Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 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)

Firmato digitalmente
da Eva Spina
Data: 2022.01.18
10:42:06 +01'00'

Roma, 18 gennaio 2022

Common Criteria

Questa pagina è lasciata intenzionalmente vuota

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

Rapporto di Certificazione

Red Hat Virtualization v4.3

OCSI/CERT/ATS/08/2020/RC

Versione 1.0

18 gennaio 2022

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	18/01/2022

2 Indice

3 Elenco degli acronimi

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
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
ODV	Oggetto della Valutazione
OS	Operating System

PAM	Pluggable Authentication Modules
PP	Protection Profile
QEMU	Quick EMUlator
RELRO	Read-only Relocation
RFV	Rapporto Finale di Valutazione
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
TDS	Traguardo di Sicurezza
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 Riferimenti

4.1 Criteri e normative

[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 Documenti tecnici

[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

[PPVIRT] Protection Profile for Virtualization, Version 1.0, NIAP, 17 November 2016

[RFV] Final Evaluation Technical Report "Red Hat Virtualization v4.3", Version 3.0, atsec information security GmbH, 9 December 2021

[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

[TDS] "Red Hat Virtualization Security Target", Version 2.3, Red Hat, Inc., 8 December 2021

5 Riconoscimento del certificato

5.1 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La versione corrente dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (Common Criteria Recognition Arrangement, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

L'elenco aggiornato delle nazioni firmatarie e dei Profili di Protezione "collaborativi" (cPP) e altri dettagli sono disponibili su https://www.commoncriteriaportal.org/.

Il logo CCRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito CCRA per tutti i componenti di garanzia dichiarati.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "Red Hat Virtualization v4.3", sviluppato dalla società Red Hat, Inc.

L'ODV è una piattaforma di virtualizzazione di livello *enterprise* basata su Red Hat Enterprise Linux. La virtualizzazione permette agli utenti di installare nuovi server e workstation virtuali, consentendo un uso più efficiente delle risorse dei server fisici.

La valutazione è stata condotta in accordo ai requisiti stabiliti dallo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione ed espressi nelle Linee Guida Provvisorie [LGP1, LGP2, LGP3] e nelle Note Informative dello Schema [NIS1, NIS2, NIS3]. Lo Schema è gestito dall'Organismo di Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Obiettivo della valutazione è fornire garanzia sull'efficacia dell'ODV nel rispettare quanto dichiarato nel Traguardo di Sicurezza [TDS], la cui lettura è consigliata ai potenziali acquirenti e/o utilizzatori. Le attività relative al processo di valutazione sono state eseguite in accordo alla Parte 3 dei Common Criteria [CC3] e alla Common Evaluation Methodology [CEM].

L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per il livello di garanzia EAL2, con l'aggiunta di ALC_FLR.3, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B – Configurazione valutata di questo Rapporto di Certificazione.

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di valutazione è stato condotto in modo conforme a quanto richiesto dai criteri di valutazione Common Criteria – ISO/IEC 15408 ([CC1], [CC2], [CC3]) e dalle procedure indicate dal Common Criteria Recognition Arrangement [CCRA] e che nessuna vulnerabilità sfruttabile è stata trovata. Tuttavia l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

7 Riepilogo della valutazione

7.1 Introduzione

Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del prodotto "Red Hat Virtualization v4.3" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti e/o utilizzatori per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

Il presente Rapporto di Certificazione deve essere consultato congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto.

7.2 Identificazione sintetica della certificazione

Nome dell'ODV	Red Hat Virtualization v4.3
Traguardo di Sicurezza	"Red Hat Virtualization Security Target", Version 2.3 [TDS]
Livello di garanzia	EAL2 con l'aggiunta di ALC_FLR.3
Fornitore	Red Hat, Inc.
Committente	Red Hat, Inc.
LVS	atsec information security GmbH
Versione dei CC	3.1 Rev. 5
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	5 novembre 2020
Data di fine della valutazione	9 dicembre 2021

I risultati della certificazione si applicano unicamente alla versione del prodotto indicata nel presente Rapporto di Certificazione e a condizione che siano rispettate le ipotesi sull'ambiente descritte nel Traguardo di Sicurezza [TDS].

7.3 Prodotto valutato

In questo paragrafo vengono sintetizzate le principali caratteristiche funzionali e di sicurezza dell'ODV; per una descrizione dettagliata, si rimanda al Traguardo di Sicurezza [TDS].

L'ODV "Red Hat Virtualization v4.3" è una piattaforma di virtualizzazione di livello *enterprise* basata su Red Hat Enterprise Linux. La virtualizzazione permette agli utenti di installare nuovi server e workstation virtuali, consentendo un uso più efficiente delle risorse dei server fisici.

Red Hat Virtualization utilizza le primitive di virtualizzazione fornite da Red Hat Enterprise Linux (RHEL) 7.9.

L'ODV comprende i componenti elencati in Tabella 1.

Nome	Descrizione
Red Hat Virtualization Host (RHVH)	Il Red Hat Virtualization Host è costituito da un'installazione minima dell'ambiente Red Hat Enterprise Linux (RHEL) che include il *kernel* Linux che fornisce l'ambiente di virtualizzazione KVM. Viene inoltre fornito il *framework* dello spazio utente QEMU che utilizza l'ambiente KVM per istanziare le macchine virtuali. Il ciclo di vita delle macchine virtuali è controllato dal sistema di gestione `libvirtd`.
Red Hat Virtualization Manager	È un servizio che fornisce un'interfaccia utente grafica e un'API REST per gestire le risorse nell'ambiente utilizzando le primitive di virtualizzazione fornite dall'*host* di virtualizzazione come descritto sopra. Il Manager è installato su una macchina fisica o virtuale che esegue Red Hat Enterprise Linux.

Tabella 1 - Componenti dell'ODV

Pur essendo il componente RHVH dell'ODV derivato da RHEL 7.9, il sistema operativo RHEL non fa parte dell'ODV.

Per una descrizione dettagliata dell'ODV, si consulti il par. 1.4 e il par. 1.5 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito.

7.3.1 Architettura dell'ODV

L'ODV è un sistema di virtualizzazione (VS). In Figura 1 è riprodotta una rappresentazione semplificata di un sistema di virtualizzazione e di una piattaforma generici, come fornita in [PPVIRT]. In questo esempio, i componenti dell'ODV sono colorati in rosso, mentre i componenti che non fanno parte dell'ODV sono colorati in blu. La piattaforma è costituita dall'hardware, dal firmware e dal software su cui è installato il VS.

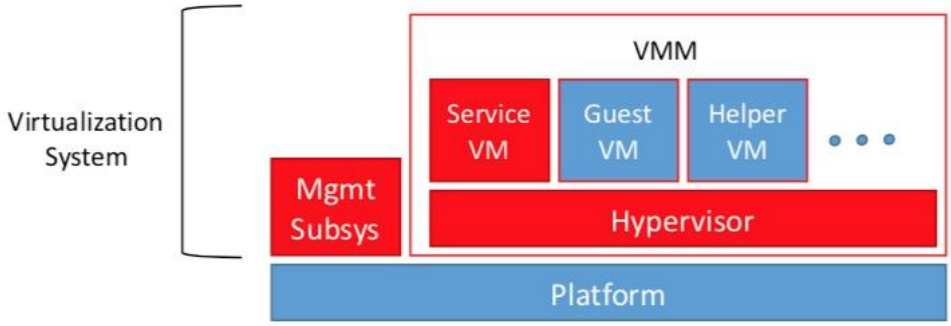

Figura 1 - Sistema di virtualizzazione e piattaforma

Red Hat Virtualization può essere distribuito come motore ospitato in uno spazio proprio (*self-hosted*) o come Manager autonomo (*standalone*). Nella configurazione valutata, l'ODV viene distribuito come motore *self-hosted*. La distribuzione completa di Red Hat Virtualization viene realizzata installando l'ODV in collaborazione con altri componenti non-ODV:

- servizio di archiviazione;

- *data warehouse*;
- *metrics store*.

7.3.1.1 Architettura del motore self-hosted

Nella configurazione valutata, Red Hat Virtualization Manager viene eseguito come una macchina virtuale su nodi del motore *self-hosted* (*host* specializzati) nello stesso ambiente che gestisce. L'ambiente di un motore *self-hosted* richiede un server fisico in meno, ma un carico maggiore per la distribuzione e la gestione. Il Manager risulta in alta disponibilità senza bisogno di una gestione HA esterna. La configurazione minima dell'ambiente di un motore *self-hosted*, illustrata in Figura 2, include:

- Una macchina virtuale Red Hat Virtualization Manager ospitata su uno dei nodi del motore *self-hosted*. Viene utilizzata la RHV-M Appliance per automatizzare l'installazione di una macchina virtuale Red Hat Enterprise Linux 7 e del Manager su di essa.
- Un minimo di due nodi del motore *self-hosted* per l'alta disponibilità della macchina virtuale. Questo può essere ottenuto utilizzando *host* Red Hat Enterprise Linux o Red Hat Virtualization Host (RHVH). Su tutti gli *host* viene eseguito VDSM (l'*host agent*) per facilitare la comunicazione con Red Hat Virtualization Manager. I servizi di HA vengono eseguiti su tutti i nodi del motore *self-hosted* per gestire l'alta disponibilità della macchina virtuale del Manager.
- Un servizio di archiviazione che può essere ospitato localmente o su un server remoto a seconda del tipo di archiviazione utilizzato. Il servizio di archiviazione deve essere accessibile a tutti gli *host*.

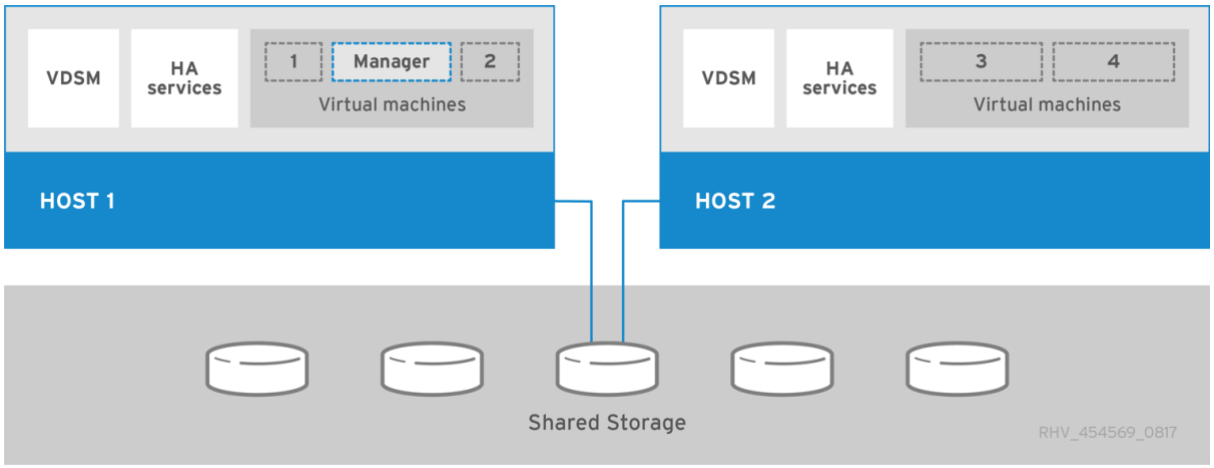

Figura 2 – Architettura del motore *self-hosted* di Red Hat Virtualization

7.3.1.2 Red Hat Virtualization

Operazioni quali l'archiviazione, la gestione degli *host*, le connessioni degli utenti e la connettività delle macchine virtuali si basano tutte sulle prestazioni ottimali che deve fornire una rete ben progettata e ben configurata. La configurazione della rete è un prerequisito vitale per un ambiente Red Hat Virtualization. Pianificare i requisiti di progetto

di rete previsti e implementare la rete di conseguenza è molto più semplice che scoprire i requisiti di rete attraverso l'uso e modificare la configurazione di rete in modo retroattivo. Red Hat Virtualization separa il traffico di rete definendo reti logiche.

Le reti logiche definiscono il percorso che un tipo di traffico di rete selezionato deve seguire attraverso la rete. Le reti logiche vengono create per isolare il traffico di rete per funzionalità o per virtualizzare una topologia di rete fisica.

Per impostazione predefinita viene creata la rete logica `ovirtmgmt`, etichettata come rete di Management. La rete logica `ovirtmgmt` è destinata al traffico di gestione tra Red Hat Virtualization Manager e gli *host*. È possibile definire ulteriori reti logiche per segregare le seguenti tipologie di traffico:

- traffico generico della macchina virtuale;
- traffico relativo all'archiviazione (come NFS o iSCSI);
- traffico di migrazione della macchina virtuale;
- traffico di visualizzazione della macchina virtuale;
- traffico di archiviazione Gluster.

7.3.1.3 Separazione dei componenti dell'ODV dai componenti non-ODV

L'ODV include i componenti elencati in Tabella 1:

- Red Hat Virtualization Host (RHVH), che è l'installazione minima dell'ambiente Red Hat Enterprise Linux (RHEL);
- Red Hat Virtualization Manager, fornito tramite il *framework* di gestione oVirt.

Il *framework* oVirt consente la configurazione di risorse complesse come l'archiviazione Gluster, NFS o iSCSI. Qualsiasi risorsa che non è locale all'istanza dell'ODV è considerata un componente non-ODV. Ad esempio, il server NFS a cui può accedere l'ODV e i sistemi operativi guest gestiti dall'ODV non fanno parte dell'ODV. Inoltre, l'ODV consente la configurazione di provider di autenticazione esterni come LDAP o Active Directory. Tutti i provider di autenticazione esterni all'ODV sono componenti non-ODV. Solamente l'autenticazione degli utenti mediante il database degli utenti locali fa parte dell'ODV.

7.3.2 Caratteristiche di sicurezza dell'ODV

Il problema di sicurezza dell'ODV, comprendente obiettivi di sicurezza, ipotesi, minacce e politiche di sicurezza dell'organizzazione, è definito nel cap. 3 del Traguardo di Sicurezza [TDS].

Per una descrizione dettagliata delle Funzioni di Sicurezza dell'ODV, si consulti il cap. 7 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito:

- **Audit**: il supporto per l'audit è implementato utilizzando il Linux Audit Framework (LAF). Il software `libvirt` genera voci di audit che vengono memorizzate su disco dal demone di audit. I dati di audit possono essere controllati mediante l'utility

`ausearch`.
Il sistema di audit LAF è progettato per rendere Linux conforme ai requisiti dei Common Criteria. LAF è in grado di intercettare tutte le chiamate di sistema e di recuperare le voci di audit dai registri delle applicazioni dello spazio utente privilegiato. Il sottosistema consente di configurare quali eventi vanno effettivamente sottoposti ad audit rispetto all'insieme di tutti gli eventi che è possibile registrare. Questi eventi vengono memorizzati in un file di configurazione specifico, sulla base del quale viene notificato al *kernel* di costruire la propria struttura interna per gli eventi da sottoporre ad audit.

- **Protezione dei dati d'utente**: per proteggere i dati d'utente l'ODV utilizza meccanismi di isolamento basati sull'hardware e controlli delle risorse della piattaforma fisica.
  L'ODV utilizza i meccanismi del *kernel* Linux, che a loro volta utilizzano meccanismi basati sull'hardware, per limitare le macchine virtuali quando queste accedono direttamente ai dispositivi fisici.
  Il *kernel* Linux utilizza vari meccanismi hardware per fornire il supporto per la virtualizzazione e garantire la corretta separazione delle macchine virtuali.
  L'ODV fornisce una postazione centralizzata in cui gli utenti possono eseguire operazioni relative alle reti logiche e cercare reti logiche in base alle proprietà di ciascuna rete o all'associazione con altre risorse.
  L'ODV protegge dalle informazioni residue lasciate dopo l'uso da una macchina virtuale sia in memoria, sia su disco.

- **Identificazione e autenticazione**: l'ODV utilizza le funzioni di autenticazione e di gestione delle password di RHEL. Tutti gli utenti amministrativi devono sempre autenticarsi quando accedono alle console. L'ODV utilizza i meccanismi sottostanti di autenticazione di Linux. L'ODV (oVirt) autentica gli utenti utilizzando la libreria PAM offerta dal sistema operativo Linux di base.
  L'uso di PAM consente l'autenticazione degli utenti con il database degli utenti locali. Per accedere a provider di autenticazione remota come LDAP o Active Directory, oVirt utilizza configurazioni PAM appropriate. I provider di autenticazione remota implementano l'autenticazione degli utenti e restituiscono le informazioni sulle decisioni di autenticazione a PAM che inoltra il risultato a oVirt per la loro applicazione. PAM si collega anche al Linux Auditing Framework per fornire la capacità di sottoporre ad audit le richieste di autenticazione.
  Gli utenti, le loro credenziali e i loro ruoli possono essere gestiti tramite un server di directory esterno. L'ODV supporta svariati prodotti di tipo server di directory.

- **Gestione della sicurezza**: gli *host*, detti anche *hypervisor*, sono i server fisici su cui girano le macchine virtuali. La virtualizzazione completa viene fornita utilizzando un modulo caricabile del *kernel* Linux chiamato Kernel-based Virtual Machine (KVM). KVM può ospitare contemporaneamente più macchine virtuali che eseguono sistemi operativi Windows o Linux. Le macchine virtuali vengono eseguite come singoli processi e *thread* Linux sulla macchina *host* e sono gestite in remoto da Red Hat Virtualization Manager. Un ambiente Red Hat Virtualization ha uno o più *host* collegati.
  La gestione della sicurezza dell'ODV copre l'intero ciclo di vita delle macchine virtuali: creazione, avvio, arresto, riavvio e cancellazione.

- **Protezione del TSF**: l'ODV fornisce funzionalità per mitigare gli effetti delle vulnerabilità di tipo *buffer overrun* nelle applicazioni e per proteggere dalle informazioni residue rimaste in memoria o su disco dopo l'uso da parte dalle diverse istanze di macchine virtuali.

- **Percorsi e canali attendibili**: l'ODV implementa percorsi e canali attendibili utilizzando i componenti dell'ambiente della macchina virtuale RHEL.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto, viene fornita al cliente insieme al prodotto.

La documentazione indicata contiene le informazioni richieste per l'inizializzazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguite le ulteriori raccomandazioni per l'utilizzo sicuro dell'ODV contenute nel par. 8.2 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] non dichiara conformità ad alcun Profilo di Protezione.

7.6 Requisiti funzionali e di garanzia

Tutti i Requisiti di Garanzia (SAR) sono stati selezionati dai CC Parte 3 [CC3].

Tutti i Requisiti Funzionali di Sicurezza (SFR) sono stati derivati direttamente o ricavati per estensione dai CC Parte 2 [CC2].

Sebbene il Traguardo di Sicurezza [TDS] non dichiari conformità ad alcun PP, esso comprende i seguenti componenti funzionali estesi basati sugli SFR di virtualizzazione definiti in [PPVIRT] (tutti tranne FMT_MOF_EXT.1) e [EPSV] (solo FMT_MOF_EXT.1):

- 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)

Il Traguardo di Sicurezza [TDS], a cui si rimanda per la completa descrizione e le note applicative, specifica per l'ODV tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, gli SFR e le funzioni di sicurezza che realizzano gli obiettivi stessi.

7.7 Conduzione della valutazione

La valutazione è stata svolta in conformità ai requisiti dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, come descritto nelle Linee Guida Provvisorie [LGP3] e nelle Note Informative dello Schema [NIS3], ed è stata inoltre condotta secondo i requisiti del Common Criteria Recognition Arrangement [CCRA].

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS atsec information security GmbH.

L'attività di valutazione è terminata in data 9 dicembre 2021 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 21 dicembre 2021. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.8 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è stata eseguita sull'ODV configurato come descritto in Appendice B – Configurazione valutata. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto di Certificazione.

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali e effettivi) sono invitati a verificare regolarmente l'eventuale insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

8 Esito della valutazione

8.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV] prodotto dall'LVS atsec information security GmbH e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "Red Hat Virtualization v4.3" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL2, con l'aggiunta di ALC_FLR.3, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B – Configurazione valutata.

La Tabella 2 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia EAL2, con l'aggiunta di ALC_FLR.3.

Classi e componenti di garanzia		**Verdetto**
Security Target evaluation	**Classe ASE**	Positivo
Conformance claims	ASE_CCL.1	Positivo
Extended components definition	ASE_ECD.1	Positivo
ST introduction	ASE_INT.1	Positivo
Security objectives	ASE_OBJ.2	Positivo
Derived security requirements	ASE_REQ.2	Positivo
Security problem definition	ASE_SPD.1	Positivo
TOE summary specification	ASE_TSS.1	Positivo
Development	**Classe ADV**	Positivo
Security architecture description	ADV_ARC.1	Positivo
Security-enforcing functional specification	ADV_FSP.2	Positivo
Basic design	ADV_TDS.1	Positivo
Guidance documents	**Classe AGD**	Positivo
Operational user guidance	AGD_OPE.1	Positivo
Preparative procedures	AGD_PRE.1	Positivo
Life cycle support	**Classe ALC**	Positivo
Use of a CM system	ALC_CMC.2	Positivo
Parts of the TOE CM coverage	ALC_CMS.2	Positivo
Delivery procedures	ALC_DEL.1	Positivo
Systematic flaw remediation	*ALC_FLR.3*	Positivo

Classi e componenti di garanzia		Verdetto
Test	**Classe ATE**	Positivo
Evidence of coverage	ATE_COV.1	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing - sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Vulnerability analysis	AVA_VAN.2	Positivo

Tabella 2 - Verdetti finali per i requisiti di garanzia

8.2 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 6 (Dichiarazione di certificazione).

Si raccomanda ai potenziali acquirenti del prodotto "Red Hat Virtualization v4.3" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo agli Obiettivi di Sicurezza per l'ambiente operativo specificati nel par. 4.2 del Traguardo di Sicurezza [TDS]. Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le ipotesi e le Politiche di Sicurezza dell'Organizzazione descritte rispettivamente nel par. 3.2 e nel par. 3.3 del Traguardo di Sicurezza [TDS].

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella sua configurazione valutata. In particolare, l'Appendice A – Indicazioni per l'uso sicuro del prodotto del presente Rapporto include una serie di raccomandazioni relative alla consegna, all'inizializzazione, all'installazione e all'utilizzo sicuro del prodotto, in accordo con la documentazione di guida fornita con l'ODV ([ECG], [RHVAG], [RHVPG], [RHVTR], [RHVPPG]).

9 Appendice A – Indicazioni per l'uso sicuro del prodotto

La presente appendice riporta considerazioni particolarmente rilevanti per il potenziale acquirente del prodotto.

9.1 Consegna dell'ODV

In Tabella 3 sono elencati i materiali dell'ODV che vengono consegnati al cliente, inclusi il software e la documentazione di guida.

#	Tipo	Identificativo	Versione	Metodo di consegna
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, Versione 0.9, 08/11/2021	Download
3	PDF	Red Hat Virtualization 4.3 Product Guide SHA-256: 595db0ff4e7698ffa9b30173bb84018d1c40c66cc70c59847def14acf970e30f	RHV 4.3.17, 20/04/2020	Download
4	PDF	Red Hat Virtualization 4.3 Technical Reference SHA-256: 77db96dcff8d8ad36ca0355e307eb6190579cebabefb6fb6fc0ab47978590d2c	RHV 4.3.17, 20/04/2020	Download
5	PDF	Red Hat Virtualization 4.3 Administration Guide SHA-256: cb116b00af290112c60cedf5c471404b042d9a80c3467c1508bab045925a00f3	RHV 4.3.17, 06/10/2020	Download
6	PDF	Red Hat Virtualization 4.3 Planning and Prerequisites Guide SHA-256: ddedfecf64b2b98c4f1502aa54ddfb6b988062abf71a148272aee95de41f9769	RHV 4.3.17, 21/05/2020	Download

Tabella 3 - Materiali consegnabili dell'ODV

Come riportato nel par. 2.3.2 (Preparazione per l'installazione) della Evaluated Configuration Guide [ECG], il metodo di consegna per la distribuzione di Red Hat Virtualization (RHV) consiste nello scaricamento dei file ISO dal Red Hat Customer Portal.

La Evaluated Configuration Guide [ECG], assieme agli altri documenti di guida associati, può essere scaricata da `https://access.redhat.com/articles/2918071`.

9.2 Identificazione dell'ODV

La procedura per l'identificazione dell'ODV è descritta nel par. 2.4.1 della Evaluated Configuration Guide [ECG].

Per verificare che l'ODV sia stato installato correttamente, è necessario utilizzare uno dei seguenti metodi.

Eseguire il comando seguente e verificare che venga utilizzato “rhvh-4.3.17”:

```
nodectl info
```

In alternativa, verificare che venga utilizzato “Red Hat Virtualization Host” nella versione “4.3.17” eseguendo:

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

9.3 Installazione, inizializzazione e utilizzo sicuro dell’ODV

L’installazione e la configurazione dell’ODV debbono essere effettuate dagli utenti seguendo le istruzioni contenute nella Evaluated Configuration Guide [ECG].

Quello che segue è un riepilogo del processo documentato in dettaglio nel par. 2.3.2 e nel par. 2.4 (Installation) di [ECG]:

1. Scaricare da `https://access.redhat.com/downloads/content/415/` utilizzando un computer separato connesso ad Internet l’immagine ISO specifica per la variante di prodotto Red Hat Virtualization versione 4.3, etichettata “Hypervisor Image 4.3.17 EUS”.

2. Verificare la correttezza del *checksum* SHA-256 del file immagine.

3. Completare tutti i passaggi illustrati nel capitolo 3 (Preparing Storage for Red Hat Virtualization) del documento [RHVCP].

4. Disconnettere tutte le connessioni di rete durante l’installazione (raccomandato) o assicurarsi che la rete connessa sia sicura.

5. Effettuare l’installazione di RHV come motore *self-hosted* rendendo disponibili alla macchina di destinazione l’ISO e i file del pacchetto tramite un supporto rimovibile (nella directory radice) o un file server (in un’unica directory).

6. Se si installa l’*host* Red Hat Virtualization, seguire i passaggi nel par. 4.1 (Installing Red Hat Virtualization Hosts) di [RHVCP]. Se si installa l'*host* Red Hat Enterprise Linux, seguire i passaggi nel cap. 4.2 (Installing Red Hat Enterprise Linux hosts) di [RHVCP].

La documentazione di guida [ECG] fornisce altresì informazioni sull’utilizzo sicuro dell’ODV in conformità con gli obiettivi di sicurezza specificati nel Traguardo di Sicurezza [TDS].

10 Appendice B – Configurazione valutata

L'oggetto di valutazione (ODV) è il prodotto "Red Hat Virtualization v4.3", sviluppato dalla società Red Hat, Inc.

La configurazione valutata dell'ODV è definita nel Traguardo di Sicurezza [TDS] come segue:

- al momento dell'installazione deve essere selezionato il set di pacchetti valutato CC che deve essere installato e configurato in conformità con le descrizioni fornite nella Evaluated Configuration Guide [ECG].
- L'ODV deve essere configurato come *self-hosted* come illustrato dall'Host 1 in Figura 2 (Self-Hosted Engine Red Hat Virtualization Architecture).
- L'ODV deve essere configurato con una rete amministrativa dedicata (una LAN fisica separata o una VLAN isolata) per la separazione delle funzioni operative e amministrative.

10.1 Ambiente operativo dell'ODV

L'ODV può essere eseguito su diversi sistemi connessi in rete. Nella configurazione valutata l'ODV supporta piattaforme Intel x86 a 64 bit (processore Xeon).

Ciascuna istanza di sistema dell'ODV implementa la propria politica di sicurezza. Se altri sistemi sono collegati alla rete, devono essere configurati e gestiti dalla stessa autorità utilizzando una politica di sicurezza appropriata che non sia in conflitto con la politica di sicurezza dell'ODV. Tutte le connessioni tra questa rete e le reti non attendibili (ad es. Internet) devono essere protette da misure di sicurezza adeguate.

11 Appendice C – Attività di Test

Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia EAL2, con l'aggiunta di ALC_FLR.3, tali attività tali attività prevedono tre passi successivi:

- valutazione dei test eseguiti dal Fornitore in termini di copertura;
- esecuzione di test funzionali indipendenti da parte dei Valutatori;
- esecuzione di test di intrusione da parte dei Valutatori.

11.1 Configurazione per i Test

Per le attività di test, i Valutatori hanno ricevuto dal Fornitore i sistemi di test con l'ODV installato (Red Hat Virtualization Host, versione 4.3.17). Le macchine predisposte per i test erano basate su architettura Intel x86_64 (CPU Xeon).

I Valutatori hanno verificato i sistemi di test sulla base delle informazioni contenute nella Evaluated Configuration Guide [ECG] e nel piano di test del Fornitore. Poiché il documento [ECG] è coerente con il Traguardo di Sicurezza [TDS], i Valutatori hanno potuto confermare che l'ambiente di test era coerente con i requisiti del TDS.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Approccio adottato per i test

Il Fornitore esegue i test del TSF utilizzando un *framework* di test quasi completamente automatizzato con alcuni test manuali aggiuntivi. I test automatizzati sono completamente indipendenti e, quando vengono eseguiti, effettuano tutti i passaggi di configurazione e pulizia necessari. Pertanto, non vi sono dipendenze da altri test da considerare, né esiste un ordinamento esplicito dei test.

Prima di eseguire i test, l'operatore deve seguire le istruzioni fornite dalla documentazione di test facendo riferimento anche alla Evaluated Configuration Guide [ECG] per impostare correttamente l'ambiente di test e portare l'ODV nella sua configurazione valutata.

I casi di test (automatici o manuali) stimolano le varie TSFI e verificano il comportamento complessivo del TSF. A livello EAL2, un'analisi della profondità del test non è applicabile e quindi non è coperta dalla valutazione.

11.2.2 Risultati dei test

Dopo l'esecuzione dei test automatizzati, i file di registro ottenuti contengono un'informazione "PASS/FAIL" sulla corrispondenza dei risultati effettivi del test con i risultati attesi contenuti nei vari casi di test. Le prove dell'esecuzione dei test fornite dal Fornitore hanno dimostrato che tutti i casi di test automatizzati sono stati eseguiti con successo.

Per i casi di test manuali relativi alla *read-only relocation* (RELRO) e all'*address space layout randomization* (ASLR), i casi di test contengono istruzioni su come eseguire i test e su come interpretare i risultati ottenuti. La documentazione di test del Fornitore ha dimostrato che anche i test manuali sono stati eseguiti con successo.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

11.3.1 Approccio adottato per i test

I Valutatori hanno eseguito la suite di test automatizzata del Fornitore e la maggior parte dei test semi-automatici (derivati dalla suite di test) e manuali. I Valutatori hanno eseguito i test su tutte le piattaforme supportate dall'ODV.

I Valutatori hanno altresì eseguito nove test aggiuntivi sull'ODV.

11.3.2 Copertura dei test

I test indipendenti dei Valutatori si sono concentrati sulle funzionalità relative alle macchine virtuali, coprendo le seguenti funzioni di sicurezza:

- protezione dei dati d'utente;
- identificazione e autenticazione;
- gestione della sicurezza;
- protezione del TSF.

La ripetizione dei test del Fornitore ha consentito di ottenere la copertura completa del TSF.

In aggiunta ai test del Fornitore, i Valutatori hanno progettato i seguenti test per un sottoinsieme delle funzionalità dell'ODV:

- Esecuzione di parti inutilizzate della suite di test del Fornitore per esercitare la funzionalità di chiamata di sistema di base (*systemcall*).
- Installazione della macchina con Ubuntu Linux utilizzando un metodo di installazione di rete. Le risorse (memoria, rete e archiviazione) sono predefinite. Verifica della loro presenza e usabilità dopo l'installazione.
- Installazione di una seconda macchina Ubuntu su uno *switch* virtuale dedicato, verificando che le macchine possano comunicare. Dopo l'installazione, impostazione della rete in modalità di isolamento e verifica che il traffico verso altre macchine virtuali non esca o entri.
- Definizione dell'archiviazione, verifica che la macchina utilizzi l'archiviazione definita e che programmi che necessitano di molta memoria vengano eseguiti più a lungo con più memoria (prima che vengano interrotti dal sistema operativo).
- Collegamento di un'unità CD-ROM virtuale alla macchina; verifica della sua rilevazione.

- Inserimento di un'immagine ISO nel CD-ROM e montaggio nella VM; verifica della sua presenza.

- Rimozione dell'ISO dal CD-ROM e verifica che i dati sull'ISO non siano più accessibili.

- Esecuzione di un programma di *fuzzing* in una VM e verifica che la VM e l'*host* rimangano indisturbati.

- Verifica del supporto dell'autenticazione basata su chiave da parte di OpenSSH.

11.3.3 Risultati dei test

Tutti i test del Fornitore sono stati eseguiti con successo. I Valutatori hanno verificato il corretto comportamento del TSF e la corrispondenza tra risultati attesi e risultati ottenuti per ogni test.

Tutti i casi di test progettati dai Valutatori hanno avuto esito positivo, ovvero tutti i risultati dei test sono risultati conformi a quelli previsti.

11.4 Analisi delle vulnerabilità e test di intrusione

I Valutatori hanno eseguito una ricerca nel portale MITRE CVE e nel database RedHat CVE per identificare le vulnerabilità dell'ODV documentate pubblicamente. Da questa ricerca non sono emerse vulnerabilità applicabili, attacchi rilevanti o ipotesi di attacchi.

I Valutatori hanno quindi condotto una ricerca sulle evidenze di valutazione, inclusi TDS, documentazione di guida, specifiche funzionali, progettazione dell'ODV e descrizione dell'architettura di sicurezza, e hanno dedotto che non vi sono potenziali vulnerabilità nell'ODV.

La principale superficie di attacco rilevante per l'ODV e il suo ambiente è rappresentata dalle interfacce esposte dalle macchine virtuali. I Valutatori hanno scelto un approccio basato su tecniche di *fuzzing* per verificare la stabilità e la corretta implementazione delle interfacce delle VM esposte dall'ODV:

1. Utilizzo del programma di analisi della CPU `sandsifter`. Questo strumento verifica i processori x86 alla ricerca di istruzioni nascoste e bug hardware, generando sistematicamente codice macchina per eseguire ricerche nel set di istruzioni del processore e monitorandone l'esecuzione per rilevare eventuali anomalie.

2. Utilizzo del programma `cpufzzer` che esegue flussi di istruzioni casuali per portare l'emulatore in stati operativi indefiniti. Lo scopo di questo strumento è trovare bug o per lo meno eseguire un test iniziale degli emulatori di CPU, ma può anche essere utilizzato per trovare bug o istruzioni non documentate nell'hardware dei processori.

Entrambi i programmi seguono un approccio simile, mirato all'operatività e all'emulazione della macchina virtuale. L'uso degli strumenti `sandsifter` e `cpufzzer` ha consentito ai Valutatori di verificare che le interfacce delle VM esposte dall'emulatore non contenessero difetti rilevabili mediante l'uso di tecniche di *fuzzing*.

Sulla base dei risultati dei test di intrusione, I Valutatori hanno quindi concluso che l'ODV, nel suo ambiente operativo, è in grado di resistere ad un attaccante che possiede un potenziale di attacco di livello Basic. Non sono state identificate vulnerabilità sfruttabili o residue.