MDCMS SonarQube Interface Manual

SonarQube Interface for MDCMS

from Midrange Dynamics

From Version 8.5

Published January 30, 2023

Overview

What is SonarQube?

SonarQube is a Code Review product from Sonar. It scans source code for a variety of open-source languages, as well as COBOL and RPG and creates a report of issues that it finds with the code.

The SonarQube product is made up of 2 parts:

1. The Sonar Server, which is an HTTP Server which provides a dashboard for administrators and developers as well as REST APIs for automated configuration and information retrieval.
2. The Sonar Scanner, which is a service running on a Linux server which performs the scan of source code.

Summary of Flow between MDCMS and SonarQube

When an RFP is installed, and it contains objects of attributes that are assigned to a Code Review Template, MDCMS copies the code to the Linux server where the Sonar Scanner is located. MDCMS then uses a shell command to execute the scan of the code.

When the scan is complete, the Sonar Scanner sends the results to the SonarQube server where the results can be viewed in detail. The SonarQube server invokes an MDCMS webhook to update the RFP with a summary of the results.

How MDCMS Communicates with SonarQube

MDCMS uses REST to communicate with the SonarQube server and SFTP for copying source code and instructions to the server that hosts the Sonar Scanner.

Additionally, the MDCMS Script Execution Service must be running on the Sonar Scanner server in order to execute the shell script for performing the code review.

Prerequisites for using the Interface

- An active MDCMS, MDOpen and MDWorkflow Pipeline license (v8.5+) on the IBM i partition used to connect to SonarQube
- The Portable App Solutions Environment IBM Licensed Program (SS1 option 33) must be installed
- The SonarQube http port must be reachable within the network by the partition
- The MDCMS REST Server http port on the partition must be reachable within the network by the SonarQube server. You configure the MDCMS REST Server from:
  MDCMS->1=MDCMSSetup Menu->10=Interface Settings->9= MDCMS REST API and Diagramming Server
- The Linux server hosting the Sonar Scanner must have SFTP running and be reachable within the network by the partition
- A user with administration rights for the SonarQube server for creating a Token
- A user with SUDO authority for the Linux server hosting the sonar scanner, in order to install the MDCMS Script execution service as well as for being able to verify and troubleshoot the Sonar Scanner
- The MDCMS-Side configuration must be performed by a user with MDSEC authority to System Settings (code 11) and Template Maintenance (code 7)

Configure the Interface

Generate a User Token in SonarQube

In order to securely authenticate a connection with the SonarQube server, a Token needs to be generated within SonarQube that will then be stored in the Pipeline Server configuration.

To generate a token, take the following steps:

1. Log into SonarQube with a user having administration rights
2. Click on the user icon at the top-right of the web page and select option My Account
3. Click on the Security tab
4. Enter a descriptive Token Name at the prompt and click Generate
5. Copy the generated string to a safe location

Install the MDCMS Command Script Service

In order to trigger a scan by the Sonar Scanner service, the MDCMS Command Script Service must be installed as a service on the same Linux server as the Sonar Scanner service. This is because it can only be systematically triggered by using a shell script.

The service and instructions are available from the MD Knowledge Base.

Configure the Pipeline Server

The Pipeline server entry provides MDCMS with the URL and credentials necessary to invoke REST APIs provided by the SonarQube server. To configure these parameters, connect MDOpen to the partition that will communicate with SonarQube and navigate to Settings->Pipeline Servers.

Right-click within the Pipeline Servers view and select option Add

Pipeline Server Parameters

Server ID	A 10-character unique ID used to reference the configuration
Description	A description of the server
Server Type	Select value SonarQube from the list
Pipeline Server URL	The URL of SonarQube. Example: https://sonarqube.myorg.com
Set New Token	Paste in the value of the generated token string (see prior section)
Proxy	If the SonarQube server is reached via a Proxy server, then provide the Proxy Address, and, if necessary, the port, user and password.
Redirects	Should not be applicable

Once the parameters are saved, right-click on the Pipeline Server entry and select option Test Connection to verify. If the connection fails, right-click on the Pipeline Server entry and select option Connection Logs.

Configure the FTP Server

The FTP server entry provides MDCMS with the address and credentials necessary to use FTP to copy source code to the Linux server hosting the Sonar Scanner. To configure these parameters, connect MDOpen to the partition that will communicate with SonarQube and navigate to Settings->FTP Servers.

Right-click within the FTP Servers view and select option Add

FTP Server Parameters

Server ID	A 10-character unique ID used to reference the configuration
Description	A description of the server

Server Address	The host name or IP address of the Linux server
FTP Method	A choice of SFTP (recommended), FTP or FTPS
Port	*DFT – the default port based on the method. This is 21 for FTP, 22 for SFTP and 990 for FTPS. Otherwise, the numeric value of a specific port number
Transfer Mode	Anonymous – no credentials necessary User/Password – a user and password are required User/SSH Key – a user and SSH public/private key pair are required
User	If not anonymous, enter the name of a user that has authority on the Linux server to FTP to the SonarQube Project Base directory
Set New Password	If for User/Password – the password registered for the user
Proxy	If the Sonar Scanner server is reached via a Proxy server, then provide the Proxy Address, and, if necessary, the port, user and password.
FTP Timeout in Seconds	The number of seconds MDCMS should wait for a file transfer to complete. This should be set long enough to handle the size of a source code file depending on network speed.
SSH Private Key in IFS including path	If for User/SSH Key, the full path in IFS to a valid SSH private key, including the name of the key. The public key must also be in the same path. The public key will also need to be registered with the SFTP server on the Linux server hosting Sonar Scanner.
Set New SSH Private Key Passphrase	If the private key is protected by a passphrase, enter it here
Script Runtime Folder on Server	This must be the full path to the drops folder for the MDCMS Command Script Service. For example: /home/root/mdcmscmd/drops
Script Timeout in Seconds	Not applicable here, as MDCMS does not wait for Sonar Scanner to complete the review, since it can potentially take a very long

	time.
Script Command Folder Symbol	Set to /-Standard

Once the parameters are saved, right-click on the FTP Server entry and select option Test Connection to verify.

If the connection fails, navigate to Settings->Services and then right-click on MDFTP if an FTP connection was configured or MDSFTP if an SFTP connection was configured. Then select option Logs. If the MDSFTP log is not legible, you will first need to end the MDSFTP service. This can be done by left-clicking on MDSFTP and clicking the End Jobs button.

Configure a Code Review Template

After the Pipeline server is configured, right-click on the entry in the Pipeline Servers view and select option Code Review Templates. One template should be created for each SonarQube project that should be used by MDCMS for code review.

Right-click within the Cide Review Templates view and select option Add

Code Review Template Parameters

Template	A 10-character unique ID used to reference the template configuration
Description	A description of the template
Quality Gate	If set to true, object requests for attributes that use this template will not be allowed to proceed to the next step in the migration path that is after the installation into the current level for the attribute, until the code review is complete and returns a SUCCESS status.
Pipeline Server ID	The ID of the Pipeline Server (see prior section)
Project Key	The exact key value for a Project within SonarQube. This key is visible within SonarQube from the Project Information section for a Project.
Project Base Directory	The full path to the base directory of the project on the Linux server where the Sonar Scanner resides.
Relative Source Path	The relative path from the Project Base Directory to the source directory. If the source directory and the Project Base Directory are

	the same, enter the value of . (a period).
FTP Server ID	The ID of the FTP Server (see prior section)
FTP Source Path	The path from the root of the FTP server for the user to the source directory for the project. This is an additional parameter because FTP can be configured to start from a path other than root.
Server Path to Scanner Command	If the Sonar Scanner command sonar-scanner is not registered on the PATH environment variable on the Linux server, the full path of the command can be entered here.
Use sudo	If true, sudo will be used when invoking the sonar-scanner command
Host URL of Server from Scanner	The URL of the SonarQube server, as it would be found from the Sonar Scanner. If the SonarQube server is on the same Linux server as the Sonar Scanner, then the URL will usually be: http://localhost:9000
Code Review Frequency	The number of units before a Code Review is triggered. A unit is based on the value of parameter Code Review Unit of Frequency.
Code Review Unit of Frequency	RFP – the code review will occur after n RFPs have been installed Object – the code review will occur after at least n Objects have been installed. If there are more than n Objects in the RFP, there will only be 1 review. Day – the code review will occur after at least n days. The current day counts as day 1. Pending code review batches will be tallied only on days that an RFP using the template is installed. For example, Frequency is set to 2. Today an install occurs – that is day 1, tomorrow, day 2, nothing is installed, so the code review does not occur yet, even though 2 has been reached. On the 5th day, an RFP is installed again, triggering the batch to be processed. Manual Only – the code review is held off for all installed RFPs until a user manually selects the option to trigger the review. The appropriate value for frequency and unit will depend on the size of the project. Small projects can be triggered after every RFP, but large ones that may requires 30 minutes or more for a review may be best to perform not more than once daily.
New Version Frequency	In SonarQube, the code review results are based on what is considered part of the most recent version. To ensure that prior

	installations are not taken into account, when unwanted, MDCMS can specify a new version ID when triggering a review. This frequency is the number of units before a batch is flagged as part of a new version.
New Version Unit of Frequency	Same units as for Code Review
Additional Parameter/Values	These pairs can be used, when necessary to set additional custom sonar-scanner properties when triggering a code review.

Apply a Code Review Template to MDCMS Attributes

Any given Code Review Template can be assigned to the attributes in MDCMS for target levels where the review should be performed.

The Template assignment occurs within MDCMS. To do so, enter command MDCMS and then navigate to:

1=MDCMS Setup Menu

5=Templates

10=Code Review

Using the Interface

Triggering a Code Review

A Code Review will be automatically triggered when an RFP containing Object Requests assigned to a Code Review template is installed, if the Code Review Frequency threshold is reached and the Code Review Unit of Frequency is not Manual Only.

The trigger occurs during the cleanup phase of the RFP, so that the application downtime window is not impacted.

If a Code Review should be manually triggered, because it is Manual Only or because the automatic trigger failed due to a configuration or connectivity error, do the following:

1. Within MDOpen, navigate to Settings->Pipeline Servers
2. Right-Click on the SonarQube server and select option Code Review Templates
3. Right-Click on the Code Review Template for the project to review and select option Batches
4. For any batch that has not yet Passed or Failed, Right-Click on the batch and select option Run Code Review

Viewing Results of a Code Review within MDCMS

Once a code review is complete, SonarQube will invoke the MDCMS webhook with the results. These can be viewed in 2 places:

1. The RFP Deployment Log in green screen and in MDOpen will include this information
2. Within MDOpen navigate to Settings->Pipeline Servers->Code Review Templates->Batches and right-click on a batch. There are 2 options for results:

View Metrics – view the list of defined metrics, their thresholds and the result per metric
Code Review Results – view the list of source code items in the batch

Troubleshooting the Interface

1. Check the RFP deployment log if a Code Review was attempted
2. Check the Code Review Template Batch if the Code Review was started and has ended
3. Check the MDFTP or MDSFTP connection log if there was any issue with copying the source to the Sonar Scanner server
4. Check in the SonarQube dashboard for the project if review results were generated
5. On the Linux server, navigate to the location of the MDCMS Command Script Service drops folder and check for contents in the NOK and NOK result folders. If nothing there, check the OK and OK result folders. If the script is still pending in the drops folder itself, then the service isn't running and needs to be restarted.

Overriding a Code Review Quality Gate

If a Code Review Quality Gate is still pending or has failed, but the object requests for the source in question must continue to the next step, option O=Override can be used during the pre-submit or pre-send validation for the RFP for the next step. If you have authority to MDSEC code 58 for the specific application level, this option will be available.

