Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica -
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

Organismo di Certificazione della Sicurezza Informatica

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

Certificato n. 9/19

(Certification No.)

Prodotto: JBoss Enterprise Application Platform 7 Version 7.2.3
(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:

EAL4+
(ALC_FLR.3)

Il Direttore
(Dott.ssa Eva Spina)

Roma, 2 dicembre 2019

Common Criteria

Fino a EAL2 *(Up to EAL2)*

Questa pagina è lasciata intenzionalmente vuota

Organismo di Certificazione della Sicurezza Informatica

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

JBoss Enterprise Application Platform 7 Version 7.2.3

OCSI/CERT/ATS/05/2018/RC

Versione 1.0

2 dicembre 2019

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	02/12/2019

2 Indice

3 Elenco degli acronimi

ACID	Atomicity, Consistency, Isolation and Durability
API	Application Programming Interface
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CM	Configuration Management
CP	Customer Portal
cPP	collaborative Protection Profile
DB	Database
DMR	Dynamic Model Representation
DN	Domain Name
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	Evaluation Assurance Level
EJB	Enterprise Java Beans
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IT	Information Technology
JAX-RS	Java API for RESTful Web Services
JAX-WS	Java API for XML-based Web Services
JAXTX	XML Transactioning API for Java
JDBC	Java DataBase Connectivity
JDK	Java Development Kit
JMS	Java Messaging Service
JNDI	Java Naming and Directory Interface
JRE	Java Runtime Environment

JSP	JavaServer Pages
JVM	Java Virtual Machine
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
MBeans	Managed Bean
MSC	Modular Service Container
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
OS	Operating System
PP	Protection Profile
POJO	Plain Old Java Object
REST	Representational State Transfer
RHEL	Red Hat Enterprise Linux
RHN	Red Hat Network
RMI-IIOP	Remote Method Invocation over Internet Inter-Orb Protocol
RPC	Remote Procedure Call
RPM	Red Hat Package Manager
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security

TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
URL	Uniform Resource Locator
VFS	Virtual File System
VM	Virtual Machine

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

[CCGUIDE] "Red Hat JBoss Enterprise Application Platform 7.2.3 Common Criteria Configuration Guide", 9 October 2019

[ETR] Final Evaluation Technical Report "JBoss Enterprise Application Platform 7.2", OCSI_CERT_ATS_05_2018_ETR_191017_v1.1, Version 1.1, atsec information security GmbH, 17 October 2019

[TDS] JBoss Enterprise Application Platform 7 Version 7.2.3 Security Target, Version 1.9, Red Hat, Inc., 5 November 2019

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 EAL 2, 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 http://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 "JBoss Enterprise Application Platform 7 Version 7.2.3" (in breve JBoss EAP), sviluppato dalla società Red Hat, Inc.

JBoss EAP è un server di applicazioni basato su Java Enterprise Edition (Java EE) e pertanto supporta una grande varietà di sistemi operativi. JBoss EAP consente ai computer o ai dispositivi client di accedere ad applicazioni Java tramite diversi protocolli di rete. JBoss EAP gestisce la logica di business dell'applicazione, incluso l'accesso e la fornitura dei dati utente richiesti dall'applicazione stessa.

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. 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 aggiunta di ALC_FLR.3, in conformità a quanto indicato 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 riassume l'esito della valutazione di sicurezza del prodotto "JBoss Enterprise Application Platform 7 Version 7.2.3" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

I potenziali acquirenti sono quindi tenuti a consultare il presente Rapporto di Certificazione 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	JBoss Enterprise Application Platform 7 Version 7.2.3
Traguardo di Sicurezza	JBoss Enterprise Application Platform 7 Version 7.2.3 Security Target, Version 1.9 [TDS]
Livello di garanzia	EAL4 con 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	11 giugno 2018
Data di fine della valutazione	17 ottobre 2019

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 capitolo 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 JBoss Enterprise Application Platform (EAP) caratterizzato dai seguenti elementi:

- JBoss EAP 7.2.3
- JBoss Core Services OpenSSL version 1.0.2n

L'ODV non include l'hardware, il firmware, il sistema operativo o la macchina virtuale Java necessari per eseguire i componenti software.

L'ODV implementa un server di applicazioni che, essendo basato su Java Enterprise Edition (Java EE), supporta una grande varietà di sistemi operativi. In qualità di server di applicazioni, JBoss EAP consente ai computer o ai dispositivi client di accedere alle applicazioni tramite diversi protocolli di rete, come HTTP, RMI-IIOP e altri. JBoss EAP gestisce la logica di business dell'applicazione, incluso l'accesso e la fornitura dei dati utente richiesti dall'applicazione stessa.

L'ODV è definito come un'istanza autonoma di JBoss EAP. Nel caso in cui venga definito un cluster di nodi JBoss EAP, l'intero cluster viene considerato come un unico ODV.

L'ODV fornisce funzionalità di identificazione e autenticazione degli utenti, controllo di accesso per vari tipi di oggetti, funzionalità di audit, *clustering*, *rollback* delle transazioni e controllo di accesso basato su ruoli per risorse e operazioni di tipo amministrativo.

Una descrizione più dettagliata delle funzioni di sicurezza dell'ODV è riportata nel cap. 7.3.2.3.

7.3.1 Architettura dell'ODV

7.3.1.1 Panoramica generale dell'ODV

L'ODV è un server di applicazioni implementato come *framework* Java EE (Enterprise Edition), che consente agli utenti di accedere alle applicazioni Java tramite diversi protocolli di rete. JBoss EAP esegue applicazioni Java che vengono registrate ed eseguite dal server di applicazioni.

JBoss EAP è interamente scritto in Java (ad eccezione del componente JBoss Core Services OpenSSL) e fornisce un ambiente conforme a Java EE, in linea con le specifiche Java EE 7. A seconda della configurazione del server JBoss EAP, è possibile disabilitare componenti richiesti dalla specifica Java EE. Le applicazioni sviluppate per essere eseguite da JBoss EAP devono essere scritte in Java. Gli sviluppatori di tali applicazioni Java implementano la logica di business e possono utilizzare le funzionalità di supporto di Java EE fornite da JBoss EAP.

La configurazione di JBoss EAP consente di abilitare o disabilitare selettivamente ogni contenitore, noto come estensione in JBoss EAP. La distribuzione di JBoss EAP fornisce una serie di estensioni che possono essere utilizzate, mentre altre possono essere implementate da terze parti. La configurazione certificata definisce le estensioni coperte dalla valutazione e che pertanto possono essere abilitate in una configurazione conforme ai CC.

L'architettura di JBoss EAP, mostrata in Figura 1, fornisce l'ambiente per l'esecuzione di diversi contenitori, che consentono alle applicazioni di utilizzare i servizi forniti dai contenitori stessi. Il *framework* JBoss EAP utilizza un caricatore di classi Java diverso per ciascun modulo. Le applicazioni in esecuzione all'interno dei contenitori JBoss EAP, nonché i componenti JBoss EAP, vengono avviati in moduli separati. Tali moduli risultano

isolati l'uno dall'altro, sulla base del meccanismo di separazione della JVM che utilizza caricatori di classi separati. Il *framework* JBoss EAP consente di stabilire collegamenti tra i moduli utilizzando dipendenze specificamente configurate.

Come parte del *framework* Java EE implementato da JBoss, le applicazioni possono mettere a disposizione la loro logica ai client remoti attraverso i seguenti protocolli di rete:

- Protocollo HTTP: i *servlet* Java forniscono le loro funzionalità in base agli URL richiesti dal client.
- Enterprise Java Beans (EJB): le classi Java possono essere rese accessibili ai client remoti consentendo a questi client di accedere alle classi EJB e ai loro metodi mediante JBoss Remoting.

Oltre a questi protocolli, per accedere alla logica di business di un'applicazione possono essere utilizzati vari altri protocolli resi disponibili dal server di applicazioni a supporto della funzionalità dell'applicazione. Tali protocolli sono forniti da diversi contenitori JBoss EAP e non sono disponibili se i contenitori sono disabilitati. Il server di applicazioni può fornire i seguenti protocolli aggiuntivi:

- un protocollo di code di messaggi utilizzabile come canale di comunicazione affidabile e possibilmente asincrono. Le code di messaggi possono essere utilizzate per la comunicazione tra parti diverse di applicazioni distribuite in cui le parti di un'applicazione sono implementate in diverse istanze del server. Inoltre, è possibile utilizzare le code di messaggi per la comunicazione tra applicazione e client.
- un servizio di risoluzione dei nomi JNDI per consentire a diverse parti di un'applicazione o al client di risolvere classi EJB e altre risorse.

JBoss EAP supporta altri protocolli incapsulati nei protocolli sopra menzionati, come HTML o SOAP trasmessi su HTTP. Tuttavia, i meccanismi di sicurezza definiti nel Traguardo di Sicurezza [TDS] vengono applicati sui protocolli di livello esterno sopra elencati.

7.3.1.2 Struttura di JBoss EAP

JBoss EAP implementa una piattaforma per applicazioni Java innovative e scalabili. Include tecnologie open source per la distribuzione e l'*hosting* di applicazioni e servizi Java in ambito aziendale.

JBoss EAP offre un bilanciamento tra innovazione e stabilità di classe *enterprise*, integrando il più diffuso server cluster di applicazioni basato su Java EE con un *framework* per applicazioni di nuova generazione. Costruito su standard aperti, JBoss EAP integra in una soluzione aziendale completa e semplice per applicazioni Java diversi contenitori che implementano funzionalità Java EE e altri contenitori che forniscono meccanismi alle applicazioni che vanno oltre lo standard Java EE.

La specifica Java EE considera i quattro livelli, chiamati anche *tier*, elencati nella Tabella 1. Le applicazioni che utilizzano la specifica Java EE possono implementare qualsiasi

combinazione di questi *tier*. Oltre a elencare i vari *tier*, la Tabella 1 specifica quali di questi possono essere implementati ed eseguiti utilizzando il *framework* di JBoss EAP.

Tier Java EE	Copertura di JBoss
Client Tier Il *Client Tier* è il livello dell'applicazione eseguita sul sistema client per visualizzare le informazioni fornite dal server di applicazioni. Il *Client Tier* può essere implementato da: • Un'*applet* eseguita dal browser Web del client. • Codice JavaScript eseguito dal browser Web del client. • Un'applicazione Java autonoma eseguita dalla Java Virtual Machine del client. • Il client JMS.	L'*applet* può essere memorizzata sul server JBoss per consentire al client di scaricarla in automatico quando accede a una pagina Web servita da JBoss. Tuttavia, né l'*applet*, né l'applicazione vengono eseguiti dal server di applicazioni JBoss EAP, ma vengono eseguiti dalla Java Virtual Machine del sistema client accedendo in remoto alle informazioni di JBoss EAP. Pertanto, il *Client Tier* non è considerato coperto da JBoss.
Web Tier Il *Web Tier* è il livello di presentazione del server di applicazioni. Raccoglie le informazioni di business dal *tier* EJB sottostante e le converte per essere presentate come pagine Web. Il *Web Tier* pertanto non implementa alcuna logica di business in quanto può essere considerato un convertitore di informazioni dalla rappresentazione dei dati interna all'applicazione a una presentazione visualizzabile e interpretabile dall'utente.	Il *Web Tier* può essere implementato utilizzando *servlet* Java in esecuzione nel *framework* JBoss. Il *Web Tier* è implementato dall'applicazione sviluppata dal cliente.
Business Tier Il *Business Tier* implementa la logica di business dell'intera applicazione. La logica di business è considerata la funzionalità che implementa il flusso di informazioni in maniera congruente con lo scopo dell'applicazione.	Il *Business Tier* può essere implementato utilizzando vari tipi di EJB in esecuzione all'interno del *framework* JBoss. JBoss EAP supporta anche l'implementazione della logica di business tramite POJO, che garantiscono un maggiore grado di libertà allo sviluppatore dell'applicazione rispetto agli EJB. Il *Business Tier* è implementato dall'applicazione sviluppata dal cliente.
Enterprise Information System Tier L'*Enterprise Information System Tier* fornisce la logica per consentire al *tier* EJB di accedere ad archivi di dati esterni. Questo *tier* copre quindi i meccanismi di accesso ai database, come ad es. un driver JDBC.	L'ODV fornisce l'interfaccia all'*Enterprise Information System Tier* ma non implementa i database che ospitano i dati aziendali. L'ODV consente agli EJB o POJO dell'applicazione di accedere ai database relazionali elencati per JDBC. L'*Enterprise Information System Tier* è implementato dall'ODV.

Tabella 1 - Elenco dei *tier* Java EE e copertura di JBoss

Fondamentalmente, nell'architettura di JBoss EAP, il *framework* JBoss Module gestisce l'insieme dei componenti modulari di servizi, implementati come POJO o come MBean. Ciò consente di costruire diverse configurazioni e offre la flessibilità necessaria a personalizzare le configurazioni per soddisfare requisiti specifici.

L'amministratore non è costretto a gestire sempre un server monolitico di grandi dimensioni, poiché i componenti non necessari possono essere rimossi (riducendo anche notevolmente i tempi di avvio del server). È anche possibile integrare servizi aggiuntivi in JBoss EAP sviluppando nuovi MBean. Inoltre, è possibile creare POJO configurati come servizi per estendere la funzionalità di JBoss EAP o implementare la logica di business.

La Figura 1 mostra l'interazione tra i diversi componenti di JBoss EAP. JBoss EAP è costituito da un *framework* modulare in cui l'amministratore può abilitare selettivamente i vari componenti. JBoss EAP è conforme alle specifiche Java EE 7 e offre servizi ulteriori rispetto a Java EE. La seguente descrizione si applica all'illustrazione:

- L'hardware insieme al sistema operativo esegue la macchina virtuale Java, che a sua volta esegue il *framework* JBoss Modules. Questo *framework* fornisce le basi sulle quali tutti i contenitori di JBoss EAP eseguono i loro compiti.
- Ciascun contenitore implementa un servizio secondo la specifica Java EE 7 o un servizio che fornisce funzionalità aggiuntive rispetto a Java EE 7.

Le applicazioni vengono eseguite come parte di contenitori (come il contenitore JAX-RS Web Services o il contenitore EJB) e possono utilizzare servizi forniti da altri contenitori.

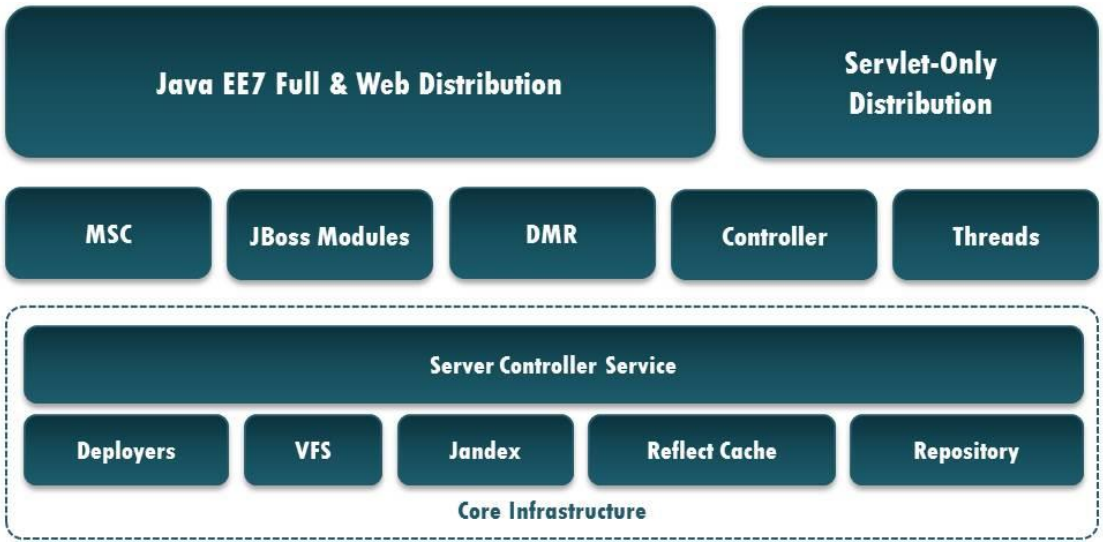

Figura 1 - Architettura di JBoss EAP

L'ODV consente l'interazione degli utenti mediante i seguenti servizi:

- protocollo di trasmissione Web HTTP
- RESTful (JAX-RS) e XML-Based (JAX-WS) Web Service
- Enterprise Java Beans (EJB)
- Java Messaging Service (JMS)
- Java Naming and Directory Interface (JNDI)

Le applicazioni utilizzano i servizi forniti dai diversi contenitori accedendo alle API esportate da ciascun contenitore. Queste applicazioni vengono caricate ed eseguite dal contenitore JSP/Servlet, dal contenitore EJB o da altri contenitori. La separazione tecnica tra le applicazioni non attendibili e l'ODV si ottiene utilizzando il Java Security Manager con una politica di sicurezza configurata in maniera opportuna.

7.3.1.3 Java Security Manager

La configurazione valutata dell'ODV consente una sola modalità operativa, che ha un impatto sul modo in cui l'ODV è in grado di proteggersi dal comportamento di applicazioni o di altro codice non attendibile. Questa modalità utilizza il Java Security Manager fornito dalla Java Virtual Machine come parte dell'ambiente dell'ODV.

Il Java Security Manager viene utilizzato con una politica di sicurezza che protegge completamente l'esecuzione di JBoss EAP da qualsiasi applicazione o altro codice non attendibile (come il driver JDBC o non consentendo le riflessioni Java) utilizzando il *framework* JBoss EAP. Il Security Manager, con la sua *policy*, impedisce a qualsiasi applicazione di interferire in modo accidentale o intenzionale con il funzionamento di JBoss EAP.

Non è consentito disabilitare il Java Security Manager o indebolire la politica di sicurezza fornita assieme all'ODV, che lo protegge da qualsiasi applicazione o altro codice non attendibile.

7.3.2 Caratteristiche di sicurezza dell'ODV

7.3.2.1 Politica di sicurezza

La politica di sicurezza dell'ODV è espressa dall'insieme dei Requisiti Funzionali di Sicurezza (SFR) implementati dallo stesso. Essa copre i seguenti aspetti:

- **Audit**: l'ODV registra l'accesso degli utenti e degli amministratori al sistema sulla base della politica di audit. È possibile configurare sia il livello, sia i dettagli della funzionalità di audit.

- **Identificazione e autenticazione**: tutti gli utenti dell'ODV vengono identificati e autenticati in base ai database degli utenti gestiti dall'ODV. Per l'autenticazione vengono presi in considerazione i nomi utente, le credenziali di autenticazione e l'appartenenza ai gruppi.

- **Controllo di accesso**: l'accesso agli oggetti dell'ODV è protetto richiedendo l'identificazione e l'autenticazione degli utenti. Utenti autorizzati possono specificare quali utenti possono accedere a quali risorse. L'ODV supporta diversi tipi di criteri per il controllo di accesso.

- **Gestione basata sui ruoli**: l'ODV consente l'accesso alle risorse e alle operazioni di tipo amministrativo sulla base del ruolo assegnato all'utente. Utenti autorizzati possono specificare quali utenti possono accedere a quali risorse.

- **Coerenza dei dati**: il TSF garantisce la coerenza dei dati dell'utente e dei dati del TSF durante la loro elaborazione. La coerenza è garantita quando vengono elaborati dati che possono essere memorizzati all'interno di istanze dell'ODV.

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:

- I responsabili dell'amministrazione dell'ODV sono competenti e fidati, in grado di gestire l'ODV e la sicurezza delle informazioni in esso contenute.

- I responsabili dell'ODV devono garantire che il sistema operativo e la macchina virtuale Java siano installati e configurati in conformità con la guida dell'ODV e che questi meccanismi funzionino come specificato. Ciò implica che solo le macchine virtuali Java elencate nel Traguardo di Sicurezza [TDS] possono essere utilizzate come piattaforma sottostante per garantire la disponibilità di informazioni corrette sulla data e l'ora per la funzionalità di audit.

- I responsabili dell'ODV devono stabilire e attuare procedure per garantire che i componenti software dell'ODV siano distribuiti, installati, configurati e gestiti in modo sicuro.

- I responsabili dell'ODV devono garantire che le parti dell'ODV fondamentali per l'applicazione della politica di sicurezza, così come l'hardware e il software sottostanti, siano protette da attacchi fisici che possono compromettere gli obiettivi di sicurezza IT.

- I responsabili dell'ODV devono garantire che siano fornite procedure e/o meccanismi per assicurare il ripristino dell'operatività a seguito di errori di sistema o altre interruzioni senza che la sicurezza venga compromessa.

- I responsabili dell'ODV devono garantire che gli sviluppatori delle applicazioni eseguite dall'ODV siano affidabili e implementino le applicazioni in conformità con le linee guida fornite con l'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

Le funzionalità di sicurezza dell'ODV sono descritte in dettaglio nel capitolo 7.1 (TOE Security Functionality) del Traguardo di Sicurezza [TDS]. Di seguito sono riassunte le principali caratteristiche di sicurezza del prodotto che sono state oggetto di valutazione:

- **Controllo di accesso**: l'ODV è in grado di limitare l'accesso per i seguenti tipi di richiesta con i seguenti meccanismi di controllo di accesso:

- EJB: è possibile proteggere gli EJB e i nomi dei metodi associati evitando che possano essere richiamati dai soggetti.

- JMS: è possibile proteggere le destinazioni delle code di messaggi (*queue*) e dei *topic* JMS dall'accesso dei soggetti.

I protocolli di rete citati in precedenza effettuano il *tunneling* delle richieste del client verso l'ODV. Una volta che l'ODV ha eseguito identificazione, autenticazione e controllo di accesso, la richiesta viene inoltrata all'applicazione di destinazione. Poiché l'ODV utilizza unicamente le informazioni sulle credenziali fornite con la richiesta di rete, solo l'aspetto della comunicazione delle credenziali dell'utente, unitamente all'oggetto richiesto e al tipo di richiesta, è rilevante ai fini dell'applicazione della politica di controllo di accesso.
L'ODV consente la gestione indipendente della politica di controllo di accesso per ciascuna applicazione e per ciascuna politica. Gli amministratori autorizzati e gli sviluppatori di applicazioni possono utilizzare a tale scopo i descrittori di distribuzione e le annotazioni.

- **Controllo di accesso basato sui ruoli per le interfacce di gestione**: le interfacce di gestione di JBoss EAP, l'interfaccia a riga di comando e l'interfaccia di amministrazione basata sul Web consentono l'accesso alla configurazione di sistema per gestire tutti gli aspetti configurabili di JBoss EAP. Gli amministratori possono accedere agli aspetti generali del sistema, come le configurazioni delle porte di rete e la configurazione dei contenitori. Inoltre, è possibile gestire gli aspetti di configurazione per i servizi offerti dai contenitori.
  Gli aspetti di configurazione relativi alle singole applicazioni, come il controllo di accesso, vengono risolti mediante i descrittori di distribuzione forniti con l'applicazione. Pertanto, questo aspetto della configurazione non è accessibile tramite l'interfaccia di amministrazione.
  Le interfacce di amministrazione possono essere associate a una specifica interfaccia di rete. Ciò consente l'instaurazione di una LAN amministrativa che impedisce ad utenti non attendibili di accedere tecnicamente alle interfacce software. Affinché un amministratore possa interagire con le interfacce di amministrazione, deve prima effettuare il login. Gli account di amministratore vengono gestiti separatamente dagli altri account d'utente.
  Ogni azione che un utente amministratore può eseguire su un oggetto è soggetta a un meccanismo di controllo di accesso basato sui ruoli. Le azioni sono classificate in:

  - Operazioni sul modello: la funzione principale di queste operazioni è quella di leggere e scrivere dal modello di dati che copre diversi aspetti della configurazione, sebbene di conseguenza vengano spesso avviati o arrestati servizi di *runtime* associati.

  - Operazioni RPC: queste operazioni invocano alcuni servizi di *runtime* con effetto solo sul loro stato. È possibile leggere lo stato di *runtime* o modificarlo. Il modello non è influenzato da queste operazioni.

  Gli oggetti sono classificati in base a quanto segue:

  - una risorsa;

- un attributo residente in una risorsa.

Ad ogni ruolo di gestione viene associata una serie di funzionalità oggetto-azione. Questa mappatura definisce il livello di accesso consentito per ogni ruolo di gestione. L'ODV fornisce una serie di ruoli predefiniti disponibili dopo l'installazione. Un ruolo è un insieme denominato di permessi. Tali permessi includono dei vincoli (ad esempio, i permessi di lettura per il ruolo Monitor sono ristretti ad azioni e obiettivi non sensibili).

- **Funzionalità di audit**: l'ODV implementa un meccanismo di audit che consente di generare record di audit per eventi rilevanti per la sicurezza che riguardano il controllo di accesso. Un utente amministratore è in grado di selezionare gli eventi che devono essere sottoposti ad audit.
  La funzione di audit si basa sul meccanismo log4j integrato nellODV. Log4j ha tre componenti principali: *logger*, *appender* e *layout*. Questi tre tipi di componenti lavorano insieme per consentire agli sviluppatori di effettuare il *log* dei messaggi in base al tipo e al livello del messaggio, di controllare il modo in cui questi messaggi vengono formattati e dove vengono segnalati in fase di esecuzione.
  Le informazioni di audit vengono registrate in file di testo, che possono essere esaminati utilizzando gli strumenti messi a disposizione dal sistema operativo sottostante, come impaginatori o editor.

- **Clustering**: un cluster è un insieme di nodi. In un cluster JBoss EAP, un nodo è rappresentato da un'istanza del server JBoss EAP. Pertanto, per creare un cluster è necessario raggruppare diverse istanze di JBoss EAP (chiamate anche "partizioni").
  Il *clustering* consente l'esecuzione di applicazioni su più server paralleli (nodi del cluster). Con JBoss EAP sono realizzabili due diversi tipi di cluster: un cluster di *failover* e un cluster per la distribuzione del carico. In entrambi i casi, lo stato del server è distribuito su server diversi e, anche in caso di errore di uno dei server, l'applicazione rimane comunque accessibile tramite altri nodi del cluster.
  La comunicazione all'interno del cluster garantisce la coerenza tra i diversi nodi dei dati relativi alle seguenti informazioni:

  - Replica dello stato di un nodo che copre la replica di sessioni HTTP, *bean* di sessione EJB 3.0, *bean* di entità EJB 3.0 e oggetti di persistenza Hibernate (servizio di replica distribuito dello stato tramite Infinispan).

  - Replica dello stato di un nodo che copre la replica delle sessioni HTTP e dei *bean* di sessione EJB 2.x.

  - Replica delle code JMS.

- **Identificazione e autenticazione**: agli utenti vengono assegnati identificativi univoci che vengono utilizzati come base per le decisioni di controllo di accesso e di audit. L'ODV autentica l'identità asserita da un utente prima di consentirgli di eseguire qualsiasi ulteriore azione mediata dal TSF. L'ODV mantiene internamente l'identificativo associato al *thread* generato per l'utente dopo la corretta autenticazione.
  L'ODV fornisce diversi meccanismi di identificazione e autenticazione per i diversi tipi di richiesta:

- HTTP e servizi Web: autenticazione BASIC, FORM, DIGEST e CLIENT_CERT.
- EJB: autenticazione basata su nome utente e password, identificazione basata su certificato client.
- JMS: autenticazione basata su nome utente e password.

Per l'identificazione e l'autenticazione mediante un certificato client, l'ODV utilizza il canale TLS sottostante instaurato dall'ambiente operativo (JDK SSL o OpenSSL). Il protocollo TLS sottostante esegue la convalida del certificato del client. Il componente EJB dell'ODV richiede alla sessione TLS la parte DN del certificato per identificare l'utente. L'informazione DN viene utilizzata per definire la mappatura dei ruoli e per creare un'entità principale all'interno dell'ODV. L'ODV si basa quindi sull'implementazione del protocollo TLS dell'ambiente operativo per eseguire l'autenticazione mediante convalida del certificato client.
L'ODV consente la gestione delle autorizzazioni in maniera indipendente per ogni applicazione e servizio. Gli amministratori autorizzati e gli sviluppatori di applicazioni possono utilizzare a tale scopo i summenzionati descrittori di distribuzione e annotazioni.

- **Rollback delle transazioni**: JBoss EAP include un'implementazione interna alla VM di un gestore veloce di transazioni compatibile con le transazioni di JBoss, utilizzato come gestore di transazioni predefinito. Una transazione è definita come un'unità di lavoro contenente una o più operazioni che coinvolgono una o più risorse condivise aventi le proprietà ACID. ACID è acronimo di *Atomicity*, *Consistency*, *Isolation*, e *Durability* (Atomicità, Coerenza, Isolamento e Durabilità), che sono le quattro proprietà importanti delle transazioni. I significati di questi termini sono:
  - Atomicità: una transazione deve essere atomica. Ciò significa che devono essere eseguite tutte le operazioni previste nella transazione o non deve esserne eseguita nessuna. Non è ammesso effettuare solo una parte di una transazione.
  - Coerenza: quando una transazione è completata, il sistema deve trovarsi in una condizione stabile e coerente.
  - Isolamento: transazioni diverse devono essere isolate l'una dall'altra. Ciò significa che l'elaborazione parziale di una transazione non è visibile ad altre transazioni fino a quando la transazione non viene confermata mediante *commit* e che ogni processo in un sistema multiutente può essere programmato come se fosse l'unico processo che utilizza il sistema.
  - Durabilità: le modifiche apportate durante una transazione vengono rese persistenti al momento del *commit*. Una volta effettuato il *commit* di una transazione, le sue modifiche non andranno perse, anche in caso di un successivo blocco del server.

Nei sistemi di transazione ACID tradizionali, le transazioni sono di breve durata, le risorse (come i database) sono bloccate per la durata della transazione e i partecipanti hanno un alto grado di fiducia reciproca. Con l'avvento di Internet e dei

servizi Web, lo scenario che sta emergendo richiede il coinvolgimento in transazioni distribuite di partecipanti sconosciuti tra loro. JBoss Transactions offre supporto nativo per le transazioni in servizi Web, fornendo tutti i componenti necessari per creare con il minimo sforzo applicazioni basate su servizi Web che siano interoperabili, affidabili e multi-utente. Le interfacce di programmazione si basano sulle Java API for XML Transactioning (JAXTX) e il prodotto include il supporto dei protocollo per le specifiche WS-AtomicTransaction e WS-BusinessActivity.
JBoss EAP è progettato per supportare protocolli di coordinamento multipli. JBoss EAP supporta transazioni sia locali, sia distribuite. Una transazione è considerata distribuita se si estende su più istanze di processo, ovvero macchine virtuali (VM). In genere una transazione distribuita contiene partecipanti posizionati all'interno di diverse VM, ma viene coordinata in una VM separata (o corrispondente ad uno dei partecipanti). Se la distribuzione richiede transazioni distribuite, è possibile utilizzare il componente per le transazioni dei servizi Web, che utilizza SOAP/HTTP.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto viene fornita al cliente finale insieme al prodotto. Questa documentazione contiene le informazioni richieste per l'installazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguiti gli ulteriori obblighi o note per l'utilizzo sicuro dell'ODV contenuti nel capitolo 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] ed includono tutti i requisiti del pacchetto EAL4 con l'aggiunta di ALC_FLR.3.

Tutti i Requisiti Funzionali (SFR) sono stati derivati direttamente o per estensione dai CC Parte 2 [CC2]. In particolare, il Traguardo di Sicurezza [TDS] include il componente esteso FDP_ROL.2-jb, che descrive la possibilità per l'ODV di eseguire un *rollback* automatico di tutte le operazioni che formano una transazione quando almeno una delle operazioni che fanno parte della transazione fallisce. Per una descrizione dettagliata delle proprietà dei componenti estesi, consultare il cap. 5 del Traguardo di Sicurezza [TDS].

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, i Requisiti Funzionali di Sicurezza (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 17 ottobre 2019 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [ETR] che è stato approvato dall'Organismo di Certificazione il 29 ottobre 2019. 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 [ETR] 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 "JBoss Enterprise Application Platform 7 Version 7.2.3" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4, 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 EAL4, 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
Complete functional specification	ADV_FSP.4	Positivo
Implementation representation of the TSF	ADV_IMP.1	Positivo
Basic modular design	ADV_TDS.3	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
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
Systematic flaw remediation	*ALC_FLR.3*	Positivo
Tests	**Classe ATE**	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
Vulnerability assessment	**Classe AVA**	Positivo
Focused vulnerability analysis	AVA_VAN.3	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 "JBoss Enterprise Application Platform 7 Version 7.2.3" 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 all'ambiente di sicurezza specificato nel capitolo 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 ([CCGUIDE]).

Si assume che l'ODV funzioni in modo sicuro qualora vengano rispettate le ipotesi sull'ambiente operativo descritte nel cap. 3.2 del Traguardo di Sicurezza [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 negligenti.

Occorre inoltre notare che la sicurezza dell'operatività dell'ODV è condizionata al corretto funzionamento delle piattaforme software e 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 Traguardo di Sicurezza [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 ed è accompagnato dalla documentazione di guida. L'ODV è costituito da componenti distribuiti sotto forma di pacchetti RPM, che vengono compilati per facilità d'uso in un'immagine ISO o resi disponibili come archivio in formato ZIP sul Red Hat Customer Portal.

In Tabella 3 sono elencati gli elementi che comprendono i diversi componenti dell'ODV, inclusi il software e le guide.

N.	Tipo	Identificativo	Release	Metodo di consegna
1	SW	JBoss ZIP Archive	7.2.3	Formato elettronico
2	SW	JBoss ISO Image	7.2.3	Formato elettronico
3	DOC	JBoss Enterprise Application Platform 7.2.3 Common Criteria 7.2.3 Configuration Guide [CCGUIDE]	7.2.3	Formato elettronico
4	DOC	Installation Guide Red Hat JBoss Enterprise Application Platform 7.2 Getting Started Guide Red Hat JBoss Enterprise Application Platform 7.2 Security Architecture Red Hat JBoss Enterprise Application Platform 7.2 How to Configure Server Security Red Hat JBoss Enterprise Application Platform 7.2 How to Configure Identity Management Red Hat JBoss Enterprise Application Platform 7.2 Configuring Messaging Red Hat JBoss Enterprise Application Platform 7.2 Development Guide Red Hat JBoss Enterprise Application Platform 7.2 Developing EJB Applications Red Hat JBoss Enterprise Application Platform 7.2 Developing Web Services Applications GA Public API JavaDocs Red Hat JBoss Enterprise Application Platform 7.2 Management CLI Guide	7.2	Formato elettronico

Tabella 3 - Materiali consegnabili dell'ODV

Lo Sviluppatore ha indicato che la distinzione tra i due metodi di consegna (ISO o ZIP) dipende semplicemente dal sistema operativo scelto dal cliente. In altre parole, i clienti che

utilizzano Red Hat Enterprise Linux (con abbonamento JBoss EAP) possono scegliere il metodo RPM, mentre i clienti che utilizzano un'altra piattaforma (ad es., Microsoft Windows) devono selezionare il metodo con archivio ZIP.

Il processo di rilascio dello Sviluppatore definisce le responsabilità dei diversi reparti all'interno della Red Hat Network come segue:

- Il reparto Release Engineering gestisce gli strumenti CM e realizza l'infrastruttura per l'assemblaggio dei materiali consegnabili del prodotto.
- Il reparto Quality Engineering valuta e garantisce la qualità del prodotto.
- Il reparto Security Response Team esamina, identifica e tiene sotto controllo le parti del prodotto suscettibili di "vulnerabilità di sicurezza".
- Il reparto Program Management consulta gli altri due reparti in merito ai preparativi per il rilascio del prodotto e prende la decisione finale del rilascio.

Il processo di assemblaggio del prodotto è definito come segue:

1. Il reparto Release Engineering assembla i componenti di distribuzione del prodotto in un "ambiente di realizzazione controllato che viene attentamente monitorato per evitare la contaminazione di codice esterno".
2. Il reparto Release Engineering firma i componenti RPM con le chiavi private GPG (GNU Privacy Guard) di Red Hat. La chiave pubblica corrispondente è disponibile sia su redhat.com, sia sul server di chiavi pubbliche pgp.mit.edu.
3. Le attività fondamentali di assicurazione qualità vengono svolte su una versione dei componenti candidata per il rilascio e includono l'installazione e i test funzionali su tutte le piattaforme supportate e il controllo dell'apposizione delle firme digitali.
4. Il gruppo di Quality Engineering notifica ai gruppi di Product Management e Release Engineering (via Email o alle riunioni di Program Management) che il prodotto è pronto per la distribuzione.
5. Il reparto Release Engineering prepara quindi i componenti per la distribuzione ai clienti, inclusa la generazione di *checksum* SHA-256 per tutti i file, la registrazione di tali *checksum* su un sistema sicuro (gestito dal reparto Release Engineering) e infine il trasferimento dei componenti tramite SSH ai centri di distribuzione di Red Hat, dove i clienti possono scaricarli tramite i canali di distribuzione CP o RHN.

I server di distribuzione di Red Hat si trovano in diverse strutture sicure di terze parti e sono accessibili solo al personale Red Hat e agli appaltatori autorizzati che hanno stipulato adeguati accordi con Red Hat e che vengono in genere scortati dal personale Red Hat.

9.2 Identificazione dell'ODV

Le copertine di ogni documento di guida mostrano come numero di versione dell'ODV 7.2. Nell'area di download del Red Hat Customer Portal, la versione di JBoss EAP 7.2.3 può anche essere indicata come 7.2 CP03, in quanto entrambi i riferimenti sono equivalenti.

Quando l'ODV viene eseguito, il *log* del server mostra le seguenti informazioni:

```
INFO [org.jboss.as] (MSC service thread 1-2) WFLYSRV0049: JBoss EAP
7.2.3.GA (WildFly Core 6.0.15.Final-redhat-00001)

INFO [org.wildfly.security] (ServerService Thread Pool -- 27)
ELY00001: WildFly Elytron version 1.6.3.Final-redhat-00001
```

La Common Criteria Configuration Guide di JBoss EAP [CCGUIDE], nella sezione "Confirming the Version of your JBoss Enterprise Application Platform Installation", fornisce tre modalità per verificare il numero di versione dell'ODV installato.

9.3 Installazione, inizializzazione ed utilizzo sicuro dell'ODV

L'installazione e la configurazione dell'ODV debbono essere effettuate seguendo le istruzioni contenute nelle apposite sezioni della documentazione di guida fornita al cliente con il prodotto, elencata ai punti 3 e 4 di Tabella 3.

In particolare, la Common Criteria Configuration Guide di JBoss EAP [CCGUIDE] contiene informazioni per l'inizializzazione sicura dell'ODV e la preparazione del suo ambiente operativo in conformità con gli obiettivi di sicurezza specificati nel Traguardo di Sicurezza [TDS].

10 Appendice B – Configurazione valutata

L'ODV è il prodotto Red Hat JBoss Enterprise Application Platform (EAP) versione 7.2.3. L'ODV è composto unicamente da software ed è accompagnato dalla documentazione di guida. Gli elementi elencati in Tabella 3 costituiscono l'ODV.

La configurazione valutata è descritta nella Common Criteria Configuration Guide di JBoss EAP [CCGUIDE]. Questo documento specifica una serie di vincoli. La descrizione include le seguenti informazioni:

- database SQL utilizzabili e driver JDBC applicabili;
- combinazione di JDK consentiti e sistemi operativi da utilizzare;
- restrizioni sulla configurazione di Elytron e riferimenti agli archivi di credenziali utente consentiti;
- configurazione della funzionalità di audit per soddisfare i requisiti specificati nel Traguardo di Sicurezza [TDS].

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 l'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

L'attività di test dell'ODV è stata ripetuta diverse volte con diversi vincoli di configurazione.

Lo Sviluppatore ha tenuto conto dei seguenti vincoli:

- i test sono stati eseguiti con il Java Security Manager abilitato e con una politica ben definita;
- i test sono stati eseguiti su tutti i JDK specificati nel TDS;
- i test hanno coperto tutti gli archivi di dati di account utente consentiti nel TDS;
- sono stati utilizzati come *back end* tutti i diversi database elencati nel TDS;
- sono stati testati gli archivi dei dati d'utente relativi ad LDAP, i database e i file delle proprietà.

L'attività di test è stata eseguita sulla versione dell'ODV specificata in [CCGUIDE] e [TDS]. Inoltre, gli ambienti e le piattaforme di test sono stati predisposti per essere conformi ai requisiti della configurazione valutata, come descritta in [CCGUIDE] e in [TDS]. Pertanto, le configurazioni di test soddisfano i requisiti per la configurazione valutata.

Nella fase di predisposizione dei test indipendenti, i Valutatori hanno installato l'ODV utilizzando la guida [CCGUIDE] e la documentazione di installazione del prodotto. I casi di test sono stati preparati come descritto nel piano di test dello Sviluppatore.

I Valutatori hanno verificato che il sistema di test utilizzato per la ripetizione dei test dello Sviluppatore comprendeva i seguenti elementi:

- JRE: OpenJDK
- OS: RHEL 7
- DB: MariaDB 10.1
- LDAP: Active Directory 2016

I Valutatori hanno verificato che il sistema di test utilizzato per l'esecuzione dei test indipendenti comprendeva i seguenti elementi:

- JRE: Oracle JDK 1.8
- OS: Windows Server 2016
- DB: MariaDB 10.1
- LDAP: Active Directory 2016

11.2 Test funzionali svolti dal Fornitore

11.2.1 Approccio adottato per i test

Il documento di mappatura dei test fornito dallo Sviluppatore elenca l'albero delle suite di test che comprendono i casi di test che a loro volta comprendono le unità di test. Questo documento di mappatura consente anche di risalire da una singola unità di test alle interfacce coperte dall'unità di test.

I test resi disponibili dallo Sviluppatore sono scritti in Java e sono completamente automatizzati.

I Valutatori riferiscono che questi casi di test sono sviluppati a monte insieme al codice sorgente di JBoss EAP. I test includono applicazioni caricate sull'ODV e programmi utente che tentano di accedere alle applicazioni interfacciandosi con l'ODV.

I casi di test contengono informazioni sui comportamenti desiderati e previsti e danno risultato positivo se l'ODV agisce conformemente a tali comportamenti. Se l'ODV si comporta come previsto, viene restituito alla piattaforma di test il risultato "pass", altrimenti viene restituito un errore. La piattaforma di test registra e raccoglie i risultati dei test e li presenta in formato leggibile come file HTML.

11.2.2 Copertura dei test

La mappatura dei casi di test identifica le interfacce coperte dai singoli test. I test coprono i seguenti tipi di TSFI:

- Le configurazioni dei protocolli di rete su cui si basano le funzionalità di controllo di accesso, identificazione e autenticazione.
- Annotazioni del codice sorgente per la configurazione della funzionalità di controllo di accesso.
- File di configurazione e descrittori di distribuzione relativi alla configurazione delle funzionalità di identificazione, autenticazione e controllo di accesso. Il supporto alle transazioni viene testato utilizzando i descrittori di distribuzione.
- L'interfaccia a riga di comando viene coperta indirettamente avviando l'ODV in due diverse modalità operative, che possono essere applicate unicamente mediante specifiche opzioni da riga di comando.

Gli stessi test previsti a copertura delle TSFI forniscono anche la necessaria profondità di test, ovvero la copertura di tutti i sottosistemi che implementano funzionalità SFR-*enforcing*. Il documento di mappatura dei test associa i casi di test ai sottosistemi coinvolti. L'analisi della profondità dei test mostra che i casi di test non riguardano solo i sottosistemi che vengono invocati direttamente, ma anche i sottosistemi che possono essere attivati solo indirettamente, come Elytron.

11.2.3 Risultati dei test

I risultati dei test dello Sviluppatore sono stati generati sulle piattaforme JDK e le configurazioni elencate nel cap. 11.1. Come descritto nell'approccio per i test, i risultati di tutti questi test automatizzati vengono registrati e raccolti dalla piattaforma e memorizzati in file HTML e file di *log* di Jenkins.

I risultati ottenuti dai test hanno mostrato piena conformità ai risultati previsti su tutte le configurazioni testate.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

L'attività di test dei Valutatori è stata suddivisa in due parti: osservazione dell'esecuzione dei test dello Sviluppatore ed esecuzione dei test ideati dai Valutatori.

Il sistema di test è stato installato e configurato come indicato nel cap. 11.1. Durante la fase di esecuzione dei test dello Sviluppatore, i Valutatori hanno utilizzato il piano di test fornito dallo Sviluppatore per impostare e avviare i test inclusi nelle specifiche configurazioni degli scenari di test già eseguiti dallo Sviluppatore. Tutti i test sono stati eseguiti con successo e i risultati dei test sono stati registrati in un file.

Oltre a ripetere tutti i test dello Sviluppatore, i Valutatori hanno ideato test specifici per un sottoinsieme delle funzionalità dell'ODV.

I test sono stati selezionati dai Valutatori sulla base delle seguenti motivazioni:

- Nella configurazione valutata è previsto un file di *audit trail* aggiuntivo nella configurazione della funzionalità di audit.
- I test dello Sviluppatore invocano un gran numero di interfacce diverse.
- I test dello Sviluppatore coprono diverse funzioni di controllo di accesso.
- Poiché i casi di test predisposti dallo Sviluppatore coprono già le funzioni principali dell'ODV con un gran numero di test, i Valutatori si sono concentrati su funzionalità di sicurezza secondarie che sono state coperte in misura minore dai test dello Sviluppatore.
- I test sull'ODV non hanno coperto la tipologia di accesso HTTP HEAD nella verifica della corretta applicazione del controllo di accesso per le connessioni HTTP.

I Valutatori hanno creato i propri casi di test espandendo gli aspetti funzionali dell'audit e del controllo di accesso su connessioni HTTP. Attraverso l'esame dei casi di test dello Sviluppatore, i Valutatori hanno acquisito sufficiente evidenza dell'impegno dello Sviluppatore nei test. I test dello Sviluppatore hanno mostrato una copertura molto ampia

del TSF, pertanto i valutatori hanno deciso di predisporre solo un numero limitato di casi di test.

I test indipendenti ideati dai Valutatori hanno riguardato le seguenti aree funzionali:

- Funzionalità di audit: sono stati eseguiti diversi test su diverse aree funzionali dell'ODV per verificare che vengano creati e conservati i record di audit appropriati per le diverse richieste di accesso.

- Controllo di accesso su connessioni HTTP: i Valutatori hanno verificato la corretta applicazione della politica di controllo di accesso nel caso di richieste di tipo HTTP HEAD.

Tutti i test hanno avuto esito positivo.

11.4 Analisi delle vulnerabilità e test di intrusione

11.4.1 Approccio adottato per i test

In una prima fase, i Valutatori hanno svolto ricerche su fonti pubbliche allo scopo di individuare vulnerabilità note del server JBoss in generale e dell'ODV in particolare. Per ogni potenziale vulnerabilità rilevata, I Valutatori hanno considerato quanto segue:

- Se la vulnerabilità avesse o meno un impatto sulla configurazione valutata dell'ODV nell'ambiente operativo previsto. In caso affermativo, i valutatori hanno eseguito un'analisi di vulnerabilità.

- Se la vulnerabilità fosse o meno già stata risolta nella configurazione valutata dell'ODV. Nel caso in cui non fosse stato introdotto un *fix* per la vulnerabilità rilevata, i Valutatori ne hanno analizzato il potenziale impatto e la sfruttabilità.

Oltre alle vulnerabilità reperibili da fonti di pubblico dominio, i Valutatori hanno verificato la presenza di altre potenziali vulnerabilità segnalate all'interno di altri rapporti di valutazione. Per ognuna di tali ipotetiche vulnerabilità, i Valutatori hanno escogitato un metodo per verificarne la presenza o l'assenza, tenendo conto del fatto che l'ODV è un prodotto Open Source e quindi i Valutatori avevano pieno accesso al codice sorgente.

Sulla base dell'analisi della vulnerabilità, i Valutatori hanno effettuato test sulle seguenti aree di interesse:

- Verifica dell'efficacia del controllo di accesso per il tipo di richiesta HTTP HEAD, poco noto e raramente utilizzato.

- Verifica che i componenti condivisi che memorizzano dati sensibili non siano soggetti a perdite di informazioni.

11.4.2 Copertura dei test

Sebbene i Valutatori abbiano deciso di effettuare solo un numero limitato di test di intrusione, per alcune delle potenziali vulnerabilità identificate i Valutatori hanno eseguito

un'analisi molto ampia, superiore ai requisiti del livello di garanzia EAL4 dichiarato per l'ODV. Le motivazioni di questa scelta sono le seguenti:

- Essendo un prodotto open source, l'ODV è già soggetto a verifica per la presenza di vulnerabilità evidenti da parte della comunità Open Source. Tuttavia, questa circostanza non può essere considerata una garanzia dell'assenza di vulnerabilità.

- Essendo un prodotto open source, l'ODV viene consegnato con il codice sorgente completo, cosa che offre l'opportunità ai Valutatori di eseguire un'analisi approfondita, solitamente considerata inconcepibile per i prodotti valutati al livello di garanzia EAL4. In generale, i Valutatori hanno considerato che la revisione del codice sorgente fosse un metodo più efficace per l'analisi delle vulnerabilità rispetto ai test. A causa della natura delle vulnerabilità, un'ipotetica vulnerabilità è di solito oscura nella realtà e pertanto può essere sfruttata solo in presenza di determinate condizioni. I test potrebbero non coprire tutti le condizioni necessarie (poiché alcune di queste non sono completamente definite o note ai tester). Di conseguenza, un test che non rilevi la presenza di alcuna vulnerabilità non dimostra necessariamente che non ve ne siano.

11.4.3 Risultati dei test

I Valutatori hanno eseguito tutti i test di intrusione su un'istanza dell'ODV installata e configurata secondo la Common Criteria Configuration Guide di JBoss EAP [CCGUIDE].

I test di intrusione hanno riguardato le seguenti proprietà di sicurezza:

- Inaggirabilità delle funzioni di sicurezza dell'ODV.

Non è stata rilevata alcuna vulnerabilità sfruttabile nell'ambiente operativo dell'ODV da attaccanti con un potenziale di attacco previsto non superiore a Enhanced-Basic.

Non sono state identificate vulnerabilità residue.