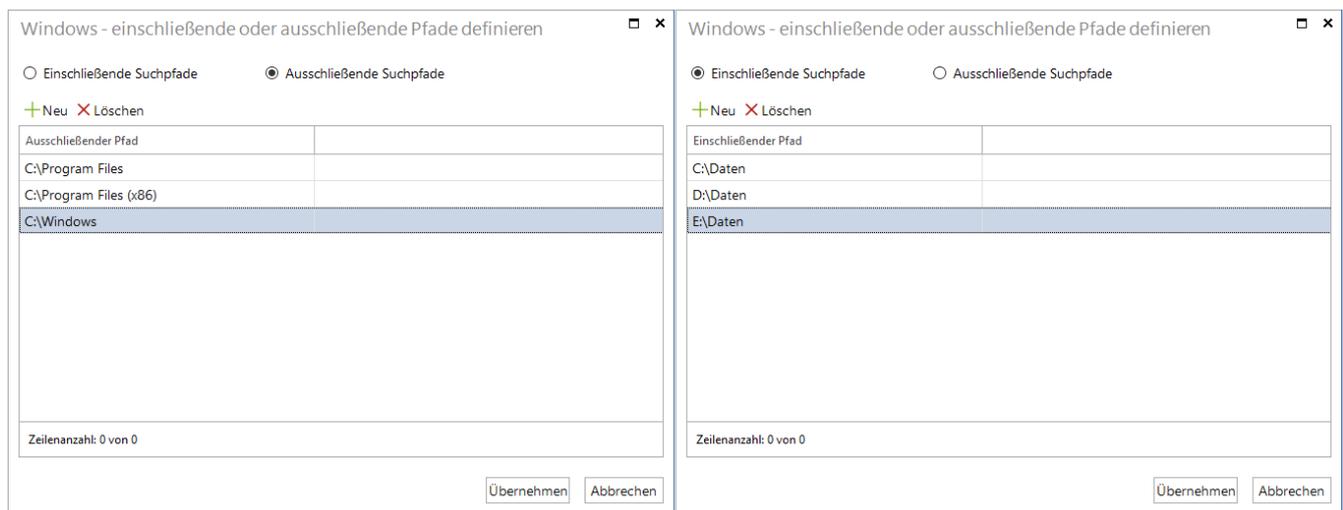


Abbildung 2 - Ein- und Ausschließende Suchpfade definieren

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:

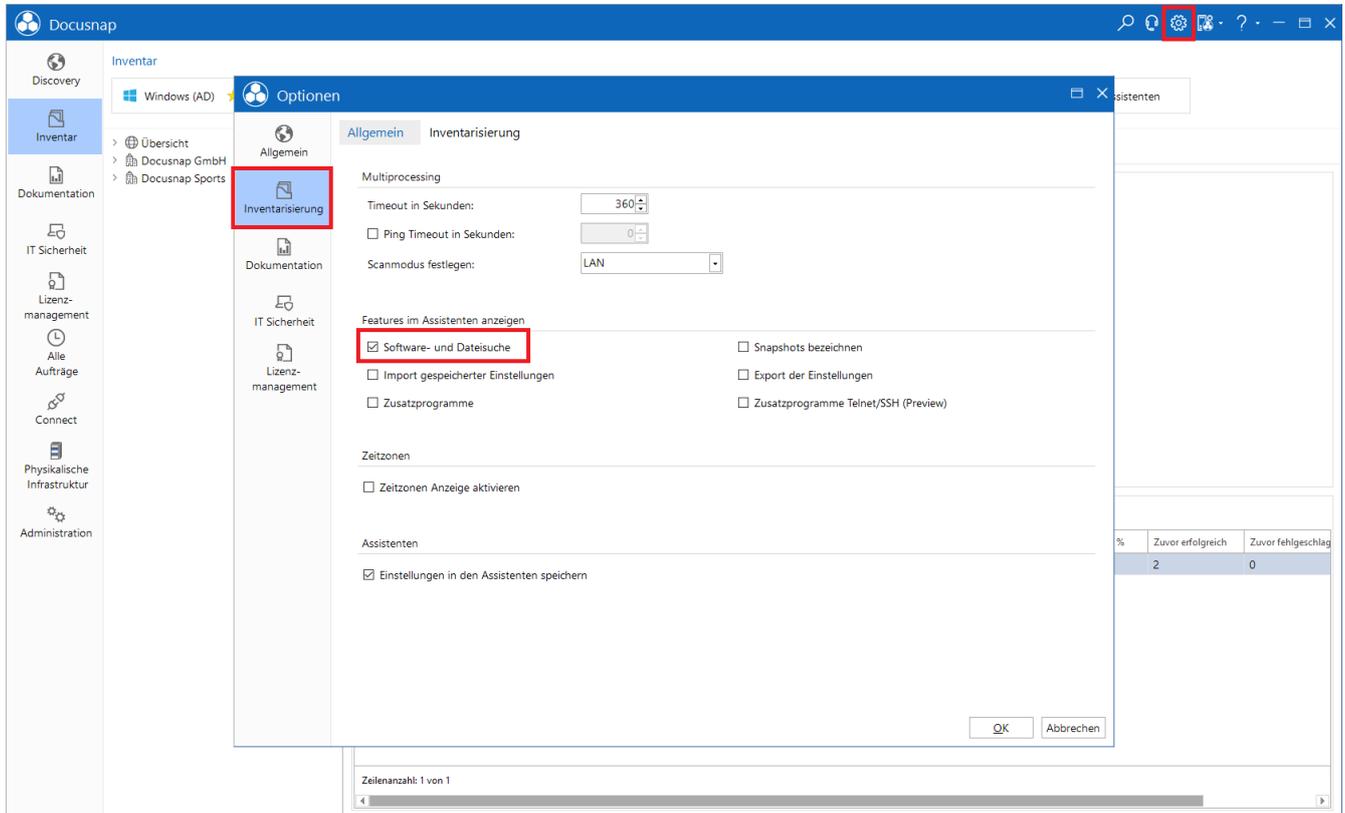


Abbildung 3 - Software- und Dateisuche aktivieren

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

Inventarisierung

Progression: ... (1-2) | 3 (Windows Systeme (IP)) | **4 (Software- und Dateisuche)** | 5 (Zusammenfassung) | 6 (Zeitplanung)

Software- und Dateisuche verwenden

<input type="checkbox"/>	Bezeichnung	Hersteller	Dateiname/Suchbegriff	Suchpfad	Kategorie	Version
<input checked="" type="checkbox"/>	 log4j-Windows		*log4j*.jar		Dateisuche Windows	
<input checked="" type="checkbox"/>	 DocusnapScript.exe		DocusnapScript.exe		Dateisuche Windows	
<input checked="" type="checkbox"/>	 Putty	Simon Tatham	putty.exe	C:	Softwaresuche Windows	0.76

Zeilenanzahl: 0 von 0

Zurück Weiter Abbrechen

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

4. Analyse

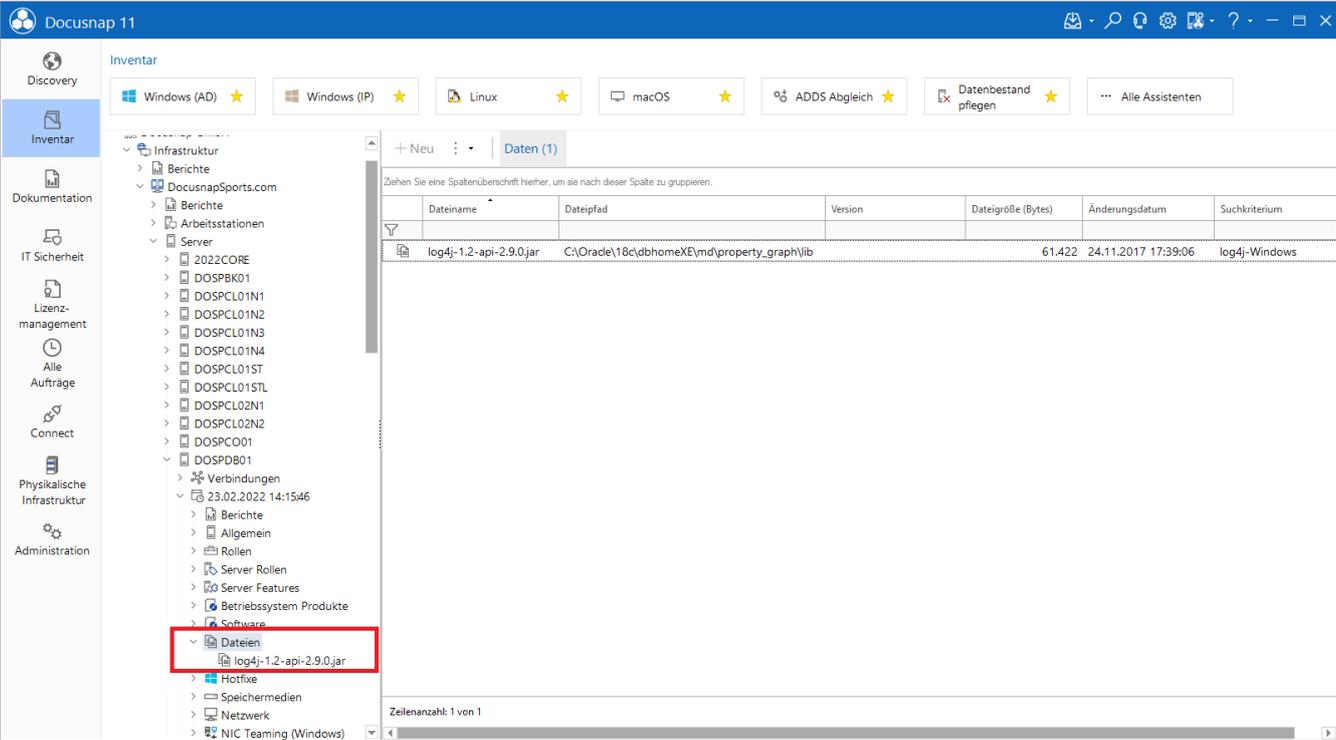
4.1 Softwaresuche

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.



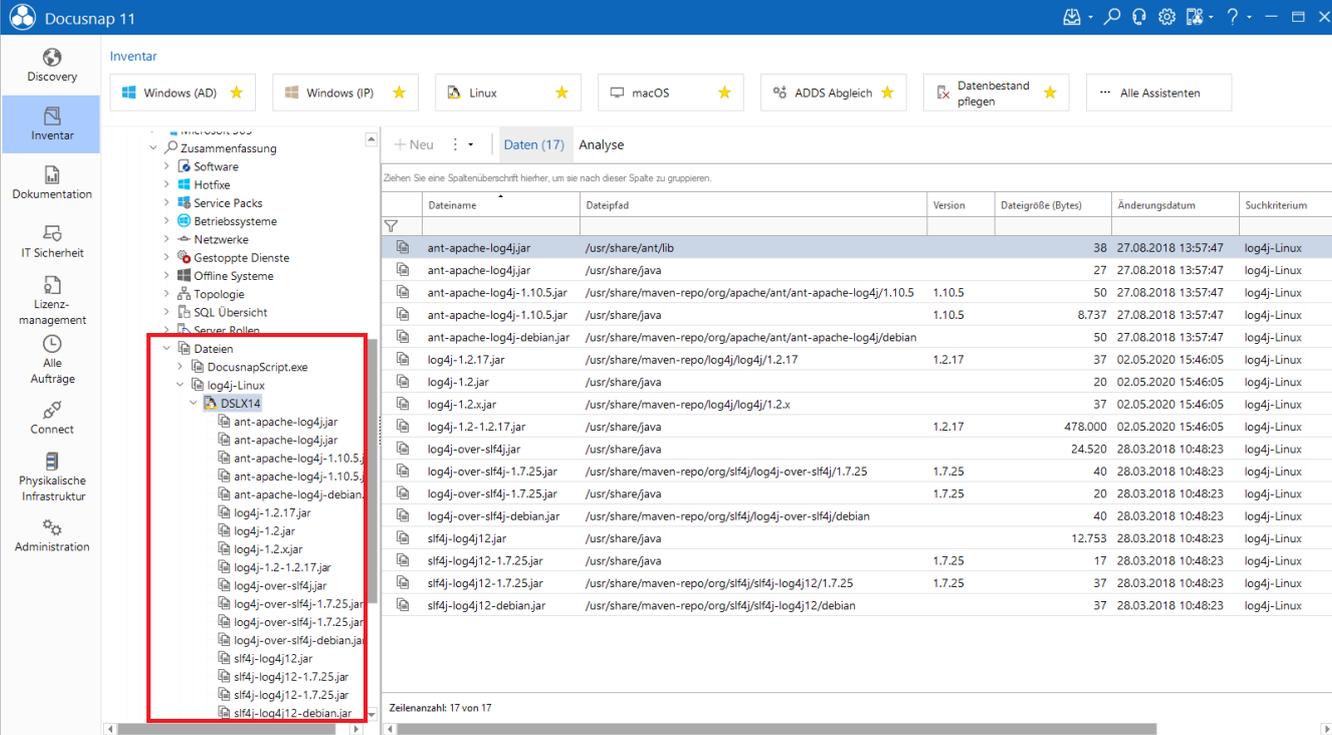
The screenshot shows the Docusnap 11 interface. The left sidebar contains navigation options like 'Discovery', 'Inventar', 'Dokumentation', etc. The main area displays a tree view of the inventory structure. Under the 'Dateien' (Files) node, a file named 'log4j-1.2-api-2.9.0.jar' is highlighted with a red box. The main pane shows a table with the following data:

Dateiname	Dateipfad	Version	Dateigröße (Bytes)	Änderungsdatum	Suchkriterium
log4j-1.2-api-2.9.0.jar	C:\Oracle\18c\ldhomeXE\md\property_graph\lib		61.422	24.11.2017 17:39:06	log4j-Windows

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.



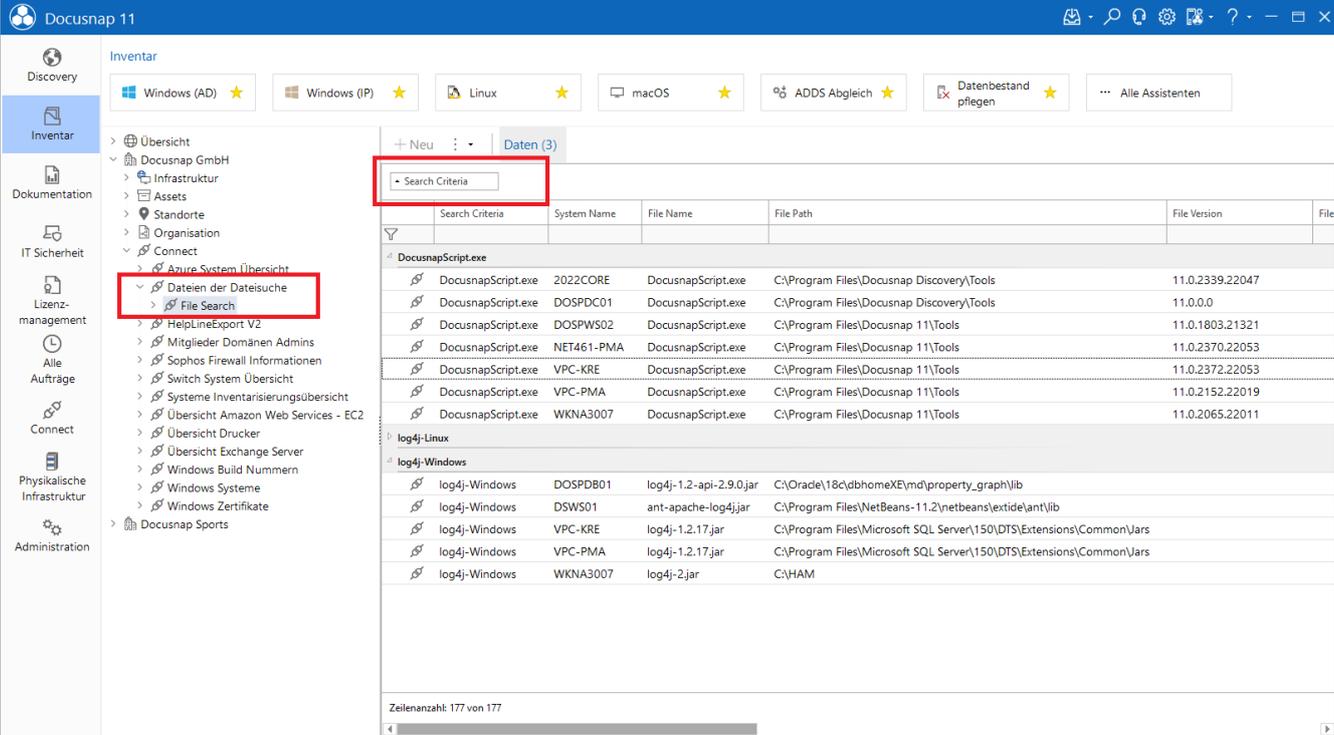
The screenshot shows the Docusnap 11 interface. The left sidebar contains a navigation menu with categories like Discovery, Inventar, Dokumentation, IT Sicherheit, Lizenzmanagement, and Administration. The main area displays a search results table for files. The table has columns for Dateiname, Dateipfad, Version, Dateigröße (Bytes), Änderungsdatum, and Suchkriterium. The search results are filtered to show 17 items. The file 'ant-apache-log4j.jar' is highlighted in the first row. The left sidebar shows a tree view with 'Dateien' selected and expanded, showing a list of files including 'ant-apache-log4j.jar', 'log4j-Linux', and 'DSLX14'.

Dateiname	Dateipfad	Version	Dateigröße (Bytes)	Änderungsdatum	Suchkriterium
ant-apache-log4j.jar	/usr/share/ant/lib		38	27.08.2018 13:57:47	log4j-Linux
ant-apache-log4j.jar	/usr/share/java		27	27.08.2018 13:57:47	log4j-Linux
ant-apache-log4j-1.10.5.jar	/usr/share/maven-repo/org/apache/ant/ant-apache-log4j/1.10.5	1.10.5	50	27.08.2018 13:57:47	log4j-Linux
ant-apache-log4j-1.10.5.jar	/usr/share/java		8.737	27.08.2018 13:57:47	log4j-Linux
ant-apache-log4j-debian.jar	/usr/share/maven-repo/org/apache/ant/ant-apache-log4j/debian		50	27.08.2018 13:57:47	log4j-Linux
log4j-1.2.17.jar	/usr/share/maven-repo/log4j/log4j/1.2.17	1.2.17	37	02.05.2020 15:46:05	log4j-Linux
log4j-1.2.jar	/usr/share/java		20	02.05.2020 15:46:05	log4j-Linux
log4j-1.2.x.jar	/usr/share/maven-repo/log4j/log4j/1.2.x		37	02.05.2020 15:46:05	log4j-Linux
log4j-1.2-1.2.17.jar	/usr/share/java	1.2.17	478.000	02.05.2020 15:46:05	log4j-Linux
log4j-over-slf4j.jar	/usr/share/java		24.520	28.03.2018 10:48:23	log4j-Linux
log4j-over-slf4j-1.7.25.jar	/usr/share/maven-repo/org/slf4j/log4j-over-slf4j/1.7.25	1.7.25	40	28.03.2018 10:48:23	log4j-Linux
log4j-over-slf4j-1.7.25.jar	/usr/share/java	1.7.25	20	28.03.2018 10:48:23	log4j-Linux
log4j-over-slf4j-debian.jar	/usr/share/maven-repo/org/slf4j/log4j-over-slf4j/debian		40	28.03.2018 10:48:23	log4j-Linux
slf4j-log4j12.jar	/usr/share/java		12.753	28.03.2018 10:48:23	log4j-Linux
slf4j-log4j12-1.7.25.jar	/usr/share/java	1.7.25	17	28.03.2018 10:48:23	log4j-Linux
slf4j-log4j12-1.7.25.jar	/usr/share/maven-repo/org/slf4j/slf4j-log4j12/1.7.25	1.7.25	37	28.03.2018 10:48:23	log4j-Linux
slf4j-log4j12-debian.jar	/usr/share/maven-repo/org/slf4j/slf4j-log4j12/debian		37	28.03.2018 10:48:23	log4j-Linux

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.



The screenshot shows the Docusnap 11 interface with the 'Inventar' section active. The left sidebar shows a tree view with 'Dateien der Dateisuche' and 'File Search' highlighted. The main area displays a table of search results for 'DocusnapScript.exe' and 'log4j-*.jar' files. The table has columns for Search Criteria, System Name, File Name, File Path, File Version, and File. The results are grouped by file name.

Search Criteria	System Name	File Name	File Path	File Version	File
DocusnapScript.exe					
DocusnapScript.exe	2022CORE	DocusnapScript.exe	C:\Program Files\Docusnap Discovery\Tools	11.0.2339.22047	
DocusnapScript.exe	DOSPD01	DocusnapScript.exe	C:\Program Files\Docusnap Discovery\Tools	11.0.0.0	
DocusnapScript.exe	DOSPW502	DocusnapScript.exe	C:\Program Files\Docusnap 11\Tools	11.0.1803.21321	
DocusnapScript.exe	NET461-PMA	DocusnapScript.exe	C:\Program Files\Docusnap 11\Tools	11.0.2370.22053	
DocusnapScript.exe	VPC-KRE	DocusnapScript.exe	C:\Program Files\Docusnap 11\Tools	11.0.2372.22053	
DocusnapScript.exe	VPC-PMA	DocusnapScript.exe	C:\Program Files\Docusnap 11\Tools	11.0.2152.22019	
DocusnapScript.exe	WKNA3007	DocusnapScript.exe	C:\Program Files\Docusnap 11\Tools	11.0.2065.22011	
log4j-Linux					
log4j-Windows					
log4j-Windows	DOSPD01	log4j-1.2-api-2.9.0.jar	C:\Oracle\18c\dbhomeXE\md\property_graph\lib		
log4j-Windows	DSWS01	ant-apache-log4j.jar	C:\Program Files\NetBeans-11.2\netbeans\extide\ant\lib		
log4j-Windows	VPC-KRE	log4j-1.2.17.jar	C:\Program Files\Microsoft SQL Server\150\DTS\Extensions\Common\Jars		
log4j-Windows	VPC-PMA	log4j-1.2.17.jar	C:\Program Files\Microsoft SQL Server\150\DTS\Extensions\Common\Jars		
log4j-Windows	WKNA3007	log4j-2.jar	C:\HAM		

Zeilenanzahl: 177 von 177

Abbildung 7 - Dateisuche - Docusnap Connect Paket

ABBILDUNGSVERZEICHNIS

ABBILDUNG 1 - SOFTWARE- UND DATEISUCHE VERWALTEN.....	5
ABBILDUNG 2 - EIN- UND AUSSCHLIEßENDE SUCHPFADE DEFINIEREN	6
ABBILDUNG 3 - SOFTWARE- UND DATEISUCHE AKTIVIEREN.....	8
ABBILDUNG 4 - SOFTWARE- UND DATEISUCHE IN DER INVENTARISIERUNG VERWENDEN (WINDOWS IP)	9
ABBILDUNG 5 - DATEISUCHE - GEFUNDENE DATEI.....	10
ABBILDUNG 6 - DATEISUCHE IN DER ZUSAMMENFASSUNG.....	11
ABBILDUNG 7 - DATEISUCHE - DOCUSNAP CONNECT PAKET.....	12

VERSIONSHISTORIE

Datum	Beschreibung
24.02.2022	Erstellung des HowTos
27.09.2022	Screenshots angepasst
