Agenzia per la Cybersicurezza Nazionale

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 5/23

(Certificate No.)

Prodotto: Qumulo Core v5.1.1

(Product)

Sviluppato da: Qumulo, Inc.

(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL2+
(ALC_FLR.2)

p. il Direttore Generale
dell'ACN

Il Vice Direttore Generale
dell'ACN
(A. Ciardi)

Roma, 7 marzo 2023

[ORIGINAL SIGNED]

This page is left intentionally blank

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Qumulo Core v5.1.1

OCSI/CERT/CCL/10/2021/RC

Version 1.0

7 March 2023

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	07/03/2023

2 Table of contents

3 Acronyms

3.1 National scheme

DPCM	Decreto del Presidente del Consiglio dei Ministri
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Arrangement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Other acronyms

AD	Active Directory
API	Application Programming Interface

CLI	Command Line Interface
CSRF	Cross-site Request Forgery
FTP	File transfer Protocol
FTPS	File Transfer Protocol Secure
GB	Gigabyte
GUI	Graphical User Interface
HDD	Hard Disk Drive
HTTP	Hyper Text Transfer Protocol
ID	Identifier
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
NFS	Network File System
NTP	Network Time Protocol
NVMe	Non-Volatile Memory Express
OS	Operating System
PC	Personal Computer
PS	Professional Services
RAM	Random-Access Memory
RC	Rapporto di Certificazione
REST	Representational state transfer
SHA	Secure Hash Algorithm
SMB	Server Message Block
SMR	Shingled Magnetic Recording
SSD	Solid-State Drive
TB	Terabyte
TLS	Transport Layer Security

UI	User Interface
USB	Universal Serial Bus
XSS	Cross-site Scripting

4 References

4.1 Normative references and national scheme documents

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

4.2 Technical documents

[AGD] Guidance Documentation Supplement Evaluation Assurance Level (EAL): EAL2+, Version 0.11, 30 November 2022

[DEL] Secure Delivery Document Evaluation Assurance Level (EAL): EAL2+, Version 0.6, 30 August 2022

[ETR] “Qumulo Core v5.1.1” Evaluation Technical Report, v3, CCLab Software Laboratory, 14 December 2022

[ST] Security Target Qumulo Core v5.1.1, Version: 0.22, Date: 6 March 2023

5 Recognition of the certificate

5.1 European recognition of CC certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT-Products. A higher recognition level for evaluations beyond EAL4 is provided for IT-Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under SOGIS-MRA for all declared assurance components.

5.2 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA]) was ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA for all declared assurance components.

6 Statement of certification

The Target of Evaluation (TOE) is the product “Qumulo Core v5.1.1”, also referred to in the following as “Qumulo Core”, developed by Qumulo, Inc..

The TOE is a software-only TOE and is comprised of Qumulo Core v5.1.1. Qumulo Core is a file data platform that is highly scalable to store files of all sizes. Qumulo Core is run with multiple nodes to provide data redundancy and system resiliency along with file backup and recovery. Qumulo Core performs continuous replication across storage clusters in order to provide recovery in the event that 1-2 drives fail or 1 node fails. It also performs audit logging and can integrate its auditing features with standard monitoring systems, such as syslog.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL2, augmented with ALC_FLR.2, according to the information provided in the Security Target [ST] and in the configuration shown in Annex B of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product “Qumulo Core v5.1.1” to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Qumulo Core v5.1.1
Security Target	“Qumulo, Inc. Qumulo Core v5 Security Target” v 0.22 [ST]
Evaluation Assurance Level	EAL2 augmented with ALC_FLR.2
Developer	Qumulo, Inc.
Sponsor	Corsec Security, Inc.
LVS	CCLab Software Laboratory
CC version	3.1 Rev. 5
PP conformance claim	No compliance declared
Evaluation starting date	26 July 2021
Evaluation ending date	3 January 2023

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description, please refer to the Security Target [ST].

The TOE Qumulo Core v5.1.1 is a file data platform that is highly scalable to store files of all sizes. Qumulo Core is run with multiple nodes to provide data redundancy and system resiliency along with file backup and recovery. It uses real-time analytics to provide instant visibility into data and users. Qumulo software assigns aggregation of real-time metadata to all data as they are ingested, giving users real-time insight into their system without performance degradation or long file system scans. The hybrid cloud file storage provides a single namespace, exposed across protocols, that provides a vast number of users centralized access to files whether the data is on-premise, multi-site, or in the cloud. This allows users to simplify storage management by symmetrically scaling capacity and

performance, removing data silos to eliminate a tangle of multi-volume mounts, and scaling to billions of files across the data center and cloud.

Qumulo Core provides the ability to take snapshots of the current state of the file system or directory at a given point in time. It provides the ability to restore single files and whole directories with snapshots. Qumulo Core performs continuous replication across storage clusters in order to provide recovery in the event that 1-2 drives fail or 1 node fails. It also performs audit logging and can integrate its auditing features with standard monitoring systems, such as syslog.

For a detailed description of the TOE, consult sections 1.3 and 1.4 of the Security Target [ST]. The most significant aspects are summarized below.

7.3.1 TOE architecture

The TOE is made of several different layers. The first layer is data access, which contains SMB, NFS, and FTP protocols. The SMB, NFS, and FTP protocols exist as independent and scalable resources on each node of a Qumulo cluster. TOE users see a single namespace which can expand in capacity and performance. This namespace can be accessed from any workstation or other computing device running Windows, Linux, or Mac OS. The authentication layer supports Active Directory connections. Qumulo data services integrate with these global identity systems as managed by customers, enabling access to be controlled across TOE users and data. Each data access protocol uses a common authentication layer to interact with data stored in the filesystem, enabling users to move between applications, operating systems, and environments. The TOE uses both stateful data access protocols, such as SMB, and stateless data access protocols, such as NFS.

The TOE contains the following feature management interfaces in the management and programmability layer: A web user interface (Web UI), a REST API, and the command line interface QQ CLI. The Web UI is a graphical user interface (GUI) used to manage and configure the TOE. It can be accessed through a web browser using the IP address of the overall cluster or using the IP address of a node. The QQ CLI is the command line interface and offers most management functionality. It can be downloaded from the Web UI as a .zip file. The REST API is an application programming interface (API) used to configure all properties of a system, such as user accounts, snapshot policies, data replication, and data management, gather information about the TOE, and read or write data. REST API can be accessed using an API client such as Postman. The TOE also contains the SMB, NFS, and FTP interfaces for file management within the designated shares.

SMB shares are used to share, read, and write files to a remote host over a local area network (LAN). The share displays files and directories the TOE user has permissions to access. If a TOE user does not have read permissions for a directory, then it is hidden from the TOE user’s view. Files can be shared within the TOE using NFS as well. NFS exports are used to export directories from an NFS server’s local hard disk to an NFS client. The NFS client mounts the directory so it can be accessed like any directory. The directory can be mounted on multiple clients, allowing all of the clients to share files with each other using this directory. The TOE allows access to the NFS share based on the client’s IP address, which is mapped to a local account in the TOE. FTP is a third method to share files. An FTP server offers access to a directory and its subdirectories. TOE users can connect to the FTP server with an FTP client to share files between hosts.

The TOE boundary consists of 4 nodes of the Qumulo Core software. One node is considered the Initiator Node while the other 3 are the Participant Nodes. Any node can act as the Initiator Node for a particular protocol request.

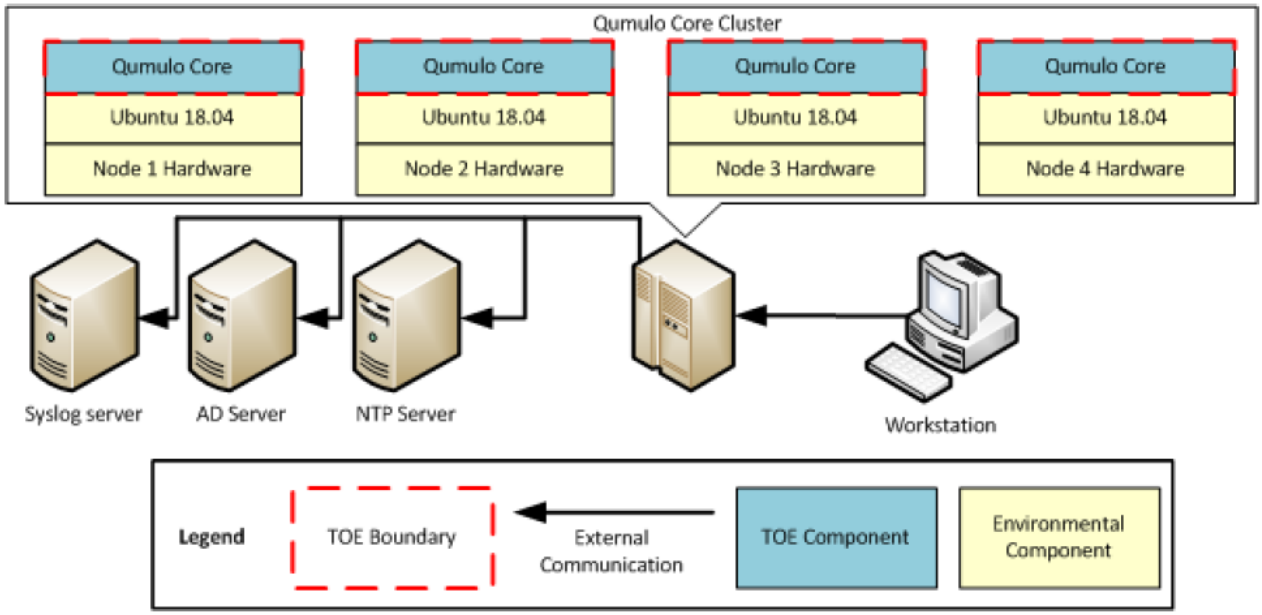

Figure 1 - Physical TOE Boundary

Figure 1 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components abovementioned of the TOE.

7.3.2 TOE security features

The logical boundary of the TOE is broken down into the following security classes which are further described in sections 6 and 7 of the Security Target [ST]. SFRs implemented by the TOE are usefully grouped under the following security function Classes:

- **Security Audit**: The TOE generates audit records for startup and shutdown of audit functions, successful authentication, unsuccessful authentication, filesystem operations and management operations. The unique file ID in audit logs is generated by the OS when a file is created. The file ID does not depend on the file name. It is able to associate audit records with the TOE user that caused the audited event. The TOE relies on the Linux OS as a time source to provide reliable timestamps.
- **User Data Protection**: The TOE enforces the Access Control Security Functional Policy (SFP) to provide access control on TOE users who are accessing nodes, shares, files, and directories. TOE users are given roles which determine their access permissions to objects. Files and directories are written to a node based on file name and directory name.
- **Identification and Authentication**: When a TOE user enters incorrect credentials, the TOE will block authentication requests on that connection for 1 second before allowing the TOE user to login again. The TOE maintains usernames, roles, and passwords as security attributes belonging to an individual user. All passwords must be secure and meet requirements detailed in section 7.1.3 of the Security Target [ST]. Passwords are obscured by bullets when entered in the Web UI. The TOE allows the user to use the API calls listed in section 7.1.3 of the Security Target [ST] prior to authentication and identification as well as the qq version QQ CLI command to determine the version of the TOE. All other actions cannot be performed until the

TOE user is properly authenticated and identified. The TOE uses two authentication mechanisms: local authentication and directory-based authentication.

- **Security Management**: The TOE restricts all management functionality to the Administrators Role while allowing the Observers Role to query TOE settings. The Data-Administrators Role has access to all file and share management. The TOE enforces restrictive default values for all security attributes. There are three pre-defined roles maintained by the TOE: Administrators Role, Data-Administrators Role, and Observers Role. Additionally, the TOE allows for custom roles to be created.
- **Protection of the TSF**: The TOE preserves a secure state when 1-2 drives fail or when 1 node fails. The TOE provides timestamps for audit logs and utilizes the Linux system time to get the accurate time.
- **Resource Utilization**: The TOE ensures full functionality when either 1-2 drives or 1 node fails.
- **TOE Access**: TOE users can manually terminate sessions in Web UI and QQ CLI. In Web UI this can be done by clicking “sign out”.
- **Trusted Path/Channel**: Communication with the REST API, Web UI, and QQ CLI interfaces are done over a secure channel using HTTP over TLS. Connections to the SMB interface is done over SMBv3 and connections to the FTP interface are secured with FTPS.

7.4 Documentation

The guidance documentation specified in Annex A is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in section 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] does not claim conformance to any Protection Profile.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

All Security Functional Requirements (SFR) have been selected from CC Part 2 [CC2].

Please refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the

Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab Software Laboratory.

The evaluation was completed on 15 December 2022 with the issuance by LVS of the Evaluation Technical Report [ETR] that has been approved by the Certification Body on 3 January 2023. Then, the Certification Body issued this Certification Report. After the conclusion of the evaluation, a public version of the Security Target including minor editorial changes was delivered on 6th March 2023.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist. It remains a probability (the smaller, the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR] issued by the LVS CCLab Software Laboratory and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "Qumulo Core v5.1.1" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL2 augmented with ALC_FLR.2, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in Annex B.

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL2 augmented with ALC_FLR.2.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Security-enforcing functional specification	ADV_FSP.2	Pass
Basic design	ADV_TDS.1	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Use of a CM system	ALC_CMC.2	Pass
Parts of the TOE CM coverage	ALC_CMS.2	Pass
Delivery procedures	ALC_DEL.1	Pass
Flaw reporting procedures	*ALC_FLR.2*	Pass
Tests	**Class ATE**	Pass
Evidence of coverage	ATE_COV.1	Pass

Assurance classes and components		Verdict
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Vulnerability analysis	AVA_VAN.2	Pass

Table 1 - Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in section 6 (Statement of Certification).

Potential customers of the product “Qumulo Core v5.1.1” are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the Security Objectives for the operational environment specified in section 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the Assumptions described in section 3.3 of the Security Target [ST] are respected.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, Annex A includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([AGD]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE delivery

The delivery steps and the procedures that are necessary to maintain security when distributing the TOE to the customer are described in the Delivery Procedures document ([DEL]).

For new installations performed by Qumulo Professional Services (PS), the PS installers use USB drives with a copy of the TOE software for installation on approved hardware. For customer self-installations and software upgrades, the TOE software is posted to the public releases folder on the Qumulo Box website (https://qumulo.app.box.com/) that is secured by a static password and an HTTPS connection. The link and password to the Public folder are delivered to the customer on a private Slack channel over an HTTPS connection and posted to the Qumulo Care Community website that requires a valid user account to access the page, which is served over an HTTPS connection.

TOE documentation is only provided in softcopy, which is available on the Qumulo Care Community website over a secure connection at https://care.qumulo.com.

Node hardware that is ordered through Qumulo, Inc. is shipped by third-party shipping companies.

4-node shipments are placed on a single pallet and shrink wrapped together for secure shipment. Shipping and tracking information is provided to customers so they know when to expect the delivery. Orders are usually shipped directly to the customer with limited redirects. The label on the pallet lists the product number, product code, brief description, and Qumulo Core version number for customer verification. Hardware shipped for new orders typically contain the latest version of Qumulo Core and may need to be replaced with the CC-evaluated version. If new nodes are added to an existing cluster, they can be flashed down to the version the rest of the cluster is running on. If the customer is creating a new cluster, any version of Qumulo Core can be installed once the hardware is received.

9.2 Identification of the TOE

If the customer downloads the Qumulo image from the Qumulo Box website, they can verify the TOE has not been tampered with by using a SHA512 checksum that is provided in the Box folder. If the checksums match, the image has not been tampered with during the HTTPS download. If the checksums do not match, the customer should contact Qumulo Support.

If hardware is delivered with the TOE software already installed on it, the customer can verify the version on the shipping label is the CC-evaluated version and inspect the packaging for tampering. If there is a different version installed or the package has been tampered with, the customer should download the Qumulo image from the Qumulo Box website and overwrite the existing installation.

Once a cluster is setup, the customer can confirm they have received the correct version of the TOE by using the Web UI, REST API or QQ CLI to check the version. The customer can view the version currently running via the Web UI by looking in the top right corner next to

"Qumulo Core". The version can also be viewed from the QQ CLI by typing the "qq version" command or from the REST API by using the /v1/version API call.

9.3 Installation, initialization and secure usage of the TOE

TOE installation, configuration and operation should be done following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the following documents contain detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure operation of the TOE in accordance with the security objectives specified in the Security Target [ST]:

- Guidance Documentation Supplement Evaluation Assurance Level (EAL): EAL2+, Version 0.11, 30 November 2022 [AGD].

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product “Qumulo Core v5.1.1”, developed by Qumulo, Inc.

The name and version number uniquely identify the TOE and its components, constituting the evaluated configuration of the TOE, verified by the Evaluators at the time the tests are carried out and to which the results of the evaluation are applied.

The TOE is a software-only TOE that provides functionality of a Data Protection product. It is comprised of four instances of the Qumulo Core software communicating in a clustered setup. Each instance run on Ubuntu Linux platform in a separate node hardware.

The evaluator has received a pre-installed version of the TOE by the developer consisting of:

- 4 C72T nodes;
- a network switch that supports 10Gb Ethernet;
- other hardware equipment necessary for the setup (such as cables).

Evaluated configuration is a TOE deployed on four Qumulo C72T nodes in the operational environment described in section 10.1.

The Evaluators have been presented with a configuration identical to the one described in the Security Target [ST] in a form of pre-installed C72T nodes sent by the Sponsor. The Ethernet switch has also been provided by the Sponsor. The other materials (NTP, Syslog, AD servers, workstation with Google Chrome) were provided by the Laboratory.

10.1 TOE operational environment

The TOE relies on the operating environment which contains the Linux OS, node hardware, servers, networking equipment, and workstations.

The TOE runs on Ubuntu 18.04 and works best with servers with minimum requirements described on section 1.5 of the Security Target [ST].

For data communication between nodes, a 10G or greater switch is also required.

The TOE requires the following servers in its operating environment:

- a syslog server for uploading the generated audit logs (Kiwi 9.8.0.405 installed on Windows Server 2022);
- an Active Directory server for directory-based authentication (installed on Windows Server 2022, Schema Version 88);
- an NTP server connected to the Linux OS to ensure the time is synchronized with the network.

A workstation is also required for accessing the file shares and managing the TOE through the TOE interfaces. The QQ CLI requires the installation of the local QQ CLI client, which can be downloaded from within the Web UI of the TOE. The REST API requires the installation of a 3rd-party application or customized program used to exercise the REST commands. The Web UI is compatible with Google Chrome 93.0.4577.63 64-bit and above.

Users should refer to section 1.5 of the Security Target [ST] for more details on software and hardware minimum requirements for the TOE operational environment.

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities. For the assurance level EAL2, augmented with ALC_FLR.2, such activities include the following three steps:

- evaluation of the tests performed by the Developer in terms of coverage;
- execution of independent functional tests by the Evaluators;
- execution of penetration tests by the Evaluators.

11.1 Test configuration

The Evaluators executed all the test cases on the test environment which was provided by the Developer. The Developer also provided all the resources needed for testing.

The minimum requirements of the TOE are described in Security Target [ST] section 1.5 and summarized in the Table 2.

System Type	Requirements
Systems with all "non-Volatile Memory Express" (NVMe) drives	• Storage: NVMe drives must support hot plug. At least 6 drives should be used; • Processor: One core per drive, fewer fast cores are better than more slow cores; • Memory: Minimum RAM should be 0.38GB per TB of drive space; • Network: Dual-100G or greater network interfaces; • Power: Redundant power supply units.
Systems with SSDs and HDDs	• Storage: HDD-to-SSD ratio 3:1 or 4:1 for better performance, or up to 6:1 for archiving. Drives must support hot plug. No Shingled Magnetic Recording (SMR) drives. Minimum SSD space should be about 2.5% of HDD space; • Processor: One core per 2 HDDs, fewer fast cores are better than more slow cores; • Memory: Minimum RAM should be 0.38GB per TB of HDD space; • Network: Dual-100G or greater network interfaces for better performance or dual-25G for archiving; • Power: Redundant power supply units.

Table 2 - Hardware requirements

The TOE requires the following components in the operational environment:

- Syslog server Kiwi 9.8.0.405 on Windows Server 2022;
- Active Directory server – OS Windows Server 2022, Schema Version 88;

- NTP server;
- Workstation (General purpose PC): Installed QQ CLI, Google Chrome, REST API client (Postman).

The Evaluators have received a pre-installed version of the TOE by the developer consisting of:

- 4 C72T nodes;
- A network switch that supports 10Gb Ethernet;
- Other hardware equipment necessary for the setup (such as cables).

The Evaluators have prepared the steps present in [AGD] section 2.2.1, 2.2.2 and 2.2.3 and verified that the TOE is installed in accordance with the guidance documents and is in a known state.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer performed extensive test to verify the functionality of the TOE. The general test approach is to provide a specific functional test for each security behaviors of the Security Functional Requirements claimed in the Security Target. The tests focus on covering all security behaviors and ensuring that the functional testing is thorough without being unnecessarily detailed.

An understanding of the internal operations of the TOE is used in the development of functional testing to avoid redundant testing of functions.

Test runs are functional tests conducted externally and manually. Test Procedures include actions taken by the tester through the following external interfaces:

- Web UI;
- QQ CLI;
- REST API;
- NFS;
- SMB;
- FTP.

All of the defined TSFIs are exercised by the following test cases:

- Test Case 01: Identification and Authentication Tests;
- Test Case 02: Security Audit Tests;
- Test Case 03: Security Management Tests;
- Test Case 04: TOE Access;
- Test Case 05: Host Failure;
- Test Case 06: Trusted Path/Channel Tests.

The Evaluators analysed the Developer’s functional tests and coverage and verified they were complete and accurate.

11.2.2 Test coverage

The Evaluators have examined the test coverage evidence and they have verified that the tests identified in the test documentation are accurate and cover all the TSFIs described in the functional specification.

11.2.3 Test results

For each test case, the Developer's test documentation describes its purpose, the relevant TSFI(s) and SFR(s), test prerequisites, step-by-step test procedures, and expected test results.

The actual test results of all Developer's tests were consistent with the expected ones.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Testing approach

The Evaluators ran all tests on the test environment provided by the Developer. The TOE test setup was prepared according to the Developer's test plan and the preparative procedures supplied in the document [AGD]. Before initiating the testing activity, the Evaluators verified that the test environment was properly set up and the TOE was configured correctly and in a known state.

The Evaluators have also selected all of the six Developer tests, and went through the test steps manually, comparing observed results with the expected results.

The Evaluators conducted the following test categories:

- Test Case 01: Identification and Authentication;
- Test Case 02: Security Audit;
- Test Case 03: Security Management;
- Test Case 04: TOE Access;
- Test Case 05: Host Failure;
- Test Case 06: Trusted Path/Channel.

11.3.2 Test results

All Developer's tests were run successfully and the Evaluators verified the correct behavior of the TSFI and correspondence between expected results and achieved results for each test.

All test cases devised by the Evaluators was passed successfully and all the actual test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

The Evaluators have inspected the TOE's configuration and its elements and concluded that the Vulnerability Analysis should specifically focus on the Web UI, REST API and the communication during the usage of third-party protocols SMB and FTP. The QQ CLI, although being a standalone client, relies on the functionality of the REST API available on the back-end, and so does the Web UI.

The Evaluators have designed following attack scenarios:

- Brute force attacks with various logins (Web UI, REST API, SMB, FTP);
- Triggering XSS in the Web UI;
- Triggering CSRF in the Web UI;
- Eavesdropping on communication channel.

The attack scenarios revealed various potential exploits, addressed by the Developer as follows:

- Strict password policies were well documented and enforced;
- Set up of secure communication was enforced;
- The TOE was updated to a newer version, where technical exploits were patched.

Moreover, the Evaluators conducted searching for publicly available information regarding third-party components of the TOE and they found two potential vulnerabilities, which were not considered in the testing activity since they would require an attack potential higher than Basic for their exploitation.

The Evaluators have also conducted a portscan on the TOE using Nmap, identifying some opened ports with active network services. It turned out that one service was used as a basis for the web server of the TOE's GUI. The Evaluators have performed online research for publicly disclosed vulnerabilities, attacking writeups and other information on potential vulnerabilities related to the findings, and concluded, that no potential vulnerabilities could be derived from the acquired information about the TOE in its operational environment.

Based on the vulnerability analysis and the penetration testing results, the Evaluators concluded that none of the identified potential vulnerabilities are applicable to the TOE. The TOE is therefore resistant to an attack potential of Basic in its intended operational environment. Therefore, no exploitable or residual vulnerabilities have been identified.

It is worthwhile to highlight that the identified potential vulnerabilities are not exploitable for the TOE if all of the assumptions described in section 3.3 of Security Target [ST] are fulfilled. Namely, the specific assumption of total trust in TOE users (A.INTERNAL_USERS) has to be verified by the TOE customer in the specific applications and contexts of use.