Qualys Custom Assessment and Remediation

Getting Started Guide

Version 2.0.1

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

About This Guide....2

About Qualys....2
Qualys Support....2

About Qualys Custom Assessment and Remediation....3

Getting Started with CAR.... 4

Working with Scripts in CAR.... 6

About Script Creation and Other Tasks....6
  Script Testing....6
  Script Reviews and Approval....7
  Script Execution....7
Managing Scripts....7
Job Status of Scripts....9

About Script Schedules....10

About CAR Dashboards.... 12

Appendix A.... 13

Required Roles and Permissions.... 13
Manifest Status....14
Data Retention Policy....14

Appendix B.... 15

CAR Use Cases....15
  Identify Your Assets with CSAM.... 15
  Create Your Custom Script for Log4Shell Detection.... 16
  Initiate Evaluation with the Script Output.... 16

About This Guide

This guide helps to get started with Qualys Custom Assessment and Remediation (CAR). However, it does not include procedural help for various operations in CAR. For step-by-step procedural help, refer to the Qualys CAR Online Help.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com.

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/.

About Qualys Custom Assessment and Remediation

Enterprises usually have a large number of assets that need to be continuously assessed and immediately remediated for any security gaps. Manually initiating assessment or remediation for each asset in the network is not only challenging, but time consuming as well. Traditional solutions do not provide response capabilities to execute commands for custom detection and initiating quick remediations, all from a single platform.

Qualys CAR provides a centralized way to proactively assess your assets for blind spots in custom configurations and zero-day vulnerabilities. It allows you to execute custom scripts to improve compliance and security posture of assets in your network. With CAR, you can execute scripts for enhanced detection and response measures. It enables you to create or upload custom logic and execute them across the environment to assess and improve the compliance and security posture of the assets, eliminating the need for third-party software for executing custom scripts.

Note: This guide does not include procedural help for various operations in CAR. For procedural help, refer to the Qualys CAR Online Help.

Getting Started with CAR

Qualys CAR includes the following features:

- Provides a framework to maintain a repository of generic scripts that can be executed on assets and the output of the scripts is shared with the applications in your Qualys subscription.

- Allows the output of a script execution to be shared with other Qualys apps that are registered to fetch the script output.

A typical CAR workflow includes the following:

- Create a script

- Test a script (optional)

- Review a script

- Execute a script on demand (Run Now) or schedule its execution.

Note: We provide a free license type for CAR to help you understand CAR and its features. To know more about it, contact support.

Prerequisites

- The CAR app must be enabled for your subscription. To get it enabled, contact your Technical Account Manager.

- For Windows, you need Qualys Cloud Agent 4.6.1.6 or later and for Linux, you need Qualys Cloud Agent 4.7.0 or later.

- For AIX, you need Qualys Cloud Agent 4.20.0.5 or later.

- For MAC, you need Qualys Cloud Agent 5.2.0 or later for Linux Intel, and 5.3.0 or later for Linux ARM.

Refer to:

Cloud Agent for Windows Installation Guide

Cloud Agent for Linux Installation Guide

Role-Based Access Control

You must have the user roles defined to get started with Qualys CAR. Not all users have access to execute all the operations; hence, user segregation is a better way to streamline the process of script execution in your environment.

Qualys CAR uses role-based access control (RBAC) permissions that control access to the various CAR functions. The four predefined roles are:

- Manager

- Author

- Auditor

- Viewer

- Operations

To know more about the roles and permissions in Qualys CAR, refer to Appendix A.

Supported Scripting Languages

Platform	Supported Scripts
Linux	Lua, Perl, Python, Shell -For Python scripts, you must have Python3 installed. -For Perl scripts, you must have any version of Perl installed.
Windows	PowerShell Command, PowerShell Script, Python, VBScript -For Python scripts, Python must be installed, and the install location should be added to SYSTEM PATH variable. Note: VBScripts are run in batch mode.
Unix	Lua, Perl, Python, Shell -For Python scripts, you must have Python3 installed. -For Perl scripts, you must have any version of Perl installed.
Mac	Lua, Perl, Python, Shell -For Python scripts, you must have Python3 installed. - For Perl scripts, you must have any version of Perl installed.

Following points must be kept in mind if you use Python on Windows platform:

- If Python is installed by using the setup, it should be installed for all users on the client machine. The installation location must be added to the system path variable.

- If Python is installed by using portable zip, the path of the directory containing python.exe must be added to the system path variable.

Supported Platforms

CAR supports Linux, Unix, Windows and MAC platforms.

Refer to the Platform Availability Matrix for complete information.

Working with Scripts in CAR

Qualys CAR has a repository of scripts stored in its database. You can also use scripts posted on the Qualys GitHub account. These scripts can be applied to multiple assets and tags.

CAR also provides you integration with GitHub for an enhanced script creation workflow. Apart from the options to manually enter or select scripts from your local drives, CAR now includes a new option to leverage the public and private repositories in GitHub.

To know more about how to import a script from GitHub public and private repositories, refer to Import a Script from GitHub.

You can share the output of the script execution job with different apps that have been registered to get the script output.

The maximum script size limit for both Linux and Windows platforms is 500 KB.

About Script Creation and Other Tasks

You can create a custom script or a custom QID script and add information in the required fields, select required assets, and assign tags.

Note: You can create up to 5000 scripts per subscription.

For information on how to create a script, refer to Creating Scripts.

Windows agent adheres to the PowerShell execution policy set on the host on which a script is executed.

Note: You may choose to bypass the PowerShell execution policy set on the host. While adding assets to a script, use the **Bypass Powershell Execution Policy** toggle switch to specify if you want to override the PowerShell execution policy on Windows hosts. When you switch this option to **Yes**, both signed and unsigned scripts are executed on the agent irrespective of the PowerShell execution policy set on the asset.

For information on how to create a custom QID script, refer to Creating Custom QID Scripts.

Script Testing

You can test the script on test assets before executing it on production assets.

This step is optional; however, it is recommended to test the script to avoid any failure in the production environment.

Testing can be done before or after a script is reviewed and approved.

In case of failure, you can edit the script and check for possible issues for failure.

For information on how to test a script, refer to Testing Scripts.

Script Reviews and Approval

Reviewing scripts is a one-time activity; therefore, **Review** option is disabled once a script is approved.

For information on how to review and approve a script, refer to Reviewing and Approving Scripts.

Script Execution

You can execute a script only after it is approved. A new job is created when you execute a script and is listed under the **Jobs** tab.

You may also want to test the script before executing.

When a script is executed, a parent job is created to contain all the activities that are carried out on individual assets added to the script. The applicable asset list for a script is evaluated at run time.

If the applicable assets list does not show any asset, it indicates that the parent job does not contain any associated asset jobs in it. The count of asset jobs for such script runs remains zero. This can happen when an imported script is executed before adding assets to it. It can also happen if a tag included in the script does not include any eligible asset to run the script depending on asset OS and activated modules.

Note: All the assets that participate in script run should have NTP sync set up. This is required for the date and time values to get interpreted correctly with Qualys Platform communication.

For information on how to execute a script, refer to Executing Scripts.

Managing Scripts

Besides script creation and execution, you can perform many other tasks such as following:

Task	Description
Export and import scripts	You can export a script and save it on your local computer and use in another environment by importing. Importing a script only imports the script details and excludes the meta data such as asset tags. You will have to add assets and tags to the script after you import. The script is exported in JSON format. **Note:** Scripts are exported in an encrypted format so that users cannot modify the script content or their metadata. This ensures that the confidentiality and integrity of the scripts are kept intact.
Edit scripts	You can edit a script if it is not approved or executed. You cannot edit a script once it is approved; you can only edit other details of the script such as the script name, its description and severity. Note: Manager user can edit the approved script.

Task	Description
Clone scripts	You can copy an existing script along with its assets and tags and other properties except the status. Even if you clone an approved script, you must get it reviewed and approved before you execute it. You cannot clone deprecated and rejected scripts.
Download scripts	You can download the script meta-data in CSV format. You can download maximum up to 5000 records for Scripts and Jobs. For Audit Logs, you can download a maximum of 100 records at a time.
Deprecate scripts	You can deprecate a script that's no longer required. Once a script is deprecated, only the View Details option is enabled in the Quick Actions drop-down menu. **Note:** A deprecated script is automatically removed after 7 days as part of a scheduled job.
View script status	Once a script is created, it moves through various statuses: **Pending Test:** A newly created or cloned (from existing script) script is displayed in the Pending Test state. **Pending Review:** When the script is tested on test assets, it is moved to Pending Review status. **Approved:** When script is reviewed and approved for production, it is displayed as 'Approved'. **Rejected:** When script is reviewed and is not approved for production, it is displayed as 'Rejected'. **Deprecated:** When a script is deprecated, it is displayed as 'Deprecated'.
View Script Details	You can view the output of all the scripts executed or tested in **Asset Jobs**.
View activity logs	The **Activity Logs** tab shows all the activities performed by users with respect to scripts. You can search the activities using the search bar or you can filter using the left navigation pane. You can narrow your search by using the following QQL tokens in the search box: - activity: - user: - targetType:
Viewing Job Details of a Script	You can view details of the most recent script execution job or all the jobs within a recurring cycle. You must have the View Jobs permission to view the job details of a script.

For information various operations related to managing scripts, refer to Managing Scripts

Job Status of Scripts

After a script is executed, you can view the details and their current statuses in the **Jobs** tab.

When a script is executed, the job name displayed is same as the script name. When a script is tested, the job name is displayed as *Test-<ScriptName-TimestampEpoch>* (milliseconds not included).

In the **Jobs** tab, you can search for script jobs by using the following QQL tokens in the search box:

- script.category:

- script.name:

- script.type:

- scriptId:

You can search for scheduled jobs by using the following QQL tokens in the search box:

- schedulerId:

- schedulerName:

According to the CAR Data Retention policy, the jobs and asset jobs are automatically deleted after seven days as part of a scheduled job. Refer to Appendix A.

About Script Schedules

You can create a schedule to enable script execution at a specific date and time in future.

Schedules can be of two types:

- One-time schedule

- Recurring schedule

In a recurring schedule, you can specify the date and time for the first script run and the date for the last script run.

Note: The status of a script is shown as ’Expired’ when the end date specified for the recurring schedule has elapsed.

For information on how to schedule a script and other related topics, refer to the Working with Script Schedules.

Here’s some brief information on the various tasks related to script schedules:

Task	Description
Schedule a script execution	A script can be scheduled to be automatically executed at a specified date and time. You can schedule a script for one-time execution or as a recurring job. A script can be scheduled from the Quick Actions menu in the Scripts sub-tab or from the Schedules sub-tab. Only an approved script can be scheduled. You can also delete a schedule or edit to make changes as per your requirement.
View Schedule Details	You can view the details of an existing schedule in the Scripts > Schedules sub-tab.
Activate and Deactivate Schedules	When you create a schedule, you can activate the schedule immediately by clicking Save & Activate. Alternatively, you can activate it later from the Schedules sub-tab. Note: You cannot activate a schedule if the script selected for the schedule is deprecated or deleted.
View job details of a Schedule	You can select a schedule and view its status and other corresponding details. You can choose to view details of the most recent job or all jobs within a recurring cycle. Select a schedule from the Schedules sub-

tab or use any of the following QQL tokens in the search box:

- name:
- id:

About CAR Dashboards

CAR allows you to create multiple dashboards and switch between them to access relevant information in an instant. The **Script Run Summary** dashboard is the default CAR dashboard and has a collection of seven default widgets showing data of your interest, which are updated in real-time.

Following are the default widgets in the CAR dashboard:

- Number of Scripts Group by Script Category

- Number of Scripts Group by Script Type

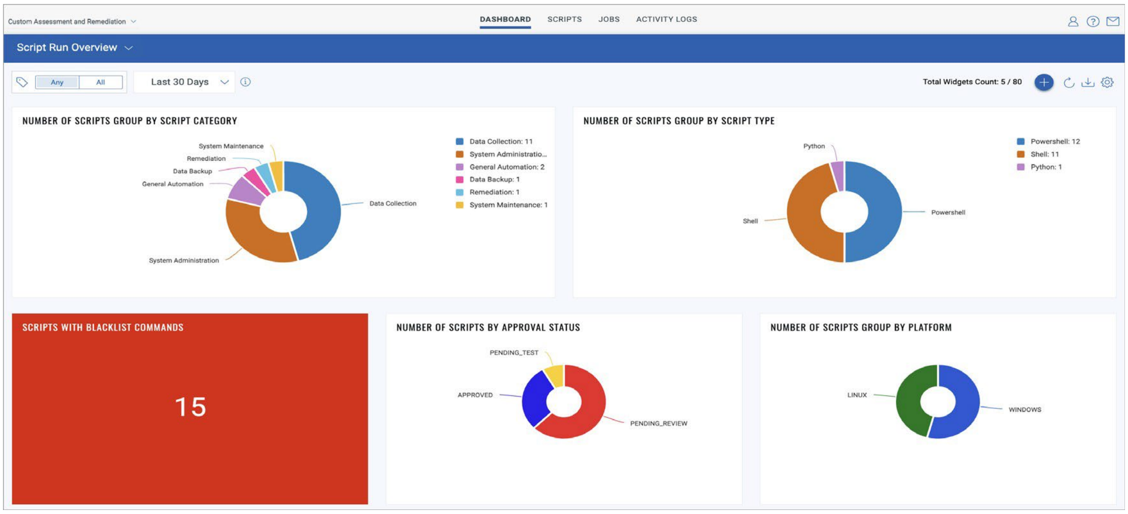
- Number of Scripts by Approval Status

- Number of Scripts Group by Platform

- Number of Scripts Created by Users

- Number of Jobs Group by Script Category

- Scripts with Potentially System-Impacting Commands



You can use the default CAR dashboard provided by Qualys or easily configure widgets to fetch information from other Qualys modules and add them to your dashboard. You can also add as many dashboards as you like to customize your application view.

CAR is integrated with Unified Dashboard (UD). UD brings information from all Qualys applications into a single place for visualization.

For information on creating widgets, dashboards, templates, and more, refer to the Unified Dashboard Online Help.

Appendix A

Required Roles and Permissions

You must have the user roles defined to get started with Qualys CAR. Not all users have access to execute all the operations; hence, user segregation is a better way to streamline the process of script execution in your environment.

These roles give an additional level of security against running a script without oversight.

Roles	Permission
Manager	**General UI:** Access **Script:** View, Create, Review and Approve, Evaluate, Update, Deprecate, Execute, Import, Export, Delete, Download **Schedule:** View, Create, Update, Delete, Activate, Deactivate, Download **Jobs:** View, Download, Delete **Audit Logs:** View, Download **Dashboard:** View, Update, Create, Download, Print, Delete **Library:** View, Import
Author	**General UI:** Access **Script:** View, Create, Evaluate, Update, Import, Export, Download **Schedule:** View, Create, Update, Delete, Download **Jobs:** View **Audit Logs:** View **Dashboard:** View **Library:** View, Import
Auditor	**General UI:** Access **Script:** View, Download **Schedule:** View, Download **Jobs:** View, Download **Audit Logs:** View, Download **Dashboard:** View, Download, Print **Library:** View
Viewer	**General UI:** Access **Script:** View **Schedule:** View **Jobs:** View **Audit Logs:** View **Dashboard:** View **Library:** View
Operations	**General UI:** Access **Script:** View, Execute, Import, Export, Download **Schedule:** View, Create, Activate, Deactivate, Update, Delete, Download **Jobs:** View **Audit Logs:** View **Dashboard:** View **Library:** View

Manifest Status

Manifest Status	Description
MANIFEST_GENERATION_IN_PROGRESS	Initial status that is displayed when an asset job is created and manifest is sent to CAS.
MANIFEST_PUBLISHED	CAS sends the 'Manifest Received' feedback to CAR.
MANIFEST_ASSIGNED	Agent sends the 'Manifest Download' confirmation.
MANIFEST_DOWNLOADED_SUCCESS	Manifest has been successfully downloaded from Qualys Cloud Platform.
MANIFEST_DOWNLOADED_FAILED	Manifest could not be downloaded from Qualys Cloud Platform.
MANIFEST_PARSED_SUCCESS	Manifest has been parsed successfully.
MANIFEST_PARSED_FAILED	Manifest parse failed.
MANIFEST_EXECUTION_SUCCESS	Manifest has been successfully executed.
MANIFEST_EXECUTION_FAILED	Manifest execution failed.
SCRIPT_RESULT_UPLOAD_SUCCESS	Script result has been uploaded on Qualys Cloud Platform.
SCRIPT_RESULT_UPLOAD_FAILED	Script result could not be uploaded on Qualys Cloud Platform.

Data Retention Policy

According to the CAR Data Retention policy, if a script is not modified/executed for 6 months, it will be automatically deprecated. And a deprecated script will be automatically deleted after 7 days as part of a scheduled job. Also, the jobs and asset jobs will be automatically deleted after 7 days as part of a scheduled job.

Appendix B

CAR Use Cases

This chapter includes use cases to show you how you can leverage Qualys CAR to identify zero-day vulnerabilities and other security threats, modify the configuration of an application or an Operating System, or even implement a security policy as a part of your response program to secure your environment - all by executing custom scripts on scoped assets within your network.

Let's consider this for an example - you want to identify the assets that have Log4j installed, and then detect instances that are infected by Log4Shell. The power of the Qualys Cloud Platform along with the detection and remediation capabilities of CAR help you to identify the potentially vulnerable assets in the environment and initiate remediation to quickly close the security gaps.

In the similar way, you can also create and execute custom scripts for sensitive data protection, identity management, zero-day threats and so on.

To know more about the use-case based script templates on Qualys GitHub account, click here.

Identify Your Assets with CSAM

Qualys CSAM accurately inventories if Log4j is installed on any of your assets or if Log4j is in the class path of a running java application. With CSAM, you can discover if Log4j is present within your environment.

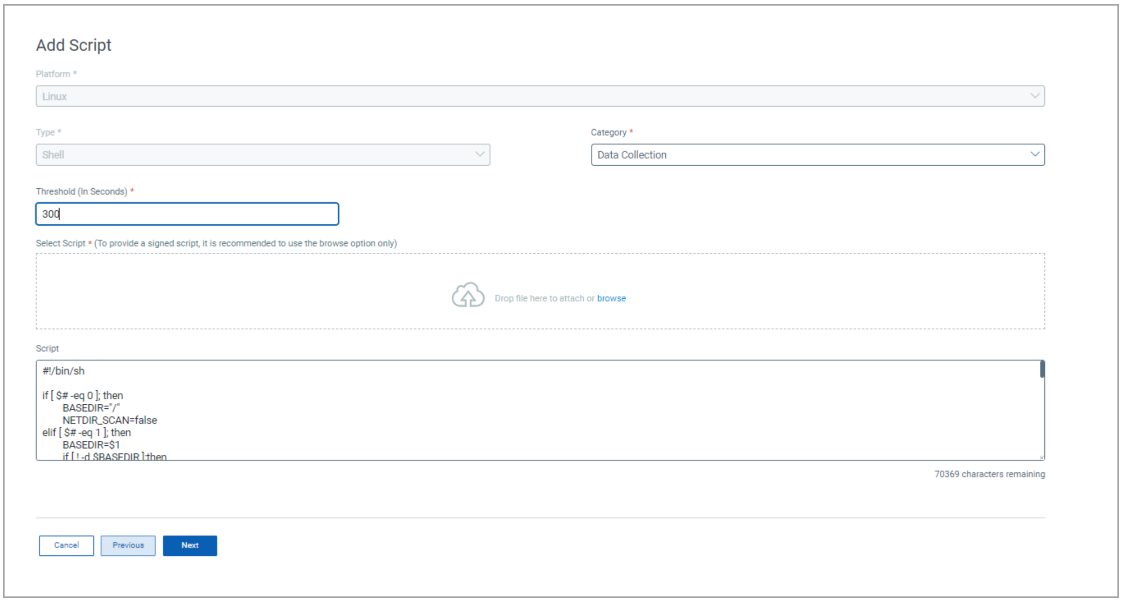
Use the following QQL query to identify such assets and create a dynamic asset tag for it:

```
software:(name:“log4j” or name:“liblog4j2”)
```

This tag automatically gets associated with all the targeted assets and you can execute a custom script on the asset scope using the same tag.

Create Your Custom Script for Log4Shell Detection

You can create your own detection script or use the one posted on Qualys GitHub account - log4j_findings.sh.



Add Script

Platform *: Linux

Type *: Shell

Category *: Data Collection

Threshold (In Seconds) *: 300

Select Script * (To provide a signed script, it is recommended to use the browse option only)

Drop file here to attach or browse

Script

```
#!/bin/sh

if [ $# -eq 0 ]; then
      BASEDIR="/"
      NETDIR_SCAN=false
elif [ $# -eq 1 ]; then
      BASEDIR=$1
      if [ ! -d $BASEDIR ];then
```

70369 characters remaining

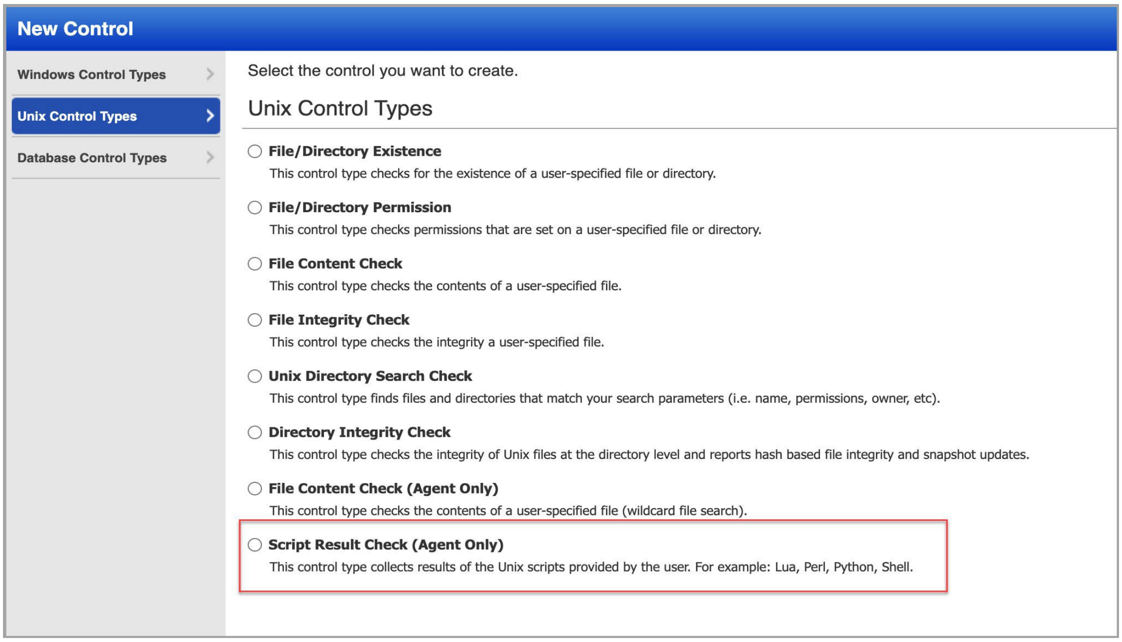
To learn about how to create a script, refer to Creating Scripts.

Once your script is reviewed and approved, you can execute the script on your scope of assets for Log4Shell detection.

Initiate Evaluation with the Script Output

Leverage the native integration of Qualys CAR with Qualys Policy Compliance to create ‘Script Result Check’ type User Defined Controls (UDCs). Control evaluation is based on the defined evaluation criteria and the actual script output.

To achieve this, Qualys has introduced a new type of UDC called 'Script Result Check' in Qualys Policy Compliance.



New Control

Select the control you want to create.

Unix Control Types

○ **File/Directory Existence**
This control type checks for the existence of a user-specified file or directory.

○ **File/Directory Permission**
This control type checks permissions that are set on a user-specified file or directory.

○ **File Content Check**
This control type checks the contents of a user-specified file.

○ **File Integrity Check**
This control type checks the integrity a user-specified file.

○ **Unix Directory Search Check**
This control type finds files and directories that match your search parameters (i.e. name, permissions, owner, etc).

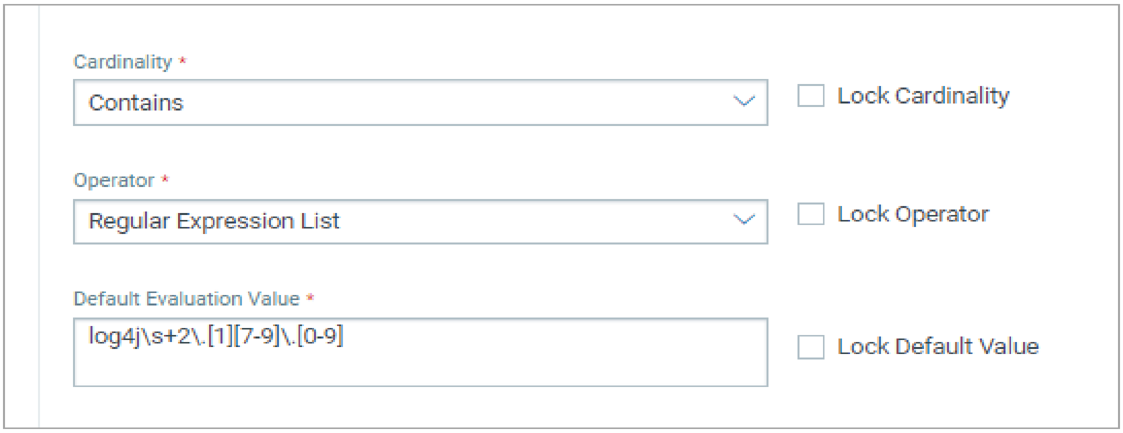
○ **Directory Integrity Check**
This control type checks the integrity of Unix files at the directory level and reports hash based file integrity and snapshot updates.

○ **File Content Check (Agent Only)**
This control type checks the contents of a user-specified file (wildcard file search).

○ **Script Result Check (Agent Only)**
This control type collects results of the Unix scripts provided by the user. For example: Lua, Perl, Python, Shell.

Script Result Check UDCs can be created to evaluate the output of the script and define the compliance and security posture of the assigned assets.

For example, the script log4j_findings.sh would fetch the log4j version as part of its output. Since log4j version 2.17 or above is considered safe, you can configure the pass or fail value for the control by setting the default evaluation value.



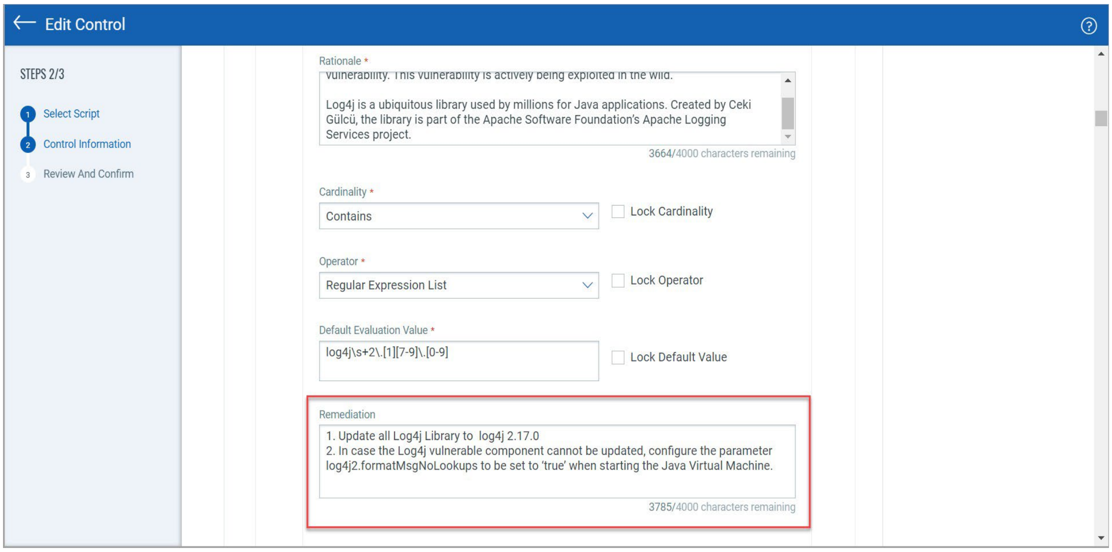
Cardinality * : Contains — □ Lock Cardinality

Operator * : Regular Expression List — □ Lock Operator

Default Evaluation Value * : log4j\s+2\.[1][7-9]\.[0-9] — □ Lock Default Value

The Qualys platform and CAR enable you to rapidly respond to security threats by executing custom scripts not only for detection and validation of security threats, but for remediations as well.

You can enter the remediation steps in the control to ensure that the appropriate response program can be carried out when the control fails.



Rationale *
vulnerability. This vulnerability is actively being exploited in the wild.

Log4j is a ubiquitous library used by millions for Java applications. Created by Ceki Gülcü, the library is part of the Apache Software Foundation's Apache Logging Services project.

3664/4000 characters remaining

Cardinality *
Contains
□ Lock Cardinality

Operator *
Regular Expression List
□ Lock Operator

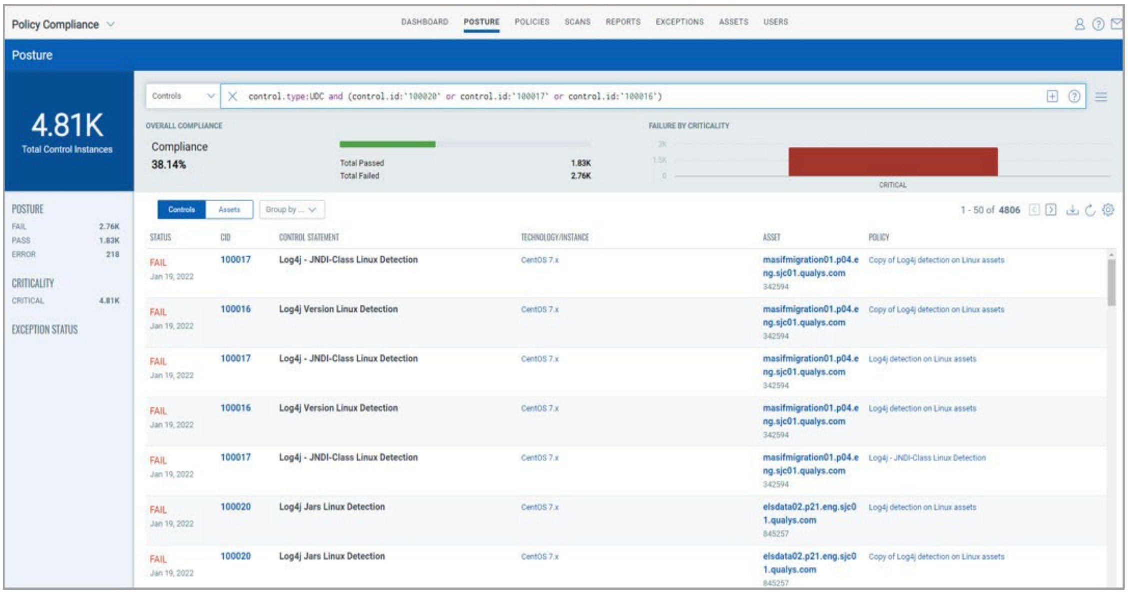
Default Evaluation Value *
log4j\s+2\.[1][7-9]\.[0-9]
□ Lock Default Value

Remediation
1. Update all Log4j Library to log4j 2.17.0
2. In case the Log4j vulnerable component cannot be updated, configure the parameter log4j2.formatMsgNoLookups to be set to 'true' when starting the Java Virtual Machine.

3785/4000 characters remaining

Note: Script Result Check type UDCs can only be created for Approved Scripts.

These controls define the compliance and security posture of your environment for the scoped assets, which is listed under the **Posture** tab.



Controls

```
control.type:UDC and (control.id:'100020' or control.id:'100017' or control.id:'100016')
```

4.81K
Total Control Instances

OVERALL COMPLIANCE
Compliance
38.14%

Total Passed	1.83K
Total Failed	2.76K

FAILURE BY CRITICALITY

POSTURE

FAIL	2.76K
PASS	1.83K
ERROR	218

CRITICALITY

CRITICAL	4.81K

EXCEPTION STATUS

1 - 50 of 4806

STATUS	CID	CONTROL STATEMENT	TECHNOLOGY/INSTANCE	ASSET	POLICY
FAIL Jan 19, 2022	100017	Log4j - JNDI-Class Linux Detection	CentOS 7.x	masifmigration01.p04.eng.sjc01.qualys.com 342594	Copy of Log4j detection on Linux assets
FAIL Jan 19, 2022	100016	Log4j Version Linux Detection	CentOS 7.x	masifmigration01.p04.eng.sjc01.qualys.com 342594	Copy of Log4j detection on Linux assets
FAIL Jan 19, 2022	100017	Log4j - JNDI-Class Linux Detection	CentOS 7.x	masifmigration01.p04.eng.sjc01.qualys.com 342594	Log4j detection on Linux assets
FAIL Jan 19, 2022	100016	Log4j Version Linux Detection	CentOS 7.x	masifmigration01.p04.eng.sjc01.qualys.com 342594	Log4j detection on Linux assets
FAIL Jan 19, 2022	100017	Log4j - JNDI-Class Linux Detection	CentOS 7.x	masifmigration01.p04.eng.sjc01.qualys.com 342594	Log4j - JNDI-Class Linux Detection
FAIL Jan 19, 2022	100020	Log4j Jars Linux Detection	CentOS 7.x	elsdata02.p21.eng.sjc01.qualys.com 845257	Log4j detection on Linux assets
FAIL Jan 19, 2022	100020	Log4j Jars Linux Detection	CentOS 7.x	elsdata02.p21.eng.sjc01.qualys.com 845257	Copy of Log4j detection on Linux assets

Qualys CAR comes with API support that helps you to fetch the script output in standardized format which can be consumed by data lakes for further correlations.