



*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. 2/21**

*(Certification No.)*

**Prodotto: IBM z/VM Version 7 Release 2**

*(Product)*

**Sviluppato da: IBM Corporation**

*(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:*

**EAL4+**  
**(ALC\_FLR.3)**

Il Direttore  
(Dott.ssa Eva Spina)

Roma, 30 aprile 2021



Fino a EAL2 (Up to EAL2)



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**

# **IBM z/VM Version 7 Release 2**

OCSI/CERT/ATS/05/2020/RC

Versione 1.1

20 ottobre 2021

## **Nota editoriale**

Il presente documento sostituisce la versione 1.0 del Rapporto di Certificazione OCSI/CERT/ATS/05/2020/RC associato al Certificato n. 2/21 del 30 aprile 2021.

La versione corrente di questo Rapporto di Certificazione include unicamente correzioni di carattere editoriale (refusi, errori di formattazione, ecc.) e non modifica in alcun modo il contenuto informativo del testo.

Il Certificato mantiene la sua validità a partire dalla data di prima emissione.

## 1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	30/04/2021
1.1	OCSI	Correzioni editoriali	20/10/2021

## 2 Indice

1	Revisioni del documento .....	5
2	Indice .....	6
3	Elenco degli acronimi .....	8
4	Riferimenti.....	10
4.1	Criteri e normative .....	10
4.2	Documenti tecnici .....	11
5	Riconoscimento del certificato.....	12
5.1	Riconoscimento di certificati CC in ambito internazionale (CCRA) .....	12
6	Dichiarazione di certificazione .....	13
7	Riepilogo della valutazione.....	15
7.1	Introduzione .....	15
7.2	Identificazione sintetica della certificazione .....	15
7.3	Prodotto valutato .....	15
7.3.1	Architettura dell'ODV .....	17
7.3.2	Caratteristiche di sicurezza dell'ODV .....	19
7.4	Documentazione .....	23
7.5	Conformità a Profili di Protezione .....	23
7.6	Requisiti funzionali e di garanzia .....	23
7.7	Conduzione della valutazione.....	23
7.8	Considerazioni generali sulla validità della certificazione.....	24
8	Esito della valutazione .....	25
8.1	Risultato della valutazione.....	25
8.2	Raccomandazioni.....	26
9	Appendice A – Indicazioni per l'uso sicuro del prodotto.....	28
9.1	Consegna dell'ODV.....	28
9.2	Identificazione dell'ODV .....	29
9.3	Installazione, inizializzazione e utilizzo sicuro dell'ODV .....	30
10	Appendice B – Configurazione valutata.....	31
11	Appendice C – Attività di Test .....	32
11.1	Configurazione per i Test .....	32

11.2	Test funzionali svolti dal Fornitore .....	33
11.2.1	Approccio adottato per i test .....	33
11.2.2	Copertura dei test .....	34
11.2.3	Risultati dei test .....	34
11.3	Test funzionali ed indipendenti svolti dai Valutatori .....	34
11.3.1	Approccio adottato per i test .....	34
11.3.2	Copertura dei test .....	34
11.3.3	Risultati dei test .....	35
11.4	Analisi delle vulnerabilità e test di intrusione .....	35

### 3 Elenco degli acronimi

<b>APAR</b>	Authorized Program Analysis Report
<b>API</b>	Application Programming Interface
<b>CC</b>	Common Criteria
<b>CCRA</b>	Common Criteria Recognition Arrangement
<b>CEM</b>	Common Evaluation Methodology
<b>CMS</b>	Conversational Monitor System
<b>CP</b>	Control Program
<b>DAC</b>	Discretionary Access Control
<b>DASD</b>	Direct Access Storage Device
<b>DPCM</b>	Decreto del Presidente del Consiglio dei Ministri
<b>DVD</b>	Digital Versatile Disk
<b>EAL</b>	Evaluation Assurance Level
<b>I/O</b>	Input/Output
<b>ID</b>	Identifier
<b>IPL</b>	Initial Program Load
<b>IUCV</b>	Inter User Communication Vehicle
<b>IT</b>	Information Technology
<b>LGP</b>	Linea Guida Provvisoria
<b>LGR</b>	Live Guest Relocation
<b>LPAR</b>	Logical Partition
<b>LVS</b>	Laboratorio per la Valutazione della Sicurezza
<b>MAC</b>	Mandatory Access Control
<b>MFA</b>	Multi-factor Authentication
<b>NIS</b>	Nota Informativa dello Schema
<b>OCSI</b>	Organismo di Certificazione della Sicurezza Informatica



<b>ODV</b>	Oggetto della Valutazione
<b>PDF</b>	Portable Document Format
<b>PP</b>	Profilo di Protezione (Protection Profile)
<b>PR/SM</b>	Processor Resource/System Manager
<b>PTF</b>	Program Temporary Fix
<b>RACF</b>	Resource Access Control Facility
<b>RFV</b>	Rapporto Finale di Valutazione
<b>RSU</b>	Recommended Service Upgrade
<b>SAK</b>	System Assurance Kernel
<b>SAR</b>	Security Assurance Requirement
<b>SDF</b>	Software Delivery and Fulfillment
<b>SFR</b>	Security Functional Requirement
<b>SIE</b>	Start Interpretive Execution
<b>SSI</b>	Single System Image
<b>SSL</b>	Secure Sockets Layer
<b>ST</b>	Security Target
<b>SW</b>	Software
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol
<b>TDS</b>	Traguardo di Sicurezza
<b>TLS</b>	Transport Layer Security
<b>TOE</b>	Target Of Evaluation
<b>TSF</b>	TOE Security Functionality
<b>TSFI</b>	TSF Interface

## 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

- [RC] Rapporto di Certificazione “IBM z/VM Version 6 Release 4”, OCSI/CERT/ATS/04/2017/RC, versione 1.0, 23 aprile 2018
  
- [RFVv1] Final Evaluation Technical Report “IBM z/VM Version 7 Release 2”, OCSI-CERT-ATS-05-2020\_ETR\_210317\_v1, Version 1, atsec information security GmbH, 17 March 2021
  
- [RFVv2] Final Evaluation Technical Report “IBM z/VM Version 7 Release 2”, OCSI-CERT-ATS-05-2020\_ETR\_210406\_v2, Version 2, atsec information security GmbH, 6 March 2021
  
- [OSPP] Operating System Protection Profile, Version 2.0, BSI-CC-PP-0067, 01 June 2010
  
- [OSPP-LS] OSPP Extended Package – Labeled Security, Version 2.0, BSI-CC-PP-0067, 28 May 2010
  
- [OSPP-VIRT] OSPP Extended Package – Virtualization, Version 2.0, BSI-CC-PP-0067, 28 May 2010
  
- [TDS] IBM z/VM Version 7 Release 2 Security Target, Version 1.0, IBM Corporation, 9 March 2021
  
- [ZVM-CPG] z/VM V7.2 Certified Product Guidance, IBM Corporation
  
- [ZVM-SCG] z/VM Version 7 Release 2 Secure Configuration Guide, SC24-6323-02, IBM Corporation, 11 December 2020

## 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 fino a EAL2.

## 6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "IBM z/VM Version 7 Release 2", sviluppato da International Business Machines Corp. (IBM), nel seguito del documento anche indicato come z/VM V7R2 o z/VM.

L'ODV è un *hypervisor* di macchine virtuali per server IBM Z sui quali dislocare server virtuali per servizi critici.

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).

Il presente Rapporto di Certificazione è stato emesso a conclusione della ri-certificazione di una precedente versione dello stesso ODV (IBM z/VM Version 6 Release 4), già certificato dall'OCSI (Certificato n. 3/18 del 23 aprile 2018 [RC]).

In seguito ad alcune modifiche apportate al prodotto da parte del Fornitore IBM Corp. è stato necessario procedere a una ri-certificazione dell'ODV. L'LVS atsec information security GmbH ha potuto riutilizzare parte della documentazione e delle evidenze già fornite nella precedente valutazione.

Si noti che le modifiche effettuate hanno comportato anche la revisione del Traguardo di Sicurezza [TDS]. Gli utenti della precedente versione dell'ODV sono quindi invitati a prendere visione anche del nuovo TDS.

Pur rimanendo valide in gran parte le considerazioni e le raccomandazioni già espresse per il precedente ODV, per facilità di lettura il presente Rapporto di Certificazione è stato riscritto nella sua interezza in modo da costituire un documento autonomo associato al nuovo ODV "IBM z/VM Version 7 Release 2".

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 EAL4, 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 "IBM z/VM Version 7 Release 2" 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

<b>Nome dell'ODV</b>	IBM z/VM Version 7 Release 2
<b>Traguardo di Sicurezza</b>	IBM z/VM Version 7 Release 2 Security Target, Version 1.0 [TDS]
<b>Livello di garanzia</b>	EAL4 con l'aggiunta di ALC_FLR.3
<b>Fornitore</b>	IBM Corporation
<b>Committente</b>	IBM Corporation
<b>LVS</b>	atsec information security GmbH
<b>Versione dei CC</b>	3.1 Rev. 5
<b>Conformità a PP</b>	Operating System Protection Profile v2.0 [OSPP] con i seguenti Extended Package (EP): <ul style="list-style-type: none"><li>• OSPP EP – Labeled Security v2.0 [OSPP-LS]</li><li>• OSPP EP – Virtualization v2.0 [OSPP-VIRT]</li></ul>
<b>Data di inizio della valutazione</b>	1° luglio 2020
<b>Data di fine della valutazione</b>	17 marzo 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 è il prodotto z/VM Version 7 Release 2 configurato in un cluster comprendente fino a quattro istanze di z/VM in collaborazione all'interno di una Single System Image (SSI).

z/VM è un sistema operativo estremamente sicuro, flessibile, robusto e scalabile che implementa un *hypervisor* di macchine virtuali per i server IBM Z sui quali dislocare server virtuali per servizi critici. z/VM è progettato per ospitare altri sistemi operativi, ciascuno nella propria macchina virtuale.

Più macchine virtuali possono essere eseguite contemporaneamente per svolgere una varietà di funzioni che richiedono accesso controllato e separato alle informazioni memorizzate nel sistema. Oltre ai server virtuali, l'ODV fornisce macchine virtuali aggiuntive per ciascun utente umano connesso, separando il dominio di esecuzione di ogni macchina virtuale dagli altri, secondo quanto stabilito nelle definizioni della macchina virtuale memorizzate nella directory di sistema. In aggiunta a questo meccanismo, l'accesso a risorse e funzioni privilegiate viene mediato dal server di sicurezza RACF.

L'ODV offre una tecnologia di *clustering* multi-sistema che consente di avere da una a quattro istanze di z/VM in un cluster SSI. La configurazione del cluster, così come il suo stato, sono conservati in risorse condivise tra i membri del cluster. Nuove istanze di z/VM possono essere aggiunte alla topologia del cluster in fase di *runtime*. Il supporto per Live Guest Relocation (LGR) consente lo spostamento dei server virtuali Linux senza interruzione della loro operatività. I membri del cluster sono a conoscenza l'uno dell'altro e possono trarre vantaggio dalle loro risorse combinate. LGR consente di evitare interruzioni del servizio dei client in caso di manutenzioni pianificate spostando gli *host* da un sistema che richiede interruzione ad un sistema che invece rimane attivo durante il periodo di manutenzione.

L'ODV è abilitato per l'autenticazione a più fattori (MFA), ovvero applica correttamente le decisioni di autenticazione prese da un provider MFA di fiducia situato nell'ambiente operativo, che utilizza più fattori per l'autenticazione degli utenti dell'ODV.

Nella configurazione valutata, l'ODV consente due modalità operative: una modalità standard e una modalità chiamata Labeled Security Mode. In entrambe le modalità di funzionamento vengono utilizzati gli stessi componenti software. Le due modalità differiscono nelle impostazioni di RACF a seconda che usino o meno la sicurezza basata su etichette. Tutti gli altri parametri di configurazione sono identici nelle due modalità.

Il database RACF utilizzato per preservare il contesto di sicurezza dell'ODV è condiviso tra i membri del cluster. Tutti i membri del cluster eseguono un'istanza separata di RACF per l'audit locale, con accesso al database RACF condiviso.

Il concetto di macchine virtuali che rappresentano utenti gestiti da una singola istanza di z/VM può essere esteso fino a corrispondere ad una topologia cluster. Una macchina virtuale configurata come USER può essere eseguita in un dato momento soltanto su uno dei membri del cluster, mentre le macchine virtuali a configurazione multipla, configurate come IDENTITY, possono essere eseguite simultaneamente su diversi membri del cluster e rappresentano generalmente macchine di servizio.

z/VM fornisce identificazione e autenticazione degli utenti mediante diversi meccanismi di autenticazione, controllo di accesso discrezionale (DAC) e vincolato (MAC) ad un gran numero di oggetti diversi, separazione delle macchine virtuali, funzionalità di audit configurabile, funzioni di gestione della sicurezza avanzate, preparazione degli oggetti per



il riutilizzo e funzionalità interne per la protezione da interferenze e manomissioni da parte di utenti o soggetti non attendibili.

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

### 7.3.1 Architettura dell'ODV

#### 7.3.1.1 Panoramica generale dell'ODV

L'ODV è il prodotto di tipo *hypervisor* z/VM, configurato come parte di un cluster SSI formato da una o più istanze di z/VM, che include i componenti software descritti nel capitolo 1.5.4 del Traguardo di Sicurezza [TDS].

z/VM è un sistema operativo progettato per ospitare altri sistemi operativi, ciascuno all'interno della propria macchina virtuale. Più macchine virtuali possono essere eseguite contemporaneamente per espletare una varietà di funzioni che richiedono accesso controllato e separato alle informazioni memorizzate nel sistema. L'ODV fornisce una macchina virtuale per ciascun utente che ha effettuato l'accesso, separando il dominio di esecuzione di ciascun utente da altri utenti, secondo quanto stabilito nelle definizioni della macchina virtuale memorizzate nella directory di sistema. Inoltre, la directory di sistema contiene informazioni relative al controllo di accesso alle funzioni privilegiate, come ad esempio l'utilizzo di alcune opzioni dell'istruzione DIAGNOSE del processore. In aggiunta a questo meccanismo, l'accesso a risorse e funzioni privilegiate viene mediato dal server di sicurezza RACF.

L'ODV è visto come un'istanza di un cluster SSI che comprende da uno a quattro sistemi z/VM individuali. Questi singoli sistemi z/VM vengono eseguiti ciascuno all'interno di una macchina astratta come unico sistema operativo a livello della macchina astratta stessa ed esercitano il pieno controllo su di essa, indipendentemente dal software in esecuzione all'interno delle macchine virtuali. Queste macchine astratte sono fornite da partizioni logiche (LPAR) dei server mainframe IBM.

Le LPAR non fanno parte dell'ODV, ma appartengono all'ambiente operativo. Si noti che, sebbene un'istanza di z/VM possa essere eseguita all'interno di un'altra istanza di z/VM, la configurazione valutata è limitata ad un'istanza di z/VM in esecuzione direttamente all'interno di una LPAR. Un'istanza di z/VM in esecuzione all'interno di una macchina virtuale è consentita, ma tali istanze di z/VM di "secondo livello" non fanno parte della configurazione valutata.

La funzione SSI di z/VM consente di configurare fino a quattro sistemi z/VM come membri di un cluster SSI, che condividono risorse diverse.

I membri del cluster SSI possono trovarsi sullo stesso apparato hardware o su apparati separati. SSI consente di gestire i membri del cluster come un unico sistema, il che consente di effettuare la manutenzione di ciascun membro del cluster senza dover interrompere l'operatività dell'intero cluster. SSI implementa anche il concetto di Live Guest Relocation (LGR) grazie al quale un sistema operativo Linux in esecuzione può essere spostato da un membro di un cluster ad un altro senza che sia necessario arrestarlo completamente durante il processo di trasferimento.

Tutte le istanze di z/VM membri di un cluster SSI condividono il database RACF, ma non condividono i dischi di audit di RACF. Ogni istanza di z/VM deve eseguire la propria istanza di RACF, la quale accede al database RACF condiviso. La condivisione del database RACF avviene condividendo tra le diverse istanze di z/VM del cluster SSI il volume DASD (Direct Access Storage Device) in cui è memorizzato il database RACF. Sebbene sia tecnicamente possibile condividere il database RACF tra z/VM e z/OS, questa possibilità è esplicitamente esclusa dalla valutazione.

Il database RACF può anche essere condiviso da diverse istanze dell'ODV. La condivisione è implementata in maniera simile alla condivisione del database RACF all'interno del cluster SSI. Tuttavia, a seconda dello scenario di utilizzo, tale condivisione potrebbe non essere consigliabile.

Le piattaforme hardware selezionate per la valutazione sono costituite da prodotti IBM che risultano disponibili alla data di chiusura della valutazione e che rimarranno disponibili anche in seguito per un certo periodo di tempo. Un prodotto eventualmente ritirato dal mercato può comunque essere ottenuto tramite richiesta speciale a IBM.

Le funzioni di sicurezza dell'ODV (TSF) sono fornite dal *kernel* del sistema operativo z/VM, denominato Control Program (CP), e dall'applicazione RACF in esecuzione all'interno di una macchina virtuale con privilegi speciali. Oltre a fornire i servizi di autenticazione dell'utente, di controllo di accesso e di audit al CP, RACF può fornire gli stessi servizi ad altre macchine virtuali autorizzate. z/VM fornisce funzioni di gestione che consentono di configurare il TSF adattandolo alle esigenze del cliente.

L'ODV include alcuni elementi che non forniscono funzionalità di sicurezza, ma vengono eseguiti in modalità autorizzata e potrebbero quindi, in caso di comportamento anomalo, compromettere l'ODV. Poiché questi elementi sono importanti per l'operatività degli ambienti di molti utilizzatori finali, sono stati inclusi all'interno dell'ODV sotto forma di applicazioni attendibili.

Nella configurazione valutata, l'ODV consente due modalità operative: una modalità standard, che soddisfa tutti i requisiti del PP base Operating System Protection Profile [OSPP] e del pacchetto esteso per la virtualizzazione [OSPP-VIRT], ed una modalità più restrittiva chiamata Labeled Security Mode, che soddisfa anche tutti i requisiti del pacchetto esteso [OSPP-LS]. In entrambe le modalità di funzionamento vengono utilizzati gli stessi componenti software. Le due modalità differiscono nelle impostazioni di RACF a seconda che usino o meno la sicurezza basata su etichette. Tutti gli altri parametri di configurazione sono identici nelle due modalità.

### 7.3.1.2 *Principali componenti software dell'ODV*

L'ODV è costituito da un massimo di quattro istanze di z/VM, ciascuna definita da tre componenti principali: il Control Program (CP), il Security Manager RACF e il componente TCP/IP. RACF e TCP/IP vengono eseguiti all'interno di macchine virtuali dedicate gestite dal CP.

Il CP di z/VM è principalmente un gestore di risorse di macchine reali. Il CP fornisce a ciascun utente un ambiente di lavoro individuale noto come macchina virtuale. Ogni macchina virtuale è l'equivalente funzionale di un sistema fisico e sfrutta in condivisione le istruzioni e le funzionalità del processore reale, le memorie, la console e le risorse dei dispositivi di I/O.

Il CP fornisce il supporto alla connettività che consente ai programmi applicativi in esecuzione all'interno di macchine virtuali di scambiarsi informazioni tra loro e di accedere alle risorse che risiedono sullo stesso sistema z/VM o su sistemi z/VM diversi.

Allo scopo di creare e mantenere queste regole (definizioni delle macchine virtuali) vengono utilizzati software aggiuntivi di gestione, che vengono eseguiti esternamente al CP ma che fanno comunque parte dell'ODV. Per questo motivo, ogni componente del software di gestione viene eseguito all'interno di una macchina virtuale. Di seguito sono elencate le funzionalità eseguite all'interno di macchine virtuali:

- **CMS:** un sistema operativo multiuso per utente singolo utilizzato per eseguire le applicazioni RACF e TCP/IP. CMS non fornisce alcuna funzionalità di sicurezza ma implementa un *file system* che può essere utilizzato dalle applicazioni in esecuzione.
- **Server RACF:** fornisce servizi di autenticazione, autorizzazione e audit al CP e ad altre macchine virtuali autorizzate che eseguono applicazioni su CMS. Viene eseguito all'interno di una macchina virtuale gestita dal CP e comunica col CP attraverso un'interfaccia ben definita strettamente controllata.
- **Server TCP/IP:** fornisce i tradizionali servizi di comunicazione basati su IP. Per le comunicazioni cifrate TLS interagisce con il server SSL, che viene visto come un sotto-componente del componente TCP/IP piuttosto che come una porzione aggiuntiva dell'ODV. Il server TCP/IP e il server SSL non fanno parte del CP, ma vengono eseguiti ognuno all'interno di una rispettiva macchina virtuale gestita dal CP.

Incorporato nello *stack* TCP/IP si trova il servizio Telnet, che consente agli utenti di accedere alle console delle loro macchine virtuali ("log on") dalla rete IP. In particolare, il servizio Telnet riceve il traffico della console dalla rete, rimuove l'incapsulamento dei protocolli Telnet o TN3270 e lo inoltra al CP utilizzando una forma speciale dell'istruzione DIAGNOSE del processore. Il CP genera una sessione di console virtuale come oggetto in memoria. Tutte le informazioni in uscita vengono restituite dal CP al servizio Telnet, che le incapsula nel protocollo Telnet o TN3270E e le invia al client. Il server TCP/IP fornisce anche servizi TLS che consentono la creazione di un canale di comunicazione protetto da cifratura.

## 7.3.2 Caratteristiche di sicurezza dell'ODV

### 7.3.2.1 Politica di sicurezza dell'ODV

La politica di sicurezza dell'ODV è espressa dall'insieme dei Requisiti Funzionali di Sicurezza (SFR) implementati dallo stesso. L'ODV implementa una politica di controllo degli accessi discrezionale e vincolata per controllare l'accesso al sistema. Inoltre, l'ODV implementa politiche relative alle seguenti classi di requisiti funzionali: Security Audit (FAU), Cryptographic Support (FCS), User Data Protection (FDP), Identification and Authentication (FIA), Security Management (FMT), Protection of the TSF (FPT), TOE Access (FTA), Trusted Path/Channels (FTP).

### 7.3.2.2 Obiettivi di sicurezza dell'ambiente operativo

Le ipotesi definite nel Traguardo di Sicurezza [TDS] ed alcuni aspetti delle minacce e delle politiche di sicurezza organizzative non sono coperte dall'ODV stesso. Tali aspetti implicano che specifici obiettivi di sicurezza debbano essere soddisfatti dall'ambiente operativo dell'ODV. In particolare, in tale ambito i seguenti aspetti sono da considerare di rilievo:

- Gli amministratori dell'ODV sono competenti e fidati.
- I sistemi IT esterni attendibili che supportano l'applicazione della politica di sicurezza dell'ODV sono protetti dagli attacchi e si trovano sotto lo stesso dominio di gestione dell'ODV.
- I dati sensibili dell'ODV sono protetti in maniera adeguata.
- I componenti dell'ODV vengono distribuiti, installati e configurati in maniera sicura.
- Le funzionalità di diagnostica del prodotto vengono invocate ad ogni intervallo di manutenzione programmato.
- Le porzioni critiche dell'ODV sono protette da attacchi fisici che possono compromettere gli obiettivi di sicurezza.
- L'ODV è in grado di riprendere l'operatività a seguito di un errore di sistema o di altre interruzioni senza che la sicurezza venga compromessa.
- I sistemi IT esterni attendibili implementano i protocolli e i meccanismi richiesti dal TSF per supportare l'applicazione della politica di sicurezza dell'ODV.

Per una descrizione completa degli obiettivi di sicurezza per l'ambiente dell'ODV, si faccia riferimento al capitolo 4.2 del Traguardo di Sicurezza [TDS].

### 7.3.2.3 Funzioni di sicurezza

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:

- **Identificazione e autenticazione:** l'ODV fornisce la funzionalità di identificazione e autenticazione degli utenti mediante un ID utente alfanumerico ed una password mantenuta cifrata dal sistema. I seguenti componenti dell'ODV eseguono l'identificazione e l'autenticazione in maniera indipendente:
  - Control Program
  - RACF

A supporto di identificazione e autenticazione, l'ODV utilizza RACF per gestire i profili di risorse e i profili utente. Le decisioni basate sull'autenticazione a più fattori possono anche essere affidate a un provider MFA esterno, se configurato. Tali decisioni basate su MFA vengono successivamente applicate dall'ODV.

- **Controllo di accesso discrezionale (DAC):** per l'implementazione di regole DAC estese viene utilizzato il componente dell'ODV RACF, che offre la funzionalità e la flessibilità richieste dal livello di valutazione in confronto all'utilizzo del sistema. In sostanza, in un sistema protetto da RACF l'autorizzazione dell'utente ad accedere ad una risorsa in un qualsiasi momento è determinata da una combinazione dei seguenti fattori:
  - identità dell'utente e gruppo di appartenenza;
  - attributi dell'utente, inclusi gli attributi a livello di gruppo;
  - autorità del gruppo dell'utente;
  - classificazione di sicurezza dell'utente e del profilo della risorsa;
  - autorità di accesso specificata nel profilo della risorsa.
  
- **Controllo di accesso vincolato (MAC) e supporto per la sicurezza basata su etichette:** oltre al DAC, l'ODV fornisce un controllo di accesso vincolato (MAC) che impone restrizioni all'accesso alle informazioni basate sulla classificazione di sicurezza. Ogni utente ed ogni oggetto controllato da RACF può avere una classificazione di sicurezza specificata nel corrispondente profilo. La classificazione di sicurezza è definita da un livello di sicurezza e da zero o più categorie di sicurezza. Le etichette di sicurezza vengono gestite da RACF separatamente dalle classi di privilegi.

Il controllo di accesso applicato dall'ODV garantisce che gli utenti possano accedere in lettura ad informazioni etichettate solamente se la loro etichetta di sicurezza domina l'etichetta delle informazioni e che possano accedere in scrittura ai contenitori di informazioni etichettate solamente se l'etichetta del contenitore domina quella del soggetto.
  
- **Separazione delle macchine virtuali:** eventuali malfunzionamenti del sistema operativo che si verificano all'interno delle macchine virtuali non possono influire sull'ODV in esecuzione sul processore reale. Poiché l'errore viene isolato sulla macchina virtuale, solo quella macchina virtuale si interrompe e l'utente può eseguire nuovamente l'IPL senza influire negativamente sulle attività di test e produzione in esecuzione su altre macchine virtuali.

Tramite il supporto del processore sottostante, l'ODV circoscrive le conseguenze di errori software (come interrupt di programma causati da eccezioni intercettate) che si verificano in una macchina virtuale a quella specifica macchina, non influenzando quindi altre macchine virtuali o il CP.

Errori del CP che non possono essere isolati su una delle macchine virtuali gestite comportano la terminazione anomala ("abend") del CP stesso. In caso di *abend*, il sistema si reinizializzerà da solo, se possibile. Alle condizioni di *abend* sono associati codici numerici speciali che ne identificano la causa.
  
- **Audit:** l'ODV fornisce una funzionalità di audit che consente di generare record di audit per eventi critici di sicurezza. RACF offre una serie di funzioni di log e reportistica che consentono agli utenti proprietari delle risorse e agli utenti con ruolo auditor di identificare gli utenti che tentano di accedere alle risorse. I record di audit generati da RACF vengono memorizzati in file residenti su dischi protetti da

modifiche o cancellazioni non autorizzate dal meccanismo MAC (in modalità Labeled Security Mode).

- **Riutilizzo degli oggetti:** l'ODV fornisce una funzione che cancella gli oggetti protetti e gli spazi di archiviazione precedentemente utilizzati dalle macchine virtuali o dall'ODV stesso prima della riassegnazione ad altre macchine virtuali o all'ODV. Ciò garantisce la riservatezza dei dati gestiti dall'ODV e dalle macchine virtuali. I dispositivi di archiviazione e i loro derivati (come minidischi o dischi temporanei) devono essere cancellati manualmente dall'amministratore in conformità con le politiche dell'organizzazione. Supporto aggiuntivo è fornito dal software IBM Directory Maintenance Facility (DirMaint), che tuttavia non fa parte della valutazione.
- **Gestione della sicurezza:** l'ODV fornisce una serie di comandi e opzioni per gestire in modo adeguato le funzioni di sicurezza. L'ODV definisce diversi ruoli che sono autorizzati ad eseguire le diverse attività di gestione relative alla sicurezza dell'ODV:
  - Le opzioni di sicurezza generali sono gestite dagli amministratori della sicurezza.
  - La gestione degli attributi MAC viene eseguita dagli amministratori della sicurezza in modalità Labeled Security Mode.
  - La gestione degli utenti e dei relativi attributi di sicurezza viene eseguita dagli amministratori della sicurezza. La gestione dei gruppi può essere delegata ad amministratori della sicurezza dei gruppi.
  - La gestione delle definizioni delle macchine virtuali viene eseguita dagli amministratori della sicurezza.
  - Gli utenti possono modificare la propria password, il loro gruppo predefinito e il loro nome utente.
  - Gli utenti possono scegliere la propria etichetta di sicurezza dall'intervallo definito nel proprio profilo al momento dell'accesso in modalità Labeled Security Mode.
  - Gli auditor gestiscono i parametri del sistema di audit (ad esempio l'elenco degli eventi controllati) e possono analizzare l'*audit trail*.
- **Protezione del TSF:** il CP dell'ODV garantisce l'integrità del proprio dominio. Nessuna macchina virtuale può accedere alle risorse dell'ODV senza un'autorizzazione appropriata. Ciò impedisce la manomissione delle risorse dell'ODV da parte di soggetti non attendibili. A supporto di questa funzionalità vi sono caratteristiche implementate in hardware, in particolare la Interpretive-Execution Facility (istruzione SIE). Pertanto, i componenti hardware e firmware che forniscono la macchina astratta per l'ODV devono essere protetti fisicamente da accessi non autorizzati.
- **Clustering SSI:** il meccanismo di *clustering* SSI integra diversi sistemi z/VM in un cluster allo scopo condividere risorse diverse. La comunicazione del cluster SSI

garantisce la serializzazione dell'accesso simultaneo alle risorse condivise, se necessario.

Uno degli obiettivi principali di SSI è il supporto al riposizionamento in tempo reale delle macchine virtuali. Il CP garantisce il trasferimento della memoria e dello stato della macchina virtuale in un altro membro del cluster SSI senza interruzione rilevante del servizio della macchina virtuale che viene riposizionata.

## 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] dichiara conformità *strict* ai seguenti Profili di Protezione e pacchetti estesi:

- Operating System Protection Profile, Version 2.0 [OSPP]
- OSPP Extended Package – Labeled Security, Version 2.0 [OSPP-LS]
- OSPP Extended Package – Virtualization, Version 2.0 [OSPP-VIRT]

## 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]. Poiché il TDS dichiara conformità *strict* al PP [OSPP], sono inclusi anche i seguenti componenti estesi definiti in tale PP:

- FDP\_RIP.3: Full residual information protection of subjects;
- FIA\_USB.2: Enhanced user-subject binding.

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

Informativa 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 17 marzo 2021 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFVv1]. Una versione aggiornata dell'RFV [RFVv2] contenente solo modifiche di lieve entità è stata approvata dall'Organismo di Certificazione il 13 aprile 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 ([RFVv1] e [RFVv2]) 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 "IBM z/VM Version 7 Release 2" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4, con aggiunta di ALC\_FLR.3, in relazione alle funzionalità di sicurezza riportate nel Traguado di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B – Configurazione valutata.

La Tabella 1 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia EAL4, con aggiunta di ALC\_FLR.3.

Classi e componenti di garanzia		Verdetto
<b>Security Target evaluation</b>	<b>Classe ASE</b>	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
<b>Development</b>	<b>Classe ADV</b>	Positivo
Security architecture description	ADV_ARC.1	Positivo
Complete functional specification	ADV_FSP.4	Positivo
Implementation representation of the TSF	ADV_IMP.1	Positivo
Basic modular design	ADV_TDS.3	Positivo
<b>Guidance documents</b>	<b>Classe AGD</b>	Positivo
Operational user guidance	AGD_OPE.1	Positivo
Preparative procedures	AGD_PRE.1	Positivo
<b>Life cycle support</b>	<b>Classe ALC</b>	Positivo
Production support, acceptance procedures and automation	ALC_CMC.4	Positivo
Problem tracking CM coverage	ALC_CMS.4	Positivo

Classi e componenti di garanzia		Verdetto
Delivery procedures	ALC_DEL.1	Positivo
Identification of security measures	ALC_DVS.1	Positivo
Developer defined life-cycle model	ALC_LCD.1	Positivo
Well-defined development tools	ALC_TAT.1	Positivo
<i>Systematic flaw remediation</i>	<i>ALC_FLR.3</i>	Positivo
<b>Test</b>	<b>Classe ATE</b>	Positivo
Analysis of coverage	ATE_COV.2	Positivo
Testing: basic design	ATE_DPT.1	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing - sample	ATE_IND.2	Positivo
<b>Vulnerability assessment</b>	<b>Classe AVA</b>	Positivo
Focused vulnerability analysis	AVA_VAN.3	Positivo

Tabella 1 - 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 "IBM z/VM Version 7 Release 2" 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 cap. 4.2 del Traguardo di Sicurezza [TDS]. Si consiglia ai potenziali acquirenti di verificare la rispondenza ai requisiti identificati e di prestare attenzione alle raccomandazioni contenute in questo Rapporto.

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 ([ZVM-CPG], [ZVM-SCG]).

Si assume che l'ODV funzioni in modo sicuro qualora vengano rispettate le ipotesi sull'ambiente operativo descritte nel par. 3.2 del documento [TDS]. In particolare, si assume che gli amministratori dell'ODV siano adeguatamente addestrati al corretto utilizzo dell'ODV e scelti tra il personale fidato dell'organizzazione. L'ODV non è realizzato per contrastare minacce provenienti da amministratori inesperti, malfidati o neglienti.

Occorre inoltre notare che la sicurezza dell'operatività dell'ODV è condizionata al corretto funzionamento delle piattaforme hardware su cui è installato l'ODV e di tutti i sistemi IT

esterni attendibili sui quali l'ODV si basa per supportare la realizzazione della sua politica di sicurezza. Le specifiche dell'ambiente operativo sono descritte nel documento [TDS].

## 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

L’ODV è composto unicamente da software; nessun componente hardware o firmware viene fornito come parte del prodotto.

In Tabella 2 sono elencati gli elementi che costituiscono l’ODV, inclusi il software e i documenti di guida.

#	Tipo	Identificativo	Release	Metodo di consegna
z/VM Version 7 Release 2.0				
1	SW	z/VM Version 7 Release 2, program number 5741-A09	V7R2	DVD / Download
2	DOC	Program Directory for z/VM V7R2 Base	GI13-4358-01	Copia cartacea
3	DOC	Program Directory for RACF function level 720	GI13-4364-01	Copia cartacea
4	DOC	Guide for Automated Installation and Service	GC24-6292-02	Copia cartacea
5	DOC	z/VM V7.2 Certified Product Guidance sha256-Checksum: 258b5d926285059a725e9827536a0e9e8a3704b7d41856b9dab7777d9f006910 2020 September zVM720 GA Collection.zip	n/d	Copia elettronica
6	DOC	z/VM V7.2 Secure Configuration Guide sha256-Checksum: 6090b1fe0b3fee9a570f3c68ee0e434073f12972795e154c9fc0d5ddc053d1c7 hcps0_v7r2.pdf	SC24-6323-02	Copia elettronica
Elementi aggiuntivi				
7	SW	RSU1 (livello di servizio z/VM 7.2 GA) Da scaricare in formato elettronico da IBM Shopz <a href="https://www.ibm.com/software/shopzseries">https://www.ibm.com/software/shopzseries</a>	n/d	Download
8	SW	PTF for APAR PH24751 Da scaricare in formato elettronico da IBM Shopz <a href="https://www.ibm.com/software/shopzseries">https://www.ibm.com/software/shopzseries</a>	n/d	Download

Tabella 2 - Elementi consegnabili dell’ODV

I clienti in possesso di un ID cliente IBM appropriato possono utilizzare il portale Web IBM Shopz ([https://www.ibm.com/software/shopzseries/ShopzSeries\\_public.wss](https://www.ibm.com/software/shopzseries/ShopzSeries_public.wss)) per effettuare l’ordine dell’ODV. Nel caso in cui il cliente necessiti di assistenza, può contattare un

rappresentante di vendita IBM che supporterà il cliente nella compilazione del modulo d'ordine.

Gli ordini del prodotto z/VM su DVD vengono elaborati da un Centro di Produzione SDF. Il file immagine di z/VM viene duplicato su un set di supporti DVD, che viene quindi imballato in una scatola di cartone e sigillato con pellicola termoretraibile. Il pacco finale viene quindi consegnato al cliente assieme alla lista del contenuto tramite un servizio di corriere.

L'intero processo che va dalla preparazione ed etichettatura dei supporti alla consegna finale del pacco sigillato al cliente, avviene sotto la supervisione di un sistema di controllo che utilizza un sistema di identificazione basato su codici a barre per tutte le parti di un ordine, fino al completamento del processo. Il codice a barre consente l'associazione univoca dei supporti e della documentazione aggiuntiva ad un numero d'ordine specifico e, quindi, al cliente che ha effettuato l'ordine corrispondente.

Una volta che il pacco è stato consegnato presso il luogo specificato nell'ordine, il cliente è in grado di verificarne la corrispondenza con quanto ordinato effettuando un controllo incrociato tra i codici prodotto riportati nella lista del contenuto inclusa nella consegna e quelli stampati sulle etichette dei supporti consegnati.

## 9.2 Identificazione dell'ODV

Durante il processo di ordine dell'ODV, il cliente deve richiedere esplicitamente la versione certificata CC di z/VM Versione 7 Release 2. Questo fornisce già la garanzia il prodotto consegnato al cliente è effettivamente l'ODV comprensivo di tutti i componenti necessari. Dopo aver effettuato l'installazione del prodotto secondo quanto indicato nel documento Secure Configuration Guide [ZVM-SCG], l'amministratore sarà in grado di verificare la versione dell'ODV mediante il comando:

```
QUERY CPLEVEL
```

Questo comando dovrà restituire a schermo la seguente stringa di versione:

```
z/VM Version 7 Release 2.0, service level 2001 (64-bit)
```

L'amministratore dovrà inoltre verificare l'elenco delle PTF installate confrontandolo con quello delle PTF richieste indicato nel Traguardo di Sicurezza [TDS]. A tale scopo, l'amministratore potrà utilizzare i comandi seguenti:

```
VMFSIM QUERY 7VMCPR20 SRVAPPS * TDATA :PTF  
VMFSIM QUERY 7VMRAC20 SRVAPPS * TDATA :PTF  
VMFSIM QUERY 7VMTCP20 SRVAPPS * TDATA :PTF
```

Questi comandi dovranno restituire in output le PTF indicate nel seguito.

Per il CP dovranno risultare installate le seguenti PTF:

```
UM35699  
UMRSU01
```

Per il componente TCP/IP dovrà risultare installata la seguente PTF:

```
UI72767
```

Per RACF non dovrà risultare installata nessuna PTF.

### **9.3 Installazione, inizializzazione e utilizzo sicuro dell'ODV**

L'installazione, la configurazione e l'operatività dell'ODV devono essere eseguite secondo le istruzioni riportate nelle sezioni appropriate della documentazione di guida fornita con il prodotto al cliente.

In particolare, i seguenti documenti contengono informazioni dettagliate per l'inizializzazione sicura dell'ODV, la preparazione del suo ambiente operativo e il funzionamento sicuro dell'ODV in conformità con gli obiettivi di sicurezza specificati nel Traguardo di Sicurezza [TDS]:

- z/VM Version 7 Release 2 Secure Configuration Guide [ZVM-SCG]
- z/VM V7.2 Certified Product Guidance [ZVM-CPG]

La Secure Configuration Guide contiene riferimenti ad altra documentazione di guida pertinente contenuta nella Certified Product Guidance di z/VM. Tutta la documentazione sopra elencata è disponibile per il download sicuro al seguente ResourceLink sul sito Web di IBM:

<https://www.ibm.com/servers/resourceLink/svc0302a.nsf/pages/zVMV7R2Library>

La Certified Product Guidance corrisponde alla "z/VM 7.2 2020 September GA PDF collection". Questa raccolta include tutti i documenti relativi a z/VM V7R2 pubblicati nel momento in cui tale versione è divenuta disponibile al pubblico.

## 10 Appendice B – Configurazione valutata

L'oggetto di valutazione (ODV) è il prodotto "z/VM Version 7 Release 2", sviluppato dalla società IBM Corp. L'ODV è composto unicamente da software ed è accompagnato dalla documentazione di guida.

L'ODV è rappresentato da un cluster SSI composto da un massimo di quattro istanze in collaborazione del prodotto z/VM, ciascuna in esecuzione su una macchina astratta. Ogni istanza di z/VM è installata come unico sistema operativo a livello della macchina astratta ed esercita il controllo completo sulla macchina astratta, indipendentemente dal software in esecuzione all'interno delle macchine virtuali. Le macchine astratte sono fornite da partizioni logiche (LPAR) di server IBM Z.

Un elenco dettagliato dei modelli di server IBM Z supportati è fornito nel par. 1.5.4.4 del Traguardo di Sicurezza [TDS].

Le LPAR non fanno parte dell'ODV, ma appartengono all'ambiente operativo dell'ODV. Si noti che, sebbene un'istanza di z/VM possa tecnicamente essere eseguita all'interno di un'altra istanza z/VM, la configurazione valutata è limitata ad istanze di z/VM eseguite direttamente all'interno di una LPAR. Un'istanza di z/VM in esecuzione all'interno di una macchina virtuale è consentita, ma tali istanze di z/VM di "secondo livello" non fanno parte della configurazione valutata.

La configurazione valutata dell'ODV è inoltre definita dai requisiti di configurazione che devono essere soddisfatti, come indicato nel documento Secure Configuration Guide [ZVM-SCG]. Il Traguardo di Sicurezza [TDS] fa riferimento nel par. 1.5.4.3 a questo documento, che fa parte dei materiali consegnabili dell'ODV.

## 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 EAL4, con aggiunta di ALC\_FLR.3, tali attività prevedono tre passi successivi:

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

### 11.1 Configurazione per i Test

I test del Fornitore e i test indipendenti dei Valutatori sono stati eseguiti sulla stessa configurazione, vale a dire sui due sistemi di test denominati GDLMCCC e GDLPCCC, ciascuno in esecuzione all'interno di una partizione logica separata.

Le partizioni logiche sono state fornite da versioni certificate di PR/SM su un server IBM z14 (GDLPCCC) e su un server IBM z15 (GDLMCCC), in accordo con l'elenco di piattaforme hardware supportate riportato nel par. 1.5.4.4 del Traguardo di Sicurezza [TDS].

Sia per le sessioni di test del Fornitore, sia per quelle dei Valutatori, l'ODV è stato installato sui sistemi di test nella sua configurazione valutata, così come richiesto dal Traguardo di Sicurezza [TDS]. Ciò è stato confermato dai Valutatori, che hanno analizzato le evidenze generate dal Fornitore ed eseguito controlli aggiuntivi durante la preparazione e l'esecuzione dei test indipendenti.

I test sono stati eseguiti sul sistema GDLMCCC come uno dei membri del cluster SSI, configurato e in esecuzione all'interno di una partizione logica di un server z15. Il test relativo alla funzione SSI ha coinvolto anche il sistema GDLPCCC come secondo membro del cluster, configurato ed in esecuzione all'interno di una partizione logica di un server z14.

Su entrambi i sistemi di test è stato installato il prodotto z/VM Version 7 Release 2 con la funzionalità SSI abilitata. Un'analisi eseguita dai Valutatori ha dimostrato che sulle macchine sono state installate tutte le RSU e le PTF richieste, come indicato nel par. 1.5.4.1 del Traguardo di Sicurezza [TDS].

L'ODV era in configurazione valutata quando sono stati eseguiti i test del Fornitore.

La scelta di eseguire i test solamente sui sistemi precedentemente identificati è stata ritenuta una limitazione accettabile, in quanto la configurazione di tali sistemi è di fatto rappresentativa di tutte le configurazioni consentite. L'ODV fa affidamento su una macchina astratta sottostante conforme alla definizione della z/Architecture. IBM ha eseguito test approfonditi dell'hardware di riferimento per tutte le configurazioni dei processori (inclusa quella selezionata) per verificare la piena conformità alla z/Architecture della macchina astratta fornita all'ODV.



## 11.2 Test funzionali svolti dal Fornitore

### 11.2.1 Approccio adottato per i test

Il Fornitore ha progettato un insieme specifico di test orientati ai CC che comprende diversi scenari di test che coprono le funzioni di sicurezza fornite dall'ODV.

I test eseguiti dal Fornitore stimolano direttamente le seguenti TSFI identificate nelle Specifiche Funzionali e ne esaminano il comportamento risultante:

- Comandi CP
- Comandi RACF
- API
- RACF Report Writer
- Server Telnet

Il supporto alla MFA è rappresentato nelle TSFI del CP (mediante il comando LOGON) e di RACF (mediante i comandi ADDUSER, ALTUSER e DELUSER e il file MFA CONTROL).

Le seguenti TSFI vengono verificate indirettamente da tutti i test eseguiti e dalla configurazione richiesta per i test:

- Directory di sistema
- Configurazione di sistema
- Comandi e file di configurazione TCP/IP
- IUCV

Tutti i casi di test tranne due sono automatizzati. Successivamente all'esecuzione di un file di script, viene eseguito un numero significativo di singoli test con l'ausilio degli strumenti di test CHUG e FACT, i risultati dei quali vengono opportunamente documentati. La corretta verifica della corrispondenza dei risultati effettivi dei test con i risultati attesi è già inclusa nei rispettivi casi di test. I casi di test che prevedono l'esecuzione manuale sono relativi a RACF Report Writer e all'autenticazione basata su certificati implementata dal server SSL e contengono informazioni sufficientemente dettagliate da consentire a chi effettua i test di decidere se i risultati effettivamente ottenuti corrispondono a quelli previsti.

In genere, IBM esegue un numero significativo di test SAK allo scopo di verificare che l'interfaccia fornita alle macchine virtuali gestite dall'ODV sia compatibile con la definizione della z/Architecture. Questi test SAK, tuttavia, sono da considerarsi test negativi, poiché non possono realmente dimostrare la conformità con la z/Architecture ma, sulla base dell'assenza di errori di sistema a fronte di massicci invii di flussi di istruzioni casuali al processore per un lungo periodo di tempo, forniscono sufficiente garanzia della corretta implementazione della z/Architecture. Si noti che per la valutazione corrente il Fornitore non ha ritenuto necessario effettuare test SAK a livello di z/VM, in quanto non sono state apportate modifiche di rilievo alla z/Architecture dalla precedente valutazione. Tuttavia,

test SAK sono stati effettivamente eseguiti a livello del sottostante PR/SM per le piattaforme hardware supportate da z/VM e non hanno rivelato alcuna deviazione rispetto a quanto verificato nelle rispettive precedenti valutazioni di PR/SM.

### **11.2.2 Copertura dei test**

I test del Fornitore hanno coperto l'architettura dell'ODV fino al livello dei sottosistemi. L'analisi di profondità dei test del Fornitore ha dimostrato che i sottosistemi dell'ODV CP, RACF e TCP/IP sono stati oggetto di casi di test che hanno sollecitato le TSFI e le parti del TSF implementate da questi componenti.

### **11.2.3 Risultati dei test**

I risultati dei test del Fornitore esaminati dai Valutatori mostrano che tutti i casi di test ad eccezione di uno hanno avuto esito positivo, ovvero il comportamento dell'ODV osservato durante i test ha coinciso con il comportamento previsto.

Si evidenzia che l'unico caso di test fallito è dovuto a un problema presente da lungo tempo che non è rilevante per la sicurezza, né ha un impatto sul TSF. Il Fornitore sta ancora esaminando una soluzione adeguata, ma ha affermato che a causa della natura del problema, che non influisce sulla sicurezza, la sua risoluzione ha una priorità bassa e verrà risolto in una fase successiva dello sviluppo. I Valutatori hanno ritenuto accettabile il caso di test non superato in quanto i requisiti di profondità e copertura restano comunque soddisfatti e la sicurezza dell'ODV non ne è influenzata.

Anche l'Organismo di Certificazione (OCSI) ritiene accettabile la presenza del test fallito in quanto è stato dimostrato che questo non ha alcun impatto sulle funzioni di sicurezza dell'ODV. Ad ogni modo, l'OCSI ribadisce la raccomandazione al Fornitore di risolvere questo problema prima della successiva richiesta di rivalutazione dell'ODV.

## **11.3 Test funzionali ed indipendenti svolti dai Valutatori**

### **11.3.1 Approccio adottato per i test**

I Valutatori hanno ripetuto un sottoinsieme casuale dei test del Fornitore. Per ciascuno dei gruppi di casi di test relativi a "Comandi CP" (incluso il 100% dei test eseguiti relativi a SSI e SSL), "Comandi RACF" e "DIAGNOSE", la strategia di campionamento ha consentito di ottenere una copertura vicina al 100%. La copertura complessiva raggiunta dal campione scelto è stata circa del 100%. Non è stato ripetuto nessun test SAK.

I Valutatori hanno altresì progettato test indipendenti per coprire le TSFI che non vengono esplicitamente ma solo implicitamente stimulate dalla ripetizione dei test del Fornitore. I test indipendenti dei Valutatori stimolano direttamente il server Telnet, i comandi e i file di configurazione TCP/IP, la directory di sistema e i comandi CP e RACF. I test indipendenti dei Valutatori hanno coperto tutte le TSFI ad esclusione delle API comprendenti le istruzioni z/Architecture e del RACF Report Writer, mentre quelle non esplicitamente elencate in precedenza sono state stimulate indirettamente.

### **11.3.2 Copertura dei test**

Utilizzando i test del Fornitore come base per i test indipendenti e ripetendo un sottoinsieme dei test del Fornitore, i Valutatori hanno raggiunto la stessa profondità di test

del Fornitore. Pertanto, i test eseguiti dai Valutatori hanno coperto la struttura dell'ODV fino al livello dei sottosistemi.

### 11.3.3 Risultati dei test

Tutti i test del Fornitore rieseguiti hanno avuto esito positivo, vale a dire che i risultati effettivi ottenuti dai Valutatori hanno coinciso con i risultati attesi. Tutti i casi di test progettati dai Valutatori sono stati eseguiti con successo e non sono state rilevate deviazioni dai risultati attesi.

Nessuno dei test eseguiti è fallito a causa di comportamenti dell'ODV non conformi a quelli attesi o in violazione dei requisiti di sicurezza dichiarati nel Traguardo di Sicurezza [TDS].

## 11.4 Analisi delle vulnerabilità e test di intrusione

I Valutatori hanno consultato fonti di informazioni di dominio pubblico per identificare vulnerabilità note da verificare mediante esecuzione di test di intrusione. Tale ricerca non ha prodotto risultati.

Per quanto riguarda i test di intrusione derivati dall'analisi indipendente delle vulnerabilità, i Valutatori hanno identificato un totale di due casi di test. Mentre il primo caso di test è stato mirato ad identificare interfacce aggiuntive che avrebbero potuto introdurre potenziali debolezze, il secondo caso di test ha avuto lo scopo di sondare esplicitamente i punti deboli dell'interfaccia del server Telnet. Tutti i test sono stati eseguiti al livello dei sottosistemi del progetto dell'ODV, andando a stimolare il sottosistema TCP/IP dell'ODV.

I Valutatori hanno eseguito una scansione delle porte sullo stesso segmento di rete dell'ODV allo scopo di eliminare eventuali interferenze con altri componenti di rete attivi. La scansione è stata effettuata utilizzando lo strumento nmap. Come previsto, lo strumento non ha rilevato altre porte aperte sull'ODV oltre alla porta Telnet, necessaria come da progetto per l'instaurazione di connessioni con l'ODV.

Sono stati eseguiti tentativi di provocare deliberatamente errori di tipo *buffer overflow* durante l'immissione delle credenziali dell'utente. Tale test è stato eseguito sia utilizzando i client standard previsti per l'accesso all'ODV, sia dalla riga di comando. Non è stata eseguita alcuna configurazione specifica relativa ad altri componenti di rete attivi. I test non hanno rivelato debolezze. Le immissioni di dati di input sovradimensionati sono state rifiutate con messaggi di errore, in conformità con i risultati attesi.

L'implementazione del protocollo TLS da parte dell'ODV è stata sollecitata con tecniche di *fuzzing* utilizzando una suite di test disponibile pubblicamente. I test non hanno rilevato errori di implementazione o comportamenti anomali dell'ODV.

L'analisi indipendente di vulnerabilità eseguita dai Valutatori non ha rilevato la presenza di vulnerabilità dell'ODV sfruttabili nell'ambiente operativo dichiarato da attaccanti con un potenziale di attacco previsto pari ad Enhanced-Basic.

Le seguenti vulnerabilità, che interessano potenzialmente tutte le tipologie di sistemi operativi, sono state individuate ed analizzate dal Fornitore e confermate dai Valutatori come residue:

- vulnerabilità a vari tipi di codici malevoli (*trojan horse*, *virus*, *worm*);

- vulnerabilità a *buffer overflow*;
- vulnerabilità legate a difetti di progettazione dell'architettura hardware sottostante (attacchi Meltdown e Spectre).

Lo sfruttamento delle vulnerabilità sopra elencate richiede un potenziale di attacco che va oltre quello previsto pari ad Enhanced-Basic. In particolare, il potenziale di attacco richiesto per sfruttare efficacemente *buffer overflow* e vulnerabilità architetturali è stato calcolato come superiore ad High.