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) ver. 3.1 rel. 5

Certificato n. *(Certificate No.)*	14/2026
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/CCL/06/2023/RC, v1.0
Decorrenza *(Date of 1st Issue)*	23 febbraio 2026
Nome e Versione del Prodotto *(Product Name and Version)*	Nutanix Cloud Platform v6.8
Sviluppatore *(Developer)*	Nutanix, Inc.
Tipo di Prodotto *(Type of Product)*	Altre categorie - Piattaforma cloud (Cloud platform)
Livello di Garanzia *(Assurance Level)*	EAL2 con l'aggiunta di ALC_FLR.2, conforme a CC Parte 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, 23 febbraio 2026

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 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

Nutanix Cloud Platform v6.8

OCSI/CERT/CCL/06/2023/RC

Version 1.0

23 February 2026

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	23/02/2026

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

AHV Acropolis HyperVisor

AOS Acropolis Operating System

API Application Program Interface

CLI Command Line Interface

CSRF Cross-Site Request Forgery

CVE Common Vulnerabilities and Exposures

CVM Controller Virtual Machine

FNS Flow Network Security

FVN	Flow Virtual Networking
GUI	Graphical User Interface
HA	High Availability
HTML	Hypert Text Markup Language
HTTP(S)	Hyper Text Transfer Protocol (Secure)
LCM	Nutanix LifeCycle Manager
LTS	Long Term Support
nCLI	Nutanix Command Line Interface
NCP	Nutanix Cloud Platform
NDB	Nutanix Data Base
NFS	Netw0rk File System
NTP	Network Time Protocol
OS	Operating System
PC	Personal Computer
REST	REpresentational State Transfer
ROBO	Remote Office/Branch Office
SHA	Secure Hashing Algorithm
SQL	Structured Query Language
SSL	Secure Socket Layer
SSRF	Server Side Request Forgery
XSS	Cross-site Scripting
VM	Virtual Machine

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

[AGD] Nutanix, Inc. Nutanix Cloud Platform v6.8 Guidance Documentation Supplement, Version: 0.13, Date: December 1st, 2025

[ETRv5] Evaluation Technical Report,"Evaluation of Nutanix Cloud Platform v6.8", date 2026-02-12, NCP-034_ETR_v5, Version 5, CCLab Software Laboratory.

[ST] Nutanix, Inc. Nutanix Cloud Platform v6.8 Security Target, Document Version: 0.16, Date: February 11, 2026

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 claimed assurance components 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 for all claimed assurance components up to EAL2 and ALC_FLR only.

6 Statement of certification

The Target of Evaluation (TOE) is the product "**Nutanix Cloud Platform v6.8**", developed by Nutanix, Inc.

The TOE is a software that provides a resilient, and self-healing platform for building a hybrid multi-cloud infrastructure to support all kinds of workloads and use cases across public and private clouds, multiple hypervisors and containers, with varied compute, storage and network requirements.

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 and 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 also review 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 "Nutanix Cloud Platform v6.8" 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	Nutanix Cloud Platform v6.8
Security Target	Nutanix, Inc. Nutanix Cloud Platform v6.8 Security Target, Document Version: 0.16, Date: 11 February 2026 [ST]
Evaluation Assurance Level	EAL2 augmented with ALC_FLR.2
Developer	Nutanix, Inc.
Sponsor	Corsec Security, Inc.
LVS	CCLab – The Agile Cybersecurity Laboratory (Debrecen site).
CC version	3.1 Rev. 5
PP conformance claim	No conformance claimed
Evaluation starting date	1st August 2023
Evaluation ending date	12 February 2026

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 refer to the Security Target [ST].

The TOE "Nutanix Cloud Platform v6.8" is a software that provides a secure, resilient, and self-healing platform for building a hybrid multicloud infrastructure to support all kinds of workloads and use cases across public and private clouds, multiple hypervisors and containers, with varied compute, storage and network requirements.

The TOE consists of all the Nutanix software that makes up Nutanix Cloud Platform in a three-node cluster:

- Acropolis Operating System (AOS) v6.8,
- Acropolis Hypervisor (AHV) v20230302.100173,
- Prism Central (PC) 2024.2.0.6,
- Flow Virtual Networking (FVN) 4.0.0,
- Flow Network Security (FNS) v4.1.0,
- Self-Service v3.8.1.1 (utilized by Nutanix Cloud Manager),
- Nutanix Database Service (NDB) v2.5.5,
- Files v5.0 (utilized by Nutanix Unified Storage),
- Objects v5.0 (utilized by Nutanix Unified Storage).

The TOE offers two web Graphical User Interfaces (GUIs), called Prism Element and Prism Central respectively. The TOE also offers management of various services via REST API v2, v3, and v4.

The Nutanix Database (NDB) Service leverages a GUI, CLI, and REST API specific to NDB, referred to as the NDB GUI, NDB CLI, and NDB REST API respectively.

Nutanix Cloud Platform provides the capabilities to run guest VMs in the operating environment via the CVM hosted by AHV. Administrative users can backup guest VM data along with user data through replication functionality available through Nutanix Cloud Platform.

The TOE enforces:

- Virtual Disk Access Security Functionality Policy (SFP) on guest VMs that the TOE hosts;
- Virtual Disk Locking SFP on clients attempting to write to or execute files stored on virtual disks.

TOE generates audit records for all configuration changes made via the management interfaces.

The TOE includes a set of management interfaces that administrative users can use to view the audit logs, configure failover functionality, manage TOE settings, manage accounts and configure the storage provided by the TOE.

The TOE requires administrative users to perform identification and authentication before accessing any TOE functionality.

It is possible to consult sections 1.3 of the Security Target [ST] for a more detailed description of the TOE.

The evaluated configuration of the TOE was tested on the three-node NX-3060N-G8 (also referred to as the NX-3360N-G8, where the "3" in the place of the “0” denotes the three nodes of the platform) hardware platform running Nutanix Cloud Platform v6.8.

NCP was not tested on but is capable of running on other host hardware and is derived from a single monolithic image, which detects the hardware platform specifications and enables the appropriate drivers to support the host’s hardware.

The Nutanix hardware platforms reported in Table 1 are also supported by the TOE software.

Series 1 - Entry-level and ROBO	Series 3 - Balanced compute and storage	Series 8 - High performance
• NX-1065-G8	• NX-3035-G9	• NX-8035-G8
• NX-1065-G9	• NX-3060-G8	• NX-8035N-G8
• NX-1065N-G8	• NX-3060-G9	• NX-8150-G8
• NX-1175S-G8	• NX-3155G-G8	• NX-8150-G9
• NX-1175S-G9	• NX-3155GN-G8	• NX-8150N-G8
	• NX-3155-G9	• NX-8155-G8
	• NX-3170-G8	• NX-8155N-G8
	• NX-3170N-G8	• NX-8155-G9
		• NX-8155A-G9
		• NX-8170-G8
		• NX-8170N-G8
		• NX-8170-G9

Table 1 - Hardware models

Hardware platforms listed with a "1" in the second numerical position (ex. NX-8170N-G8) are available only as single-node platforms. Single-node platforms are intended to scale out infrastructure and provide an additional node to an existing cluster.

Platforms with a "0" in the second numerical position (ex. NX-1065-G8) are available in 2, 3, and 4-node configurations, in which case the "0" in the model number may be replaced by the number of nodes in the system (ex. A 4-node NX-1065-G8 may also be referred to as the NX-1465-G8).

The exact same software binaries are loaded onto all of the Nutanix Enterprise Cloud NX-appliances and the TOE will provide the same functionality. There are no code branches or execution branches that are appliance or processor specific for the NX-appliances.

The TSF is implemented entirely within the software binaries. Its logic, security mechanisms, and enforcement of SFRs do not change when deployed on different hardware models.

7.3.1 TOE architecture

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

The TOE boundary includes:

- the Nutanix-developed AOS and AHV of the three-node deployment for NCP;
- the Nutanix software components running on AOS;
- Nutanix-modified third-party source code or software.

The TOE boundary does not include the following environmental components:

- guest VMs running on AHV;
- workstations;

- host hardware, chassis, or disks;
- NTP server.

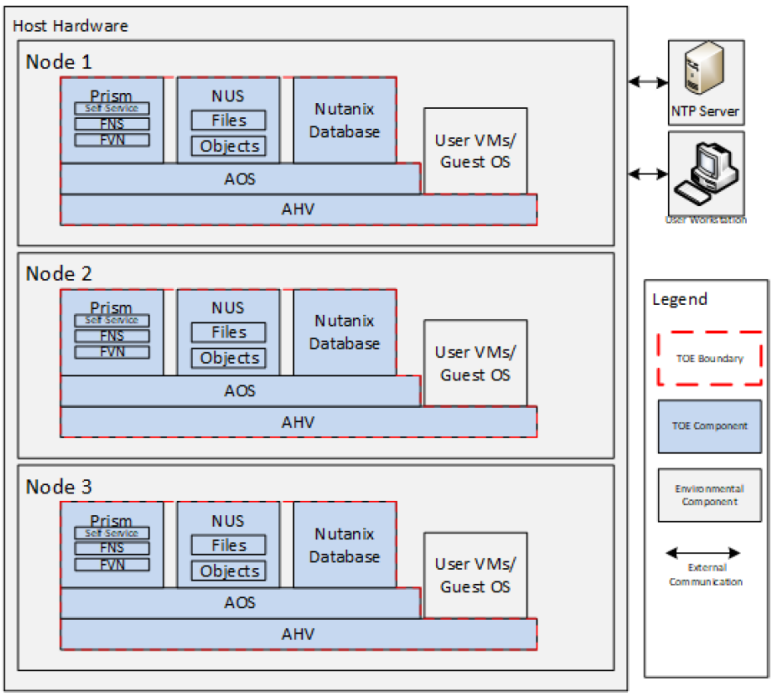

Figure 1 - TOE architecture diagram

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in section 3 of the Security Target [ST].

The TOE provides several security functionalities:

- **Security Audit** - The TOE records the actions of administrative users made through the management interfaces. Audit records can only be reviewed through Prism.
- **User Data Protection** - Storage for the cluster is provisioned as units called containers which are created from one or more tiers of disk storage (storage pools). The TOE can provide access to containers via NFS shares, which provide access to storage to guest VMs on the network.
    - The TOE implements a Virtual Disk Access SFP that controls what storage guest VMs can access on the TOE. This SFP controls access based on an NFS whitelist stored on the TOE.
    - The TOE enforces a Virtual Disk Locking SFP, which allocates access to Virtual Disks via a mechanism called virtual disk locking. Virtual disk locking occurs when a process on a guest VM requests access to storage represented by a virtual disk from the leader host.
    - The Role Based Access Control SFP is used to govern access to the Prism management interface.

- **Identification and authentication** - Administrative users must identify and authenticate themselves to the TOE or the Nutanix Database Service before being granted access to any of the management functionality provided via the management interfaces.
- **Security Management** - The TOE provides the following interfaces that administrative users can use to manage the TOE: Prism Element GUI, Prism Central GUI, NDB GUI, NDB CLI, NDB REST API, REST API v2, REST API v3 and REST API v4.

  Administrative users can manage security attributes related to the Virtual Disk Access policy via these interfaces. The Virtual Disk Access policy allows any storage access requests (using the Storage Access Interface) to be made by default, unless a virtual disk is already locked. Administrative users can also manage accounts, containers, storage, virtual disks, and NTP servers.
- **Protection of the TSF** - In the event of a host or disk failure, the TOE maintains a secure state by continuing to offer all of its functionality in the event of:
  - Failure of a single host in a multi-host cluster
  - Failure of one or up to all disks on a host in a multi-host cluster
- **Resource Utilization** - The TOE duplicates virtual disk data across multiple hosts to provide redundancy in the event of:
  - Failure of a single host in a multi-host cluster
  - Failure of one or up to all disks on a host in a multi-host cluster

A detailed description of the TOE security functionality is provided in section 7.1 of the Security Target [ST].

7.4 Documentation

The Nutanix Guidance Documentation Supplement [AGD] provides guidance on the secure installation and secure use of the TOE in the Common Criteria evaluated configuration and provides clarifications and changes to the Nutanix documentation.

The Nutanix Guidance Documentation Supplement [AGD] document is available at the following address:

> https://www.nutanix.com/viewer/content/dam/nutanix/documents/certifications/nutanix-ncp-v68-guidance-supplement-v013.pdf

In order to check the integrity of the document, you can execute the command “sha256sum file_name”. The obtained value must match the SHA-256 hash value:

> 59f36bdc4c97903607d11456223610056bd44b080606aa4c1825df7c18c3864b.

The hash strings for the other guides are present in Table 1, pages 4 and 5 of the Nutanix Guidance Documentation Supplement [AGD]. It is possible to download the other guides from the following address:

> https://www.nutanix.com/trust/compliance-and-certifications/common-criteria-auditorevaluation

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 (PP).

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 component ALC_FLR.2.

All the SFRs have been selected from CC Part 2 [CC2].

Security Target [ST] provides a 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 it 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 – The Agile Cybersecurity Laboratory (Debrecen site).

The evaluation was completed on 12 February 2026 with the issuance by LVS of the Evaluation Technical Report v5 [ETRv5], which was approved by the Certification Body on 13 February 2026. 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. 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 v5 [ETRv5] issued by the LVS CCLab – The Agile Cybersecurity Laboratory (Debrecen site) and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "Nutanix Cloud Platform v6.8" 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 2 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 (augmentations are represented in italics in Table 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
Basic Flaw remediation	*ALC_FLR.2*	Pass
Test	**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 2 - 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 "Nutanix Cloud Platform v6.8" 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 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 (CC guidance [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

There are two shipping processes for customers to obtain the TOE:

1. If the TOE is ordered without the host hardware (software-only), then the TOE software is delivered over the HTTPS connection of the Nutanix Support Portal where the packaged software can be downloaded.
2. If the TOE is ordered with the host hardware, the TOE is shipped from the Supermicro manufacturing facility direct to Nutanix customers via distributor-nominated carrier. Products are protected during shipment by the shipping carrier. Supermicro uses the carrier selected by the Distributor to provide shipment to the customer. Tracking information is provided by the carrier to Nutanix Fulfillment in an automated process and Nutanix Fulfillment emails the tracking information to the customer. A customer can verify the package with the tracking information provided against the tracking information printed on the label attached to the package.

For both order types, TOE documentation is only provided in softcopy, which is available for download from the Nutanix Support Portal. The Nutanix Support Portal also requires the end customer to authenticate with credentials that Nutanix has provided.

The software images for each component are provided as follows in Table 3:

Component	Filename	Hash SHA256
AHV	ISO: AHV-DVD-x86_64-el8.nutanix.20230302.100173.iso	05f392a5e02ddcac9b84d010715f4d2d993b87b1430643e09524295e3a8282ff
	LCM: lcm_ahv_el8.nutanix.20230302.100173.tar.gz	0e41e56a772570c5bc50a4db393c479e7787cfa51fb5e52495813cfaff5f1315
AOS	Upgrade: nutanix_installer_package-release-fraser-6.8-stable-9b27c8bcb5fcaac58016f3bed74009655a157049-x86_64.tar.gz	f8192c654ac45a714dc56d0532595c9dfa18bdc9183122d53b79b1daefa242db
	LCM: lcm_nos_6.8.tar.gz	b7b850d5fb8e90399b464b3422cb562720e686195cd4a37c8edb977b4714fa36
Prism Central	Upgrade: pc.2024.2.0.6-e7141238ee6a3838cb87a1467496b119224bb219-x86_64.tar.gz	b2731240c1d33b071c08b3d2699367cd71f8d7ab1610e1c4bf5036c22bb2edc1
	LCM: lcm_pc_pc.2024.2.0.6.tar.gz	bac961593477e6dcc8fcee00ebab5962034013265 7c58cd0f25004133aa30d22
Flow Network Security	LCM: lcm_flow_pc_4.1.0.tar.gz	565e17a2d1335c2c61e7093d1e14954b077ab4a323b40b1af537a551f20871d2
Flow Virtual Networking	LCM: 4.0.0.tar.gz	14ebfe2139807a070b0ef4f04b7c0ab6cb2d534609a1d267a609b0d9e6d11970
Files	Upgrade: nutanix-afs-el8.5-release-afs-5.0.0.1-stable-	86635e87ef0313606c1dcee5c9451a11a4a6182cf8619e878544774f9bc140f7

Component	Filename	Hash SHA256
	8da0965291d7453229238d58dc1abc3f09f4031d.qcow2	
	LCM: lcm_file_server_5.0.0.1.tar.gz	72a4bbc00a17098c229a7fa794028cf736e7a1588e9b12a705953a84e8ab438a
Objects	LCM: objects-5.0.tar.gz	f6d8384aab4800a92c0b9fe9eda2ed87b2368d5e2b88aff17e32dc633d1bc62b
Self-Service	Epsilon-3.8.1.1.zip	f05b8af12c56daeeb7d2913417e8d90d76d5859cdecaba5368397d37714c5c78
Nutanix Database	Install: NDB-Server-build-2.5.5-e6a22438d6f5bdbda5f6c72e910e113d22655c6d.qcow2	0b83d4c5b7b02e568b37d2a19470b039336c33f9c7f023005131003e7ce3ef5e
	Upgrade: era_upgrade_bundle-2.5.5-e6a22438d6f5bdbda5f6c72e910e113d22655c6d.zip	84fdca9a59319e9bfeff2540f8e045c2cbe916269cfe16bca6548d9c63be7ea1

Table 3 - TOE Component Software

9.2 Installation, configuration, and secure usage of the TOE

TOE installation, configuration and secure usage must be performed following the instructions contained in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the Common Criteria guidance [AGD] contains 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].

Customers shall obtain and verify the integrity of the Nutanix Guidance Documentation Supplement [AGD] following the steps defined in section 7.4 Documentation.

10 Annex B – Evaluated configuration

The evaluated configuration of the TOE uses the three-node NX-3060-G8 hardware appliance, connected to ethernet sources, with the following components installed:

- Acropolis Operating System (AOS) v6.8,
- Acropolis Hypervisor (AHV) v20230302.100173,
- Prism Central (PC) 2024.2.0.6,
- Flow Virtual Networking (FVN) 4.0.0,
- Flow Network Security (FNS) v4.1.0,
- Self-Service v3.8.1.1 (utilized by Nutanix Cloud Manager),
- Nutanix Database Service (NDB) v2.5.5,
- Files v5.0 (utilized by Nutanix Unified Storage),
- Objects v5.0 (utilized by Nutanix Unified Storage).

The TOE offers two web Graphical User Interfaces (GUIs), called Prism Element and Prism Central respectively. The TOE also offers management of various services via REST API v2, v3, and v4.

The TOE does not include the following environmental components:

- Guest VMs running on AHV
- Workstations
- Host hardware, chassis, or disks
- NTP server

The TOE is designed to run and store multiple guests VMs that in turn offer services to end users. At least one guest VM must be running in order to make use of the storage functionality provided by the TOE.

10.1 TOE operational environment

The TOE environment contains the hardware of three hosts and can optionally contain additional hosts with their own instances of the TOE to provide increased redundancy and scalability. The TOE is capable of running on any of the Nutanix appliance hardware platforms listed in

Series 1 - Entry-level and ROBO	Series 3 - Balanced compute and storage	Series 8 - High performance
• NX-1065-G8	• NX-3035-G9	• NX-8035-G8
• NX-1065-G9	• NX-3060-G8	• NX-8035N-G8
• NX-1065N-G8	• NX-3060-G9	• NX-8150-G8
• NX-1175S-G8	• NX-3155G-G8	• NX-8150-G9
• NX-1175S-G9	• NX-3155GN-G8	• NX-8150N-G8
	• NX-3155-G9	• NX-8155-G8

	• NX-3170-G8	• NX-8155N-G8
	• NX-3170N-G8	• NX-8155-G9
		• NX-8155A-G9
		• NX-8170-G8
		• NX-8170N-G8
		• NX-8170-G9

Table 1 - Hardware models.

A management workstation is required to access the TOE's management interfaces and administrative users should access Prism Element, Prism Central, and NDB GUI through the web browser.

The REST API interfaces may be accessed using any REST API client.

In addition, the host hardware components are intended to be deployed in a physically secure cabinet, room, or data center with the appropriate level of physical access control and physical protection (e.g. badge access, fire control, locks, alarms, etc.).

The TOE must have access to an NTP server that can provide reliable time stamps to the TOE.

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities.

11.1 Test configuration

The evaluated configuration of the TOE is composed of three-node NX-3060-G8 hardware appliance, connected to ethernet sources, with the three guest virtual machines (VM1, VM2 and VM3) hosted by Acropolis HyperVisor.

The test environment consists of an administrator workstation running a browser, the local Nutanix nCLI client and REST API client.

Testing activities were carried out in the LVS site and the Evaluators verified the configuration of the test environment, including the TOE, and found it to be consistent with the AGD documentation [AGD] and the Security Target [ST].

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer covered the functionalities of the TOE with manual tests. Namely, different test cases were designed, for the general purpose of guaranteeing each security function was tested and verified. The Developer performed extensive tests to verify the functionality of the TOE with tests related to the following categories:

- Test case 01 - Identification and Authentication Tests
- Test case 02 - Security Audit Tests
- Test case 03 - Security Management Tests
- Test case 04 - User Data Protection (Access Control)
- Test case 05 - User Data Protection (Information Flow Control)

11.2.2 Test coverage

The Evaluators have examined the test plan presented by the Developer and verified the complete coverage of the functional requirements (SFRs) and the TSFIs described in the functional specification. The Evaluators verified that the test cases are sufficient to demonstrate the internal behavior and the 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

Before initiating the testing activity, the Evaluators verified that the TOE was configured correctly.

All Developer's tests were repeated by the Evaluators to confirm the validity of expected results.

In addition, the Evaluators created 5 new test cases which focused on a specific area to increase the coverage and depth:

- Test case 01 - NCP-AUDIT_TEST - Check on creation of audit records for the interfaces REST API v2 and Prism Central, when performing operations on VMs.
- Test case 02 - NCP-REST_API_TEST - The Evaluators authorized the Postman with valid credentials, got the list of existing VMs, then made the credentials invalid and finally attempted to disable one of the VMs.
- Test case 03 - NCP-NDB_USER_TEST - The Evaluators created a new local user in the NDB GUI, then tried to perform specific operations with this newly created user in the NDB GUI.
- Test case 04 - NCP-ROLE_TEST - The Evaluators performed operation tests on specific user types which were not covered by the Developer tests.
- Test case 05 - NCP-NDB_REST_API_TEST - This test aimed to test the NDB through REST API.

The Evaluators performed manual tests using:

- Prism Central Web GUI
- NDB Web GUI
- REST API client and the NDB Rest API Explorer.

11.3.2 Test results

All Developer's tests were run successfully; the Evaluators verified the correct behavior 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 the actual test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

The Evaluators conducted vulnerability analysis and penetration testing activities.

A search on public vulnerabilities on TOE and TOE components (e.g. OS) has been conducted. The analysis was supported by the use of Nessus plugins (for AOS and AHV), and an API endpoint search was performed on TOE. The analysis confirmed that there are no public vulnerabilities which were exploitable in the TOE evaluated configuration.

The Evaluators designed the following attack scenarios:

- Injection attacks on TOE and REST API (such as Cross-Site Scripting (XSS), SQL Injection, HTML injection)
- Excessive Data Exposure
- Exploiting nCLI by malicious input
- Role Privilege Escalation
- CSRF by REST API
- Function execution without authentication in REST API
- Force unencrypted HTTP connection

- Secure boot attack
- Information disclosure on other web services
- SSL Attacks
- User enumeration on Prism Central
- SSRF (CVE-2024-40718)

The Evaluators conducted penetration testing activities on the same instance of the TOE configured for functional and independent testing.

The Evaluators could then conclude that the TOE is resistant to a basic attack potential in its intended operational environment. No exploitable or residual vulnerabilities have been identified.