Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

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. 8/20

(Certification No.)

Prodotto: Nutanix Enterprise Cloud (AOS & AHV) v5.15

(Product)

Sviluppato da: Nutanix, 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)

Il Direttore
(Dott.ssa Eva Spina)

[ORIGINAL DIGITALLY SIGNED]

Roma, 9 ottobre 2020

Common Criteria

SOGIS IT SECURITY CERTIFIED

This page is intentionally left blank

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Nutanix Enterprise Cloud (AOS & AHV) v5.15

OCSI/CERT/CCL/01/2020/RC

Version 1.0

9 October 2020

Courtesy translation

Disclaimer: this translation into English language is provided for informational purposes only; it is not a substitute for 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

Release	Authors	Information	Date
1.0	OCSI	First issue	09/10/2020

2 Table of contents

1 Document revisions 5
2 Table of contents 6
3 Acronyms 8
4 References 10
4.1 Criteria and regulations 10
4.2 Technical documents 11
5 Recognition of the certificate 12
5.1 CC Certificates recognition in Europe (SOGIS-MRA) 12
5.2 International CC Certificates recognition (CCRA) 12
6 Statement of certification 13
7 Summary of the evaluation 14
7.1 Introduction 14
7.2 Executive summary 14
7.3 Evaluated product 14
7.3.1 TOE architecture 15
7.3.2 TOE security features 16
7.4 Documentation 17
7.5 Protection profile conformance claims 17
7.6 Functional and assurance requirements 17
7.7 Evaluation conduct 17
7.8 General considerations about the certification validity 18
8 Evaluation outcome 19
8.1 Evaluation results 19
8.2 Recommendations 20
9 Annex A – Guidelines for the secure use of the product 21
9.1 TOE Delivery 21
9.2 Installation, initialization and secure usage of the TOE 21
10 Annex B – Evaluated configuration 22
11 Annex C – Test Activities 23
11.1 Test configuration 23

11.2 Functional tests performed by the Developer 23
11.2.1 Testing approach 23
11.2.2 Test coverage 24
11.2.3 Test results 24
11.3 Functional and independent tests performed by the Evaluators 25
11.4 Vulnerability assessment and penetration tests 25

3 Acronyms

AHV	Acropolis Hypervisor
AJAX	Asynchronous JavaScript and XML
AOS	Acropolis Operating System
API	Application Programming Interface
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CSRF	Cross-site Request Forgery
CVM	Controller Virtual Machine
EAL	Evaluation Assurance Level
HDD	Hard Disk Drive
ETR	Evaluation Technical Report
HW	Hardware
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IT	Information Technology
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
nCLI	Nutanix Command Line Interface
NFS	Network File System
NIS	Nota Informativa dello Schema
NTP	Network Time Protocol
OCSI	Organismo di Certificazione della Sicurezza Informatica
OLE	Object Linking and Embedding
OPC	OLE for Process Control

OS	Operating System
PCIe	Peripheral Component Interconnect Express
PP	Protection Profile
REST	Representational State Transfer
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SOGIS	Senior Officials Group Information Systems Security
SOGIS-MRA	SOGIS – Mutual Recognition Arrangement
SSD	Solid-state Drive
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
VM	Virtual Machine
XML	eXtensible Markup Language

4 References

4.1 Criteria and regulations

[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

[AA] Nutanix AOS 5.15 Acropolis Advanced Administration Guide, Nutanix, Inc., 31 March 2020

[AG] Nutanix AHV 5.15 AHV Administration Guide, Nutanix, Inc., 31 March 2020

[AGD] Nutanix Enterprise Cloud (AOS & AHV) v5.15 Guidance Documentation Supplement; Evaluation Assurance Level (EAL): EAL2+, v0.3, Nutanix, Inc., 16 July 2020

[API] Nutanix AOS 5.10 Acropolis v1 API Reference, Nutanix, Inc., 31 March 2020

[AS] Nutanix AOS 5.15 Acropolis Advanced Setup Guide, Nutanix, Inc., 31 March 2020

[CMC] Nutanix Enterprise Cloud (AOS & AHV) v5.15 Configuration Management Document; Evaluation Assurance Level (EAL): EAL2+, v0.4, Nutanix, Inc., 24 September 2020

[CR] Nutanix AOS 5.15 Command Reference, Nutanix, Inc., 31 March 2020

[DEL] Nutanix Enterprise Cloud (AOS & AHV) v5.15 Secure Delivery Document; Evaluation Assurance Level (EAL): EAL2+, v0.1, Nutanix, Inc., 25 March 2020

[ETR] “Nutanix Enterprise Cloud (AOS & AHV) v5.15” Evaluation Technical Report, v.3, CCLab Software Laboratory, 23 September 2020

[GS] Nutanix AOS 5.15 Acropolis Getting Started Guide NX Series, March 31, 2020

[NS] Nutanix Security 5.15 Security Guide, Nutanix, Inc., 31 March 2020

[ST] “Nutanix Enterprise Cloud (AOS & AHV) v5.15” Security Target, Nutanix, Inc., Version 0.7, 17 July 2020

[WP] Nutanix Prism 5.15 Prism Web Console Guide, Nutanix, Inc., 31 March 2020

5 Recognition of the certificate

5.1 CC Certificates recognition in Europe (SOGIS-MRA)

The European mutual recognition arrangement (SOGIS-MRA, version 3, [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) for the assurance levels 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 recognized under the terms of this agreement by signatory nations.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

5.2 International CC Certificates recognition (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 assurance components selected.

6 Statement of certification

The Target of Evaluation (TOE) is the software product “Nutanix Enterprise Cloud (AOS & AHV) v.5.15”, also referred to in the following as “Nutanix Enterprise Cloud v5.15”, developed by Nutanix, Inc.

The TOE is a virtualization platform that can host VMs offering services and storage to users (typically as virtual servers) such as web, email, or others. Additionally, the TOE scales linearly to meet increased virtual server processing or storage needs by allowing additional nodes to be added to the cluster individually, which reduces hardware needs significantly as compared to a traditional server infrastructure.

The evaluation has been conducted according to the requirements established by the Italian Scheme for the evaluation and security certification of systems and products in the information technology sector and described in the Provisional Guidelines [LGP1, LGP2, LGP3] and in the 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 TOE complies with the requirements specified in the Security Target [ST]; the potential consumers and/or users of the product should review also the Security Target, in addition to the present Certification Report. 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 – 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 Enterprise Cloud (AOS & AHV) v.5.15” to provide assurance to the potential consumers and/or users 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	Nutanix Enterprise Cloud (AOS & AHV) v.5.15
Security Target	“Nutanix Enterprise Cloud (AOS & AHV) v5.15” Security Target, Version 0.7 [ST]
Evaluation Assurance Level	EAL2 augmented with ALC_FLR.2
Developer	Nutanix, Inc.
Sponsor	Nutanix, Inc.
LVS	CCLab Software Laboratory
CC version	3.1 Rev. 5
PP conformance claim	No compliance declared
Evaluation starting date	15 January 2020
Evaluation ending date	23 September 2020

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 “Nutanix Enterprise Cloud v5.15” is a software that provides the security functionality defined below. The TOE consists of all the Nutanix software that makes-up Nutanix Enterprise Cloud in a three-host cluster. All of the hardware necessary for the TOE operation is considered to be within the TOE environment.

The TOE consists of the following software components:

- Acropolis Operating System (AOS) v5.15 LTS.
- Acropolis Hypervisor (AHV) v20170830.395.

The TOE enforces a Virtual Disk Access Security Function Policy (SFP) on guest VMs that the TOE hosts. This SFP controls guest VM access to the storage that the TOE provides. To determine if a guest VM can access a virtual disk, the TOE first checks an NFS whitelist and then checks if the guest VM has been configured to access the NFS share.

The TOE enforces a Virtual Disk Locking SFP on clients attempting to write to or execute files stored on virtual disks. This SFP allows a read or execute operation if the process requesting the operation has obtained a virtual disk lock. If a virtual disk lock does not currently exist for the virtual disk, the TOE allows the process to obtain a virtual disk lock. Otherwise, the operation request is denied.

The TOE generates audit records for all configuration changes made via the management interfaces. Within these audit records, the TOE includes basic information about the event in a human-readable format. The TOE provides reliable time stamps that are used to preserve the order of events for the audit records.

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 management interfaces can also be used to configure the Virtual Disk Access SFP and Virtual Disk Locking SFPs. Storage options include access type (pass-through or virtual disk format), tiering options (PCIe SSD, SSD, or HDD), and maximum capacity allocated. There are three administrative roles defined for the TOE: User Administrator, Cluster Administrator, and View-Only. Administrative users can log out of their management sessions at any time.

The TOE requires administrative users to perform identification and authentication before accessing any TOE functionality. During authentication via Prism, only obscured feedback is provided to the administrative user. The TOE also maintains passwords for local accounts and their associated usernames.

7.3.1 TOE architecture

Within TOE boundary the Nutanix-developed AOS and AHV of the three-host deployment for Nutanix Enterprise Cloud are included. Also the parts of third-party source code or software that Nutanix has modified for Nutanix Enterprise Cloud is also considered to be TOE software.

The TOE boundary does not include the following operational environment components shown in Figure 1:

- guest VMs running on AHV;
- workstations;
- host hardware, chassis, or disks;
- NTP server.

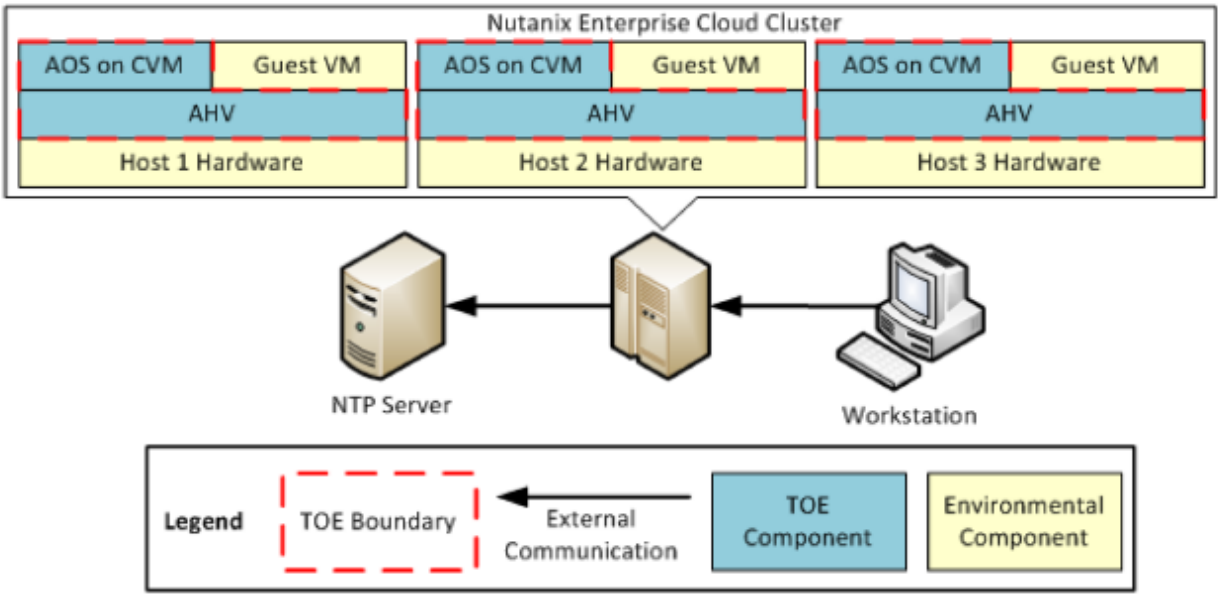

Figure 1 – TOE boundary

The following components are not depicted in Figure 1 and are considered to be part of the TOE operational environment:

- local nCLI client running on the workstation;
- REST API client running on the workstation;
- web browser running on the workstation;
- management tools or products used to access AHV.

7.3.2 TOE security features

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

For a detailed description of the TOE Security Functions, consult sect. 7.1 of the Security Target [ST]. The most significant aspects are summarized below:

- **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**: the TOE enforces access controls on storage allocated to VMs. This storage is provided via NFSv4 shares. Access to this storage is controlled via an NFS whitelist that lists the IP address of every guest VM that is allowed to access the storage. The TOE also provides information controls so that only one client can modify virtual disk data at a time.
- **Identification and Authentication**: the TOE requires users to identify and authenticate themselves to the TOE before granting permission to access any of the TOE's functionality. Administrative users are required to define strong passwords for themselves. The TOE stores each local account's username and

password. While logging into Prism, the TOE obscures passwords for administrative users.

- **Security Management**: the TOE provides the REST API, Prism, and nCLI that administrative users can use to manage the TOE. 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 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. Administrative users can assume the User Administrator role, Cluster Administrator role, View-Only role or can be assigned multiple sets of privileges at once.

- **Protection of the TSF**: the TOE maintains its full capabilities when a physical disk or host fails.

- **Resource Utilization**: the TOE makes use of redundant hosts to prevent a single point of failure. The TOE remains fully operational with all data intact even if an entire physical disk or host fails.

- **TOE Access**: the TOE provides the capability for administrative users to log out from Prism and nCLI.

7.4 Documentation

The guidance documentation specified in Annex A – Guidelines for the secure use of the product is delivered to the customer together with the product.

The guidance documentation contains all 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 sect. 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], whose review is recommended to potential consumers. 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 23 September 2020 with the issuance by the LVS of the Evaluation Technical Report [ETR] that has been approved by the Certification Body on 24 September 2020. 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; 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] released by the LVS and documents required for the certification, and considering the evaluation activities carried out, on the basis of the evidence examined by the Certification group, OCSI concluded that the TOE "Nutanix Enterprise Cloud (AOS & AHV) v.5.15" 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 functions described in the Security Target [ST] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 1 summarises the final verdicts for 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
Flaw reporting procedures	*ALC_FLR.2*	Pass
Delivery procedures	ALC_DEL.1	Pass

Assurance classes and components		Verdict
Tests	**Class ATE**	Pass
Evidence of coverage	ATE_COV.1	Pass
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 the assurance requirements

8.2 Recommendations

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

Potential customers of the product “Nutanix Enterprise Cloud (AOS & AHV) v.5.15” are suggested to properly understand the specific purpose of this certification reading this Report with reference to the Security Target [ST].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the Organizational security policies and the assumptions described, respectively, in sect. 3.2 and 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 – Guidelines for the secure use of the product includes a number of recommendations relating to delivery, initialization and secure usage of the product, according to the guidance documentation provided together with the TOE ([AA], [AG], [AGD], [AS], [CMC], [CR], [DEL], [GS], [NS], [WP], [API]).

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

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

9.1 TOE Delivery

The Secure Delivery Document [DEL] provides information about the delivery of the product and how to check the product after receiving it.

There are two possibilities, either acquiring the TOE only as a software, then install and configure it on the already available hardware, or ordering it together with the hardware appliance from the Developer.

If it is software only, it can be downloaded from the Developer's Web site. In this case, the customer can verify that the software is original by comparing its SHA-256 checksum with the one mentioned on the download page.

If the delivered product is hardware + software, the tracking number (UPS or FEDEX) and the list of the ordered and shipped product (from the invoice) can be verified to make sure it is the original product. After the hardware is built in and started, the software version can be verified within the Prism.

9.2 Installation, initialization and secure usage of the TOE

The Getting Started Guide [GS] provides information about the preparation steps to start the TOE. The documentation describes it for multiple hardware configurations (e.g., 1U1N, 2U4N). The Administration Guide [AG] recommends minimum 3 nodes to build a cluster. Further details are given in the guidance documentation supplement [AGD] as for 2U3N configuration. All user procedures necessary to securely prepare the TOE and its operational environment are described in [GS], [AG], [NS], and [AGD].

It is required to separate management traffic from storage replication (or backplane) traffic by creating a separate network segment (LAN) for storage replication, as described in the Nutanix Security Guide [NS].

For secure usage of the TOE, users should refer to [AA], [AG], [CR], [WP] and [API].

10 Annex B – Evaluated configuration

The TOE has been evaluated in the configuration described in sect. 1.6.1 of the Security Target [ST] and summarized in sect. 7.3.1. Additional details are provided on the HW environment for the TOE in this section.

The physical scope of the TOE includes the following software components:

- AOS v5.15 LTS.
- AHV v20170830.395.

The evaluated configuration of the TOE was tested on the NX-1365-G7 hardware platform running Nutanix Enterprise Cloud 5.15.

Note that the NX-1365-G7 is the same as the NX-1065-G7 but the “3” in place of the “0” means that there are 3 nodes in the chassis. Nutanix Enterprise Cloud was not tested on, but is capable of running on, other host hardware and is derived from a single image with different functionality enabled or disabled to support the host’s hardware. The following host hardware can be used with the TOE software:

- NX-1065-G7, NX-1175S-G7, NX-3060-G7, NX-3155-G7, NX-3170-G7, NX-8170-G7, NX-8150-G7, NX-8155-G7, NX-8035-G7, DX360-4-G10, DX360-8-G10, DX360-10-G10-NVMe, DX380-8-G10, DX380-12-G10, DX380-24-G10, DX560-24-G10, DX2200-DX170R-G10-12LFF, DX2200-DX190R-G10-12LFF, DX2600-DX170R-G10-24SFF, DX4200-G10-24LFF, DX8000-DX910.

11 Annex C – Test Activities

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 test environment had a physical and a virtual environment. The Physical environment was built from a Nutanix appliance, a Workstation and from network devices. The AHV and AOS required pre-configuration for the test as defined in the test documentation of the Developer. The virtual environment for the test consisted in 3 VMs – all prepared with installed Ubuntu OS and with a super user account. To test Prism only a browser was needed on a Workstation, but to test REST API, the Postman software had to be installed on Workstation. The nCLI client had to be also downloaded from Prism.

Prior the execution of the tests the Evaluators examined the test plan to verify that the TOE test configuration was consistent with the Developer's documentation, as also detailed in sections 1.4, and 1.6.1 of the Security Target [ST].

The test documentation provided by the Developer included sufficiently detailed instructions and description for identifying any test execution ordering dependencies, and all enlisted tests included the expected results.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Evaluators checked that the test documentation included test plans, expected test results and actual test results. The following test cases were planned:

- 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.
- Test Case 05: User Data Protection (Information Flow Control).
- Test Case 06: Host Failure.

The cases were defined to cover all SFRs. They had all to be tested externally and manually. The test plan also mentioned some prerequisites for the hardware with a detailed guide on how to prepare the TOE for the tests. Preparation included the completion of the steps described in [AGD], upload of a disk image, creating virtual machines and install OS on them, Postman application install and other configuration steps. Every step was described with enough detail to ensure that the test preparation and the test itself was reproducible.

11.2.2 Test coverage

The Evaluators verified that the correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification was accurate.

All TSFIs identified in the functional specification were included in the planned test cases:

1. Prism – which is an AJAX based web graphical interface for remote management of the AHV&AOS cloud system.

2. nCLI – which is a text-based command line interface also used remotely from a workstation to manage the TOE.

3. REST API – which is a programmatic interface, also for remotely manage the TOE through API calls.

4. Storage access Interface – which is a data access interface, provides access to NFS shares and virtual disks.

11.2.3 Test results

The Evaluators checked that the actual test results in the test documentation were consistent with the expected test results in the test documentation.

Execution of test case 01 proved that configuration data was replicated across the cluster when an attempt to disable CVMs was made.

The purpose of test case 02 was to test the Security Audit functionality of the TOE through Prism, nCLI and the REST API. It was verified that the audit records were replicated to the other hosts in the cluster when the VM was powered off or when a clone VM was created and deleted.

The test case 03 verified the enforcement of the Security Management SFRs by showing that an administrative user can provide storage, manage user accounts, and modify Network Time Protocol (NTP) settings. The tester powered down a CVM to verify that the TOE replicated management data to the other CVMs in the cluster.

The test case 04 verified the Storage Access Interface by showing that users can access storage in an NFS share and that access is not allowed by default. The tester removed a hard disk from the server chassis in order to simulate a disk failure and force the TOE to provide stored data via the Data Request Interface.

The purpose of the test case 05 was to verify that the disk locking functionality provided by the TOE would control the flow of information to virtual disks from guest VMs. The tester

displayed information about a specific host to check which virtual disks were being accessed by specific VMs.

The purpose of the test case 06 was to demonstrate preservation of a secure state and limited fault tolerance in case of a node failure. The tester demonstrated host redundancy and fault tolerance.

11.3 Functional and independent tests performed by the Evaluators

The developer provided a Nutanix appliance for testing purposes. This is an NX-1365-G7 appliance, which is a NX-1065-G7 with three nodes (for more information refer to sect. 1.6.1 of [ST]). The Evaluators followed the preparation steps defined in [AGD] to create the secure configuration for the TOE. This includes the upgrade of the AOS to version 5.15 LTS, the disabling of IPMI interface, configuring NTP server, disabling SNMP and disabling remote support and SSH password challenge. Both the hardware and software versions were consistent with the [ST]. As the [AGD] document describes how to configure the TOE to reach the secure configuration and the TOE was configured following step by step this guidance, the configuration was also consistent with the [ST]. The test documentation described the exact hardware appliance used by the developer to perform the functional tests, which was NX-1365-G7, corresponding to the same version the Evaluators used to perform the tests.

The Evaluators executed a sample of tests in the test documentation to verify the Developer test results with various tools (Firefox v77.0.1, Chrome v83.0.4103.116, Java SE v8 update 251, Postman v7.27.1, nCLI – downloadable from the Prism). Namely, the Evaluators selected two test steps from each of the defined test cases and executed the steps. The Evaluators tried to perform actions such as unauthorized access attempts and access with correct credentials, creation and deletion of VMs and of storage containers, resizing of vDisks, provoking of host failures by disconnecting nodes from the network.

The Evaluators were able to reproduce some chosen test steps following the test documentation provided by the Developer. The results of these tests were correspondent to the results by the Developer tests.

After examination of test cases 01-03, the Evaluators found room for devising new tests. Therefore, relatively to such cases, they designed a subset of the TSF to confirm that the TSF operated as specified. The Evaluators produced the documentation of the designed tests, executed the tests and observed that the obtained results were correspondent to the expected results.

11.4 Vulnerability assessment and penetration tests

The very first phase of the vulnerability assessment was the information gathering about the TOE. As the first step, multiple public searches were conducted with different keyword combinations to identify the publicly available bugs and vulnerabilities for the TOE. For this phase, not only search engines were used, but public vulnerability databases were also consulted The publicly known vulnerability list was not too long, and they were all outdated and therefore not relevant for the TOE. The Evaluators also searched through the Developer’s website and support forums for documentation and/or reported vulnerabilities. The conclusion of this first phase was that the TOE is well documented, and an attacker can get deep understanding of the TOE based on the documentation and forum searches,

which is relevant for the attack potential calculations. However, no relevant public vulnerability exists for the TOE.

As a second step, the Developer documentation was used to get familiar with the TOE and to identify the possible attack surfaces. As mentioned before, the publicly available documentation on the Developer's website is rich and is almost the same as the documentation provided for the evaluation. The Evaluators got the first impression about the TOE based on the documentation and by using the administrative interfaces of the TOE. During this step a couple of possible attack vectors against the administrative interfaces were also identified. As the TOE administrative interfaces include a command-line interface, which is a downloadable executable file, the Evaluators also conducted a source code analysis on this executable to understand its functionalities and the underlying communication with the TOE. This source code analysis also drew attention to some possible vulnerabilities. The result of the second phase in the information gathering was multiple possible vulnerabilities that were included in the penetration test plan.

As the last part of the information gathering, the Evaluators started an active search for open ports on the TOE provided within the test environment. With the identified open ports, the Evaluators started reviewing the documentation and also looked into public sources for additional information to identify the services running behind the ports, as most of the services used custom ports. The results of the search were some blog posts where these ports and services were presented in detail. With these findings, the active information gathering also led to some possible vulnerabilities, which could be included in the penetration test plan.

With all the gathered intelligence about the TOE and the possible vulnerabilities, the Evaluators created a penetration test plan broken down in different attack scenarios. For the attack scenarios, exact attack potentials were calculated, considering the fact that the publicly available information about the TOE is very detailed and rich.

With the defined attack scenarios, the Evaluators conducted penetration tests against the TOE to identify the existing vulnerabilities. The results of the tests were documented and detailed enough for the repeatability and the results were also gathered in a table for the sake of clarity.

The executed penetration test could not identify exploitable vulnerabilities in the TOE with Basic attack potential.

On the basis of such results, the evaluators concluded that no attack scenario with potential Basic can be completed successfully in the operational environment of the TOE as a whole. Therefore, none of the identified potential vulnerabilities can be exploited effectively. However, Evaluators have identified three residual vulnerabilities, i.e., vulnerabilities that could be exploited by an attacker with an attack potential beyond Basic.

It is recommended that the user contacts the Developer to obtain further technical details on the residual vulnerabilities and information on mitigation solutions.