Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

Rubrik Security Cloud- Private v2.3

Version 1.0, 04 June 2024

Document reference: AISEP-CC-CR-2024-EFT-T037-CR-V1.0
(Certification expires five years from certification report date)

cyber.gov.au

Table of contents

Executive summary

This report describes the findings of the IT security evaluation of Rubrik Security Cloud – Private (SC-P) v2.3 against Common Criteria EAL2+ALC_FLR.2.

The Target of Evaluation (TOE) is Rubrik Security Cloud – Private v2.3. The TOE permits administration and management of multiple Rubrik clusters through a single web user interface. A Rubrik cluster is a collection of objects that includes sources from where data is being backed up, targets where backups are stored, and security principals, the users and service accounts, that manages the cluster. The TOE is a software product that runs on an on-premises virtual machine (VM).

This report concludes that the TOE has complied with the Common Criteria (CC) evaluation assurance level EAL2 augmented with ALC_FLR.2 and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australian Information Security Evaluation Program (AISEP).

The evaluation was performed by Teron Labs and was completed on 2 May 2024.

With regard to the secure operation of the TOE, the Australian Certification Authority (ACA) recommends:

- potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed
- the users should make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings
- the users must maintain the confidentiality, integrity and availability of security relevant data for TOE initialisation, start-up and operation if stored or handled outside the TOE
- system auditors should review the audit trail generated and exported by the TOE periodically
- the users should verify the integrity of the TOE software prior to installation by comparing the MD5 hash of the downloaded software against the value available from Rubrik.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target and read this Certification Report prior to deciding whether to purchase the product.

Introduction

Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

Purpose

The purpose of this Certification Report is to:

- report the certification of results of the IT security evaluation of the TOE against the requirements of the Common Criteria
- provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target [6] which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

Identification

The TOE is Rubrik Security Cloud – Private (SC-P) v2.3.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	Rubrik Security Cloud – Private (SC-P)
Software version	v2.3
Security Target	*Rubrik Security Cloud – Private v2.3 Security Target Version 1.0, 09 May 2024*
Evaluation Technical Report	*Evaluation Technical Report Rubrik Security Cloud Private dated 02 May 2024* Document reference EFT-T037-ETR 1.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Conformant and Part 3 Conformant, April 2017, Version 3.1 Rev 5
Methodology	Common Methodology for Information Technology Security, April 2017 Version 3.1 Rev 5
Conformance	EAL 2 augmented with ALC_FLR.2 (Flaw reporting procedures)
Developer	Rubrik Inc.

	3495 Deer Creek Road Palo Alto, CA 94304 United States of America
Evaluation facility	Teron Labs Pty Ltd Unit 3, 10 Geils Court Deakin ACT 2600 Australia

Target of Evaluation

Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, the scope of evaluation, its security policies and its secure usage.

Description of the TOE

The TOE is Rubrik Security Cloud – Private (SC-P) v2.3.

The Target of Evaluation (TOE) permits administration and management of multiple Rubrik clusters through a single web user interface. A Rubrik cluster is a collection of objects that includes sources from where data is getting backed up, targets where backups are stored, and security principals, the users and service accounts, that manages the cluster.

Rubrik Security Cloud - Private (SC-P) provides a global management view of the daily operations of the connected Rubrik clusters. The SC-P software applications monitor the protection and compliance status of Rubrik clusters. Generate reports and charts using current and historical data about the health, protection and compliance status of all of the objects that the Rubrik clusters protect.

The TOE's major security features consist of:

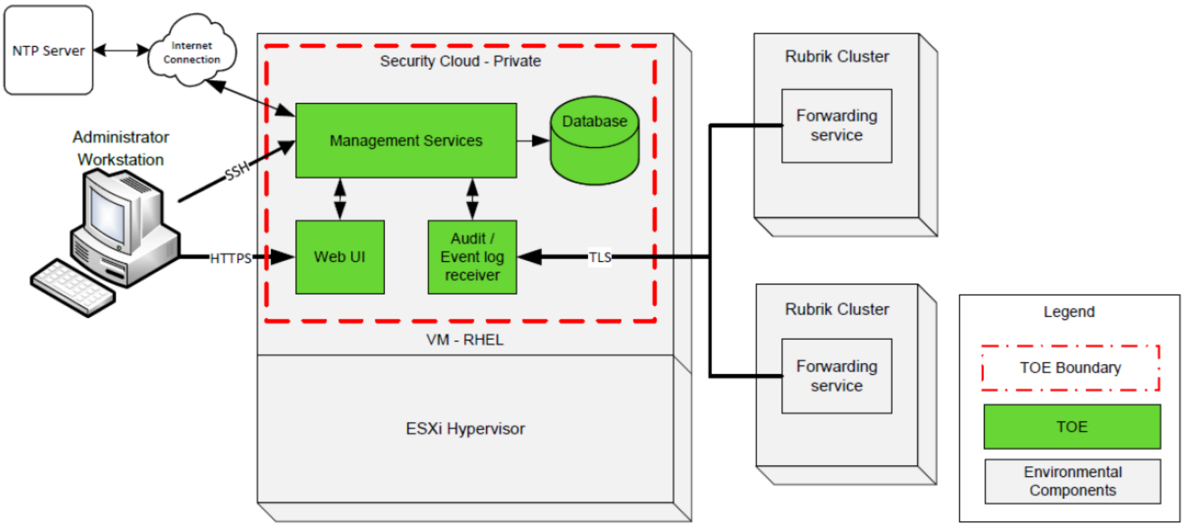
- Web Admin Console
  - The Web Admin Console is a web-based graphical interface used to configure and manage the TOE's security functionality.
  - The Web Admin Console can also be configured to display a custom advisory warning when accessing the login page.
- Local Authentication and Identification
  - The TOE requires that users must be successfully authenticated and identified before the user is allowed to perform any other TSF-mediated actions.
- Cryptographic Support
  - A cryptographic module is used by the TOE for secure communication via TLS and SSH.

TOE Functionality

The TOE functionality that was evaluated is described in section 1.4.2 of the Security Target [6].

TOE physical boundary

The TOE physical boundary is shown below. TOE architecture components listed are located within the Web UI and Audit/Event Log Receiver sections of the TOE.



TOE Architecture

Rubrik Security Cloud - Private (SC-P) runs on an on-premises Virtual Machine (VM), and consists of the components described in the following table. The TOE physical boundary is identified for each component

Component	Description	Physical Boundary Location
Dashboard	Top-down view of all Rubrik clusters using aggregated summary information. Provides a large screen-type view of overall events, compliance, capacity, and alerts.	Web UI
Clusters	Status-at-a-glance summary view of each of the Rubrik clusters and the ability to take a closer look at a selected cluster.	
Inventory	Summary view of the inventory list of data sources on all Rubrik clusters. When this feature is enabled for the PMC account, the Inventory tab and the feature inventory card are available.	
SLA Domains	Continually updating view of all SLA Domains created on all Rubrik clusters that are managed by SC-P. The SLA Domain tab is available when this feature is enabled for the SC-P account.	Audit/ Event Log Receiver
Events	Continually updating view of all events on all Rubrik clusters, with filters to focus on a specific Rubrik cluster, event, protection object, or user.	
Reports	Customizable reports and charts. Use reports for auditing purposes and to get a snapshot view of specific events on Rubrik clusters.	Web UI

Clarification of scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The scope of the evaluation was limited to those claims made in the Security Target [6].

Non-evaluated functionality and services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

Australian Government users should refer to the *Australian Government Information Security Manual* [4] for policy relating to using an evaluated product in an unevaluated configuration.

Security

The TOE Security Policy is a set of rules that defines how information within the TOE is managed and protected. The Security Target [6] contains a summary of the evaluated functionality.

Usage

Evaluated configuration

Instructions for using the TOE in the evaluated configuration are provided in the *Rubrik Security Cloud – Private v2.3 Guidance Documentation Supplement, Version 1.0, 09 May 2024* [5].

Software delivery procedures

The TOE is delivered to customers in the form of a *.zip* or *.ova* file. The download can be checked by comparison with a MD5 hash provided on the Rubrik website.

Installation of the TOE

The *Guidance Documentation Supplement* [5] contains all relevant information for the secure configuration of the TOE.

Version verification

The Rubrik software version evaluated is described as v2.3 but it should be noted that in full detail the version is 2-3-0-29. The version string “2-3-0-29” is expected in the virtual machine image filenames.

Documentation and guidance

The *Guidance Documentation Supplement* [5] available from Rubrik must be used as guidance on the secure installation and secure use of the TOE in the evaluated configuration. Additional guidance documents are referenced in the supplement documentation.

Generic Common Criteria information is available at https://www.commoncriteriaportal.org.

The *Australian Government Information Security Manual* is available at https://www.cyber.gov.au/ism [4].

Secure usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

- the IT environment provides the TOE with the necessary reliable timestamps
- the TOE is located within a controlled access facility
- the TOE software will be protected from unauthorized modification
- there are one or more competent individuals assigned to manage the TOE and the security of the information it contains
- the users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.

Evaluation

Overview

This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

Evaluation procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the *Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3* [1, 2].

Testing methodology was drawn from *Common Methodology for Information Technology Security, April 2017 Version 3.1 Revision 5* [3].

The evaluation was carried out in accordance with the operational procedures of the Australian Information Security Evaluation Program [9]. In addition, the conditions outlined in the *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security* were also upheld [8].

Functional testing

To gain confidence that the developer testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining the test coverage, test plans and procedures, and expected and actual results. The evaluators found that the developer tests covered all Security Functional Requirements specified in the Security Target.

The evaluators examined the TOE prior to testing and determined that the test configuration was consistent with the configuration under evaluation as specified in the Security Target. The evaluators followed the user installation and configuration guidance to ensure that the TOE had been installed correctly and was in a known state prior to conducting testing.

The evaluators drew upon the developer testing evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers. The evaluators also devised and conducted additional functional testing.

Penetration testing

A vulnerability analysis of the TOE was conducted in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE.

The evaluator performed a vulnerability analysis of the TOE in order to identify any obvious security vulnerability in the product, and if identified, to show that the security vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible security vulnerabilities in publicly-available information.

The following factors have been taken into consideration during the penetration tests:

- time taken to identify and exploit (elapsed time)
- specialist technical expertise required (specialist expertise)
- knowledge of the TOE design and operation (knowledge of the TOE)
- window of opportunity
- IT hardware/software or other equipment required for exploitation.

Certification

Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

Assurance

EAL2 provides assurance by providing a full Security Target and an analysis of the Security Functional Requirements (SFRs) in that Security Target, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TOE Security Functionality (TSF), evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis (in addition to the search of the public domain), and independent testing based upon more detailed TOE specifications.

Certification result

Teron Labs **has determined** that the TOE upholds the claims made in the Security Target [6] and **has met** the requirements of Common Criteria EAL2 augmented with ALC_FLR.2 (Flaw reporting procedures).

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the Evaluation Technical Report [7], the Australian Certification Authority **certifies** the evaluation of Rubrik Security Cloud – Private v2.3 performed by the Australian Information Security Evaluation Facility, Teron Labs.

Certification is not a guarantee of freedom from security vulnerabilities.

Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian Government users. For further guidance, Australian Government users should refer to the *Australian Government Information Security Manual* [4].

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

In addition to ensuring that the assumptions concerning the operational environment are fulfilled, and the guidance document is followed, the Australian Certification Authority also recommends:

- potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed
- the users should make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings

- the users must maintain the confidentiality, integrity and availability of security relevant data for TOE initialisation, start-up and operation if stored or handled outside the TOE
- system auditors should review the audit trail generated and exported by the TOE periodically
- the users should verify the integrity of the TOE software prior to installation by comparing the MD5 hash of the downloaded software against the value available from Rubrik.

Annex A – References and abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017, Version 3.1 Revision 5*

2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5*

3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5*

4. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism

5. *Rubrik Security Cloud – Private v2.3 Guidance Documentation Supplement, Version 1.0, 09 May 2024*

6. *Rubrik Inc. Security Cloud – Private v2.3 Security Target, Version 1.0, 09 May 2024*

7. *Evaluation Technical Report - EFT-T037-ETR V1.0 dated 2 May 2024*

8. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2-July-2014*

9. *AISEP Policy Manual (APM):* https://www.cyber.gov.au/sites/default/files/2023-03/2022_AUG_REL_AISEP_Policy_Manual_6.3.pdf

Abbreviations

AISEP	Australian Information Security Evaluation Program
ACA	Australian Certification Authority
ALC_FLR	Assurance in Life Cycle – Flaw Remediation
ASD	Australian Signals Directorate
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
EAL2	Evaluation Assurance Level 2
MD5	Message Digest #5 – 128 bit non-cryptographic hash function
.ova	Open Virtual Appliance format for virtual machine
PMC	Polaris / Rubrik Management Console
SC-P	Security Cloud – Private (by Rubrik)
SFR	Security Functional Requirement
SLA	Service Level Agreement
ST	Security Target document
TOE	Target of Evaluation

TSF	TOE Security Functionality
.zip	Compressed archive file