REF: 2016-46-INF-2342 v1	Created by: CERT11
Target: Público	Revised by: CALIDAD
Date: 24.04.2018	Approved by: TECNICO

CERTIFICATION REPORT

File: 2016-46 Dell EMC VxRail Appliance

Applicant: Dell Technologies, Inc.

References:

[EXT-3180] Certification request of Dell EMC VxRail Appliance

[EXT-3895] Evaluation Technical Report of Dell EMC VxRail Appliance.

The product documentation referenced in the above documents.

Certification report of the product Dell EMC VxRail Appliance with VxRail 4.0.400-6628128 on 160 and Dell EMC VxRail Appliance with VxRail 4.0.400-6628128 on 160F, as requested in [EXT-3180] dated 08/11/2016, and evaluated by the laboratory Epoche & Espri S.L.U, as detailed in the Evaluation Technical Report [EXT-3895] received on 17/04/2018.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification dossier of the product Dell EMC VxRail Appliance with VxRail 4.0.400-6628128 on 160 and Dell EMC VxRail Appliance with VxRail 4.0.400-6628128 on 160F.

The TOE is a software and hardware product, which provides a software defined data center that can support hundreds virtual machines and their associated data.

Developer/manufacturer: Dell Technologies, Inc.

Sponsor: Dell Technologies, Inc.

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Epoche & Espri S.L.U.

Protection Profile: None.

Evaluation Level: EAL 2 + ALC_FLR.2.

Evaluation end date: 17/04/2018.

All the assurance components required by the evaluation level EAL 2 (augmented with 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 EAL 2, 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 Dell EMC VxRail Appliance with VxRail 4.0.400-6628128 on 160 and Dell EMC VxRail Appliance with VxRail 4.0.400-6628128 on 160F, a positive resolution is proposed.

TOE SUMMARY

VxRail appliances are built to provide all mission-critical services for a SDDC, including virtualization, compute, and storage. Full integration with VMware’s vSphere, and Virtual SAN (vSAN) provide the backbone of the appliance. The appliances are deployed in clusters ranging from 4 to 16 nodes. A node provides computation for the appliance and contains multiple processors. Each 2U appliance includes the 4-node base that is required for cluster operations. A single appliance can support up to 200 virtual machines (VMs). VxRail’s hyper-converged infrastructure provides customer VMs with the power of an entire Storage Attached Network (SAN) in a single appliance.

Hyper-convergence is an emerging technology that refers to complete systems that provide compute resources for running a VM infrastructure and shared storage for use by VMs. Hyper-converged solutions run entirely on x86 servers with commodity internal solid-state and hard-disk drives for storage. Customers deploy the system as

appliances that scale in a linear fashion; each node added to a VxRail cluster contributes a fixed amount of computational power and storage capacity. Hyper-convergence relies on software-defined storage as an underlying technology that is provided by VMware vSphere and vSAN. This software-defined storage allows the storage within individual servers to be shared across every node in a VxRail cluster.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL 2 and the evidences required by the additional component ALC_FLR.2, according to Common Criteria v3.1 R4.

Class	Family/Component
ASE: Security Target Evaluation	ASE_INT.1. ST Introduction ASE.CCL.1. Conformance claims ASE_SPD.1. Security problem definition ASE_OBJ.2. Security objectives ASE_ECD.1. Extended component definition ASE_REQ.2. Derived security requirements ASE_TSS.1. TOE summary specification
ADV: Development	ADV_ARC.1. Security architecture ADV_FSP.2. Functional specification ADV_TDS.1. TOE design
AGD: Guidance documents	AGD_OPE.1. Operational user guidance AGD_PRE.1. Preparative procedures
ALC: Life cycle support	ALC_CMC.2. CM capabilities ALC_CMS.2. CM Scope ALC_DEL.1. Delivery ALC_FLR.2. Flaw remediation
ATE: Tests	ATE_COV.1. Coverage ATE_FUN.1. Functional tests ATE_IND.2. Independent testing
AVA: Vulnerability assessment	AVA_VAN.2. Vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

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

Class	Component
FAU: Security audit	GEN.1 Audit data generation STG.1 Protected audit trail STG.4 Prevention of audit data loss
FDP: User data protection	ACC.1 Subset access control ACF.1 Security attribute based access control SDI.2 Stored data integrity

FIA: Identification and authentication	UAU.2 User authentication before any action UAU.7 Protected authentication feedback UID.2 User identification before any action
FMT: Security management	MSA.1 Management of security attributes MSA.3 Static attribute initialisation SMF.1 Specification of management functions SMR.1 Security roles
FPT: Protection of the TSF	FLS.1 Failure with preservation of secure state STM.1 Reliable time stamps TDC.1 Inter-TSF basic TSF data consistency
FRU: Resource Utilization	FLT.2 Limited fault tolerance RSA.1 Maximum quotas
FTA: TOE Access	SSL.4 User-initiated termination
FHA: High Availability (extended)	TST.1 TSF health testing

IDENTIFICATION

Product: Dell EMC VxRail Appliance with VxRail 4.0.400-6628128 on 160 and Dell EMC VxRail Appliance with VxRail 4.0.400-6628128 on 160F

Security Target: Dell Technologies, Inc. Dell EMC VxRail Appliance Security Target, version.1.0. 23/02/2018.

Protection Profile: None.

Evaluation Level: Common Criteria v.3.1 R4 - EAL 2 + ALC_FLR.2.

SECURITY POLICIES

There are no Security Policies imposed upon the TOE or its operational environment.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. 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.

The detail of these assumptions is documented in the Security Target, section 3.3.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Dell EMC VxRail Appliance with VxRail 4.0.400-6628128 on 160 and Dell EMC VxRail Appliance with VxRail 4.0.400-6628128 on 160F, although the agents implementing attacks have the attack potential according to the BASIC of EAL 2 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 detail of these threats is documented in the Security Target, section 3.1.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

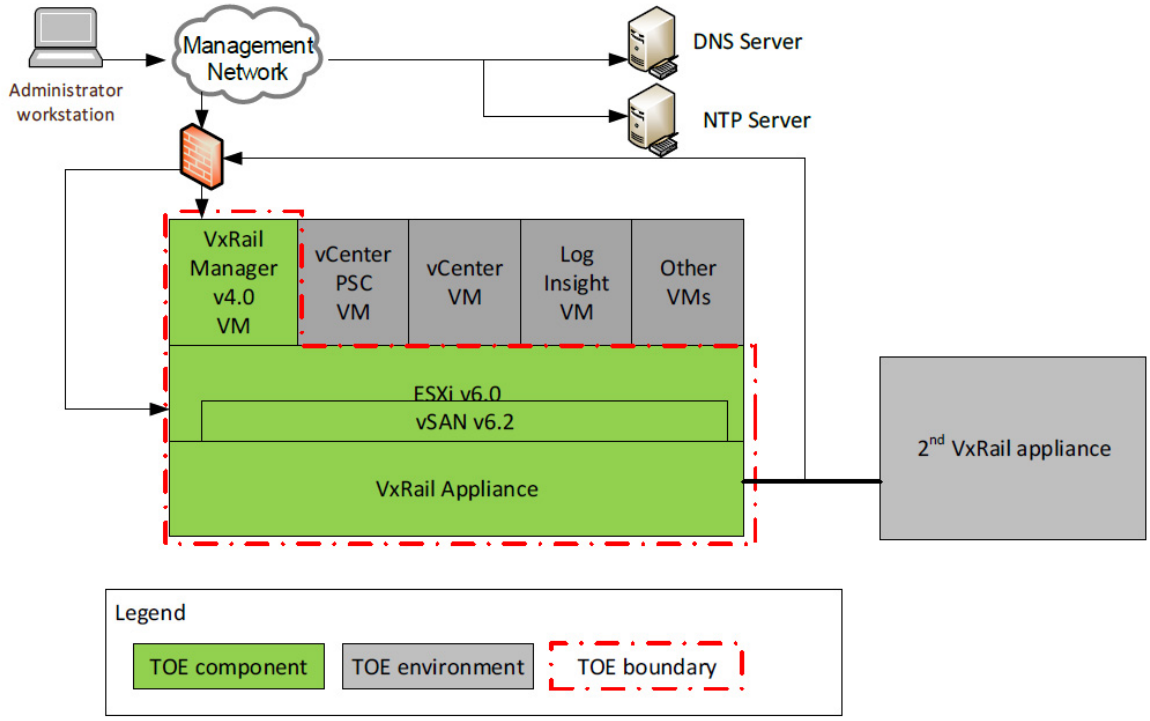
The detail of these security objectives for the TOE operational environment is documented in the Security Target, section 4.2.

ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE consists of the following components:

- VxRail Appliance – VxRail 160 or 160F appliance
- VMware ESXi v6.0.0 build-6509460 – ESXi is the hypervisor running in the VxRail appliance. ESXi includes VMware vSAN v6.2 in its kernel.
- VxRail 4.0.400-6628128 – VxRail Manager is the software that monitors nodes, disks, power supplies, and VMs to alert an Administrator9 to potential issues. The VxRail software includes:
    - VxRail Manager application – presents the VxRail GUI
    - SUSE Linux operating system (OS) – host OS on the VxRail VM



PHYSICAL ARCHITECTURE

The appliances included in the TOE boundary for this evaluation includes one of the following appliances:

- VxRail 160
- VxRail 160F

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

The following guides are required reading and part of the TOE:

- Dell EMC VxRail Appliance Version 4.0 Administration Guide, REV 01
- Administering VMware Virtual SAN, Virtual SAN 6.2, EN-002061-03, VMware
- VMware Virtual SAN 6.2 Release Notes, Updated on: 24 February 2017, 15 March 2016
- vSphere Virtual Machine Administration, Update 1, ESXi 6.0, vCenter Server 6.0, EN-001887-04, VMware
- vSphere Web Services SDK Programming Guide vSphere Web Services SDK 6.0, EN-001411-02, VMware

- vSphere Single Host Management – VMware Host Client, Update 2, VMware vSphere 6.0, VMware ESXi 6.0, VMware Host Client 1.4, EN-001982-00, VMware
- Dell Technologies, Inc. Dell EMC VxRail Appliance Guidance Documentation Supplement, Evaluation Assurance Level (EAL): EAL2+, Document Version: 0.5.26/02/2018.

PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator has repeated all the developer functional tests in the developer premises. Likewise, he has selected and repeated all the developer functional tests in the testing platform implemented in the evaluation laboratory.

In addition, the lab has devised a test for each of the security functions of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation, in respect to the expected results, was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product Dell EMC VxRail Appliance with VxRail 4.0.400-6628128 on 160 and Dell EMC VxRail Appliance with VxRail 4.0.400-6628128 on 160F it is necessary that the TOE should be installed and set up by a qualified Dell Support Engineer, as described in the Dell Technologies, Inc. Dell EMC VxRail Appliance Guidance Documentation Supplement, document v0.5.

Dell installs all cables, networking equipment, and hardware components during the installation procedure. Additionally, Dell installs all Virtual Machines (VMs) needed to run the base system at this time. After installation is complete, the TOE should be running the following VMs:

- VMware vCenter Server Appliance

- VMware vCenter Server Platform Services Controller
- VMware vRealize Log Insight
- VxRail Manager

The configuration selected for the evaluation is the following:

- VxRail 160 and
- VxRail 160F

EVALUATION RESULTS

The product Dell EMC VxRail Appliance with VxRail 4.0.400-6628128 on 160 and Dell EMC VxRail Appliance with VxRail 4.0.400-6628128 on 160F has been evaluated against the Security Target "Dell Technologies, Inc. Dell EMC VxRail Appliance Security Target, version 1.0. 23/02/2018".

All the assurance components required by the evaluation level EAL 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 EAL 2, as defined by 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. Nonetheless, the following usage recommendations are 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 obtained evidences during the instruction of the certification request of the product Dell EMC VxRail Appliance with VxRail 4.0.400-6628128 on 160 and Dell EMC VxRail Appliance with VxRail 4.0.400-6628128 on 160F, a positive resolution is proposed.

GLOSSARY

CCN Centro Criptológico Nacional

CNI Centro Nacional de Inteligencia

EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
SAN	Storage Area Network (vSAN: Virtual SAN)
TOE	Target of Evaluation
VM	Virtual Machine

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, September 2012.

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

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

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

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

- Dell Technologies, Inc. Dell EMC VxRail Appliance Security Target, version 1.0. 23/02/2018.

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at *https://www.sogis.org*.

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

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including

EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: *http://www.commoncriteriaportal.org*.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.