

Log4j Issue -Jar files

In this post, I am going to download and configure CB (Configuration Baseline) and deploy to All Systems to check and make sure there is no breach with Log4j within the network.

The screenshot shows the Microsoft Configuration Manager console. On the left is the 'Community' hub with a sidebar containing 'Documentation', 'Community hub', 'Assets and Compliance', 'Software Library', 'Monitoring', 'Administration', and 'Community'. The main area displays 'Top Downloads' and 'Latest Updates'. A red arrow points to the 'Log4j - Jar files containing JndiLookup.class' item in the 'Latest Updates' section. The item's description states: 'This CI searches for all jar-files on a system that contains the string JndiLookup.class which contains the potentially vulnerable Log4j vulnerability'.

This screenshot shows the details page for the 'Log4j - Jar files containing JndiLookup.class' item. It includes the source 'Community curated' and the creator 'Matt Benninge'. A red arrow points to the 'Download' button. Below the button, it says 'Share' and 'Download success!'.

This screenshot shows the 'Description' and 'Source' information for the 'Log4j - Jar files containing JndiLookup.class' item. The description states: 'This CI searches for all jar-files on a system that contains the string JndiLookup.class which contains the potentially vulnerable Log4j vulnerability'. The source is 'Community curated' by 'Matt Benninge'. It also includes the 'Created date' (12/16/2021 7:41 AM) and 'Changed date' (12/17/2021 1:16 AM). A disclaimer at the bottom states: 'Disclaimer: Content stored within GitHub and accessed from the Community hub isn't supported by Microsoft. Microsoft doesn't validate content collected from or shared by the general community. GitHub is an external service subject to its own privacy and licensing terms. Your download and use of any files from GitHub here is subject to the license terms of those files provided on GitHub.'

This screenshot shows the 'Download success!' message for the 'Log4j - Jar files containing JndiLookup.class' item. It includes the source 'Community curated' and the creator 'Matt Benninge'. It also includes the 'Created date' (12/16/2021 7:41 AM) and 'Changed date' (12/17/2021 1:16 AM). A disclaimer at the bottom states: 'Disclaimer: Content stored within GitHub and accessed from the Community hub isn't supported by Microsoft. Microsoft doesn't validate content collected from or shared by the general community. GitHub is an external service subject to its own privacy and licensing terms. Your download and use of any files from GitHub here is subject to the license terms of those files provided on GitHub.'

Assets and Compliance > Overview > Compliance Settings > Configuration Items

Configuration Items 23 items

Icon	Name	Type	Device Type	Revision	Child	Relationships	User Setting	Date Modified
	Log4j - Jar files containing JndiLookup.class	Operating System	Windows	1	No	No	No	17-Dec-2021 11:32 AM
	CVE-2021-36934	Operating System	Windows	1	No	Yes	No	22-Jul-2021 12:06 PM
	Microsoft Exchange 2013, 2016, 2019 SSRF vulnerab...	Application	Windows	7	No	Yes	No	22-Mar-2021 1:29 PM
	Microsoft Exchange 2013, 2016, 2019 SSRF vulnerab...	Application	Windows	7	No	Yes	No	22-Mar-2021 12:04 PM
	WVD Windows 10 Multi-Session	Operating System	Windows	1	No	No	No	31-Jan-2021 11:46 AM
	MS Teams Compliance Status	Operating System	Windows	1	No	Yes	No	29-Nov-2020 9:06 AM
	CI - DNS Server Vulnerability (CVE-2020-1350)	Operating System	Windows	1	No	Yes	No	15-Jul-2020 9:22 AM
	CI - ESU - Server 2008 Status	Operating System	Windows	1	No	Yes	No	11-May-2020 11:26 AM
	CI - ESU - Windows 7 status	Operating System	Windows	2	No	Yes	No	11-May-2020 11:24 AM
	Check Client Boundary Groups	Operating System	Windows	1	No	Yes	No	17-Feb-2020 10:36 AM
	CustomerReady_ESU - Windows 7/Windows Server...	Operating System	Windows	7	No	Yes	No	04-Feb-2020 4:04 PM
	ESU - WinServer 2008 SP2 - KB check - KB4493730 (...)	Operating System	Windows	4	No	Yes	No	04-Feb-2020 3:36 PM
	ESU - WinServer 2008 R2 SP1 - KB check - Multiple...	Operating System	Windows	7	No	Yes	No	04-Feb-2020 3:36 PM
	ESU - Win7 - KB check - Multiple Servicing Stack Up...	Operating System	Windows	8	No	Yes	No	04-Feb-2020 3:36 PM
	ESU - Win7 - KB check - Multiple Cumulative Updates	Operating System	Windows	4	No	Yes	No	04-Feb-2020 3:36 PM
	ESU - Win7 - KB check - KB4490628 (SSU-SHA2)	Operating System	Windows	5	No	Yes	No	04-Feb-2020 3:36 PM
	ESU - Win7 - KB check - KB4474419 (SHA-2)	Operating System	Windows	6	No	Yes	No	04-Feb-2020 3:36 PM
	ESU - WinServer 2008 SP2 - KB check - Multiple Ser...	Operating System	Windows	7	No	Yes	No	04-Feb-2020 3:36 PM
	ESU - WinServer 2008/2008 R2 SP1 - KB check - KB...	Operating System	Windows	7	No	Yes	No	04-Feb-2020 3:36 PM
	ESU - WinServer 2008 R2 SP1 - KB check - KB449062...	Operating System	Windows	5	No	Yes	No	04-Feb-2020 3:36 PM
	ESU - WinServer 2008 R2 SP1 - KB check - Multiple S...	Operating System	Windows	10	No	Yes	No	04-Feb-2020 3:36 PM

Log4j - Jar files containing JndiLookup.class Properties

General Supported Platforms Settings Compliance Rules Relationships Security

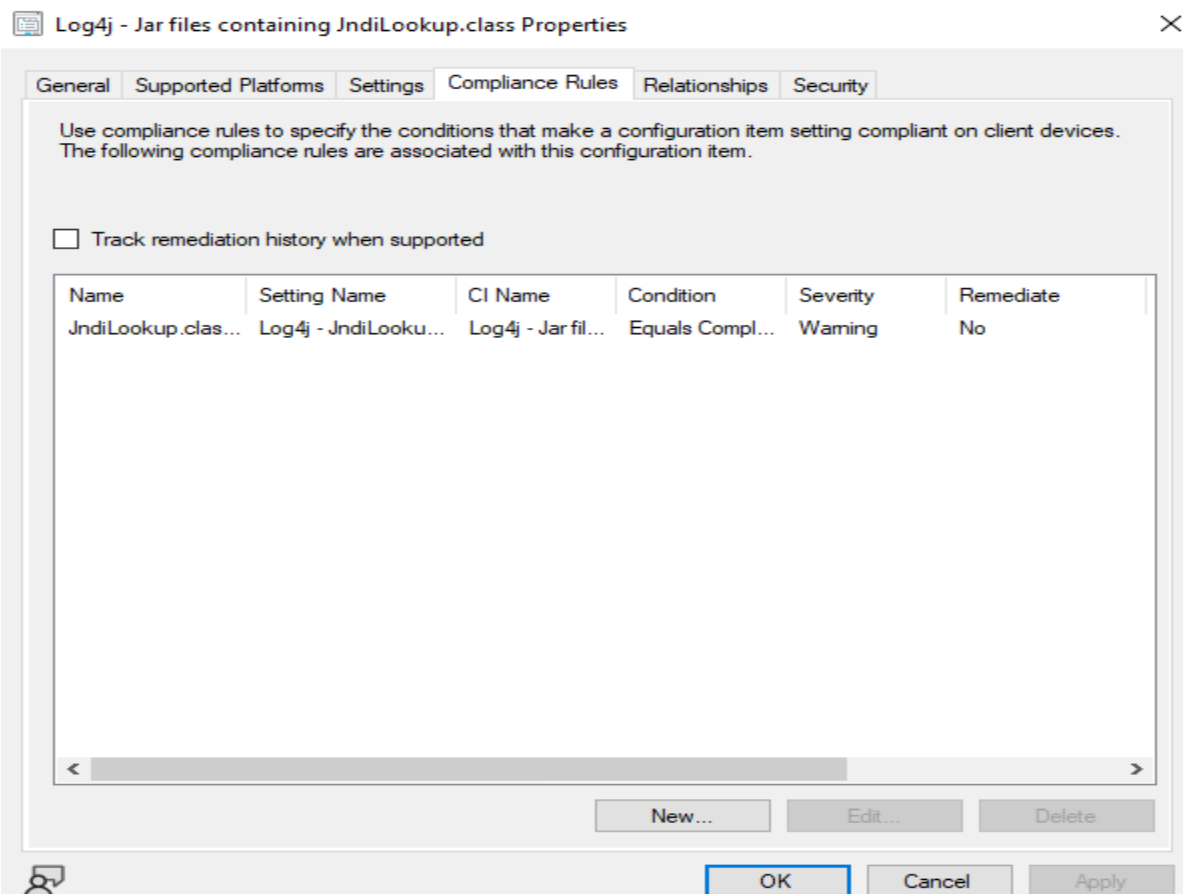
Use settings to represent business or technical conditions to assess for compliance on client devices. The following settings are associated with this configuration item.

Filter...

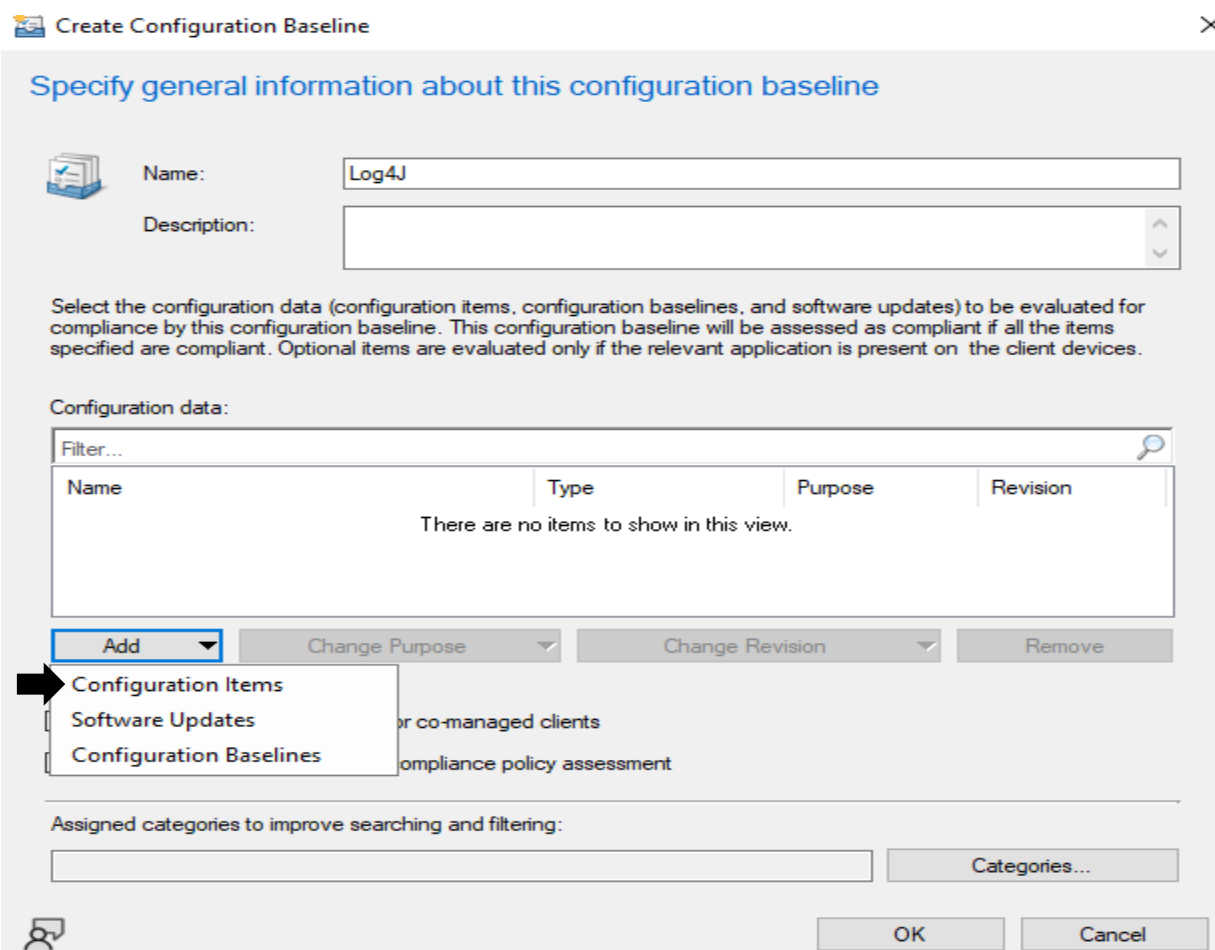
Name	Setting Type	Inherited	User Setting
Log4j - JndiLookup.class	Script	No	No

New... Edit... Delete

OK Cancel Apply



Will create Configuration Baseline



Select the configuration items that you want to add to this configuration baseline

Available configuration items:

Filter...				
Name	Type	Latest Revision	Description	Status
ESU - WinServer 200...	Operating System	Revision 4	checks for kb4493730, ES...	Enabled
ESU - WinServer 200...	Operating System	Revision 7	checks for Sept./Nov./De...	Enabled
ESU - WinServer 200...	Operating System	Revision 7	checks for kb4474419, ES...	Enabled
ESU - WinServer200...	Operating System	Revision 5	checks for KB4490628, ES...	Enabled
ESU - WinServer200...	Operating System	Revision 10	checks for KB4516655, KB...	Enabled
Log4j - Jar files contai...	Operating System	Revision 1	This CI searches for all jar-fi...	Enabled
Microsoft Exchange 2...	Application	Revision 7	This Configuration Item will ...	Enabled
Microsoft Exchange 2...	Application	Revision 7	This Configuration Item will ...	Enabled
MS Teams Compliance	Operating System	Revision 1		Enabled

Add

Remove

Configuration items that will be added to this configuration baseline:

Filter...				
Name	Type	Latest Revision	Description	Status
There are no items to show in this view.				

OK

Cancel

Select the configuration items that you want to add to this configuration baseline

Available configuration items:

Filter...				
Name	Type	Latest Revision	Description	Status
ESU - WinServer 200...	Operating System	Revision 4	checks for kb4493730, ES...	Enabled
ESU - WinServer 200...	Operating System	Revision 7	checks for Sept./Nov./De...	Enabled
ESU - WinServer 200...	Operating System	Revision 7	checks for kb4474419, ES...	Enabled
ESU - WinServer200...	Operating System	Revision 5	checks for KB4490628, ES...	Enabled
ESU - WinServer200...	Operating System	Revision 10	checks for KB4516655, KB...	Enabled
Microsoft Exchange 2...	Application	Revision 7	This Configuration Item will ...	Enabled
Microsoft Exchange 2...	Application	Revision 7	This Configuration Item will ...	Enabled
MS Teams Complianc...	Operating System	Revision 1		Enabled
Office Activation Statu...	Operating System	Revision 1		Enabled

Add

Remove

Configuration items that will be added to this configuration baseline:

Filter...				
Name	Type	Latest Revision	Description	Status
Log4j - Jar files contai...	Operating System	Revision 1	This CI searches for all jar-fi...	Enabled

OK

Cancel

Specify general information about this configuration baseline



Name:

Log4J

Description:

Select the configuration data (configuration items, configuration baselines, and software updates) to be evaluated for compliance by this configuration baseline. This configuration baseline will be assessed as compliant if all the items specified are compliant. Optional items are evaluated only if the relevant application is present on the client devices.

Configuration data:

Filter...			
Name	Type	Purpose	Revision
Log4j - Jar files containing JndiLookup.class	Operating System	Required	Latest

Add

Change Purpose

Change Revision

Remove

- ☐ Always apply this baseline even for co-managed clients
- ☒ Evaluate this baseline as part of compliance policy assessment

Assigned categories to improve searching and filtering:

"Client", "Server"

Categories...



OK

Cancel

Now deploy Configuration Baseline to All Systems

Icon	Name	Status	Deployed	User Setting	Date Modified	Compliance Count	Noncompliance Count	Failure C
	CB - Check client bound...	Enabled	Yes	No	17-Feb-2020 10:3...	4	0	0
	CB - DNS Server Vulner...	Enabled	Yes	No	15-Jul-2020 9:22 A...	3	0	0
	CB - ESU - Server 2008...	Enabled	No	No	11-May-2020 11:2...	0	0	0
	CB - ESU - Windows 7 a...	Enabled	Yes	No	11-May-2020 11:2...	0	0	0
	CB - Office Activation	Enabled	Yes	No	13-Sep-2019 9:57...	0	0	0
	CVE-2021-36934	Enabled	Yes	No	22-Jul-2021 12:06...	0	0	0
	HAFNIUM Exchange 2019	Enabled	Yes	No	22-Mar-2021 12:5...	0	1	0
	Log4J	Enabled	No	No	17-Dec-2021 11:3...	0	0	0
	Microsoft Exchange Ser...	Enabled	Yes	No	22-Mar-2021 1:29...	0	1	0
	Teams Baseline Rule	Enabled	Yes	No	29-Nov-2020 9:11...	0	4	0

Deploy Configuration Baselines

Select the configuration baselines that you want to deploy to a collection

Available configuration baselines:

Selected configuration baselines:

☐ Remediate noncompliant rules when supported

☐ Allow remediation outside the maintenance window

☐ Generate an alert:

When compliance is below:
90 %
Date and time:
17-Dec-2021 11:39 AM
☐ Generate System Center Operations Manager alert

Select the collection for this configuration baseline deployment.
Collection:
All Systems
Browse...

Schedule
Specify the compliance evaluation schedule for this configuration baseline:
☒ Simple schedule
Run every:
7 Days
☐ Custom schedule
No custom schedule defined.
Customize...

OK Cancel

You can monitor from Control Panel – Configurations – Make sure to run Machine and User policy cycle, so it will show up in Configuration as Compliant.

Configuration Manager Properties

General	Components	Actions	Site
Cache	Configurations		Network

Assigned configuration baselines:

Name	Revision	Last Evaluati...	Complian...	Eva
CB - Check client ...	1	13-Dec-2021...	Compliant	Idle
CB - DNS Server ...	1	15-Dec-2021...	Compliant	Idle
CB - Office Activa...	1	N/A	Unknown	Idle
CoMgmtSettingsPr...	4	17-Dec-2021...	N/A	Idle
Log4J	1	17-Dec-2021...	Compliant	Idle
Teams Baseline R...	1	12-Dec-2021...	Non-Com...	Idle

Evaluate
View Report
Refresh

OK
Cancel
Apply

Repeat above steps for these as well.

Latest Updates

Log4j - Jar files containing JndiLookup.class
Source: ☒ Community curated Configuration Item
This CI searches for all jar-files on a system that contains the string JndiLookup.class which contains the potentially vulnerable Log4j vulnerability

Check if file exists (Log4j)
Source: ☒ Community curated Configuration Item
This CI checks for the existence of the file specified in the value \$searchName (in this example it is searching for "log4j-core-*.jar" but can be changed to any value. This works with Powershell 2.0 ...

LOG4J - Hash Level Evaluation
Source: ☒ Community curated Configuration Item
This CI Evaluates all fixed drives for the existence of any file with the name LOG4J*.JAR. If a file with this name is found, it checks the current as of 12.15.2021 known bad hashes and reports if it...

LOG4J - Existence Test
Source: ☒ Community curated Configuration Item
This CI checks for the existence of any file with LOG4J*.JAR in the name. If found it raises a warning level event.

Configuration Items 26 items

Icon	Name	Type	Device Type	Revision	Child
	LOG4J - Existence Test	Operating System	Windows	1	No
	Check if file exists (Log4j)	Operating System	Windows	2	No
	LOG4J - Hash Level Evaluation	Operating System	Windows	1	No

Created Configuration Baseline for above.

	LOG4J EXISTENCE TEST	Enabled	No	No	17-Dec-2021 11:56 AM
	LOG4J EXISTS	Enabled	No	No	17-Dec-2021 11:56 AM
	LOG4J HASH EVALUATION	Enabled	No	No	17-Dec-2021 11:57 AM

Deployed Configuration Baseline to All Systems

	LOG4J EXISTENCE TEST	Enabled	Yes	No	17-Dec-2021 11:56 AM
	LOG4J EXISTS	Enabled	Yes	No	17-Dec-2021 11:56 AM
	LOG4J HASH EVALUATION	Enabled	Yes	No	17-Dec-2021 11:57 AM

Here it will display whether client/server are Compliant or Non Compliant.

Overview > Compliance Settings > Configuration Baselines >

Configuration Baselines 13 items

Icon	Name	Status	Deployed	User Setting	Date Modified	Compliance Count	Noncompliance Count	Failure Count
	LOG4J HASH EVALUATION	Enabled	Yes	No	17-Dec-2021 11:57 AM	0	0	0
	LOG4J EXISTS	Enabled	Yes	No	17-Dec-2021 11:56 AM	0	0	0
	LOG4J EXISTENCE TEST	Enabled	Yes	No	17-Dec-2021 11:56 AM	0	0	0
	Log4j	Enabled	Yes	No	17-Dec-2021 11:38 AM	1	0	0

Overview > Compliance Settings > Configuration Baselines >

Configuration Baselines 13 items

Icon	Name	Status	Deployed	User Setting	Date Modified	Compliance Count	Noncompliance Count	Failure Count
	LOG4J HASH EVALUATION	Enabled	Yes	No	17-Dec-2021 11:57 AM	1	0	0
	LOG4J EXISTENCE TEST	Enabled	Yes	No	17-Dec-2021 11:56 AM	0	1	0
	LOG4J EXISTS	Enabled	Yes	No	17-Dec-2021 11:56 AM	1	0	0
	Log4j	Enabled	Yes	No	17-Dec-2021 11:38 AM	1	0	0

This concludes Log4j CI and CB.

Thanks

Ram
17th Dec 2021