



Find log4j files with DocuSnap 11
Analyze Windows and Linux systems

TITLE	Find log4j files with Docusnap 11
AUTHOR	Docusnap Consulting
DATE	12/22/2021
VERSION	1.2 valid from 12/21/2021

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.

CONTENTS

1.	Introduction	4
2.	Find log4j files with Docusnap	5
2.1	Windows Systems	5
2.2	Linux systems	5
3.	Requirements	6
4.	Log4j search on Windows systems	6
4.1	Enable Software Search	6
4.2	Set up Software Search	7
4.2.1	Suggestion Search Term *log4j*.jar	8
4.2.2	Suggestion search term *log4j*-2*.jar	8
4.3	Execute Software Search	9
4.4	Display search result	10
4.5	Alternative DocusnapScript	11
4.5.1	Extension software search per parameter	11
5.	Log4j search on Linux systems	12

1. Introduction

The German Federal Office for Information Security (BSI) has declared the highest warning level Red (IT threat level 4) for the vulnerability known as "log4shell" or also "log4j" (National Vulnerability Database -NVD- CVE-2021-44228). This means that the IT threat level is classified as extremely critical. As a result, both the failure of many services and regular operations are not possible.

The Java log4j libraries from version 2.0.1 to 2.14.x are affected. Version 2.15.0 is already fixed but contains further security vulnerabilities. For this reason, an update to version 2.16.0 is urgently recommended at the current time, December 2021. In general, however, the recommendation always applies to install the latest update as soon as possible.

Older versions $\leq 1.x$ are not affected by the log4shell vulnerability. However, since these versions have long since reached end-of-life status, an update to the latest version is also strongly recommended here wherever possible.

The vulnerability allows attackers to execute their own program code on the target system and thus compromise the server. In addition, it can also be used to disclose sensitive data, such as API keys.

Below you will learn how Docusnap can help you find log4j files on Windows and Linux systems.

Docusnap itself is not affected by this vulnerability. This technology is not used for the product.

2. Find log4j files with Docusnap

Docusnap can search the file system of Windows and Linux systems for log4j files.

[The December 2021 Docusnap patch \(11.0.1928.21348\)](#) is limited to required Linux inventory enhancements. No update to Docusnap 11 is required for the Windows software search suggested below.

2.1 Windows Systems

Software search allows to search the file system from all Windows systems in an organization for files with a specific naming.

Checking the file system extends the scan times and may cause additional load on the involved systems during execution. The CPU of the Docusnap server is heavily utilized when the software search is executed with more than one search term. With the first hit, Docusnap ends the search and adds a corresponding entry in the system's software list. Thus, a first statement is available on which systems versions of this framework are available.

We therefore recommend performing the Windows inventory with software search using the DocusnapScript method described in this [HowTo](#) as far as possible.

Depending on the selected search criterion, all systems with log4j or a subset (e.g. only files with a version 2.x in the name) are then listed.

2.2 Linux systems

The Linux scan has been extended to help with this problem. The complete file system is scanned and all hits are documented with version and directory path.

An increased scan time and additional load on the target systems must also be calculated here.

3. Requirements

The scan must be performed with the required rights to the file system. The scan user must have at least read access to the file system.

4. Log4j search on Windows systems

4.1 Enable Software Search

In Docusnap Management - Options - Inventory, check the box for the Software Search. Now this is enabled for both the Windows IP scan and the Windows AD scan and can be found in the respective inventory wizards.

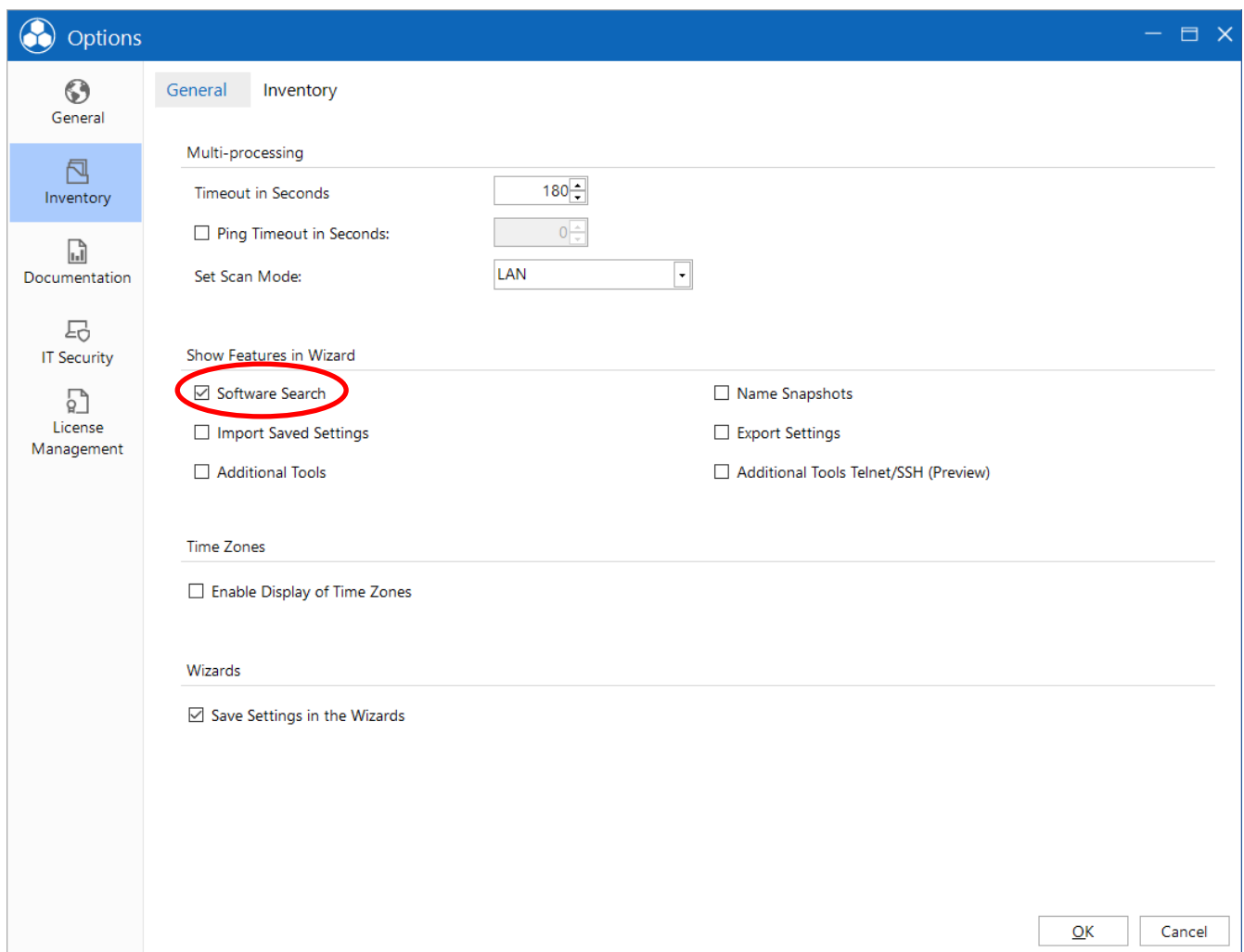


Figure 1 - Enable Software Search

4.2 Set up Software Search

Then switch to the Inventory section in the Management and there to the Software Search tab to create a new Software Search. For detailed information on the Software Search function, please refer to the [Docusnap 11 manual](#).

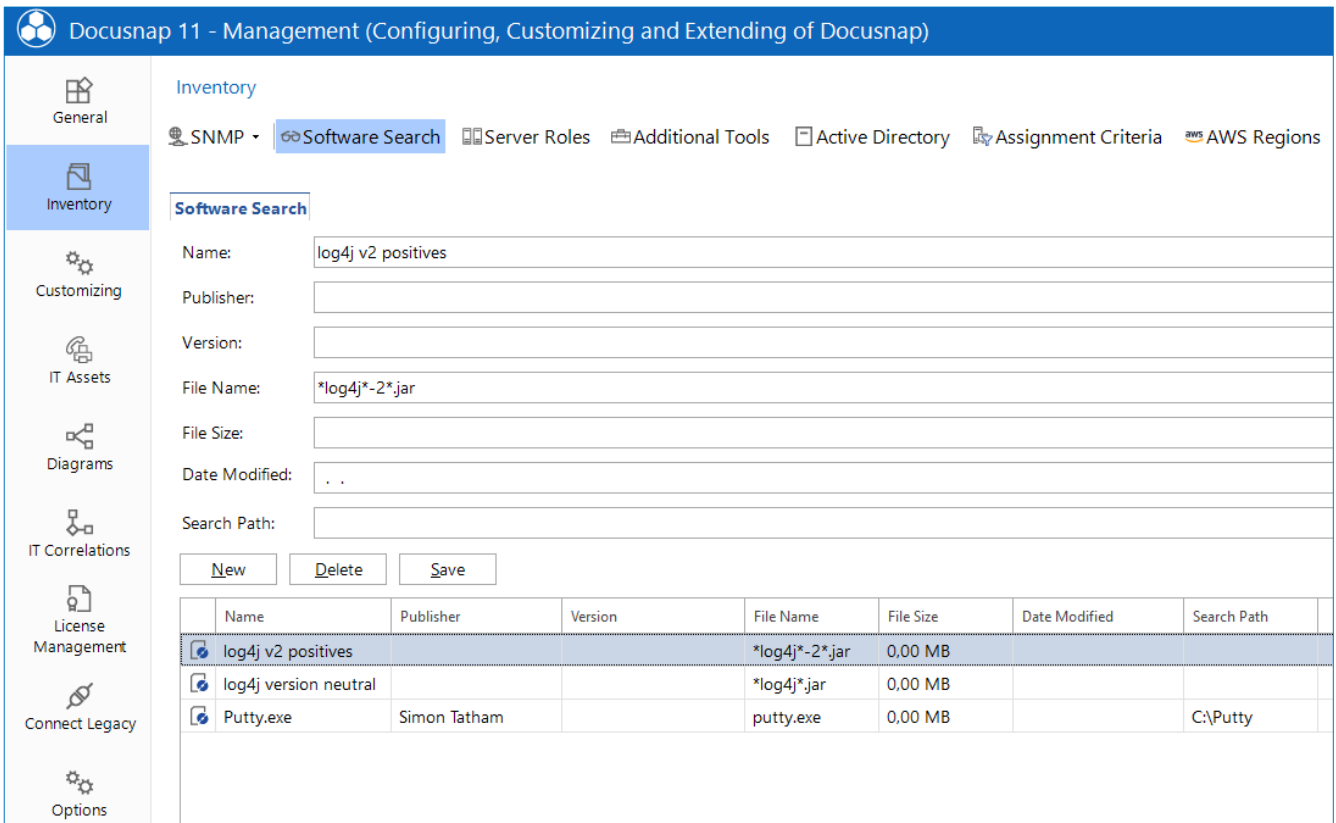
Use the **New** button to set up a new Software Search.

The **Name** will be displayed later in the software list and should therefore be chosen in a meaningful and understandable way.

The search term is entered in the **File Name** field. Wildcards can be set with *****.

The fields **Publisher**, **Version**, **File Size** and **Date Modified** are irrelevant in this case and can be left empty.

The **Search Path** field, on the other hand, **must be empty** so that Docusnap searches the entire file system.



	Name	Publisher	Version	File Name	File Size	Date Modified	Search Path
	log4j v2 positives			*log4j*-2*.jar	0.00 MB		
	log4j version neutral			*log4j*.jar	0.00 MB		
	Putty.exe	Simon Tatham		putty.exe	0.00 MB		C:\Putty

Figure 2 - Set up Software Search

4.2.1 Suggestion Search Term *log4j*.jar

Our recommendation is to use the search term ***log4j*.jar**. With this search term **all systems** are listed on which log4j files are found. This also includes 1.x versions. These are now obsolete and should be updated as far as possible according to the BSI recommendation. This search term provides a complete overview.

However, it is not possible to distinguish between 1.x and 2.x in this way. For this, the file system of the identified systems must still be examined in detail.

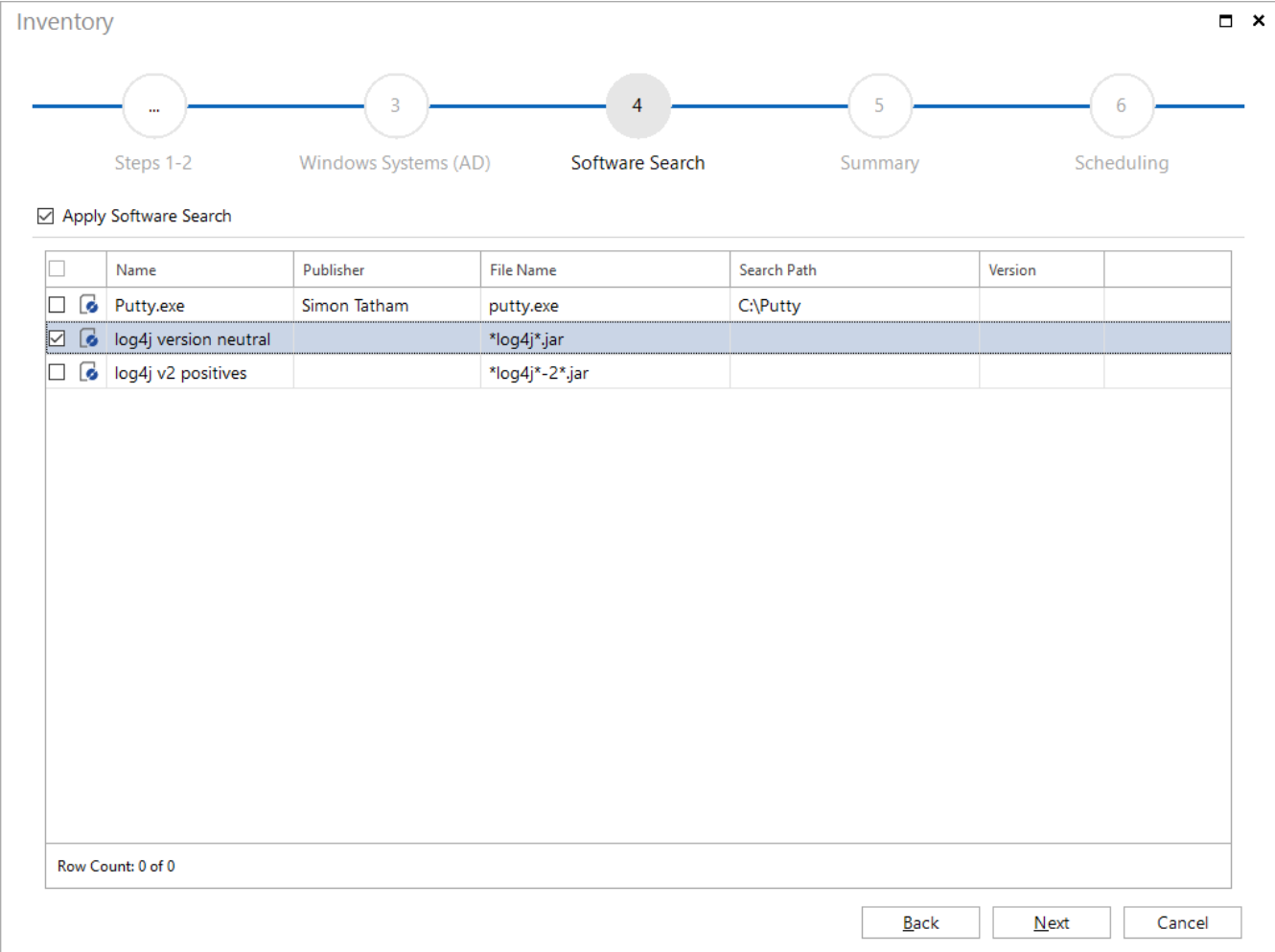
4.2.2 Suggestion search term *log4j*-2*.jar

Alternatively, you can also use the search term ***log4j*-2*.jar**. This will then only find log4j files with **version 2.x**. Not affected 1.x versions will not be displayed.

With the reduction to files with 2.x versions the number of systems to be analyzed is reduced. However, completeness cannot be achieved this way.

4.3 Execute Software Search

If the software search was enabled in the options, it can be found in the Windows IP scan and Windows AD scan inventory wizards. In step 4 of the respective wizard you can select the previously created search.



Inventory

Steps 1-2 Windows Systems (AD) **Software Search** Summary Scheduling

Apply Software Search

<input type="checkbox"/>	Name	Publisher	File Name	Search Path	Version	
<input type="checkbox"/>	Putty.exe	Simon Tatham	putty.exe	C:\Putty		
<input checked="" type="checkbox"/>	log4j version neutral		*log4j*.jar			
<input type="checkbox"/>	log4j v2 positives		*log4j*-2*.jar			

Row Count: 0 of 0

Figure 3 - Execute Software Search

4.4 Display search result

The result of the software search can be found in the Data Explorer in the respective Domain - Infrastructure - Summary - Software. If you filter here according to the Name you assigned to the search, you will see on how many systems the search term was found. By double-clicking, you can display a list of these systems. This list can also be exported, for example in Excel format.

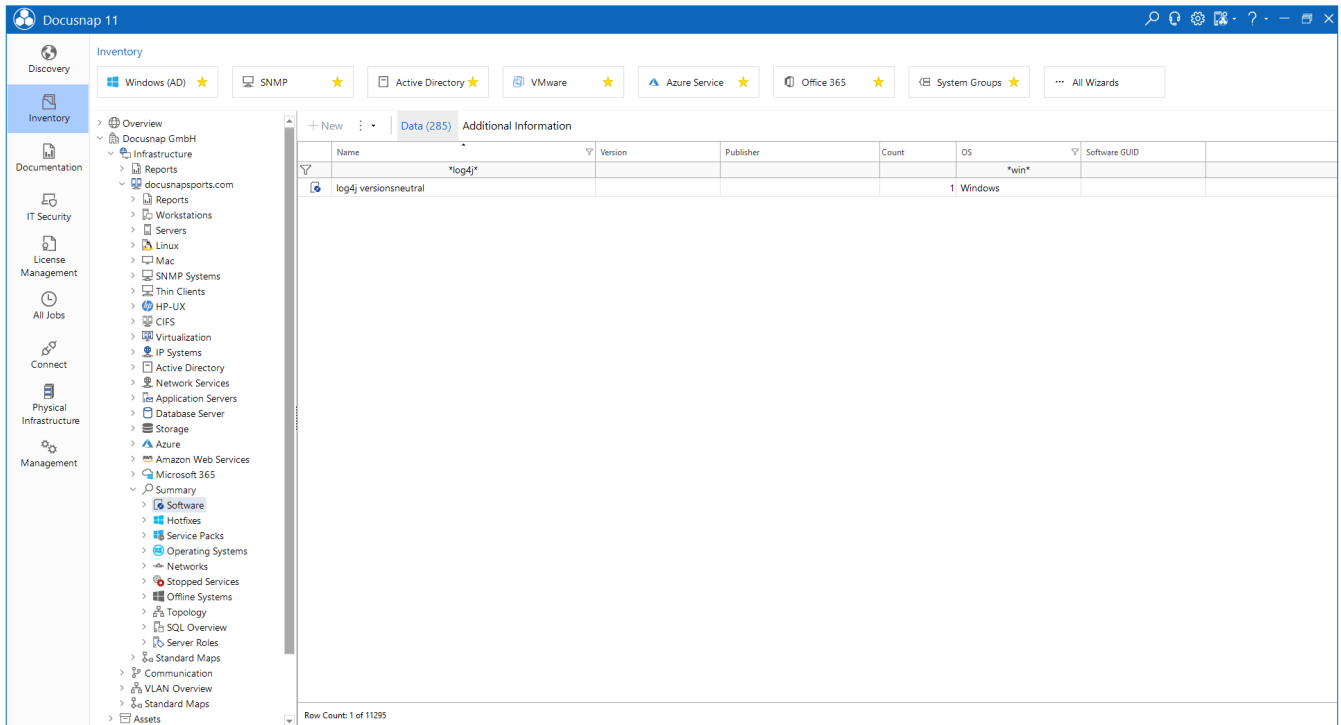


Figure 4 - Search result - number of systems found

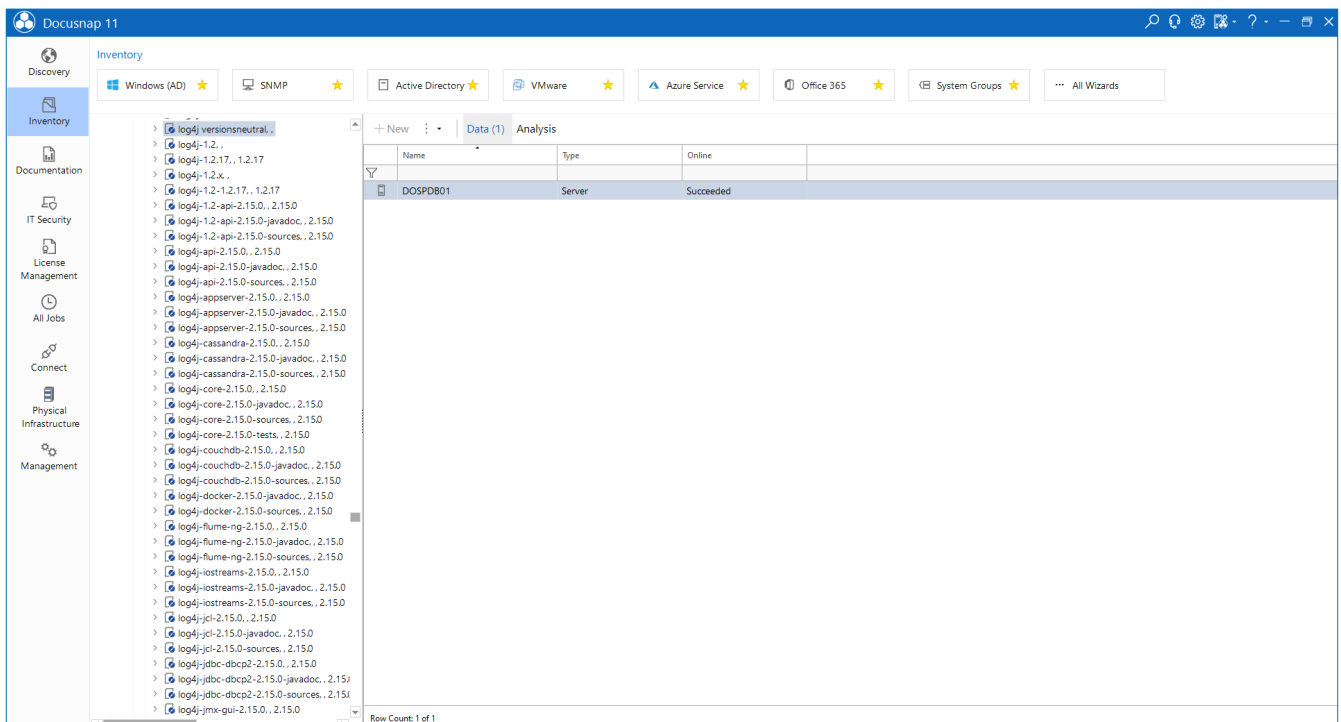


Figure 5 Search result - found systems

4.5 Alternative DocusnapScript

In addition to the Software Search using the Inventory Wizard, this can also be performed using the DocusnapScript. For detailed information about the DocusnapScript, please refer to the [HowTo Docusnap Script for Windows](#).

The software name in the wizard and the software name in the XML search file should not differ. This way, with the same notation, all found systems will be listed together in the software list, regardless of the inventory technology used.

4.5.1 Extension software search per parameter

According to the above search terms `*log4j*.jar` and `*log4j*-2*.jar`, the XML search files would look like the following:

Search term `*log4j*-2*`:

```
<SoftwareItem>
  <SoftwareName>log4j v2 positives</SoftwareName>
  <SoftwarePublisher /> <!-- optional-->
  <SoftwareVersion /> <!-- optional-->
  <FileName>*log4j*-2*.jar</FileName>
  <SearchPath /> <!-- global-->
  <FileSize /> <!-- optional byte-->
  <ModifyDate /> <!-- optional-->
</SoftwareItem>
```

Search term `*log4j*`:

```
<SoftwareItem>
  <SoftwareName>log4j version neutral</SoftwareName>
  <SoftwarePublisher /> <!-- optional-->
  <SoftwareVersion /> <!-- optional-->
  <FileName>*log4j*.jar</FileName>
  <SearchPath /> <!-- global-->
  <FileSize /> <!-- optional byte-->
  <ModifyDate /> <!-- optional-->
</SoftwareItem>
```

DocusnapScript execution - example:

```
DocusnapScript.exe -O C:\Temp -S C:\Temp\DocusnapScript\log4jv2positives.xml
```

Explanation of parameters:

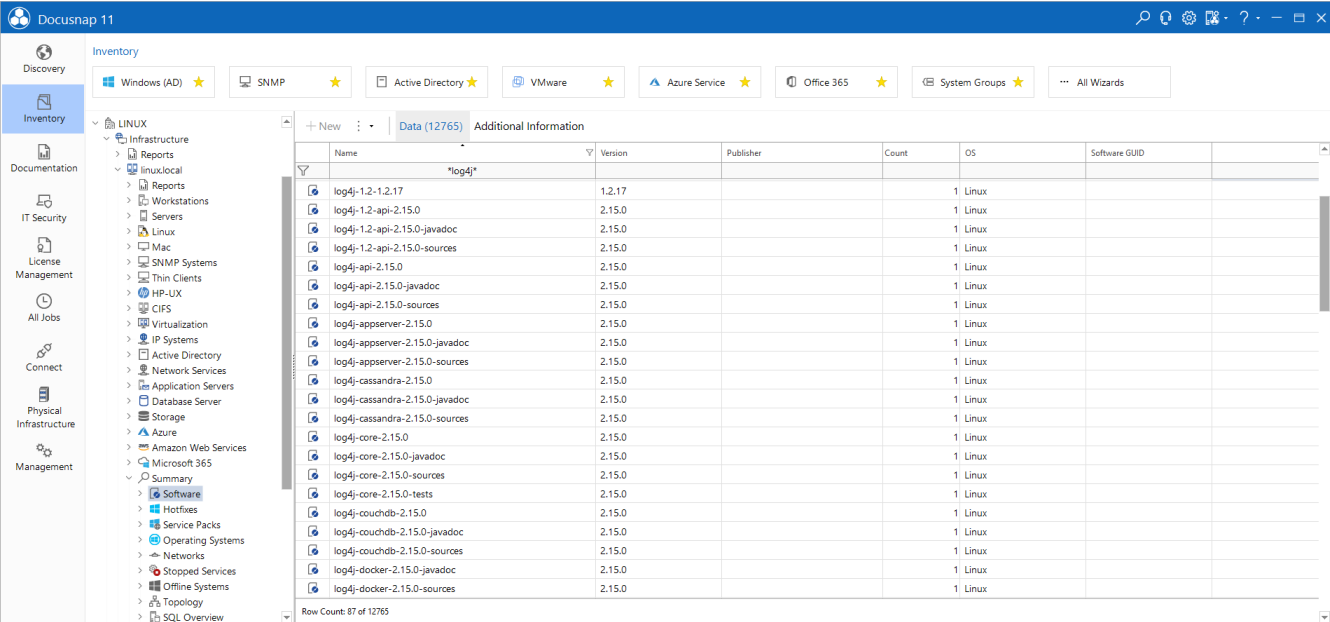
- -O (output path for scan result).
- -S (Path for the XML file with the Software Search definition)
- -H (Call DocusnapScript help function if needed)

5. Log4j search on Linux systems

Software search on Linux systems is not available until the [December 2021 patch of Docusnap 11 \(11.0.1928.21348\)](#). The procedure is identical to that for Windows systems, described in 4. Log4j search on Windows systems.

Please note: DocusnapScript for Linux has not yet been extended and therefore does not currently provide this information.

Unlike the search on Windows systems, you get more information on Linux systems. The search does not stop after the first hit on a system, but displays all files found on a system that contain the search term. In addition, the version is displayed for each file.



Name	Version	Publisher	Count	OS	Software GUID
log4j-1.2-1.2.17	1.2.17		1	Linux	
log4j-1.2-api-2.15.0	2.15.0		1	Linux	
log4j-1.2-api-2.15.0-javadoc	2.15.0		1	Linux	
log4j-1.2-api-2.15.0-sources	2.15.0		1	Linux	
log4j-api-2.15.0	2.15.0		1	Linux	
log4j-api-2.15.0-javadoc	2.15.0		1	Linux	
log4j-api-2.15.0-sources	2.15.0		1	Linux	
log4j-appserver-2.15.0	2.15.0		1	Linux	
log4j-appserver-2.15.0-javadoc	2.15.0		1	Linux	
log4j-appserver-2.15.0-sources	2.15.0		1	Linux	
log4j-cassandra-2.15.0	2.15.0		1	Linux	
log4j-cassandra-2.15.0-javadoc	2.15.0		1	Linux	
log4j-cassandra-2.15.0-sources	2.15.0		1	Linux	
log4j-core-2.15.0	2.15.0		1	Linux	
log4j-core-2.15.0-javadoc	2.15.0		1	Linux	
log4j-core-2.15.0-sources	2.15.0		1	Linux	
log4j-core-2.15.0-tests	2.15.0		1	Linux	
log4j-couchdb-2.15.0	2.15.0		1	Linux	
log4j-couchdb-2.15.0-javadoc	2.15.0		1	Linux	
log4j-couchdb-2.15.0-sources	2.15.0		1	Linux	
log4j-docker-2.15.0-javadoc	2.15.0		1	Linux	
log4j-docker-2.15.0-sources	2.15.0		1	Linux	

Figure 6 - Software Search on Linux systems incl. version number

In addition, when searching on Linux systems, the path of the found files is also output, which significantly simplifies further processing.

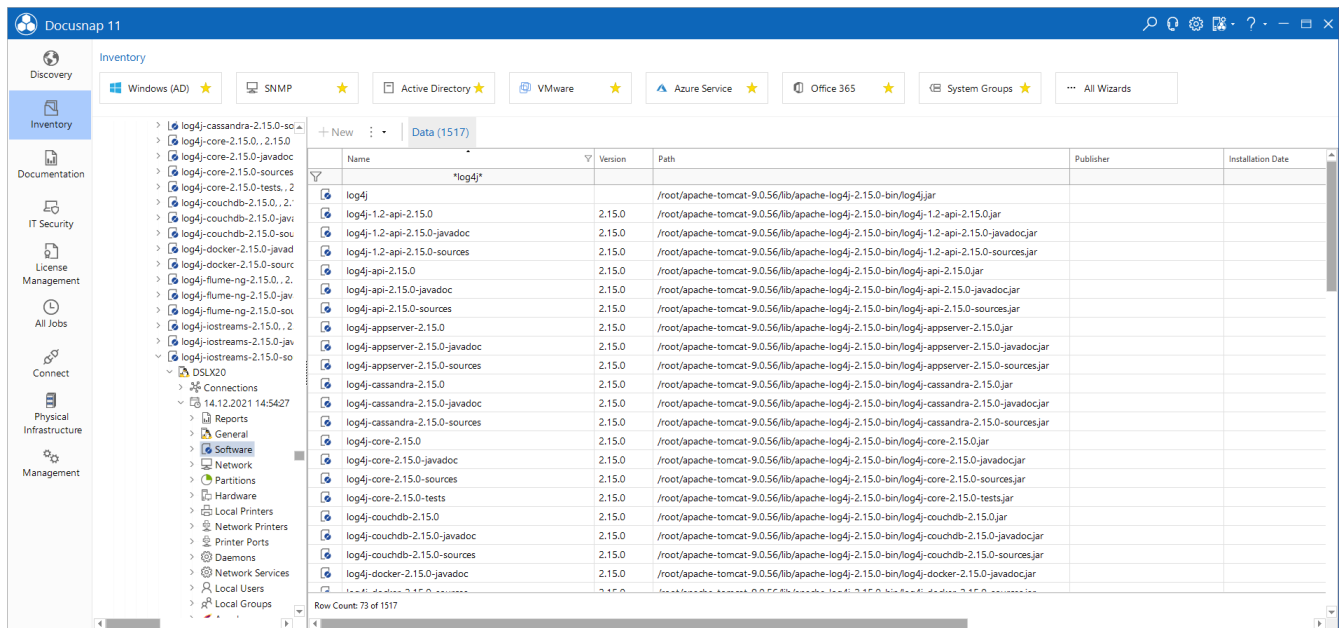


Figure 7 - Software Search on Linux systems incl. file path

For the analysis of the Linux software these new reports were developed. The Excel variant allows easy further processing.

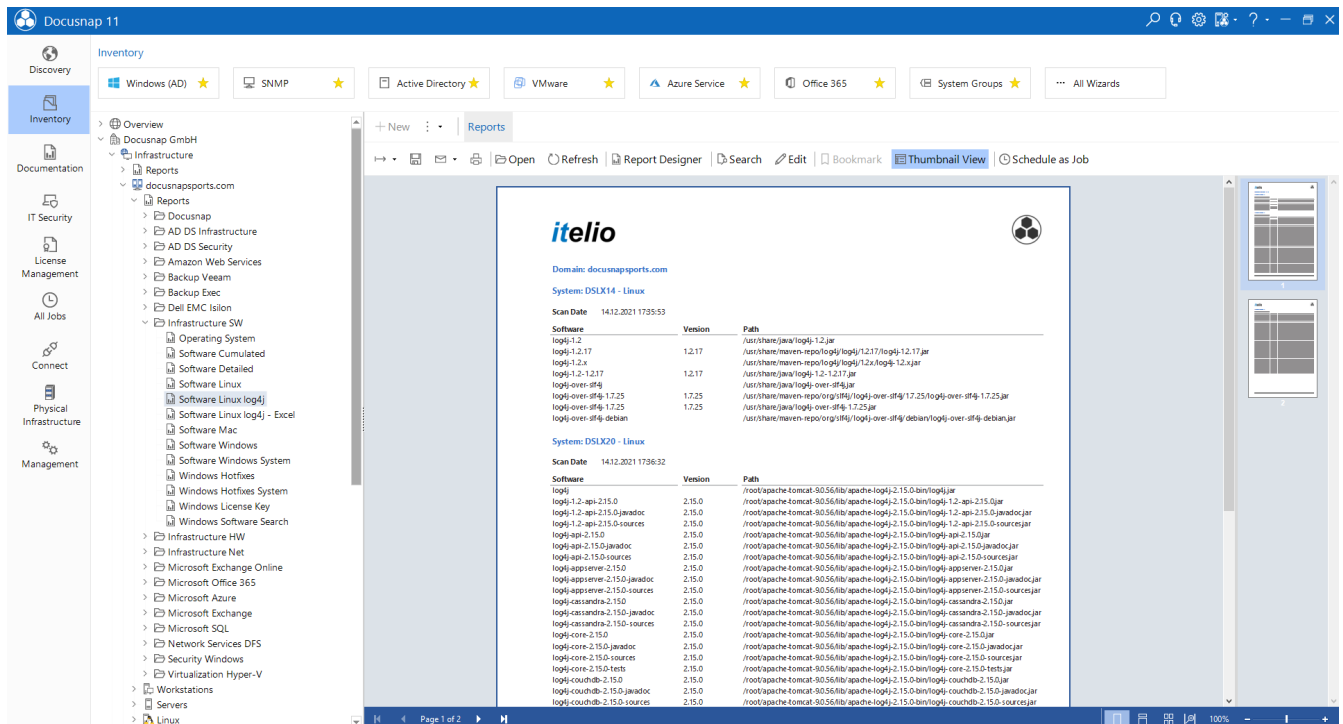


Figure 8 - Report Linux

The screenshot shows the Docusnap 11 interface. The left sidebar contains navigation options like Discovery, Inventory, Documentation, IT Security, License Management, All Jobs, Connect, Physical Infrastructure, and Management. The main window displays a report titled 'Reports' with a table of software inventory data.

Domain	System Name	Scan Date	Software	Version	Path
docusnapports.com	DS1020	1412.2021.1736.32	loggly		/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly.jar
docusnapports.com	DS1014	1412.2021.1735.53	loggly-1.2		/usr/share/java/loggly-1.2.jar
docusnapports.com	DS1014	1412.2021.1735.53	loggly-1.2.17	1.2.17	/usr/share/maven-repo/loggly/loggly-1.2.17.jar
docusnapports.com	DS1014	1412.2021.1735.53	loggly-1.2.x		/usr/share/maven-repo/loggly/loggly-1.2.x.jar
docusnapports.com	DS1014	1412.2021.1735.53	loggly-1.2-1.2.17	1.2.17	/usr/share/java/loggly-1.2-1.2.17.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-1.2-apti-2.15.0-javadoc	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-1.2-apti-2.15.0-javadoc.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-1.2-apti-2.15.0-sources	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-1.2-apti-2.15.0-sources.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-apti-2.15.0	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-apti-2.15.0.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-apti-2.15.0-javadoc	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-apti-2.15.0-javadoc.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-apti-2.15.0-sources	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-apti-2.15.0-sources.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-appriever-2.15.0	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-appriever-2.15.0.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-appriever-2.15.0-javadoc	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-appriever-2.15.0-javadoc.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-appriever-2.15.0-sources	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-appriever-2.15.0-sources.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-cassandra-2.15.0	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-cassandra-2.15.0.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-cassandra-2.15.0-javadoc	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-cassandra-2.15.0-javadoc.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-cassandra-2.15.0-sources	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-cassandra-2.15.0-sources.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-core-2.15.0	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-core-2.15.0.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-core-2.15.0-javadoc	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-core-2.15.0-javadoc.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-core-2.15.0-sources	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-core-2.15.0-sources.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-core-2.15.0-tests	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-core-2.15.0-tests.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-coarchb-2.15.0	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-coarchb-2.15.0.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-coarchb-2.15.0-javadoc	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-coarchb-2.15.0-javadoc.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-coarchb-2.15.0-sources	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-coarchb-2.15.0-sources.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-docker-2.15.0-javadoc	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-docker-2.15.0-javadoc.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-docker-2.15.0-sources	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-docker-2.15.0-sources.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-flume-ng-2.15.0	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-flume-ng-2.15.0.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-flume-ng-2.15.0-javadoc	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-flume-ng-2.15.0-javadoc.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-flume-ng-2.15.0-sources	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-flume-ng-2.15.0-sources.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-iodstreams-2.15.0	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-iodstreams-2.15.0.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-iodstreams-2.15.0-javadoc	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-iodstreams-2.15.0-javadoc.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-iodstreams-2.15.0-sources	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-iodstreams-2.15.0-sources.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-jdt-1.15.0	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-jdt-1.15.0.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-jdt-1.15.0-javadoc	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-jdt-1.15.0-javadoc.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-jdt-1.15.0-sources	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-jdt-1.15.0-sources.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-jdbc-dbpq-2.15.0	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-jdbc-dbpq-2.15.0.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-jdbc-dbpq-2.15.0-javadoc	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-jdbc-dbpq-2.15.0-javadoc.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-jdbc-dbpq-2.15.0-sources	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-jdbc-dbpq-2.15.0-sources.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-jms-gua-2.15.0	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-jms-gua-2.15.0.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-jms-gua-2.15.0-javadoc	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-jms-gua-2.15.0-javadoc.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-jms-gua-2.15.0-sources	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-jms-gua-2.15.0-sources.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-jpa-2.15.0	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-jpa-2.15.0.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-jpa-2.15.0-javadoc	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-jpa-2.15.0-javadoc.jar
docusnapports.com	DS1020	1412.2021.1736.32	loggly-jpa-2.15.0-sources	2.15.0	/root/apache-tomcat-9.0.56/ibm/apache-loggly-2.15.0/bin/loggly-jpa-2.15.0-sources.jar

Figure 9 - Report Linux Excel

LIST OF FIGURES

FIGURE 1 - ENABLE SOFTWARE SEARCH	6
FIGURE 2 - SET UP SOFTWARE SEARCH	7
FIGURE 3 - EXECUTE SOFTWARE SEARCH	9
FIGURE 4 - SEARCH RESULT - NUMBER OF SYSTEMS FOUND	10
FIGURE 5 SEARCH RESULT - FOUND SYSTEMS	10
FIGURE 6 - SOFTWARE SEARCH ON LINUX SYSTEMS INCL. VERSION NUMBER	12
FIGURE 7 - SOFTWARE SEARCH ON LINUX SYSTEMS INCL. FILE PATH	13
FIGURE 8 - REPORT LINUX	13
FIGURE 9 - REPORT LINUX EXCEL	14

VERSION HISTORY

Date	Description
12/14/2021	Creation of the HowTo
12/16/2021	Update of the recommended log4j version
12/21/2021	Adaptation of search terms, addition of note on CPU utilization
