Agenzia per la Cybersicurezza Nazionale

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti ISO/IEC 15408 Common Criteria (CC) v.3.1 rel. 5

Certificato n. *(Certificate No.)*	06/2024
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/CCL/01/2022/RC, v1.0
Decorrenza *(Date of 1st Issue)*	30 luglio 2024
Nome e Versione del Prodotto *(Product Name and Version)*	Veritas NetBackup v9.1.0.1
Sviluppatore *(Developer)*	Veritas Technologies LLC.
Tipo di Prodotto *(Type of Product)*	Altri dispositivi e sistemi (sistema per il backup dati)
Livello di Garanzia *(Assurance Level)*	EAL2+ (ALC_FLR.2) conforme a CC Parte 3
Conformità a PP *(PP Conformance)*	Nessuna
Funzionalità di sicurezza *(Conformance of Functionality)*	TDS specifico per il prodotto conforme a CC Parte 2

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR
(CCRA recognition for components up to EAL2 and ALC_FLR only)

Riconoscimento SOGIS MRA per componenti fino a EAL4
(SOGIS MRA recognition for components up to EAL4)

Roma, 30 luglio 2024

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)

[ORIGINAL SIGNED]

Il prodotto IT (*Information Technology*) identificato nel presente certificato è stato valutato presso un LVS (Laboratorio per la Valutazione della Sicurezza) accreditato e abilitato/approvato utilizzando la Metodologia Comune per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5. Questo certificato si applica solo alla versione e al rilascio specifici del prodotto nella sua configurazione valutata e unitamente al Rapporto di certificazione completo. La valutazione è stata condotta in conformità alle disposizioni dello Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004) e le conclusioni dell'LVS nel Rapporto di Fine Valutazione sono coerenti con le evidenze addotte. Il presente Certificato non costituisce un sostegno o promozione del prodotto IT da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosca o dia effetto a questo certificato, e nessuna garanzia del prodotto IT, da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosce o dà effetto a questo certificato, è espressa o implicita.

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using Common Methodology for Information Technology Security Evaluation version 3.1 release 5 for conformance to *Common Criteria for Information Technology Security Evaluation version 3.1 release 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of the National scheme for the evaluation and certification of the security in the sector of information technology (Prime Ministerial Decree of 30 October 2003 - Official Journal no. 93 of 27 April 2004) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product, by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.*

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Veritas NetBackup v9.1.0.1

OCSI/CERT/CCL/01/2022/RC

Version 1.0

30 July 2024

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	30/07/2024

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 Agreement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Other acronyms

AES	Advanced Encryption Standard
API	Application Programming Interface

CLI	Command Line Interface
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CS	Customer Support
DB	Database
DRBG	Deterministic Random Bit Generator
GUI	Graphical User Interface
NIST	National Institute of Standards and Technology
OS	Operating System
PDF	Portable Document Format
QA	Quality Assurance
RHEL	Red Hat Enterprise Linux
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
SQL	Structured Query Language
TSP	Trust Service Provider
UI	User Interface
UTC	Coordinated Universal Time
WebUI	Web User Interface
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. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, 21 agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, 21 agosto 2023

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

4.2 Technical documents

[ETR] Evaluation Technical Report Veritas NetBackup v9.1.0.1, VERITAS-025_ETR_v3, CCLab Software Laboratory, 13 May 2024

[GUIDE_ADM] Veritas NetBackup Administrator's Guide, Volume I, Release 9.1, 02 September 2021

[GUIDE_CC] Veritas NetBackup v9.1.0.1 - Guidance Documentation Supplement - Evaluation Assurance Level (EAL): EAL2+ Document Version: 1.1, 15 December 2023

[GUIDE_CODE] Veritas NetBackup Status Codes Reference Guide, Release 9.1, 07 June 2021

[GUIDE_ENCR] Veritas NetBackup Security and Encryption Guide UNIX, Windows, and Linux, Release 9.1, 07 June 2021

[GUIDE_INST] Veritas NetBackup Installation Guide, Release 9.1, 07 June 2021

[GUIDE_REF] Veritas NetBackup Commands Reference Guide, Release 9.1, 07 June 2021

[GUIDE_TRBSH] Veritas NetBackup Troubleshooting Guide UNIX, Windows, and Linux, Release 9.1, 07 June 2021

[GUIDE_WEBUI] Veritas NetBackup Web UI Administrator's Guide, Release 9.1, 11 June 2021

[ST] Veritas NetBackup v9.1.0.1 Security Target - Evaluation Assurance Level (EAL): EAL2+ Document Version: 1.3, 08 May 2024

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 up to EAL4.

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 recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA up to EAL2 and ALC_FLR only.

6 Statement of certification

The Target of Evaluation (TOE) is the product named "**Veritas NetBackup v9.1.0.1**", developed by Veritas Technologies LLC.

The Target of Evaluation (TOE) is an enterprise data backup and recovery system. It provides cross-platform backup functionality for a variety of Windows and Linux operating systems. TOE users can set up periodic or calendar-based schedules to perform automatic, unattended backups for clients across a network. A TOE user can carefully schedule backups to achieve systematic and complete backups over a period of time and optimize network traffic caused by the backups during off-peak hours. The TOE includes both server and client software.

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 version 3.1 Revision 5 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 – Evaluated configuration" 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 named "Veritas NetBackup v9.1.0.1" 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 also review the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Veritas NetBackup v9.1.0.1
Security Target	Veritas NetBackup v9.1.0.1 Security Target - Evaluation Assurance Level (EAL): EAL2+ Document Version: 1.3, 08 May 2024
Evaluation Assurance Level	EAL2, augmented with ALC_FLR.2
Developer	Veritas Technologies LLC.
Sponsor	Corsec Security, Inc.
LVS	CCLab Software Laboratory (Debrecen site)
CC version	3.1 Rev. 5
PP conformance claim	No conformance claimed
Evaluation starting date	January 14, 2022
Evaluation ending date	May 13, 2024

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 and in the configuration shown in "Annex B – Evaluated configuration" of this Certification Report.

7.3 Evaluated product

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

The Target of Evaluation (TOE) is a distributed software, with both client and server components, providing data backup and recovery functionality. Data can be located in many network nodes running different operating systems, such as Linux and Windows. Backup and recovery operations can be configured and scheduled during time by authorised TOE users.

The TOE includes the guidance documentation for establishing the certified configuration [GUIDE_CC].

TOE software components are the following:

- NetBackup Primary Server – This software component resides on a computer that is used to manage the backups, archives, and restores, and is responsible for selecting the NetBackup Media Server to which data is backed-up. The Primary Server contains all binaries and services to allow it to serve in the roles of the Media Server and Client, in addition to its primary function. The NetBackup Primary Server contains the NetBackup catalog, which contains the internal databases with information about NetBackup's backed-up data and configuration.
- NetBackup Media Server – This software component resides on the servers or appliances that are used to store the backed-up data. With two or more NetBackup Media Servers, the network load can be distributed, and performance increased.
- NetBackup Windows Client and NetBackup Linux Client – These software components reside on computers that contain data that needs to be backed up.
- NetBackup Remote Administration Console – This software component resides on a Windows computer that is used to manage the TOE's functionality.
- NetBackup Local Administration Console - This software component resides on the same computer as the Primary Server and is used to manage the TOE's functionality.

TOE users are able to authenticate to the NetBackup Remote Administration Console, NetBackup Local Administration Console, Web User Interface (WebUI), and Command Line Interface (CLI) to manage the TOE. Using these interfaces, TOE users connect to the NetBackup Primary Server to have access to review audit records, manage encryption policies, manage backup policies, restore data from backups, and manage local accounts.

When creating backup policies to control how data on managed systems is backed up, a TOE user must specify the required security attributes to successfully create a backup policy. The TOE will enforce the backup policy on any system the policy is applied to.

During a backup, the target NetBackup Client sends information to the NetBackup Primary Server. The NetBackup Primary Server manages the location of storage that is specified in the backup policy and ensures that the backup data is encrypted for storage. Backups that are created by the TOE are encrypted using the TOE's Federal Information Processing Standards (FIPS)-validated cryptography (https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2340.pdf) certificate 2340. During a restore, TOE users can browse, and then select, the files and directories to recover. The TOE finds the selected files and directories, decrypts them, and restores them to the disk on the target NetBackup Client's system.

For a detailed description of the TOE, refer to sections 1.3 and 1.5 of the Security Target [ST].

7.3.1 TOE architecture

The TOE is a data backup solution running on multiple hardware platforms in the environment that are compliant to the requirements listed in section 1.4 of the Security Target [ST]. The TOE is installed on an internal network as depicted in Figure 1.

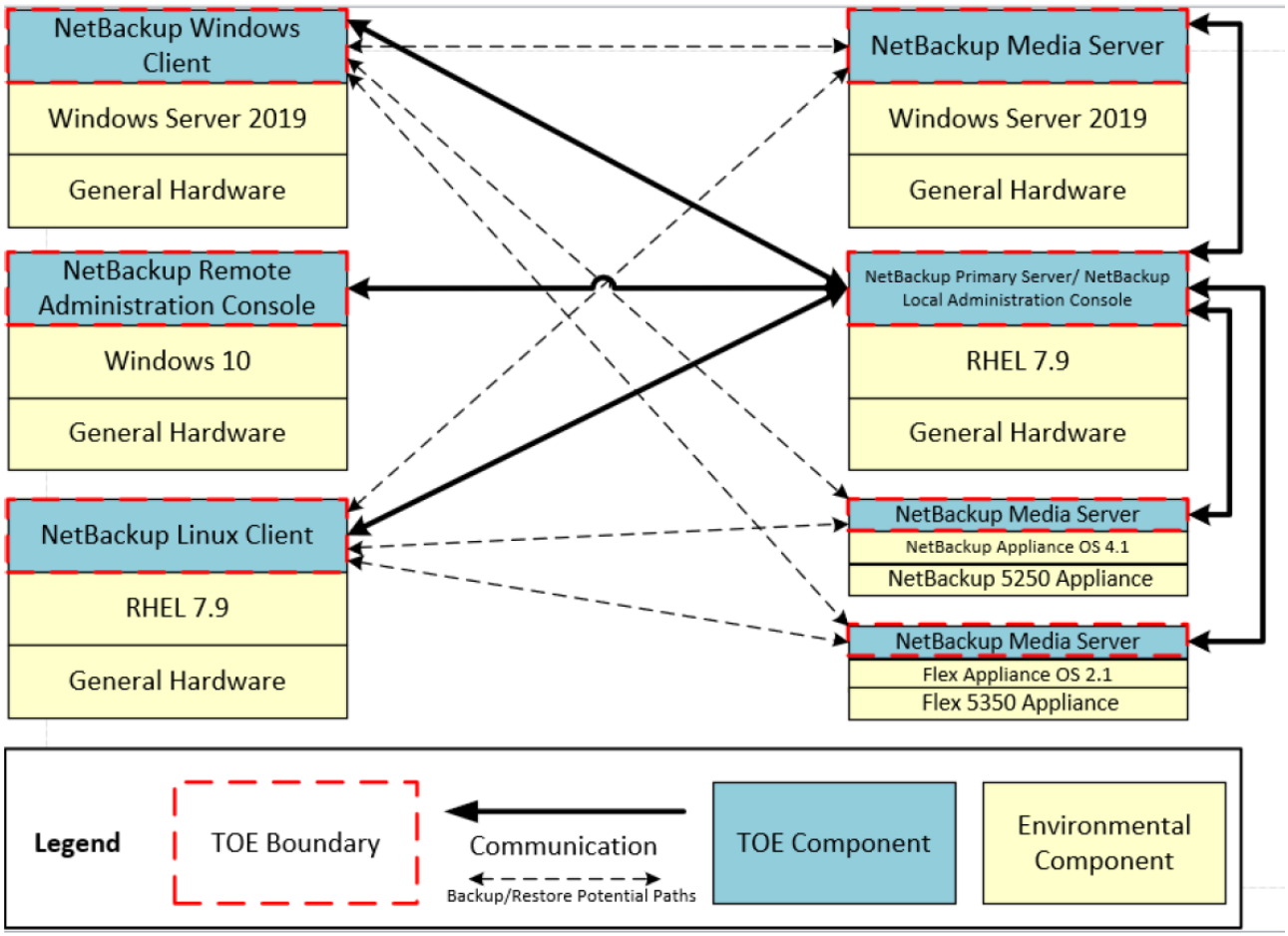

Figure 1 – TOE components and their relationship

7.3.2 TOE security features

Assumptions, threats, and security objectives are defined in section 3 and 4 of the Security Target [ST].

The major security features of the TOE are summarised in the following:

1) Security Audit

Audit entries are generated by the TOE for events related to TSF mediating actions, starting up the TOE, and shutting down the TOE. The recorded events include relevant information to the event include the identity of the TOE user that initiated the action. Audit entries may be reviewed by authorized TOE users. While reviewing the audit data, filters may be applied to control what is being displayed.

2) User Data Protection

The TOE provides backup and restore functionality to TOE users that are controlled using backup policies. Backup policies are access controlled by the TOE to ensure that only authorized TOE users may query, create, modify, or delete them. The TOE will determine access to the backup policies based on the security attributes of the TOE user's account and the backup policy.

3) Identification and Authentication

The TOE ensures that access to TSF-mediated actions is only provided to TOE users that are authenticated and identified before any actions take place within the TOE. While entering a password into the password fields of the TOE, the TOE will obfuscate the input.

4) Security Management

The TOE provides the following management functionality: audit reviewing, managing encryption policies, managing backup policies, restoring backup data, and managing local accounts. When accessing the TOE to manage these areas, the TOE will associate TOE users to the roles that it maintains. This ensures that TOE users will be restricted to the areas of the TOE for which their roles have access. When managing the backup policies or local accounts, the TOE enforces access control on which roles are able to manage the security attributes for the backup policies and local accounts.

5) Protection of the TSF

To ensure the correct time for its operation, the TOE will provide a reliable timestamp, received from the TOE environment, and processed and transmitted in a protected way in every step.

For a detailed description of the security features of the Supervisory Body, please refer to sections 1.5.2 and 7 of the Security Target [ST].

7.4 Documentation

The guidance documentation specified in "Annex A – Guidelines for the secure usage of the product" 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 with any Protection Profile.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3] and are from EAL 2 assurance package, augmented with the CC part 3 components ALC_FLR.2.

All the security functional requirements (SFRs) have been selected from CC Part 2 [CC2] except from family "FDP_BCK_EXT: User Data Backup/Restore" that is CC Part 2 extended.

It is possible to 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 [NIS5] 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 (Debrecen site).

The evaluation was completed on 13 May 2024 with the issuance by LVS of the Evaluation Technical Report [ETR] that has been approved by the Certification Body on 29 May 2024. Then, the Certification Body issued this Certification Report.

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 – Evaluated configuration”.

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; there is a probability, however small, that exploitable vulnerabilities can be discovered after the issuance of the certificate.

The Certification Body informs that a residual vulnerability (not exploitable with the basic attack potential relevant for the claimed assurance level) has been found during the evaluation. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to regularly check 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 [ETR3] issued by the LVS CCLab Software Laboratory (Debrecen site) and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE named "Veritas NetBackup v9.1.0.1" 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 – Evaluated configuration".

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 (augmentation *in italics* in Table 1).

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
Complete functional specification	ADV_FSP.2	Pass
Basic modular 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
Production support, acceptance procedures and automation	ALC_CMC.2	Pass
Problem tracking CM coverage	ALC_CMS.2	Pass
Delivery procedures	ALC_DEL.1	Pass
Flaw reporting procedures	*ALC_FLR.2*	*Pass*
Test	**Class ATE**	Pass
Analysis 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
Advanced methodical 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 "Veritas NetBackup v9.1.0.1" are suggested to properly understand the specific purpose of the certification by 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 Assumptions described in section 3.3 of the Security Target [ST] shall be satisfied.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, "Annex A – Guidelines for the secure usage of the product" includes a number of recommendations relating to delivery, installation, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE (Ref. [GUIDE_CC]). [GUIDE_CC] refers also to the additional guidance documents [GUIDE_ADM], [GUIDE_REF], [GUIDE_CODE], [GUIDE_ENCR], [GUIDE_WEBUI], [GUIDE_INST], [GUIDE_TRBSH].

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 Veritas NetBackup v9.1.0.1 TOE software is available for download through the Veritas Support website. The TOE is identified on the Downloads page of the Veritas Support website as Veritas NetBackup.

There are two separate packages available for download depending on the server machine type to be installed on. To verify the version of the product installed and that the product received is the product that they ordered, customers can run /usr/openv/netbackup/version (for servers) and /usr/openv/netbackup/bin/version (for clients) on Linux machines. To verify the version on Windows, customers can use the Windows Backup, Archive and Restore console by navigating to Help > About Backup, Archive and Restore.

Customers can download a list of checksums (NetBackup_9.1_Download_README-Info.txt) from the Veritas Support site[1]. Customers can also verify the .zip or .tar files downloaded from the Downloads page by performing the following steps depending on the platform.

In order to verify that the Windows .zip file has not been tampered with, perform the following steps in Windows:

1. Copy the SHA256 checksum that is displayed when downloading the NetBackup_9.1.0.1_Win.zip file by clicking “Copy” next to the checksum.
2. Open Notepad and paste the checksum into the text file. Save the text file in the same location as the .zip file and name the file winhash.txt.
3. Open a Command Prompt and navigate to where the .zip file is located. Type the following command to generate the hash: certutil -hashfile NetBackup_9.1.0.1_Win.zip sha256 > checksum.txt.
4. Isolate the hash with the following command: findstr /v “SHA256 CertUtil” checksum.txt > hash.txt.

Compare the newly generated hash file with the file created in step 2: fc hash.txt winhash.txt. If the message “FC: no differences found” is displayed, the checksums match and the .zip file has not been tampered with.

In order to verify that the .tar file on Linux has not been tampered with, perform the following steps:

1. Copy the SHA256 checksum that is displayed when downloading the NetBackup_9.1.0.1_LinuxR_x86_64.tar.gz file by clicking Copy next to the checksum.
2. Open a text editor and paste the checksum into the text file. Save the text file in the same location as the tar file and name the file hash.
3. Open a terminal and navigate to where the tar file is located. Type the following command to generate the hash: sha256sum NetBackup_9.1.0.1_LinuxR_x86_64.tar.gz.
4. Isolate the hash with the following command: cut -d ‘ ‘ -f 1 < checksum > checksum2.

[1] https://www.veritas.com/content/support/en_US/downloads/detail.REL283803#item2

5. Compare the newly generated hash file with the file created in step 2: diff hash checksum2. If no text is displayed, the checksums match and the tar file has not been tampered with.

To verify the .rpm and .iso update files for the Flex 5350 and NetBackup 5250 Appliances, copy the SHA256 checksum that is displayed when downloading each file, and paste it to a text file. Use platform-appropriate tools as available to generate the SHA256 checksum for each file, and compare it with the SHA256 checksum that was provided when downloading the file.

Trusted couriers, such as FedEx, and tamper-proof packaging are used to deliver TOE hardware. The shipment includes the appliance and a USB key downloaded via a secure link. Customers can verify that they are receiving the product from Veritas rather than imposter by seeing the package is delivered by trusted couriers such as FedEx and uses tamper-proof packaging.

The TOE delivery includes also the guidance documentation to establish the TOE certified configuration, i.e. [GUIDE_CC]. TOE customers will be directed to the following URL to request this document: “https://www.veritas.com/why-veritas/trust/customer”. The personnel at Veritas who are sent inquiries via this web page, are aware of the document in question and will send the customer the document.

[GUIDE_CC] refers also to the additional guidance documents ([GUIDE_ADM], [GUIDE_REF], [GUIDE_CODE], [GUIDE_ENCR], [GUIDE_WEBUI], [GUIDE_INST], [GUIDE_TRBSH]), which can be downloaded from the Veritas Support website.

9.2 Installation, configuration and secure usage of the TOE

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

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

10 Annex B – Evaluated configuration

The TOE was tested with the NetBackup 5250 Appliance and Flex 5350 Appliance simultaneously in the environment. However, the TOE also runs on the following appliances with the same functionality as the evaluated configurations, but they have not been evaluated: NetBackup 5240, 5330, 5340, 5330HA, and 53440HA Appliances and Flex 5150, 5250, and 5340 Appliances. The TOE can run with any combination of media servers configured in the environment.

In the evaluated configuration, the NetBackup Primary Server, with the NetBackup Local Administration Console included, runs on RHEL. Although it can also run on Windows Server 2019 or one of the appliances with the same functionality, running it on a non-RHEL host has not been evaluated. Similarly, the NetBackup Media Server can run on Windows or RHEL but has not been evaluated on RHEL.

10.1 TOE operational environment

Table 2 specifies the system requirements for the TOE environment that hosts the various parts of the TOE. The TOE environment will also require any networking equipment needed to allow the TOE components to communicate with each other.

TOE component	Requirements
NetBackup Primary Server NetBackup Local Administration Console	General purpose computer hardware • 4 CPU cores • 16 GB RAM Red Hat Enterprise Linux (RHEL) 7.9
NetBackup Media Servers	General purpose computer hardware • 4 CPU cores • 32 GB RAM Windows Server 2019
	NetBackup 5250 Appliance • NetBackup Appliance OS v4.1
	Flex 5350 Appliance • Flex Appliance OS v2.1
NetBackup Linux Client	General purpose computer hardware • RHEL minimum requirements[2] RHEL 7.9
NetBackup Windows Client	General purpose computer hardware • Window Server 2019 minimum requirements[3] Windows Server 2019
NetBackup Remote Administration Console	General purpose computer hardware • Windows 10 minimum requirements[4] Windows 10
Cryptographic Support	The host system for the TOE contains a cryptographic module that provides cryptographic services to the TOE.

Table 2 - TOE Environment Minimum Requirements

[2] https://access.redhat.com/articles/rhel-limits
[3] https://learn.microsoft.com/en-us/windows-server/get-started/hardware-requirements
[4] https://support.microsoft.com/en-us/windows/windows-10-system-requirements-6d4e9a79-66bf-7950-467c-795cf0386715

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities. During these activities, the TOE has been updated by applying patches made available by the Developer that fixed public available vulnerabilities and any possible problem found during the evaluation. Non regression tests and vulnerability assessment and penetration test have been performed again each time.

11.1 Test configuration

The evaluator conducted the tests locally. The test configuration was installed by the evaluator who followed the steps described in the [GUIDE_CC] document.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The TOE and its environment were tested on an isolated network. The Developer provided seven test cases.

11.2.2 Test coverage

The Evaluators verified the complete coverage between the test cases in the test documentation provided by Developer and the TSFIs described in the functional specification. The Evaluators verified that the test cases are sufficient to demonstrate the internal behaviour and properties of the TSF.

11.2.3 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 Test approach

Due to the relatively small sample size, all Developer's tests were repeated by the Evaluators to confirm the validity of expected results. Moreover, during the independent testing phase, the Evaluator created exhaustive tests to cover every TOE feature. Performed test cases are:

- Test Case 1 – Policy creation and deactivation
- Test Case 2 – FIPS Status
- Test Case 3 - User creation and backup/restore preparation
- Test Case 4 - Local Administration Console verification
- Test Case 5 - Audit restrictions
- Test Case 6 - Backup/restore functions
- Test Case 7 - RBAC verification
- Test Case 8 - Reliable timestamp verification

11.3.2 Test results

All Developer's tests were run successfully, and the Evaluators verified the correct behaviour of the TSFIs and TSFs and correspondence between expected results and achieved results for each test.

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

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked with the TOE already used for the functional test activities and verified that the TOE and the test environment were properly configured.

The Evaluators designed the following attack scenarios:

- *Brute force attack*
- *Privilege escalation*
- *Remote code execution*
- *XSS on Audit*
- *Extract log information as unauthenticated*
- *Access TSF when unauthenticated*
- *Reach unassigned functions*
- *SQL injection*
- *Information leakage*
- *XSS*
- *Exploit the primary server*

The Evaluators has concluded that the TOE is resistant to BASIC potential in its intended operating environment. During the penetration testing the Evaluators found one residual vulnerability.