Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

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. 2/22

(Certification No.)

Prodotto: **Red Hat Virtualization v4.3**

(Product)

Sviluppato da: **Red Hat, 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.3)

Il Direttore
(Dott.ssa Eva Spina)

[ORIGINAL DIGITALLY SIGNED]

Roma, 18 gennaio 2022

Common Criteria

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

Red Hat Virtualization v4.3

OCSI/CERT/ATS/08/2020/RC

Version 1.0

18 January 2022

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	18/01/2022

2 Table of contents

3 Acronyms

ASLR	Address Space Layout Randomization
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CD-ROM	Compact Disc - Read-Only Memory
CEM	Common Evaluation Methodology
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HA	High Availability
I/O	Input / Output
iSCSI	Internet Small Computer Systems Interface
IT	Information Technology
KVM	Kernel-based Virtual Machine
LAF	Linux Audit Framework
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NFS	Network File System
NIAP	National Information Assurance Partnership
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
OS	Operating System

PAM	Pluggable Authentication Modules
PP	Protection Profile
QEMU	Quick EMUlator
RELRO	Read-only Relocation
RHEL	Red Hat Enterprise Linux
RHV	Red Hat Virtualization
RHV-M	Red Hat Virtualization Manager
RHVH	Red Hat Virtualization Host
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
VDSM	Virtual Desktop Server Manager
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMM	Virtual Machine Manager
VS	Virtualization System

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

4.2 Technical documents

[ECG]	“EAL2 Evaluated Configuration Guide for Red Hat Virtualization 4.3”, Version 0.9, Red Hat, Inc., 8 November 2021
[EPSV]	Extended Package for Server Virtualization, Version 1.0, NIAP, 17 November 2016
[ETR]	Final Evaluation Technical Report “Red Hat Virtualization v4.3”, Version 3.0, atsec information security GmbH, 9 December 2021
[PPVIRT]	Protection Profile for Virtualization, Version 1.0, NIAP, 17 November 2016
[RHVAG]	“Red Hat Virtualization 4.3 Administration Guide”, Red Hat, Inc., 6 October 2020
[RHVCP]	“Red Hat Virtualization 4.3, Installing Red Hat Virtualization as a selfhosted engine using the Cockpit web interface”, Red Hat, Inc., 10 September 2020
[RHVPG]	“Red Hat Virtualization 4.3 Product Guide”, Red Hat, Inc., 20 April 2020
[RHVTR]	“Red Hat Virtualization 4.3 Technical Reference”, Red Hat, Inc., 20 April 2020
[RHVPPG]	“Red Hat Virtualization 4.3 Planning and Prerequisites Guide”, Red Hat, Inc., 21 May 2020
[ST]	“Red Hat Virtualization Security Target”, Version 2.3, Red Hat, Inc., 8 December 2021

5 Recognition of the certificate

5.1 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 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 declared assurance components.

6 Statement of certification

The Target of Evaluation (TOE) is the product “Red Hat Virtualization v4.3”, developed by Red Hat, Inc.

The TOE is an enterprise-grade virtualization platform built on Red Hat Enterprise Linux. Virtualization allows users to provision new virtual servers and workstations and provides more efficient use of physical server resources.

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 [ST]; 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.3, 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 “Red Hat Virtualization v4.3” 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 [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Red Hat Virtualization v4.3
Security Target	“Red Hat Virtualization Security Target”, Version 2.3 [ST]
Evaluation Assurance Level	EAL2 augmented with ALC_FLR.3
Developer	Red Hat, Inc.
Sponsor	Red Hat, Inc.
LVS	atsec information security GmbH
CC version	3.1 Rev. 5
PP conformance claim	No compliance declared
Evaluation starting date	5 November 2020
Evaluation ending date	9 December 2021

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 “Red Hat Virtualization v4.3” is an enterprise-grade virtualization platform built on Red Hat Enterprise Linux. Virtualization allows users to provision new virtual servers and workstations and provides more efficient use of physical server resources.

Red Hat Enterprise Linux (RHEL) 7.9 provides virtualization primitives used by Red Hat Virtualization.

The components listed in Table 1 are part of the TOE.

Name	Description
Red Hat Virtualization Host (RHVH)	A minimal installation of the Red Hat Enterprise Linux (RHEL) environment establishes the Red Hat Virtualization Host. It contains the Linux kernel providing the KVM virtualization environment. In addition, the user space QEMU framework is provided which utilizes the KVM environment to instantiate virtual machines. The `libvirtd` management system controls the life-cycle of virtual machines.
Red Hat Virtualization Manager	A service that provides a graphical user interface and a REST API to manage the resources in the environment using virtualization primitives provided by the virtualization host as described above. The Manager is installed on a physical or virtual machine running Red Hat Enterprise Linux.

Table 1 - TOE components

While the RHVH component of the TOE is derived from RHEL 7.9, the RHEL OS itself is not part of the TOE.

For a detailed description of the TOE, consult sects. 1.4 and 1.5 of the Security Target [ST]. The most significant aspects are summarized below.

7.3.1 TOE architecture

The TOE is a Virtualization System. A simplified view of a generic Virtualization System and platform, provided in [PPVIRT], is reproduced in Figure 1. In this example, TOE components are shaded red and non-TOE components are shaded blue. The platform is the hardware, firmware, and software onto which the VS is installed.

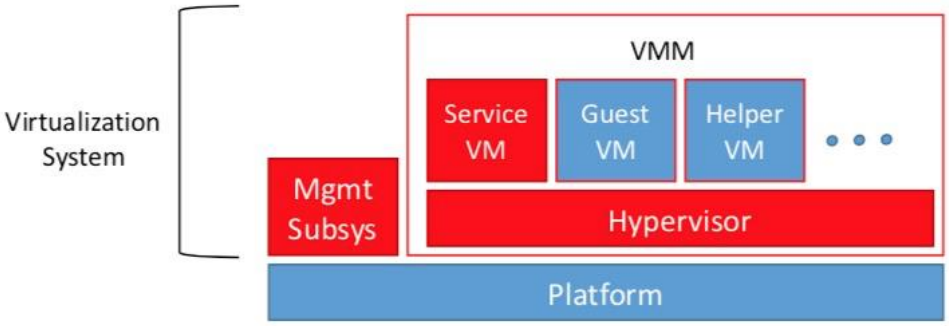

Figure 1 - Virtualization System and Platform

Red Hat Virtualization can be deployed as a self-hosted engine or as a standalone Manager. In the evaluated configuration, the TOE is deployed as a self-hosted engine. The complete Red Hat Virtualization deployment is created by installing the TOE in cooperation with other non-TOE components:

- storage service;
- data warehouse;
- metrics store.

7.3.1.1 Self-Hosted Engine Architecture

In the evaluated configuration, the Red Hat Virtualization Manager runs as a virtual machine on self-hosted engine nodes (specialized hosts) in the same environment it manages. A self-hosted engine environment requires one less physical server, but more administrative overhead to deploy and manage. The Manager is highly available without external HA management. The minimum setup of a self-hosted engine environment, as depicted in Figure 2, includes:

- One Red Hat Virtualization Manager virtual machine hosted on one of the self-hosted engine nodes. The RHV-M Appliance is used to automate the installation of a Red Hat Enterprise Linux 7 virtual machine and the Manager on that virtual machine.
- A minimum of two self-hosted engine nodes for virtual machine high availability. This can be achieved using Red Hat Enterprise Linux hosts or Red Hat Virtualization Hosts (RHVH). VDSM (the host agent) runs on all hosts to facilitate communication with the Red Hat Virtualization Manager. The HA services run on all self-hosted engine nodes to manage the high availability of the Manager virtual machine.
- One storage service which can be hosted locally or on a remote server depending on the storage type used. The storage service must be accessible to all hosts.

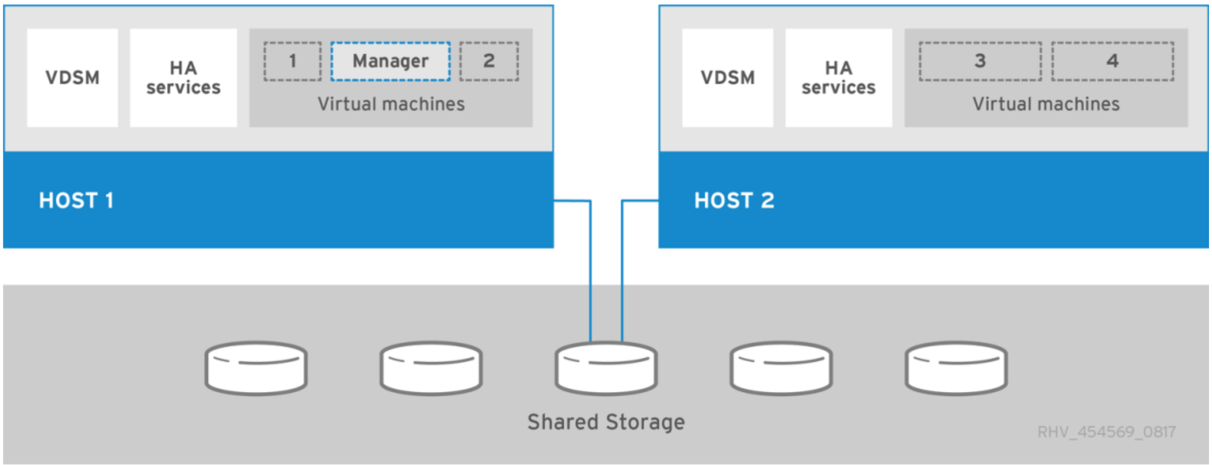

Figure 2 - Self-Hosted Engine Red Hat Virtualization Architecture

7.3.1.2 Red Hat Virtualization

Operations such as storage, host management, user connections, and virtual machine connectivity all rely on a well-planned and well-configured network to deliver optimal performance. Setting up networking is a vital prerequisite for a Red Hat Virtualization environment. Planning for projected networking requirements and implementing the network accordingly is much simpler than discovering networking requirements through use and altering the network configuration retroactively. Red Hat Virtualization separates network traffic by defining logical networks.

Logical networks define the path that a selected network traffic type must take through the network. They are created to isolate network traffic by functionality or to virtualize a physical topology.

The `ovirtmgmt` logical network is created by default and labeled as the Management network. The `ovirtmgmt` logical network is intended for management traffic between the Red Hat Virtualization Manager and hosts. Additional logical networks may be defined to segregate:

- general virtual machine traffic;
- storage-related traffic (such as NFS or iSCSI);
- virtual machine migration traffic;
- virtual machine display traffic;
- Gluster storage traffic.

7.3.1.3 Segregation of TOE Components from non-TOE Components

The TOE includes the components outlined in Table 1:

- the Red Hat Virtualization Host (RHVH), which is minimal installation of the Red Hat Enterprise Linux (RHEL) environment;
- the Red Hat Virtualization Manager which is provided via the oVirt management framework.

The oVirt framework allows the configuration of complex resources like Gluster, NFS or iSCSI storage. Any resource that is not local to the TOE instance is considered to be a non-TOE component. For example, the NFS server that may be accessed by the TOE and the guest operating systems managed by the TOE are not part of the TOE. In addition, the TOE allows the configuration of external authentication providers like LDAP or Active Directory. All authentication providers external to the TOE are non-TOE components. Only the authentication of users using the local user database is part of the TOE.

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 of the Security Target [ST]. The most significant aspects are summarized below:

- **Audit**: auditing support is implemented using the Linux Audit Framework (LAF). `libvirt` generates audit entries which are stored on disk by the audit daemon. The audit data can be reviewed using the `ausearch` utility.
  LAF is designed to be an audit system making Linux compliant with the requirements from Common Criteria. LAF is able to intercept all system calls as well as retrieving audit log entries from privileged user space applications. The subsystem allows configuring the events to be actually audited from the set of all

events that are possible to be audited. Those events are configured in a specific configuration file and then the kernel is notified to build its own internal structure for the events to be audited.

- **User Data Protection**: the TOE uses hardware-based isolation mechanisms and physical platform resource controls to protect user data.
  The TOE uses Linux kernel mechanisms, which in turn use hardware-based mechanisms, to constrain VMs when VMs have direct access to physical devices. The Linux kernel uses various hardware mechanisms to provide the virtualization support and ensure proper separation of virtual machines.
  The TOE provides a central location for users to perform logical network-related operations and search for logical networks based on each network's property or association with other resources.
  The TOE protects against residual information being left behind in both memory and on disk after use by a virtual machine.

- **Identification and Authentication**: the TOE uses RHEL authentication and password management functions. All administrative users must always authenticate when accessing consoles. The TOE utilizes the underlying Linux authentication mechanisms. The TOE (oVirt) authenticates users by using the PAM library offered by the basic Linux operating system.
  Using PAM authentication of users with the local user database is achieved. To access remote authentication providers like LDAP or Active Directory, oVirt uses appropriate PAM configurations. Remote authentication providers implement the authentication of users and return the information about authentication decisions to PAM which forwards the result to oVirt for enforcement. PAM also links with the Linux Auditing Framework to provide the capability to audit authentication requests. Users and their credentials and roles are allowed to be managed via an external directory server. A variety of directory server products are supported by the TOE.

- **Security Management**: hosts, also known as hypervisors, are the physical servers on which virtual machines run. Full virtualization is provided by using a loadable Linux kernel module called Kernel-based Virtual Machine (KVM).
  KVM can concurrently host multiple virtual machines running either Windows or Linux operating systems. Virtual machines run as individual Linux processes and threads on the host machine and are managed remotely by the Red Hat Virtualization Manager. A Red Hat Virtualization environment has one or more hosts attached to it.
  The security management of the TOE covers the entire life-cycle of Virtual Machines from the creation, starting, stopping, restarting and deletion of VMs.

- **Protection of the TSF**: the TOE provides functionality to mitigate the effects of buffer overrun vulnerabilities in applications and to protect against residual information remaining in memory or on disk between uses by different virtual machine instances.

- **Trusted Path/Channel**: the TOE implements trusted paths and trusted channels using components of the RHEL virtual machine environment.

7.4 Documentation

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

The guidance documentation contains all the information for secure initialization, configuration and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in 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 the SFRs have been selected or derived by extension from CC Part 2 [CC2].

Although it does not claim conformance to any PP, the Security Target [ST] defines the following extended functional components based on the virtualization SFRs defined in [PPVIRT] (all except FMT_MOF_EXT.1) and [EPSV] (FMT_MOF_EXT.1 only):

- FDP_HBI_EXT.1 (Hardware-Based Isolation Mechanisms)
- FDP_PPR_EXT.1 (Physical Platform Resource Controls)
- FDP_RIP_EXT.1 (Residual Information in Memory)
- FDP_RIP_EXT.2 (Residual Information on Disk)
- FDP_VMS_EXT.1 (VM Separation)
- FDP_VNC_EXT.1 (Virtual Networking Components)
- FIA_AFL_EXT.1 (Authentication Failure Handling)
- FIA_PMG_EXT.1 (Password Management)
- FIA_UIA_EXT.1 (Administrator Identification and Authentication)
- FMT_MOF_EXT.1 (Management of Security Functions Behavior)
- FMT_MSA_EXT.1 (Default Data Sharing Configuration)
- FMT_SMO_EXT.1 (Separation of Management and Operational Networks)
- FPT_DVD_EXT.1 (Non-Existence of Disconnected Virtual Devices)

- FPT_EEM_EXT.1 (Execution Environment Mitigations)
- FPT_HAS_EXT.1 (Hardware Assists)
- FPT_RDM_EXT.1 (Removable Devices and Media)
- FPT_VDP_EXT.1 (Virtual Device Parameters)
- FPT_VIV_EXT.1 (VMM Isolation from VMs)
- FTP_UIF_EXT.1 (User Interface: I/O Focus)
- FTP_UIF_EXT.2 (User Interface: Identification of VM)

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]. 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) atsec information security GmbH.

The evaluation was completed on 9 December 2021 with the issuance by LVS of the Evaluation Technical Report [ETR] that has been approved by the Certification Body on 21 December 2021. 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] issued by the LVS atsec information security GmbH and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "Red Hat Virtualization v4.3" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL2 augmented with ALC_FLR.3, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 2 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL2 augmented with ALC_FLR.3.

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
Systematic flaw remediation	*ALC_FLR.3*	Pass
Tests	**Class ATE**	Pass

Assurance classes and components		Verdict
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 2 - 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 “Red Hat Virtualization v4.3” are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the Assumptions and the Organizational Security Policies described, respectively, in sects. 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 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 ([ECG], [RHVAG], [RHVPG], [RHVTR], [RHVPPG]).

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

Table 3 contains the items that comprise the different elements of the TOE, including software and guidance.

#	Type	Identifier	Release	Form of delivery
Red Hat Virtualization v4.3				
1	ISO	Hypervisor Image 4.3.17 EUS SHA-256: f6267ccee75c8cfb027f891e20cd38d1ac3da75d43740e11f3ec7b576f06a6e2	RHV 4.3.17	Download
2	PDF	EAL2 Evaluated Configuration Guide for Red Hat Virtualization 4.3 SHA-256: f8f61dadaca9b99762f2c22c0ef3a3cda459cd5876b98b056f5df70816fe45b8	RHV 4.3.17, Version 0.9, Date 2021-11-08	Download
3	PDF	Red Hat Virtualization 4.3 Product Guide SHA-256: 595db0ff4e7698ffa9b30173bb84018d1c40c66cc70c59847def14acf970e30f	RHV 4.3.17, Date 2020-04-20	Download
4	PDF	Red Hat Virtualization 4.3 Technical Reference SHA-256: 77db96dcff8d8ad36ca0355e307eb6190579cebabefb6fb6fc0ab47978590d2c	RHV 4.3.17, Date 2020-04-20	Download
5	PDF	Red Hat Virtualization 4.3 Administration Guide SHA-256: cb116b00af290112c60cedf5c471404b042d9a80c3467c1508bab045925a00f3	RHV 4.3.17, Date 2020-10-06	Download
6	PDF	Red Hat Virtualization 4.3 Planning and Prerequisites Guide SHA-256: ddedfecf64b2b98c4f1502aa54ddfb6b988062abf71a148272aee95de41f9769	RHV 4.3.17, Date 2020-05-21	Download

Table 3 - TOE Deliverables

The delivery method employed to deliver the Red Hat Virtualization (RHV) distribution is via online delivery of the ISO files according to the Evaluated Configuration Guide [ECG] section 2.3.2 (Preparing for installation). This delivery occurs through the Red Hat Customer Portal.

The Evaluated Configuration Guide [ECG] as well as the associated guides can be obtained from `https://access.redhat.com/articles/2918071`.

9.2 Identification of the TOE

The Evaluated Configuration Guide [ECG] describes in section 2.4.1 how the TOE is identified.

To verify the TOE was successfully installed one must use one of the following methods.

Either run the following command and verify that “rhvh-4.3.17” is used:

```
nodectl info
```

Or verify that “Red Hat Virtualization Host” in version “4.3.17” is used by executing:

```
cat /etc/os-release
```

9.3 Installation, initialization and secure usage of the TOE

Users should refer to the Evaluated Configuration Guide [ECG] for instructions on how to install and configure the TOE.

The following is a summary of the process documented in detail in sections 2.3.2 and 2.4 (Installation) of [ECG]:

1. Download the ISO image for product variant Red Hat Virtualization version 4.3 with the specific ISO image labelled “Hypervisor Image 4.3.17 EUS” from `https://access.redhat.com/downloads/content/415/` on a separate Internet-connected computer.

2. Verify that the SHA-256 checksum of the image file is correct.

3. Complete all the steps in chapter 3 (Preparing Storage for Red Hat Virtualization) of the document [RHVCP].

4. Either disconnect all network connections during installation (recommended) or ensure that the connected network is secure.

5. Make Install RHV as a self-hosted engine by either making the ISO and package files available to the target machine via removable media (at the top level directory) or file server (in a single directory).

6. If installing the Red Hat Virtualization host, follow the steps in section 4.1 (Installing Red Hat Virtualization Hosts) of [RHVCP]. If installing the Red Hat Enterprise Linux host, follow the steps in section 4.2 (Installing Red Hat Enterprise Linux hosts) of [RHVCP].

The guidance documentation [ECG] also provides information on TOE secure usage in accordance with the security objectives specified in the Security Target [ST].

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product “Red Hat Virtualization v4.3”, developed by Red Hat, Inc.

The evaluated configuration of the TOE is defined in Security Target [ST] as follows:

- The CC evaluated package set must be selected at install time and installed and configured in accordance with the descriptions provided in the Evaluated Configuration Guide [ECG].
- The TOE is configured self-hosted as shown by Host 1 in Figure 2 (Self-Hosted Engine Red Hat Virtualization Architecture).
- The TOE is configured with a dedicated administrative network (either a separate physical LAN or an isolated VLAN) for separation of operational and administrative functions.

10.1 TOE operational environment

The TOE may be run on several systems on a network. The TOE supports Intel x86 64bit platforms (Xeon processor) in the evaluated configuration.

Each TOE system implements its own security policy. If other systems are connected to the network, they must be configured and managed by the same authority using an appropriate security policy that does not conflict with the security policy of the TOE. All connections between this network and untrusted networks (e.g., the Internet) must be protected by appropriate security measures.

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.3, 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 Developer provided the test systems with the TOE installed (Red Hat Virtualization Host, version 4.3.17). Test machines were based on x86_64 Intel architecture (Xeon CPU).

The Evaluators verified the test systems according to the documentation in the Evaluated Configuration Guide [ECG] and the Developer's test plan. Since the document [ECG] is consistent with the Security Target [ST], the Evaluators concluded that the test configuration was consistent with the ST.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer performs tests of the TSF by using an almost fully automated test framework with some additional manual tests. The automated tests are self-contained and perform all necessary setup and cleanup steps when being executed. Therefore, there are no dependencies to other tests that need to be considered nor is there an explicit ordering of the tests.

Prior to executing the tests, the tester must follow instructions provided by the test documentation referring also to the Evaluated Configuration Guide [ECG] to properly setup the test environment and the TOE, and to bring the latter into its evaluated configuration.

The test cases (automated or manual) trigger the various TSFI and in turn test the behavior of the TSF. At level EAL2, an analysis of test depth is not applicable and therefore not covered by the Evaluators assessment.

11.2.2 Test results

After execution of the automated tests, the log files obtained contain a "PASS/FAIL" information on whether the actual test results matched the expected results contained in the various test cases. The evidence of test execution provided by the Developer demonstrated that all automated test cases passed.

For the manual test cases of read-only relocation (RELRO) and address space layout randomization (ASLR), the test cases contain instructions on how to perform the tests and on how to interpret the results obtained. Developer's test documentation demonstrated that also the manual tests passed.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Testing approach

The Evaluators performed the automated test suite of the Developer and the majority of the semi-automated (derived from the test suite) and manual tests. The Evaluators executed tests on all supported TOE platforms.

The Evaluators also performed nine additional tests on the TOE.

11.3.2 Test coverage

The Evaluators in their independent testing focused on virtual machine related security functions, covering the following TSFs:

- User Data Protection
- Identification & Authentication
- Security Management
- Protection of the TSF

By rerunning the Developer's tests full TSF coverage has been achieved.

In addition to the Developer tests, the Evaluators devised tests for a subset of the TOE functionality as follows:

- Run the unused parts of the Developer's test suite to exercise the basic systemcall functionality.
- Install machine with Ubuntu Linux using a network installation method. The resources (memory, network and storage) are pre-defined. After the installation, check their presence and usability.
- Install a second Ubuntu machine on a dedicated virtual switch, check that the machines can communicate. After the installation, set the network into isolation mode and check that traffic to other virtual machines does not get out or in.
- Define storage, check that machine uses the storage and memory hungry programs run longer with more memory (before they are killed by the OS).
- Attach a virtual CD-ROM drive to machine, check that it is detected.
- Insert an ISO image into CD-ROM and mount it in the VM, check that it is present.
- Remove the ISO from CD-ROM and check that the data on the ISO can no longer be accessed.

- Exercise a fuzzing program in a VM and check that the VM as well as the host remains undisturbed.

- Verify that OpenSSH supports key based authentication.

11.3.3 Test results

All Developer's tests were run successfully. The Evaluators verified the correct behavior of the TSF and correspondence between expected results and achieved results for each test.

All test cases devised by the Evaluators passed, i.e., all the actual test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

The Evaluators performed a search in the MITRE CVE portal and the RedHat CVE database to identify publicly documented TOE vulnerabilities. No applicable vulnerabilities, relevant attacks or hypothesis for attacks could be deduced from this research.

The Evaluators then conducted a search of the ST, guidance documentation, functional specification, TOE design and security architecture description evidence and determined that there are no potential vulnerabilities in the TOE.

The major attack surface relevant for the TOE and its environment are the interfaces exposed by the virtual machines. The Evaluators chose a fuzzing approach to verify the stability and correctness of the VM interfaces exposed by the TOE:

1. Use a program that exercises the CPU called `sandsifter`. This tool audits x86 processors for hidden instructions and hardware bugs, by systematically generating machine code to search through a processor's instruction set, and monitoring execution for anomalies.

2. Use a program that runs random instruction streams in order to bring the emulator in undefined operational states called `cpufzzer`. This tool's purpose is to find bugs or at least do an initial testing in CPU emulators, but it could also be used to find bugs or undocumented instructions in hardware CPUs.

Both programs follow a similar approach, targeting the operation and emulation of the virtual machine. Using the `sandsifter` and `cpufzzer` tools, the Evaluators verified that the VM interfaces exposed by the emulator do not to contain flaws that are exposed using a fuzz testing approach.

Based on the penetration testing results, the Evaluators could then conclude that the TOE is resistant to an attack potential of Basic in its intended operational environment. No exploitable or residual vulnerabilities have been identified.