Ministero dello Sviluppo Economico

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. 5/19

(Certification No.)

Prodotto: **Dell EMC VxRail Appliance 4.5**
(Product)

Sviluppato da: **Dell Technologies, 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)

Roma, 16 luglio 2019

Common Criteria

SOGIS IT SECURITY CERTIFIED

This page is intentionally left blank

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Dell EMC VxRail Appliance 4.5

OCSI/CERT/CCL/10/2018/RC

Version 1.0

16 July 2019

Courtesy translation

Disclaimer: this translation in 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

Version	Author	Information	Date
1.0	OCSI	First issue	16/07/2019

2 Table of contents

3 Acronyms

API	Application Programming Interface
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
DNS	Domain Name Service
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza (ITSEF)
NIS	Nota Informativa dello Schema
NTP	Network Time Protocol
OCSI	Organismo di Certificazione della Sicurezza Informatica
PP	Protection Profile
REST	Representational State Transfer
RFV	Rapporto Finale di Valutazione (Evaluation Technical Report)
SAN	Storage Attached Network
SAR	Security Assurance Requirement
SDDC	Software-Defined Data Center
SFR	Security Functional Requirement
SOGIS	Senior Officials Group Information Systems Security
SSD	Solid State Device
SSO	Single Sign-On
TDS	Traguardo di Sicurezza (Security Target)
TOE	Target of Evaluation

TSF	TOE Security Functionality
TSFI	TSF Interface
2U	Two rack Units
VM	Virtual Machine
vSAN	Virtual Storage Attached Network

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

[ADM] Dell EMC VxRail Appliance, Version 4.5.x, Administration Guide, Rev. 04, April 2018

[CONF] VxRail Application, Version 4.5.x, Security Configuration Guide, Rev. 01, March 2018

[DEL] Dell EMC VxRail Appliance 4.5 Secure Delivery Document, v0.2, 7 January 2019

[RFV] Dell EMC VxRail Appliance 4.5, Evaluation Technical Report, v1, 3 June 2019

[TDS] Dell EMC VxRail Appliance 4.5, Security Target, v0.6, 22 May 2019

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 http://www.sogisportal.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 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] has been 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 EAL 2, 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 product “Dell EMC VxRail Appliance 4.5”, developed by Dell Technologies, Inc.

The TOE is a hyper-converged infrastructure hardware appliance providing a software defined data center, that can support hundreds virtual machines and their associated data. Multiple appliances can be clustered together to extend the storage resource and provide high availability options for the stored data.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [TDS]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL2, augmented with ALC_FLR.2, according to the information provided in the Security Target [TDS] 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 “Dell EMC VxRail Appliance 4.5” 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 review also the Security Target [TDS], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Dell EMC VxRail Appliance 4.5
Security Target	“Dell EMC VxRail Appliance 4.5” Security Target, v0.6, 22 May 2019
Evaluation Assurance Level	EAL2 augmented with ALC_FLR.2
Developer	Dell Technologies, Inc.
Sponsor	Corsec Security, Inc.
LVS	CCLab Software Laboratory
CC version	3.1 Rev. 5
PP conformance claim	No compliance declared
Evaluation starting date	4 December 2018
Evaluation ending date	3 June 2019

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 [TDS] are fulfilled.

7.3 Evaluated product

This section summarizes the main functional and security requirements of TOE; for a detailed description, please refer to the Security Target [TDS].

The TOE is a hyper-converged infrastructure hardware appliance providing a software defined data center, that can support hundreds virtual machines and their associated data. Multiple appliances can be clustered together to extend the storage resource and provide high availability options for the stored data.

VxRail appliances are built to provide all mission-critical services for a Software-Defined Data Center (SDDC), including virtualization, compute, and storage. The appliances are deployed in clusters ranging from 3 to 32 nodes. A node provides computation for the appliance and contains multiple processors. With the exception of the E Series appliances, each appliance is a two rack units (2U) form factor supporting either one node (the V, P, and S Series) or up to four nodes (the G Series). The E Series is a 1U form factor supporting one node. A single E, G, V, P, or S Series appliance can support up to 200 virtual machines (VMs). VxRail's hyper-converged infrastructure provides customer VMs with the power of an entire 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. This software-defined storage allows the storage within individual servers to be shared across every node in a VxRail cluster.

7.3.1 TOE Architecture

For a detailed description of the TOE, please refer to sect. 1.5 "TOE Description" of the Security Target [TDS]. The most significant aspects are summarized below (see Figure 1).

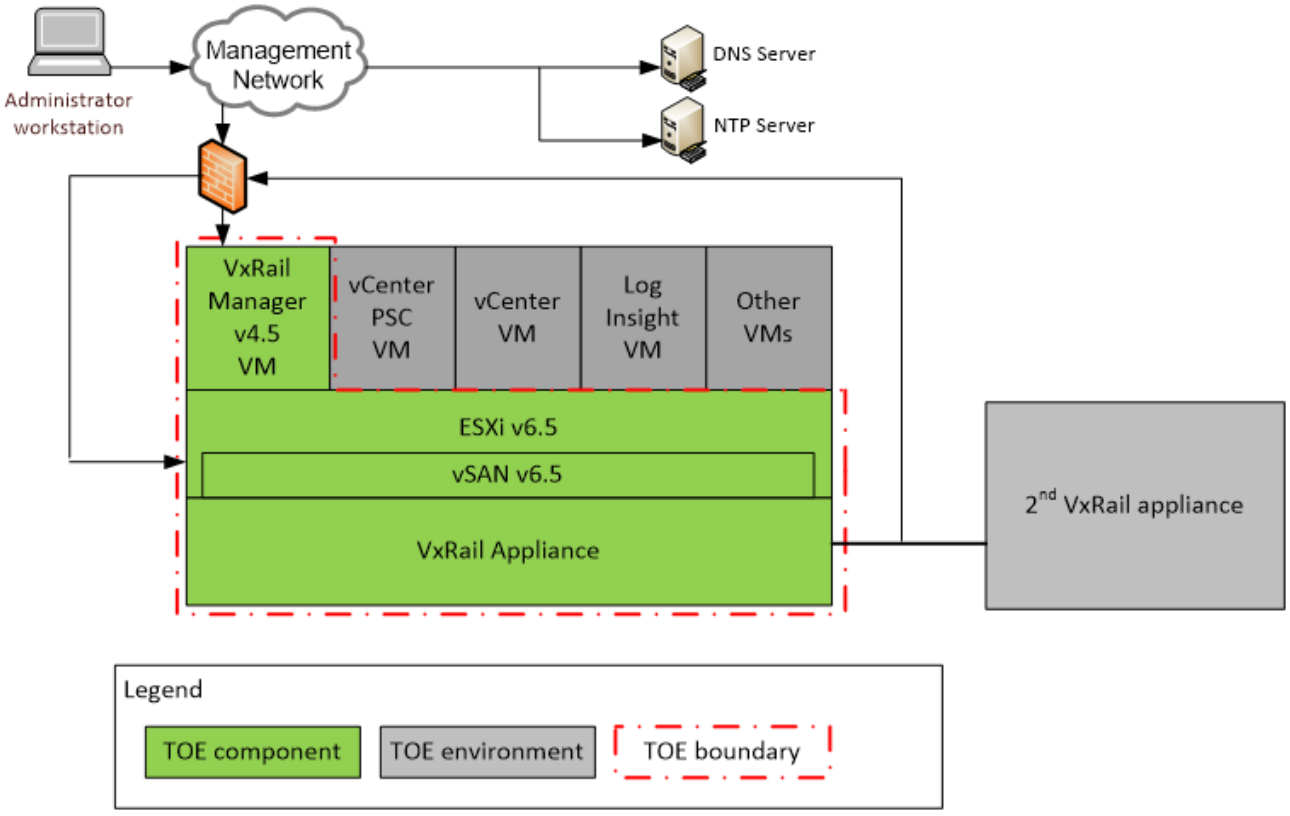

Figure 1 – Deployment Configuration of the TOE

The TOE consists of the following components:

- VxRail Appliance – VxRail E560, E560F, P570, P570F, V570, V570F, S570, G560, or G560F appliance
- VMware ESXi v6.5 EP 9 build-10175896 – ESXi is the hypervisor running in the VxRail appliance. ESXi includes VMware vSAN v6.5 EP 9 build-10175896 in its kernel
- VxRail Manager v4.5.225-10233140 – VxRail Manager is the software that monitors nodes, disks, power supplies, and VMs to alert an Administrator to potential issues. The VxRail software includes:
    - VxRail Manager application – presents the VxRail Manager GUI and VxRail REST API
    - SUSE Linux operating system (OS) – host OS on the VxRail VM

The TOE boundary does not include customer supplied VMs or any external components such as a DNS or NTP server or network infrastructure. VMware vCenter is also excluded from the boundary. Though not included in the TOE boundary, all components are required in the TOE environment.

Administrators of the TOE can access security services through the following interfaces:

- VxRail Manager GUI – The VxRail Manager GUI provides statistics and alerts about monitored hardware, networks, and VMs as well as functionality to power down the appliance and deploy VMs.
- VxRail REST API – The VxRail REST API provides limited functionality that can be used to view information about the TOE by using REST calls to get and set data.
- Linux Shell Interface – The Linux Shell Interface provides limited access to the host OS on the VxRail Manager VM. Authorized Administrators can access audit logs through this interface and power off the VxRail Manager VM.
- vSphere API – The vCenter VM in the TOE environment uses the vSphere API for communicating storage policies and VM configurations to the ESXi hypervisor. The vSphere Web API is also an exposed web service running on both the vCenter VM and on each ESXi host. In the evaluated configuration is recommended that only the vSphere API on the vCenter Server be used to maintain consistency on all ESXi hosts.
- VMware Host Client – Each ESXi host maintains a VMware Host Client interface that can be used to manage the single ESXi host. In the evaluated configuration it is recommended that this interface only be used for emergency management when vCenter Server is unavailable.

Each ESXi node offers a vSphere Web UI and access to the vSphere API, but these should not be used for administrative actions. The nodes should be administered through vCenter. The TOE can be deployed in various configurations from a single appliance to multiple appliances clustered across physically separate datacenters. In the evaluated

configuration a single appliance and two appliances clustered together have been considered

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 [TDS].

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

- **Security Audit**. The TOE generates audit records and stores them in the VxRail Manager filesystem. Each log type has a maximum file size and maximum number of files that are saved. If all files become full, the oldest file is overwritten with a new log file. Audit events include startup and shutdown of the appliance, disk failures, node failures, and authentication events. The log file is protected from unauthorized deletion and modification. Only an authorized Administrator can modify or delete these files.

- **User Data Protection**. The TOE uses a data access approach defined by the Virtual Disk Access SFP. VMs are assigned a virtual disk when created. The TOE ensures that VMs can only access files stored in their assigned virtual disk. The TOE monitors the stored data for integrity errors using an end-to-end checksum. If an error is detected, the TOE will attempt to repair the data, update the disk statistics, and record an event in the event log.

- **Identification and Authentication**. The TOE requires Administrators to identify and authenticate themselves prior to accessing the TSF, except when receiving the output of the host API. The TOE relies on vCenter's Single Sign-On (SSO) service to authenticate Administrators. Rules for creating usernames and passwords are determined by policies established in vSphere. When an Administrator enters their password, the TSF provides obscured feedback on its interfaces.

- **Security Management**. The TOE provides the Administrator, vCenter System, ESXi Root, and CLI Root roles. The Administrator roles have access to the VxRail Manager GUI and VxRail REST API to perform various tasks including system monitoring, deploy a VM, and gracefully shutdowns of VMs. The CLI Root role has access to the Linux shell interface to view information and submit commands and can access log files. The vCenter Server is provided the vCenter System role within ESXi to communicate storage policies and VM configurations. Storage policies are restrictive by default and can only be modified in vCenter and sent to the TOE using the proxy account. Both the Administrator and vCenter proxy account can change a VM name. The ESXi Root role is used to access individual ESXi hosts for maintenance purposes and troubleshooting only.

- **Protection of the TSF**. The TOE will maintain a secure state when disk read errors cause various disks on a node to fail. Different storage policies can be set for each VM, allowing the protection level to vary per VM. VxRail monitors the appliances' power supplies, nodes, and disks to ensure they are operational and it will show an alert in the VxRail Manager GUI if an error is detected. TSF data is sent from the vCenter VM to the ESXi hypervisor for enforcement of the storage policies and VM

configurations. The TOE consistently interprets this data by ensuring that available CPU, storage, and network data is sent to vCenter. The TOE verifies that vCenter does not allocate more than the available resources for these components when it receives updates. When an update is sent, the TOE will replace any previous data with the updated data.

- **Resource Utilization**. The TOE provides continuous functionality when disk read errors cause various disks on a node to fail. Increased fault tolerance can be assigned to individual VMs. The TSF can enforce maximum size restrictions on VMs.

- **TOE Access**. The TOE's interfaces provide Administrators with an option to log out and end the session. This prevents the session from sitting open when the Administrator is not at their workstation.

- **High Availability**. The TOE monitors underlying disks, networks, and nodes to determine overall health and statistics on these components. Alerts are shown on the VxRail Manager GUI if a component fails or is in a degraded state. Additionally, if a disk has been improperly removed an alert is shown.

7.4 Documentation

The guidance documentation specified in Annex A – Guidelines for the secure usage of the product is delivered to the customers together with the product. The guidance documentation contains all the information for secure installation, initialization, configuration and secure usage the TOE in accordance with the requirements of the Security Target [TDS].

Customers should also follow the recommendations for the security use of the TOE contained in sect. 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [TDS] 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 or derived by extension from CC Part 2 [CC2]. In particular, the extended component FHA_TST.1: System Testing has been defined, which provides the capability for the TOE to perform tests on assigned functions to ensure its proper function. For a detailed description of the extended component properties, consult sect. 5.2 of the Security Target [TDS].

Please refer to the Security Target [TDS] 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 [TDS]. 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 3 June 2019 with the issuance by LVS of the Evaluation Technical Report [RFV], which was approved by the Certification Body on 25 June 2019. 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 [TDS], with reference to the operating 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 [RFV] issued by the LVS Systrans CCLAB and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE “Dell EMC VxRail Appliance 4.5" 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 [TDS] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL2, augmented with ALC_FLR.2.

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
Flaw reporting procedures	ALC_FLR.2	Pass

Assurance classes and components		Verdict
Test	**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 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 "Dell EMC VxRail Appliance 4.5" are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [TDS].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 4.2 of the Security Target [TDS]. It is assumed that, in the operating environment of the TOE, all the assumptions and the organizational security policies described in the Security Target are respected.

This Certification Report is valid for the TOE in the evaluated configuration; in particular, Annex A – Guidelines for the secure usage of the product includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([ADM], [CONF]).

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

Several procedures are necessary for Dell EMC to maintain security of the TOE during distribution. Before shipping, some preliminary activities are performed:

- pre-delivery activities for the software, hardware, and documentation components of the TOE shipment;
- TOE labeling, which includes serial numbers, model numbers and logos;
- TOE Packaging.

The TOE is shipped from Dell EMC and delivered to the customer by a commercial shipping carrier with a package tracking system.

More detail on such a procedure are contained in “Secure Delivery Document” [DEL].

9.2 Installation, initialization and secure usage of the TOE

Once the TOE is delivered to the customer, an authorized Dell EMC Professional Service Team member must physically install the appliance on-site. If software installation is required on-site, the Dell EMC Professional Service Team member will verify software downloads with a hash that is provided on the Dell EMC Support site. Additionally, TOE software can be installed on the TOE appliance prior to shipment.

Dell EMC Professional Services Team members can verify the contents of the TOE shipment by reviewing the packing list, which is included in the TOE packaging, and the shipping label, which is affixed to the side of the box in which the TOE is shipped, and matching the internal model numbers to the corresponding external Dell EMC VxRail model numbers.

All TOE deliveries are installed for the customer by a member of the Dell EMC Professional Services team following the following deployment documentation:

- “Dell EMC VxRail Appliance, Version 4.5.x, Administration Guide” [ADM], containing detailed steps for how to properly configure and maintain the TOE;
- “VxRail Application, Version 4.5.x, Security Configuration Guide” [CONF], providing an overview of security configuration settings for the VxRail Appliance and best practices for using those settings to ensure secure operation of the product.

Once the installation is complete, customers can verify the TOE’s software versions by logging in to the VxRail Manager Graphical User Interface (GUI) with a username and password and navigating to the General tab.

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product “Dell EMC VxRail Appliance 4.5”, developed by Dell Technologies, Inc.

The appliances must be setup in a cluster that include at least 3-nodes. A single appliance can support up to 200 VMs. All software components are pre-installed on the appliance prior to shipment to customers.

The TOE’s functionality is the same regardless of the hardware appliance on which they are installed. The software varies only according to low-level driver differences needed for the different appliance models.

The TOE is identified in the Security Target [TDS] with the version number 4.5. The name and version number uniquely identify the TOE and the set of its subsystems, constituting the evaluated configuration of the TOE, verified by the Evaluators at the time the tests are carried out and to which the results of the evaluation are applied.

For more details, please refer to sect. 1.5 of the Security Target [TDS].

10.1 TOE operational environment

The TOE relies on non-TOE hardware/software for its essential operation. Though this hardware/software is necessary for the TOE’s operation, it is not part of the TOE. The following non-TOE hardware/software is required for essential operation of the TOE:

- VMware vCenter Server – The TOE is delivered with vCenter pre-installed on the VxRail appliance. The TOE relies on vCenter for authentication, creation of storage policies, and to maintain the list of VMs installed on the appliance. The vCenter component consists of two VMs on the appliance.

- Log Insight VM – v4.3.0 build 5084751 – Log Insight collects and analyzes log data on customer installed VMs.

- DNS server – A DNS server is required for network address resolution.

- NTP server – An NTP server is required as a time source.

- Customer installed VMs – The TOE provides virtualization and storage for customer VMs to suit their business needs. An arbitrary number of VMs can be deployed, not exceeding the physical resources provided by the TOE.

- Firewall – A firewall protects the TOE interfaces.

- At least one 10GbE network switch with eight switch ports is also required to provide network switching for the TOE.

- Cabling – the following cables or equivalent are required for each type of port:

  - RJ45 Network Interface Cards (NIC) ports – 2 x CAT6 or higher cables per node which are shipped with the TOE
  - SFP+ NIC ports – 2 x compatible twinax DAC cables per node or 2 x fiber cables per node

- Administrator workstation – This workstation is used to access the VxRail GUI via an industry-standard browser and VxRail REST API via a REST client.

For more details, please refer to sect. 1.4.2 and 1.5.1.1 of the Security Target [TDS].

11 Annex C – Test activity

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

For the execution of these activities a test environment has been arranged at the LVS site with the support of the developer, which provided the necessary resources.

The installation of the test environment was in accordance with the guidance documentation ([ADM], [CONF]), as indicated in Annex A – Guidelines for the secure usage of the product.

After configuration of the TOE the evaluators checked the status and found that the TOE was installed properly, and the needed services were running.

The test environment is the same as the developer used for testing the TSFI.

11.2 Functional tests performed by the developer

11.2.1 Test coverage

The evaluators have examined the test plan presented by the developer and verified the complete coverage of the functional requirements SFR and the TSFIs described in the functional specification.

11.2.2 Test results

The evaluators executed a series of tests, a sample chosen from those described in the test plan presented by the developer, positively verifying the correct behavior of the TSFI and correspondence between expected results and achieved results for each test.

11.3 Functional and independent tests performed by the evaluators

Therefore, the evaluators have designed independent testing to verify the correctness of the TSFI.

They did not used testing tools in addition to the specific components of the TOE that allowed to check all TSFI selected for independent testing.

In the design of independent tests, the evaluators have considered aspects that in the developer test plan were not present, or ambiguous, or inserted in more complex tests, which covered a mix of interfaces but with a level of detail not adequate.

The evaluators also designed and executed some tests independently from similar tests of the developer, based only on the evaluation documentation.

All independent tests performed by evaluators generated positive results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities the same test environment already used for the activities of the functional tests has been used (see sect. 11.1)

The evaluators have first verified that the test configurations were consistent with the version of the TOE under evaluation, that is indicated in the [TDS], sect. 1.2.

In a first phase, the evaluators have conducted researches using various sources in the public domain, such as Internet, books, publications, conference proceedings, etc., in order to identify known vulnerabilities applicable to types of products similar to the TOE. In this research the Linux operating system has been also considered, part of the operational environment, but needed for the correct operation of the TOE. Some potential vulnerabilities have thus been identified.

In a second step, the evaluators examined the evaluation documentation (Security Target, functional specification, TOE design, security architecture and operational documentation) and used the automatic scanning tool Burp Suite, to identify any additional potential vulnerabilities of the TOE. From this analysis, the evaluators have actually determined the presence of other potential vulnerabilities.

The evaluators have analyzed in detail the potential vulnerabilities identified in the two previous steps, to ensure their effective exploitability in the TOE operating environment. This analysis led to identify some actual potential vulnerabilities.

Therefore, the evaluators have designed some possible attack scenarios, with Basic attack potential, and penetration tests to verify the exploitability of the potential candidate vulnerabilities. The penetration tests have been described with sufficient detail for their repeatability using for this purpose test sheets, also used, appropriately compiled with the results, as the report of the tests themselves. For executing the tests, the evaluator used the above mentioned Burp Suite tool.

The execution of the penetration tests confirmed the presence of vulnerabilities potentially exploitable by an attacker with a potential of attack Basic. These results were promptly reported to the Developer, via an Observation Report. The Developer has replied, accepting the evaluators' observations and releasing a new version of the Security Target with less stringent identification and authentication SFRs (FIA_UAU.1 and FIA_UID.1 instead of FIA_UAU.2 and FIA_UID.2). The evaluators checked such a new version of the TOE in the test environment, and were able to verify that the solution proposed by the Developer solved all the problems raised with the previous observations.

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