MarkLogic Server

Common Criteria Evaluated Configuration Guide

MarkLogic 9
May, 2017

Last Revised:9.0-3, September, 2017

Table of Contents

Common Criteria Evaluated Configuration Guide

1.0 About the Evaluated Configuration

This chapter introduces the Evaluated Configuration of MarkLogic Server, which is currently under evaluation for the Common Criteria. This chapter includes the following sections:

1.1 Common Criteria

The Common Criteria for Information Technology Security Evaluation (the Common Criteria, or CC) and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for the Common Criteria Recognition Arrangement (CCRA), which ensures:

- Commercial products are evaluated by independent licensed evaluation laboratories that determine the fulfilment of specified security properties to a specified level of assurance
- Certificate Authorizing Schemes certify the evaluation results produced by the evaluation labs and issue evaluation certificates accordingly
- Issued certificates are mutually recognized by the signatories to the CCRA.

MarkLogic Server 9 is currently under evaluation for Common Criteria Evaluation Assurance Level 2 (EAL2+).

For the documentation describing the Common Criteria evaluation process and methodology, see the documents at http://www.commoncriteriaportal.org/.

1.2 The Evaluated Configuration

The evaluated configuration of MarkLogic Server is the configuration in which the Common Criteria evaluation was performed. This is a specific version of MarkLogic Server set up in a specific way. That configuration is outlined in this guide. This guide does not explain the various features of MarkLogic Server. For information on the MarkLogic Server features, see the MarkLogic Server documentation.

This guide includes the list of features that cannot be used in an evaluated configuration, along with any needed guidelines for how to exclude these features from your configuration. The evaluated configuration assumes that the configuration is set up according to these guidelines; configurations that do not follow these guidelines are not considered evaluated configurations.

1.3 Authorized Administrator

An Authorized Administrator is any user that has the `admin` role or any user that has the privilege(s) needed to run the Admin API (`admin-module-read` and `admin-module-write`), the Security API (any of the privileges in the `security` role), or the PKI API (`pki-read` and `pki-write`). These privileges exist in roles that are installed in the TOE, such as the `security` role, or can be added to any role by an Authorized Administrator. Any role that provides access to administering security functional requirements, whether the role is predefined at installation time or user-created (by an Authorized Administrator), must be granted by an Authorized Administrator; it is the responsibility of Authorized Administrators to be aware of these privileges when granting privileges or roles to users. Furthermore, any user who has any such privileges is considered an Authorized Administrator.

Additionally, there are other administrative XQuery built-in functions (https://docs.marklogic.com/xdmp/admin) that perform functions such as starting and stopping the server, and these functions each have privileges associated with them. Any user that is granted any of the privileges associated with these functions (for example, `xdmp-shutdown`) is also considered an Authorized Administrator.

Administrators with the `admin` role have full privileges to the system. Administrators who have any of the privileges to run functions in the security-related APIs (Admin API, Security API, PKI API, and XQuery Admin built-in functions) only have those privileges that have been granted to them (via roles) by an Authorized Administrator. Those privileges each protect specific functions or sets of functions; the functions are primitives and must be used in a program with the proper logic in order to perform Security Functional Requirements. It is up to the Authorized Administrator who grants these privileges to determine which privileges a user is granted.

If administration is performed using the Admin API, Security API, PKI API, and/or the built-in Admin functions, those APIs must run against an HTTP or XDBC App Server that is set up to use TLS. Actions against the Admin Interface, HTTP interfaces, and XDBC interfaces are auditable, based on the configuration for the App Server. You should audit actions based on your own security policies.

Only Authorized Administrators can manage the target of evaluation (TOE) using the Admin Interface or using the various XQuery administrative functions included with MarkLogic (the Admin API, the Security API, the PKI API, or the built-in Admin functions). Additionally, all code must be evaluated through an interface that is set up to use TLS. Authorized administrators are assumed to be non-hostile, appropriately trained, and follow proper administrative procedures. For more details about the Authorized Administrator and about performing administrative tasks in MarkLogic Server, see the *Administrator's Guide* and *Security Guide*. For more details about the TOE, see "Target of Evaluation (TOE)" on page 8.

1.4 TOE Requirements

This section lists the requirements for the target of evaluation (TOE). This is a subset of the platforms in which MarkLogic Server runs (see the *Installation Guide* for those details), and includes the following parts:

- MarkLogic Server TOE Platform
- Licence Key for TOE
- Admin Interface App Server Configured to Use HTTPS
- All TOE Access App Server Configured to Use HTTPS and Digest Authentication
- Features Not Part of the TOE
- MarkLogic Server 9.0

1.4.1 MarkLogic Server TOE Platform

In its evaluated configuration, MarkLogic Server is supported on Red Hat Enterprise Linux 7 (x64). This platform provides the following capabilities that fulfil certain security objectives for the operational environment: its system clock provides a reliable time source that is used by MarkLogic Server to timestamp audit records (OE.TIME); it is a multi-processing platform that provides applications with dedicated processes for their exclusive use, isolating applications from one another in the operational environment (OE.PROCESS). For further details about this platform, see the *Installation Guide*.

1.4.2 Licence Key for TOE

The TOE requires the 9.0 Essential Enterprise Edition of MarkLogic Server, which is enabled by a license key. Contact your sales representative or MarkLogic Support for information about obtaining a license key.

1.4.3 Admin Interface App Server Configured to Use HTTPS

The App Server in which the Admin Interface runs must be configured to use HTTPS. To configure HTTPS on the Admin App Server, follow the procedure described in “Configure the Admin App Server to Use HTTPS” on page 13. Additionally, any App Server where Admin API or Security API functions are run must also be set up to use HTTPS.

1.4.4 All TOE Access App Server Configured to Use HTTPS and Digest Authentication

Any application that runs in the TOE should have its App Server(s) configured to use HTTPS. To configure HTTPS on an App Server, follow the procedure in Configuring SSL on App Servers in the *Security Guide*. Additionally, all App Servers must be configured to use digest authentication, which is the default.

1.4.5 Features Not Part of the TOE

MarkLogic Server must be configured so it does not use any features that are not part of the TOE. For details, see “Not Allowed in the TOE” on page 9.

1.4.6 MarkLogic Server 9.0

The evaluated configuration requires MarkLogic Server Essential Enterprise 9.0.

2.0 Target of Evaluation (TOE)

This chapter describes the target of evaluation (TOE) configuration for MarkLogic Server.

2.1 Overview of the TOE

The target of evaluation (TOE) is the configuration of MarkLogic Server that is certified by the Common Criteria evaluation process as the proper setup of the environment in which an evaluated configuration of MarkLogic Server can run. All of the requirements for setup set forth in this guide must be met for a configuration to be considered an evaluated configuration. This section briefly describes the TOE and includes the following parts:

2.1.1 Common Criteria Evaluation Process

MarkLogic Server has gone through a rigorous process for the Common Criteria evaluation. The process includes detailed specifications and testing of the security architecture and implementation of MarkLogic Server. It also includes processes for development, support, and maintenance of the product through all phases of product development. These tests and processes are conducted by MarkLogic Corporation and by the Common Criteria evaluation labs. They follow the process outlined in the Common Criteria Evaluation Methodology (CEM). The documents describing this process are available at http://www.commoncriteriaportal.org.

2.1.2 Security Features of MarkLogic Server

MarkLogic Server is designed as a multi-user system, where each user can only see content or execute code according to the security policy implemented in the configuration. MarkLogic Server has many security features, including:

- auditing
- last-login database
- role-based security model to protect documents and code evaluation
- session-level limits
- encryption at rest

- element level security

For details on the MarkLogic Server role-based security model, see *Security Guide*. For details on administrative procedures in MarkLogic Server, including security administrative procedures, see the *Administrator's Guide*.

2.2 Not Allowed in the TOE

The MarkLogic Server TOE was tested in a secure configuration that specifically excludes certain product capabilities and functionality that might make the system more vulnerable to attack. The following features of the TOE should not be enabled or used in an evaluated configuration to ensure a secure configuration. Note that all system administration tasks must be performed by an Authorized Administrator, as described in "Authorized Administrator" on page 5, according to the guidance described in this guide and in the rest of the MarkLogic Server documentation. Excluded functionality is as follows:

- WebDAV Servers are not part of the TOE; do not create any WebDAV servers in an evaluated configuration. The rationale for excluding WebDAV servers is not any inherent problem with MarkLogic Server, but rather with the clients that access a WebDAV Server. WebDAV servers require access by WebDAV clients, and WebDAV clients are not nearly as mature as web browsers and often do not have very secure implementations. The warning not to create a WebDAV Server in an evaluated configuration is specifically to ensure there is no possibility of WebDAV client access to the TOE. While these clients are not provided as part of the TOE, they are freely available, and therefore the Administrator must take action to ensure there is no possibility of WebDAV client use with the TOE.
- Basic authentication and application-level authentication are not part of the TOE; all App Servers (HTTP Servers, XDBC Servers, and ODBC Servers) in an evaluated configuration must use digest authentication. Digest authentication (what the TOE requires) is the default. For details on configuring HTTP, XDBC, or ODBC Server authentication, see the *Administrator's Guide*.
- UDFs (user-defined functions) are not part of the TOE. MarkLogic includes an interface to create UDFs to perform custom aggregate tasks, written in C++, but that interface is not allowed in the TOE.

2.3 Admin Interface, Admin API, and Security API Must Run With HTTPS

Any administration activities on the MarkLogic Server TOE must be performed on an App Server that is configured to use Transport Layer Security (TLS), which allows communication over HTTPS. For information about configuring the Admin Interface to use TLS (HTTPS), see "Configure the Admin App Server to Use HTTPS" on page 13.

Additionally, if you are using the Admin API, Security API, PKI API, or the Admin Built-in functions to perform TOE Security Functions, the HTTP or XDBC servers on which the Admin API, Security API, PKI API, or Admin Built-In API code runs must be configured to use HTTPS. For details on configuring App Servers, see the *Administrator's Guide*.

2.4 TOE Version

The evaluated configuration of MarkLogic Server must run on the following version:

9.0, Essential Enterprise 9

Additionally, the TOE must be installed on the platform supported in the evaluated configuration, as specified in “MarkLogic Server TOE Platform” on page 6.

Any software updates, patches, fixes, or changes from this configuration will render the TOE out of is evaluated configuration.

2.5 TOE Assumptions

The following assumptions (from section 3.1 of the *Security Target*) are made about the TOE:

- A.NO_EVIL
- A.OS_TIME
- A.TRUSTED_OS
- A.NO_GENERAL_PURPOSE
- A.PHYSICAL
- A.AUTH
- A.CLIENT

2.5.1 A.NO_EVIL

TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

2.5.2 A.OS_TIME

The OS in the environment shall be able to provide reliable time stamps for use by the TOE.

2.5.3 A.TRUSTED_OS

The underlying OS is trusted to provide protection of the DBMS processes and stored data from other processes running on the underlying OS.

2.5.4 A.NO_GENERAL_PURPOSE

It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the DBMS, other than those services necessary for the operation, administration and support of the DBMS.

2.5.5 A.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

2.5.6 A.AUTH

Passwords are encrypted during the authentication process.

2.5.7 A.CLIENT

The web browsers used to access the Admin Interface perform correctly such that when the browser is closed, the active Admin session is terminated. Client applications used to access the Admin API, Security API, and PKI API will perform correctly and when the application is closed, the active Admin session will be terminated.

3.0 Installing MarkLogic Server in an Evaluated Configuration

This chapter describes the steps needed to install MarkLogic Server in an evaluated configuration.

3.1 Ensure that All TOE Requirements Are Met

As described in "TOE Requirements" on page 6, all of the requirements for the target of evaluation must be met. In particular, make sure that the platform is supported in the evaluated configuration (see "MarkLogic Server TOE Platform" on page 6) and make sure none of the excluded features are being used (see "Not Allowed in the TOE" on page 9). As noted in Section 1.2 of the *Installation Guide*, MarkLogic Server assumes it has all the resources of the machine on which it is installed available to it. As such, ensure prior to installation there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE platform, other than those services necessary for the operation, administration, and support of the TOE.

3.2 Download the TOE

Download the TOE from developer.marklogic.com/download. Ensure that the TOE version is the same as described in "TOE Requirements" on page 6.

Once downloaded, contact MarkLogic Technical Support (support@marklogic.com) to get the SHA-256 hash corresponding to the installation binary you downloaded. MarkLogic Technical Support will supply you with the SHA-256 hash as well as instructions to verify the download corresponds to the appropriate SHA-256 hash.

3.3 Run Installation Process

Run the installation process as described in the *Installation Guide*. When it is time to enter the license key, make sure you have a license key for Essential Enterprise. Contact your sales representative or MarkLogic Support for information about obtaining a license key.

Warning: When the installation prompts you for a username and password for the initial user, what you enter will be the username and password for the initial authorized administrator for your evaluated configuration. Additionally, it prompts you for the realm (set to `public` by default), which is used in calculating the digest passwords—any subsequent change in the realm would invalidate all existing passwords. As the authorized administrator is assumed to be non-hostile, make sure you take the appropriate precautions with guarding the credentials of this authorized administrator.

3.4 Configure the Admin App Server to Use HTTPS

After completing the installation and starting MarkLogic Server, perform the following steps to configure HTTPS on the Admin App Server:

1. Log into the Admin Interface by accessing port 8001 on a host in which MarkLogic Server runs (for example, `http://my-server:8001`).
2. Select Clusters > *host-name* and ensure that FIPS-mode is enabled. If it is not enabled, then enable it.
3. Select Groups > Default > App Servers > Admin from the left tree menu.
4. Follow the procedures in Configuring SSL on App Servers in the *Security Guide* to configure SSL on the Admin Server.

4.0 Technical Support

MarkLogic provides technical support according to the terms detailed in your Software License Agreement or End User License Agreement.

We invite you to visit our support website at http://help.marklogic.com to access information on known and fixed issues, knowledge base articles, and more. For licensed customers with an active maintenance contract, see the Support Handbook for instructions on registering support contacts and on working with the MarkLogic Technical Support team.

Complete product documentation, the latest product release downloads, and other useful information is available for all developers at http://developer.marklogic.com. For technical questions, we encourage you to ask your question on Stack Overflow.

5.0 Copyright

MarkLogic Server 9.0 and supporting products.
Last updated: April 28, 2018

COPYRIGHT

This technology is protected by U.S. Patent No. 7,127,469B2, U.S. Patent No. 7,171,404B2, U.S. Patent No. 7,756,858 B2, and U.S. Patent No 7,962,474 B2, US 8,892,599, and US 8,935,267.

The MarkLogic software is protected by United States and international copyright laws, and incorporates certain third party libraries and components which are subject to the attributions, terms, conditions and disclaimers set forth below.

For all copyright notices, including third-party copyright notices, see the Combined Product Notices for your version of MarkLogic.