REF: 2016-50-INF-2187 v2	Created by: CERT11
Target: Público	Revised by: CALIDAD
Date: 08.02.2018	Approved by: TECNICO

CERTIFICATION REPORT

File: 2016-50 NimbleOS v4.2

Applicant: Nimble Storage Inc.

References:

[EXT-3200] Certification request of Nimble Storage Inc. NimbleOS, version 4.2.0.1-499435-opt.

[EXT-3654] Evaluation Technical Report of Nimble Storage Inc. NimbleOS, version 4.2.0.1-499435-opt.

The product documentation referenced in the above documents.

Certification report of the product Nimble Storage Inc. NimbleOS, version 4.2.0.1-499435-opt, as requested in [EXT-3200] dated 01/12/2016, and evaluated by the laboratory Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-3654] received on 22/11/2017.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product “Nimble Storage Inc. NimbleOS, version 4.2.0.1-499435-opt”.

NimbleOS is a predictive flash storage solution that can be deployed on Nimble’s all-flash or hybrid flash arrays. NimbleOS protects data while providing unparalleled efficiency in a SAN array. The array can be accessed over iSCSI or FC. Data protection is offered with triple+ parity RAID 6 and optional data at rest encryption. NimbleOS supports scheduled and manual volume snapshots and application synchronization as well as data replications across the cluster. Data is compressed and de-duplicated inline.

Developer/manufacturer: Nimble Storage, INC.

Sponsor: Nimble Storage, INC.

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Epoche & Espri S.L.U.

Protection Profile: None

Evaluation Level: Common Criteria v3.1 R4 EAL2+ALC_FLR.2

Evaluation end date: 22/11/2017.

All the assurance components required by the evaluation level of the [CC_P3] have been assigned a “PASS” verdict. Consequently, the laboratory Epoche & Espri S.L.U assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL2 + ALC_FLR.2 assurance level packages, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4. Considering the obtained evidences during the instruction of the certification request of the product “Nimble Storage Inc. NimbleOS, version 4.2.0.1-499435-opt”, a positive resolution is proposed.

TOE summary

The TOE is an OS running on Nimble Storage arrays that provides data protection and storage and backup management. It implements several key security features:

- Access control – Storage is provisioned by way of volumes accessed over a storage network via either iSCSI or FC. The iSCSI clients, or initiators, with the proper CHAP account credentials can access associated volumes. Volumes may also be accessed by both iSCSI and FC clients alike with the use of initiator groups. In this case, CHAP credentials are not required, as access is dictated by authorized user mappings between IQNs/WWPNs and volumes.

- Management with RBAC via the NimbleOS GUI, CLI, or API – Authorized TOE administrators are restricted to security functions and TSF data based on their role(s) assigned through a user account. There are four roles: Administrator, Power User, Operator, and Guest.

- Multiple authentication mechanisms – Both local and AD authentication can be configured to identify and authenticate TOE administrators at the NimbleOS GUI, CLI, or API.
- Data protection and fault tolerance – NimbleOS protects against user data errors with checksums and continuous data integrity monitoring. It protects against hardware failures with an active/standby controller design and triple-parity RAID. It sustains failover for up to two disk failures or a single controller failure on an array.
- Auditing – Audit records are created for startup and shutdown and all administrator-initiated, non-read operations performed on an array. Every record identifies the administrator taking the action.
- Snapshots – Snapshots of volumes and volume groups can be created to preserve a point-in-time copy of one or more volume's metadata. These snapshots can be used to roll back all the operations on a volume to restore it to a desired point-in-time.
- Export of user data – Authorized TOE administrators can create protection schedules to export copies of volumes (or replicas) to replication partners. The copies have a checksum associated with them to ensure the data is consistent. In addition, if the volume has been encrypted, the replica that is exported remains encrypted.
- FIPS-validated cryptographic module – The TOE uses the Nimble Storage, Inc. FIPS Object Module to provide all cryptographic functionality. This includes encryption of data at rest on selected volumes; a protected path from remote users of the NimbleOS GUI, CLI, or API; protection of keys at rest and in transit; a trusted channel to replication partners for transfer of wrapping keys; and X.509 certificate management. TLSv1.2, HTTPS, and SSH are supported.

TOE major security features

The major security features implemented by the TOE and subject to evaluation can be summarised as follows:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management

- Protection of the TSF
- Trusted Path/Channels

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidences required to fulfil the assurance packages of EAL2 + ALC_FLR.2, according to Common Criteria v3.1 R4.

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

In addition, as for the augmentation defined, the ALC_FLR.2 assurance component is also included in the evaluation.

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R4:

Class	Component
Security Audit (FAU)	Audit data generation (FAU_GEN.1)
	User Identity Association (FAU_GEN.2)
	Audit review (FAU_SAR.1)
	Protected audit trail storage (FAU_STG.1)
Cryptographic Support (FCS)	Cryptographic key generation (FCS_CKM.1)
	Cryptographic key destruction (FCS_CKM.4)
	Cryptographic operation (FCS_COP.1)

User Data Protection (FDP)	Subset access control (FDP_ACC.1 (a) &(b))
	Security attribute based access control (FDP_ACF.1 (a) & (b))
	Export of user data with security attributes (FDP_ETC.2)
	Advanced rollback (FDP_ROL.2)
	Stored data integrity monitoring and action (FDP_SDI.2)
Identification & Authentication (FIA)	User attribute definition (FIA_ATD.1)
	User authentication before any action (FIA_UAU.2)
	Multiple authentication mechanisms (FIA_UAU.5)
	Protected authentication feedback (FIA_UAU.7)
	User identification before any action (FIA_UID.2)
Security Management (FMT)	Management of security attributes (FMT_MSA.1 (a) & (b))
	Static attribute initialisation (FMT_MSA.3)
	Specification of management functions (FMT_SMF.1)
	Security roles (FMT_SMR.1)
Protection of the TSF (FPT)	Failure with preservation of secure state (FPT_FLS.1)
	Reliable time stamps (FPT_STM.1)
Trusted Path/Channels (FTP)	Trusted channel (FTP_ITC.1)
	Trusted path (FTP_TRP.1)

IDENTIFICATION

Product: Nimble Storage Inc. NimbleOS, version 4.2.0.1-499435-opt

Security Target: Nimble Storage, Inc. NimbleOS Security Target, version 0.9, November 2017

Protection Profile: None

Evaluation Level: Common Criteria v3.1 R4: assurance packages EAL2 + ALC_FLR.2

SECURITY POLICIES

There are no Organizational Security Policies defined for this evaluation.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions included in the [ST], are constraints to the conditions used to assure the security properties and functionalities compiled by the security target [ST]. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

Assumptions	Description
A.NETWORK	The TOE environment provides the network infrastructure required for management and storage traffic.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.
A.LOCATE	The TOE, the arrays, storage clients, switches, storage and management networks, firewall, and NTP and LDAP servers are located within a controlled access facility.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	TOE administrators (Administrator, Power User, Operator, and Guest role) who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.ADMIN_PROTECT	No malicious software is installed or running on the TOE administrator workstation.
A.ENVIRON_ADMIN	There are one or more competent, non-hostile individuals assigned to manage TOE environmental components.

THREATS

The following threats do not suppose a risk for the product Nimble Storage Inc. NimbleOS, version 4.2.0.1-499435-opt, although the agents implementing attacks have a **Basic** attack potential according to the assurance package EAL2 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are categorized below.

Threats Name	Description
T.DATA_CORRUPTION	Data could become corrupted or security functionality compromised due to hardware failure caused by natural threats or incorrect system operations.
T.INTERCEPT	The TOE may communicate with remote IT entities and TOE administrator workstations that lie outside of the organization's trusted network. An attacker who is not a TOE user may attempt to intercept these communications in order to read or modify critical TSF data.
T.UNAUTH	An unauthorized person may gain access to security data on the TOE.
T.UNINTENDED_ACCESS	An attacker who is not a TOE user could attempt to

	bypass the access controls provided by the TOE by using one of the systems connected to the TOE.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem. The security objectives declared for the TOE operational environment in the [ST] are categorized below.

IT Security Objectives

IT Security Objectives Name	Description
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.NETWORK	The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.
OE.ADMIN_PROTECT	The TOE administrator workstation must be protected from any external interference or tampering.

Non-IT Security Objectives

Non-IT Security Objectives Name	Description
OE.MANAGE	Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.
OE.PHYSICAL	The physical environment must be suitable for supporting a computing device in a secure setting.

ARCHITECTURE

LOGICAL ARCHITECTURE

Logical boundaries

Conceptually the TOE can be thought of as a collection of the following security services which the security target describes with increasing detail:

Security Audit

The TOE generates audit records for startup and shutdown of the appliance and all administrator-initiated, non-read operations performed on an array through the NimbleOS API, NimbleOS CLI, or NimbleOS GUI. Only TOE

administrators with the Administrator role can view the audit records for all administrator-initiated, non-read operations performed on an array. All TOE administrators can view the startup and shutdown events. All TOE administrators are prevented from deleting the audit records. The audit records show the identity of the user that performed the operation.

Cryptographic Support
The TOE uses the Nimble Storage, Inc. FIPS Object Module cryptographic module to perform cryptographic operations. These cryptographic operations are used to secure communications from remote administrators at the NimbleOS GUI, API, and CLI. They are also used to encrypt data at rest on selected volumes within an array, protect the keys used for data encryption, and provide X.509 certificates. All cryptographic keys generated by the TOE. Keys are destroyed according to FIPS 140-2 zeroization methods. The master key that encrypts volume keys is zeroized when destroyed.

User Data Protection
The TOE enforces the Storage Access Control SFP to control iSCSI and FC client access to Nimble array volumes. An authorized TOE administrator configures this access by setting security attributes using the NimbleOS GUI, CLI, or API. If these security attributes are not configured, clients have no access to volumes on the Nimble arrays.

The Encrypted Volume Access Control SFP ensures that only authorized TOE administrators with the Administrator, Power User, or Operator role can encrypt and replicate volumes, manage iSCSI and FC clients' security attributes, manage volume ACLs, and manage user roles. Once a volume is set as encrypted, it is stored and replicated in an encrypted form.
Data storage integrity is provided with triple+ parity RAID capabilities that monitor checksums on user data for errors. If an error cannot be repaired, the corresponding drive is declared failed.

The TOE provides volume and volume collection snapshot capabilities, allowing for the rollback of a volume or volume collection to the point in time a chosen snapshot was created. All of the operations on a volume can be rolled back.

Identification and Authentication
TOE administrator authentication can be performed in multiple ways on the TOE. NimbleOS supports local and AD authentication. All TOE administrators must be identified and authenticated prior to performing any actions at the NimbleOS GUI, API, or CLI. Note that end-users are not authenticated directly by the TOE. They connect to the iSCSI and FC clients, which are restricted access based on the Storage Access Control SFP.

The TOE maintains the following list of security attributes belonging to local user accounts: username, password, and role. The TOE obscures passwords

entered at the NimbleOS GUI during authentication using a bullet (•) in place of each character.

Security Management
The TOE is managed by TOE administrators in one of four roles: Administrator, Power User, Operator, or Guest. The TOE is capable of performing the following management functions: configuring arrays and volumes, configuring NTP, viewing the audit logs, configuring user authentication, performing snapshots and rollbacks, setting access controls, and configuring X.509 certificates for TLS. Only the NimbleOS CLI can be used to configure X.509 certificates. The TOE will restrict access to management functions based on the user's privilege level.

The TOE enforces the Encrypted Volume Access Control SFP to restrict the ability to manage security attributes to TOE administrators with the Administrator, Power User, and Operator role. These security attributes restrict access to NimbleOS arrays by default.

Protection of the TOE Security Functionality (TSF)
The TOE is able to preserve a secure state when up to two drives or a single controller on an array fails.

The TOE will provide reliable timestamps that are used for the audit trail. The TOE's time will be synchronized with an NTP server in the TOE environment.

Trusted Path/Channels
The TOE provides a trusted channel between itself and another trusted IT product (a replication partner in this case) by making secure connections over TLSv1.2. It uses this trusted channel to transfer wrapping keys that are used to protect volume encryption keys.

Using a supported Web browser, a remote TOE administrator initiates a secure connection to the TOE. The secure path is established using HTTPS for the NimbleOS GUI and NimbleOS API. Using an SSH client, a remote TOE administrator initiates a secure connection to the NimbleOS CLI over SSH. The HTTPS and SSH connections are used to protect data communications from modification or disclosure and ensure end point identification.

PHYSICAL ARCHITECTURE

Physical boundaries

The TOE is NimbleOS. NimbleOS v4.2 is a single binary that is pre-installed on each of the iSCSI and FC arrays (both Adaptive Flash and All Flash) shipped to a customer. The same binary is pre-installed on each array supported by the TOE. In the evaluated configuration, the TOE is installed on a CS1000 iSCSI array and an AF1000 FC array.

DOCUMENTS

The guides listed below are required reading and part of the TOE. This Nimble documentation (in PDF format) is available to authorized users on the Nimble InfoSight Support Portal at https://infosight.nimblestorage.com/InfoSight/login.

- Nimble Storage Hardware Guide, AF1000, AF3000, AF5000, AF7000, AF9000, AFS2, Version 3, Revision A

- Nimble Storage Array Quick Start Guide – Array Installation – All Flash, Revision C, 03/20/2017

- Nimble Storage Hardware Guide, CS1000H, CS1000, CS3000, CS5000, CS7000, ES2-H, ES2-AFS2, June 9, 2017

- Nimble Storage Array Installation – Adaptive Flash Quick Start Guide, Revision A, 05/02/2017

- Nimble Storage GUI Administration Guide, Version 4, Published Date: April 20, 2017

- Nimble Storage CLI Administration Guide, Version 4, Published Date: April 20, 2017

- Nimble Storage Command Reference, Version 4, Published Date: April 20, 2017

- Nimble Storage REST_API_ 4.2.0.1.zip (a collection of HTML files)

- Nimble Storage, Inc.; NimbleOS v4.2; Guidance Documentation Supplement; Evaluation Assurance Level (EAL); EAL2+; Document version: 0.7 (available only with the TOE link)

PRODUCT TESTING

The tests performed by both the evaluator and the developer are based on the TSFIs description included in the functional specification and the SFRs description included in the security target [ST].

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals. The TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to security target [ST]. The evaluator has repeated all the cases specified by the developer in the test documentation and has compared the obtained results with those obtained by the developer and documented in each associated report. The test repetition performed by the evaluator has demonstrated that the test plan and report provided by the vendor

contains information enough to make a reader able to repeat all tests included. Additionally, after the repetition, the evaluator has obtained the same results as the expected ones. The independent testing has covered 100% of SFRs of the [ST] and TSFIs defined in the functional specification for the TOE, sampling has not been performed. The test cases have taken into account critical parameters values, searching that the TOE behaves in a non-expected manner. There has not been any deviation from the expected results under the environment defined in security target [ST].

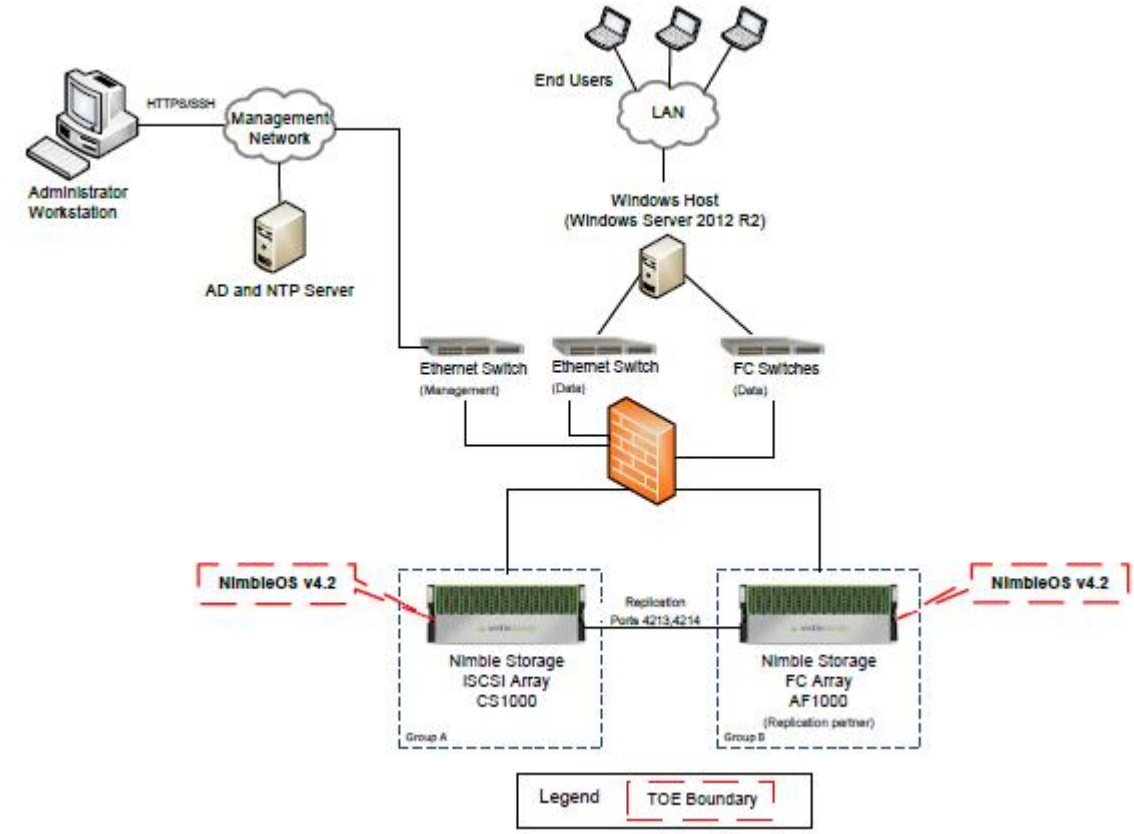
PENETRATION TESTING

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals. The TOE does NOT present exploitable vulnerabilities under the environment defined in the security target [ST]. All identified vulnerabilities can be considered closed if the TOE is installed and operated according to the security target [ST] and related documentation. The overall test result is that no deviations were found between the expected and the actual test results taking into account that environment. No attack scenario with the attack potential “Basic” has been successful in the TOE’s operational environment as defined in the security target [ST] when all measures required by the developer are applied.

EVALUATED CONFIGURATION

The TOE under evaluation is “Nimble Storage Inc. NimbleOS, version 4.2.0.1-499435-opt”.

The evaluated configuration consists of two groups that each consist of a single array. One group includes a CS1000 iSCSI array; the other includes an AF1000 FC array. The following figure depicts the detailed deployment diagram for the TOE components in the evaluated configuration with the two groups indicated as Group A and Group B



EVALUATION RESULTS

The product “Nimble Storage Inc. NimbleOS, version 4.2.0.1-499435-opt” has been evaluated against the “Nimble Storage, Inc. NimbleOS Security Target, version 0.9, November 2017”.

All the assurance components required by the evaluation level EAL2 + ALC_FLR.2 have been assigned a “PASS” verdict. Consequently, the laboratory Epoche & Espri S.L.U assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL2 + ALC_FLR.2, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

The TOE usage is recommended given that there are not exploitable vulnerabilities in the operational environment. The following usage recommendation is given:

- The fulfilment of the assumptions indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.

CERTIFIER RECOMMENDATIONS

Considering the evidences obtained during the instruction of the certification request of the product “Nimble Storage Inc. NimbleOS, version 4.2.0.1-499435-opt”, a positive resolution is proposed.

GLOSSARY

ACL Access Control List.

CCN Centro Criptológico Nacional

CHAP Challenge-Handshake Authentication Protocol

CNI Centro Nacional de Inteligencia

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

IQN iSCSI Qualified Name

iSCSI Internet Small Computer System Interface

OC Organismo de Certificación

RAID Redundant Array of Independent Disks

RBAC Role Based Access Control

SAN Storage Area Network

SFR Security Functional Requirement

TOE Target Of Evaluation

TSF TOE Security Functionality

TSFI TSF Interface

WWPN World Wide Port Name

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R4 Final, Sept. 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, Sept. 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, Sept. 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, Sept. 2012.

[ST] Nimble Storage, Inc. NimbleOS Security Target, version 0.9, November 2017

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- Nimble Storage, Inc. NimbleOS Security Target, version 0.9, November 2017