REF: 2015-12-INF-2167 v1	Created by: CERT10
Target: Expediente	Revised by: CALIDAD
Date: 15.12.2017	Approved by: TECNICO

CERTIFICATION REPORT

File: 2015-12 HP OpsBridge

Applicant: HP Hewlett-Packard development Company

References:

[EXT-2782] Certification request of HP OpsBridge

[EXT-3674] Evaluation Technical Report of HP OpsBridge.

The product documentation referenced in the above documents.

Certification report of the product **HPE Operations Bridge Premium v2016.05 including: HPE Operations Manager i v10.11 Build 016.001.63210 Hotfix: QCCR8D53202_1011, HPE Operations Agent v12.01 Build 020 and HPE Operations Bridge Reporter v10.01 Build 953.00001** as requested in [EXT-2782] dated 24/07/2015, and evaluated by the laboratory Epoche & Espri S.L.U, as detailed in the Evaluation Technical Report [EXT-3674] received on 17/11/2017.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product “HPE Operations Bridge Premium v2016.05 including: HPE Operations Manager i v10.11 Build 016.001.63210 Hotfix: QCCR8D53202_1011, HPE Operations Agent v12.01 Build 020 and HPE Operations Bridge Reporter v10.01 Build 953.00001”.

HPE Operations Bridge Premium, also referred to as “HPE OpsBridge”, is an IT event correlation and management software product. The HPE OpsBridge software includes the following components:

- HPE Operations Manager i (OMi)
- HPE Operations Agent (OA)
- HPE Operations Bridge Reporter (OBR)

The HPE OA is responsible for collecting event data from monitored systems. HPE OMi is responsible for receiving the event data and performing event data processing, automation and correlation. HPE OBR is a cross domain performance reporting tool.

Developer/manufacturer: Hewlett Packard Enterprise Development LP

Sponsor: Hewlett Packard Enterprise Development LP

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Epoche & Espri S.L.U.

Protection Profile: None

Evaluation Level: Common Criteria v3.1 R4 EAL2+ALC_FLR.2

Evaluation end date: 17/11/2017.

All the assurance components required by the evaluation level of the [CC_P3] have been assigned a “PASS” verdict. Consequently, the laboratory Epoche & Espri S.L.U assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL2 + ALC_FLR.2 assurance level packages, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4. Considering the obtained evidences during the instruction of the certification request of the product “HPE Operations Bridge Premium v2016.05 including: HPE Operations Manager i v10.11 Build 016.001.63210 Hotfix: QCCR8D53202_1011, HPE Operations Agent v12.01 Build 020 and HPE Operations Bridge Reporter v10.01 Build 953.00001”, a positive resolution is proposed.

TOE summary

The TOE is an IT event correlation and management software suite that includes the following HPE OpsBridge components:

- HPE OMi Software
- HPE OA Software
- HPE OBR Software

HPE OMi 10.11

HPE OMi is the central component of the HPE OpsBridge product. HPE OMi receives events and topology information from HPE OA and processes, correlates, and analyzes events to identify service conditions. HPE OMi provides the following security features:

- Generates audit records for security relevant events (which can only be reviewed by authorized users)
- Provides automatic failover services to ensure the secure state and continued operations of the TOE
- Distributes certificates to HP OAs for the secure transmission of configuration and event data
- Enforces TOE user access control and provides a login banner warning against unauthorised use of the TOE
- Provides cryptographic support to protect event data from disclosure or modification when transferred internally between TOE components
- Provides cryptographic support to secure trusted paths and channels between itself and user workstations and external servers

HPE OA 12.01

HPE OA is responsible for collecting event data from monitored systems and consists of the Operations Monitoring Component and the Performance Collection Component. The Operations Monitoring Component builds up the monitoring and messaging capabilities of HPE OA and the Performance Collection Component provides the data collection and storage functionality. These components provide security management CLI tools that aid in the enforcement of the data collection and analysis functionality of the TOE. The HPE OA also utilizes cryptographic support to ensure that event data is protected when transmitted between TOE components.

The Operations Monitoring Component includes the following sub-components:

- Monitor Agent
- Action Agent
- Message Agent
- Trap Interceptor
- WMI Interceptor
- Message Interceptor
- Logfile Encapsulator
- Event Correlation Agent1.4.2 HPE OA 12.01
- Embedded Performance Component

HPE OBR v10.01

HPE OBR processes event and topology information from HPE OMi and the HPE OA and displays them in reports. HPE OBR is a historical infrastructure reporting tool that displays high level cross-domain reports and detailed domain level reports. Domains include the server, network and application environments from which HPE OBR collects data. Cross-domain reports display data from related domains to give a broad picture of the health and performance of an IT infrastructure. HPE OBR reports can be used to analyze patterns in the IT environment, forecast IT resource performance based on historical data, and perform a custom analysis of the data using report filters.

HPE OBR reports are available in content packs. Content packs contain the rules that define how the performance metrics will be collected, transformed, and aggregated in the reports. A typical content pack defines the metrics for a specific domain along with the necessary rules for analysis required in that domain.

HPE OBR provides cryptographic support to ensure that event data is protected from disclosure or modification when transmitted between TOE components and to secure trusted path and channels between itself and user workstations and external servers.

HPE OBR provides the web-based HPE OBR Admin console and OBR CLI for configuration and management of the platform and installed content packs. The HPE OBR Admin console provides security management tasks, enforces authentication mechanisms, and presents a login banner warning against unauthorised use of the TOE.

The OBR CLI utilizes the following tools and services for security management tasks:

- Create Vertica Database Tool

- Configure Poller Tool
- OBR Full Restore Tool
- OBR Backup Tool
- License Manager Tool
- Dimension Manager Tool
- Downtime Utility Tool
- Admin Server Client Auth Tool

TOE major security features

The major security features implemented by the TOE and subject to evaluation can be summarised as follows:

- Security Audit
- Communication
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Resource Utilization
- TOE Access
- Trusted Path/Channels
- Data Collection and Analysis

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidences required to fulfil the assurance packages of EAL2 + ALC_FLR.2, according to Common Criteria v3.1 R4.

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

In addition, as for the augmentation defined, the ALC_FLR.2 assurance component is also included in the evaluation.

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R4:

Class	Component
Security Audit (FAU)	Audit data generation (FAU_GEN.1)
	Audit review (FAU_SAR.1)
	Guarantees of audit data availability (FAU_STG.2)
Communication (FCO)	Selective proof of origin (FCO_NRO.1)
Cryptographic Support (FCS)	Cryptographic key generation (FCS_CKM.1)
	Cryptographic key destruction (FCS_CKM.4)
	Cryptographic operation (FCS_COP.1)
User Data Protection (FDP)	Subset access control (FDP_ACC.1)
	Security attribute based access control (FDP_ACF.1)
	Export of user data without security attributes (FDP_ETC.1)
Identification & Authentication (FIA)	User authentication before any action (FIA_UAU.2)
	Multiple authentication mechanisms (FIA_UAU.5)
	User identification before any action (FIA_UID.2)

Security Management (FMT)	Management of security functions behaviour (FMT_MOF.1)
	Management of security attributes (FMT_MSA.1)
	Static attribute initialisation (FMT_MSA.3)
	Specification of management functions (FMT_SMF.1)
	Security roles (FMT_SMR.1)
Protection of the TSF (FPT)	Failure with preservation of secure state (FPT_FLS.1)
	Basic internal TSF data transfer protection (FPT_ITT.1)
Resource Utilization (FRU)	Degraded fault tolerance (FRU_FLT.1)
TOE Access (FTA)	Default TOE access banners (FTA_TAB.1)
Trusted Path/Channels (FTP)	Trusted channel (FTP_ITC.1)
	Trusted path (FTP_TRP.1)

Extended components

Class	Component
Data Collection and Analysis (FDC)	System scan (FDC_SCN.1)
	System analysis (FDC_ANA.1)
	Scanned data storage (FDC_STG.1)

IDENTIFICATION

Product: HPE Operations Bridge Premium v2016.05 including: HPE Operations Manager i v10.11 Build 016.001.63210 Hotfix: QCCR8D53202_1011, HPE Operations Agent v12.01 Build 020 and HPE Operations Bridge Reporter v10.01 Build 953.00001

Security Target: Hewlett Packard Enterprise Development LP HPE Operations Bridge Premium v2016.05 including HPE Operations Manager i v10.11, HPE Operations Agent v12.01, and HPE Operations Bridge Reporter v10.01 Security Target, v1.2, November 2017

Protection Profile: None

Evaluation Level: Common Criteria v3.1 R4: assurance packages EAL2 + ALC_FLR.2

SECURITY POLICIES

There are no Organizational Security Policies defined for this evaluation.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions included in the [ST], are constraints to the conditions used to assure the security properties and functionalities compiled by the security

target [ST]. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

Assumptions	Description
A. AUTH	The TOE environment will provide the identification and authentication repository of users attempting to manage and use the TOE.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains. Administrators of the TOE are assumed to be appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner.
A.LOCATE	The TOE, and all components of the TOE environment, including the authentication servers and database servers are located within a controlled access facility and appropriately located within the network to perform their functions. The devices with which the TOE communicates for exporting events are also located within a controlled access facility. Administrative and user workstations are located within a separate controlled access facility.
A.OS_ACCESS	The TOE environment is in a secure state and provides a sufficient level of protection to itself and the TOE components.
A.PROTECT	The TOE software will be protected from unauthorised modification.
A.NOEVIL	The administrators and users of the TOE are non-hostile, appropriately trained, and follow all guidance.
A.SECURE_COM	The TOE environment provides the necessary network infrastructure required for its operation and ensures the TOE is secured and protected from interference or tampering by using a firewall to prevent access from non-trusted entities. Additionally, the TOE environment provides a sufficient level of protection to secure communications between the TOE and network-attached devices within the secure access facility.
A.TIMESTAMP	The TOE environment provides the TOE with the necessary reliable timestamps.
A.ADMIN_PROTECT	The workstations in the TOE environment used to access the TOE are free of malicious software.

THREATS

The following threats do not suppose a risk for the certified product, although the agents implementing attacks have the attack potential according to the basic attack potential of EAL2 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are categorized below.

Threat Name	Threat Definition
T.DATA_AVAILABILITY	TOE data or capabilities may become unavailable due to DP server failures caused by an attacker who is not a TOE user (e.g. performing a denial of service attack), or an operational condition (power failures, etc.).
T.ADMIN_ERROR	A TOE user may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.AUDIT_COMPROMISE	An attacker who is not a TOE user may view audit records cause audit records to be lost or modified, or prevent future records from being recorded, thus masking an attacker who is not a TOE user's actions.
T.BAD_STATE	An attacker who is not a TOE user may exploit vulnerabilities in monitored IT entities that reach an insecure state without the network administrators becoming aware.
T.DATA_COMPROMISE	An attacker who is not a TOE user may read, modify, delay, or destroy security critical TOE configuration data stored on the TOE or being transmitted between physically separated parts of the TOE.
T.UNAUTHORISED_ACCESS	A TOE user may gain unauthorised access (view, modify, delete) to user data through possible misuse.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem. The security objectives declared for the TOE operational environment in the [ST] are categorized below.

IT Security Objectives

IT Security Objectives Name	Description
OE.TIMESTAMP	The TOE environment must provide reliable timestamps to the TOE.
OE.NET_CON	The TOE environment must be implemented such that the TOE is appropriately located within and connected to the network to perform its intended function.
OE.AUTH	The TOE environment must provide the authentication and identification repository of users attempting to use the TOE.
OE.OS_ACCESS	The operating system upon which the TOE is installed provides a sufficient level of protection for itself and the TOE software it contains.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference and tampering.
OE.SECURE_COM	The TOE environment must provide mechanisms to secure communications between TOE components and other devices to which the TOE is attached (including routers, switches, cabling, connectors, and firewalls) and must be properly implemented such that the TOE is secured and protected from interference or tampering. Firewalls must be configured to restrict all external access from outside the internal network where the TOE is accessible.
OE.ADMIN_PROTECT	The administrative and user workstations must be protected from any external interference and tampering by having all security updates and anti-malware software installed.

Non-IT Security Objectives

Non-IT Security Objectives Name	Description
OE.MANAGE	The TOE environment will provide competent, non-hostile administrators and users of the TOE who are appropriately trained and follow all administrator and user guidance. Administrators of the TOE will ensure the system is used securely.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

ARCHITECTURE

LOGICAL ARCHITECTURE

Logical boundaries

Conceptually the TOE can be thought of as a collection of the following security services which the security target describes with increasing detail:

Security Audit

The Security Audit functionality provides the capability to generate audit data for HPE OMi security relevant events and records the identity of the subject responsible for initiating the event. TOE users or administrators with sufficient audit log permissions have access to view the audit logs. The TOE prevents any unauthorised deletion and modification of the audit logs.

Communication

The Communication functionality ensures that HPE OMi servers distribute certificates to HPE OAs for the secure transmission of configuration and event data. Signatures are applied to configuration payloads sent between the HPE OMi GW server and HPE OAs.

Cryptographic Support

The Cryptographic Support functionality utilizes the FIPS-validated RSA BSAFE® Crypto-J Module (software version 6.2.1) for Java based components of HPE OMi and the OpenSSL FIPS Object Module (software version 2.0.12) for C++ based components of HPE OMi. These FIPS-validated modules are used by the HPE OMi TOE component to perform all cryptographic functions.

HPE OBR also utilizes the FIPS-validated RSA BSAFE® Crypto-J Module (software version 6.2.1) and the OpenSSL FIPS Object Module (software version 2.0.12). The TOE destroys all keys according to the FIPS 140-2 standard (by overwriting with zeroes).

User Data Protection

The User Data Protection functionality enforces the Resource Access Control SFP for controlling the access of HPE OMi users to resources. The Resource Access Control SFP is also enforced when exporting event data from HPE OMi servers to targeted systems.

Identification and Authentication

The Identification and Authentication functionality requires TOE users and administrators to be identified and authenticated before gaining access to any TOE functionality. The TOE utilizes LDAP and X.509 certificate-based remote authentication.

Security Management

The Security Management functionality provides the capability for administrators with authorized roles to manage the security functionality, TSF data, and attributes provided by the TOE. HPE OMi provides the Super-Admin role and custom roles.

Protection of the TSF
The Protection of the TSF functionality ensures that the TOE maintains a secure state in the event of an HPE OMi DP server failure. The TOE also ensures that event data is protected from disclosure or modification when transferred internally between TOE components.

Resource Utilization
The Resource Utilization functionality provides the capability for the TOE to perform automatic failover procedures to ensure that all capabilities of the TOE are still operational in the event of an HPE OMi DP server failure.

TOE Access
The TOE Access functionality ensures that an advisory TOE access banner is displayed on the HPE OMi Web UI and HPE and OBR Admin console warning the TOE user or administrator against unauthorised access.

Trusted Path/Channels
The Trusted Path/Channels functionality provides Inter-TSF trusted channels for LDAP authentication via LDAP/S connections, HPE OMi external database communications via JDBC over TLS, and HPE OBR external database communications via JDBC over TLS. This functionality also provides a trusted path for HTTPS connections from TOE user or administrator workstations to the HPE OMi Web UI and HPE OBR Admin console interface.

Data Collection and Analysis
The Data Collection and Analysis functionality provides the capability for the TOE to monitor systems and gather event data. After the event data is gathered, the TOE performs an analysis of the event data to discover potential security violations. Event data is stored in an embedded or external database and the TOE does not allow deletion or modification of event data by unauthorised TOE users.

PHYSICAL ARCHITECTURE

Physical boundaries

The software-only TOE is a distributed system composed of the HPE OMi, OA, and OBR software. The HPE OMi software includes the GW and DP server components and the Management packs. The HPE OBR software includes the OBR Server, OBR Remote Collector, and Content packs.

The TOE is packaged along with the electronic documentation (PDF format) as an ISO-9660 image for HPE OBR, and as multiple .zip files for HPE OMi. The HPE OA software binary is available as part of the HPE OMi package and as a separate ISO image.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

The following TOE guidance documents are also available on the HPE Software Support website (https://softwaresupport.HPE.com/) for registered customers to download.

HPE Operations Manager i; Software Version: 10.11; OMi Administration Guide; Document Release Date: 25 May 2016; Software Release Date: May 2016
HPE Operations Manager i; Software Version: 10.11; OMi User Guide; Document Release Date: 25 May 2016; Software Release Date: May 2016
HPE Operations Manager i; Software Version: 10.11; OMi Extensibility Guide; Document Release Date: 25 May 2016; Software Release Date: May 2016
HPE Operations Manager i; Software Version: 10.11; OMi FIPS Configuration Guide; Document Release Date: 25 May 2016; Software Release Date: May 2016
HPE Operations Manager i; Software Version: 10.11; OMi Database Guide; Document Release Date: 25 May 2016; Software Release Date: May 2016
HPE Operations Manager i; Software Version: 10.11; RTSM Administration Guide; Document Release Date: May 2016; Software Release Date: May 2016
HPE Operations Agent; Software Version: 12.01; Reference Guide; Document Release Date: May 2016; Software Release Date: May 2016
HPE Operations Agent and Infrastructure SPIs; Software Version: 12.01; Installation Guide; Document Release Date: May 2016; Software Release Date: May 2016
HPE Operations Agent; Software Version: 12.01; User Guide; Document Release Date: May 2016; Software Release Date: May 2016
HPE Operations Bridge Reporter; Software Version: 10.01; Administration Guide; Document Release Date: June 2016; Software Release Date: June 2016
HPE Operations Bridge Reporter; Software Version: 10.01; Configuration Guide; Document Release Date: June 2016; Software Release Date: June 2016
HPE Operations Bridge Reporter; Software Version: 10.01; Release Notes; Document Release Date: May 2017; Software Release Date: June 2016
Hewlett Packard Enterprise Development LP; HPE Operations Bridge Premium v2016.05 including HPE Operations Manager i v10.11, HPE Operations Agent v12.01, and HPE Operations Bridge Reporter v10.01; Security Target; Evaluation Assurance Level (EAL): EAL2+ v1.2

Hewlett Packard Enterprise Development LP; HPE Operations Bridge Premium v2016.05 including HPE Operations Manager i v10.11, HPE Operations Agent v12.01, and HPE Operations Bridge Reporter v10.01; Guidance Documentation Supplement Document; Evaluation Assurance Level (EAL): EAL2+ v1.1

PRODUCT TESTING

The tests performed by both the evaluator and the developer are based on the TSFIs description included in the functional specification and the SFRs description included in the security target [ST].

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals. The TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to security target [ST]. The evaluator has repeated all the cases specified by the developer in the test documentation and has compared the obtained results with those obtained by the developer and documented in each associated report. The test repetition performed by the evaluator has demonstrated that the test plan and report provided by the vendor contains information enough to make a reader able to repeat all tests included. Additionally, after the repetition, the evaluator has obtained the same results as the expected ones. The independent testing has covered 100% of SFRs of the [ST] and TSFIs defined in the functional specification for the TOE, sampling has not been performed. The test cases have taken into account critical parameters values, searching that the TOE behaves in a non-expected manner. There has not been any deviation from the expected results under the environment defined in security target [ST].

PENETRATION TESTING

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals. The TOE does NOT present exploitable vulnerabilities under the environment defined in the security target [ST]. All identified vulnerabilities can be considered closed if the TOE is installed and operated according to the security target [ST] and related documentation. The overall test result is that no deviations were found between the expected and the actual test results taking into account that environment. No attack scenario with the attack potential “Basic” has been successful in the TOE’s operational environment as defined in the security target [ST] when all measures required by the developer are applied.

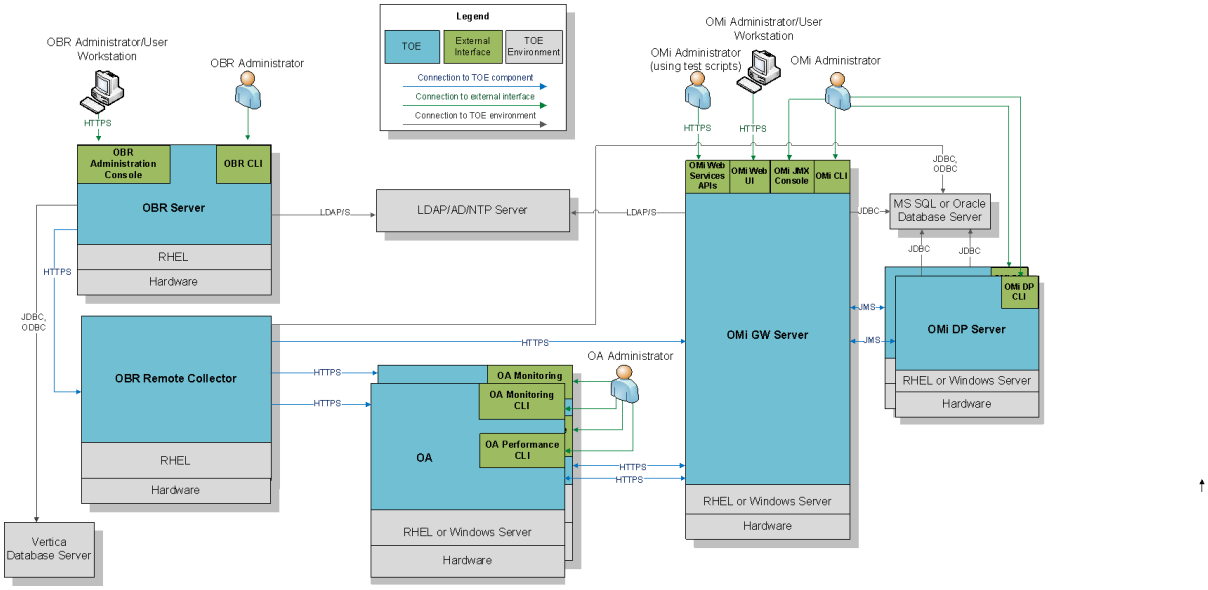
EVALUATED CONFIGURATION

The TOE under evaluation is “HPE Operations Bridge Premium v2016.05 including: HPE Operations Manager i v10.11 Build 016.001.63210 Hotfix: QCCR8D53202_1011, HPE Operations Agent v12.01 Build 020 and HPE Operations Bridge Reporter v10.01 Build 953.00001”.

The evaluated configuration includes the HPE Operations Bridge Premium v2016.05 media kit (English) with both the Windows (Server 2012 R2) and Linux (RHEL 6.7) versions of the HPE OMi and HPE OA media kit zip files and the Linux (RHEL 6.7) version of the HPE OBR media kit.

The TOE includes two instances of the HPE OMi GW server, four instances of the HPE OMi DP servers, and two instances of the HPE OAs. The TOE also includes one HPE OBR Server and one HPE OBR Remote Collector (installed from the HPE OBR software binary).

The following figure depicts the detailed deployment diagram for the TOE components in the evaluated configuration



EVALUATION RESULTS

The product “HPE Operations Bridge Premium v2016.05 including: HPE Operations Manager i v10.11 Build 016.001.63210 Hotfix: QCCR8D53202_1011, HPE Operations Agent v12.01 Build 020 and HPE Operations Bridge Reporter v10.01 Build 953.00001” has been evaluated against the “Hewlett Packard Enterprise Development LP HPE Operations Bridge Premium v2016.05 including HPE Operations Manager i v10.11, HPE Operations Agent v12.01, and HPE Operations Bridge Reporter v10.01 Security Target, v1.2, November 2017”.

All the assurance components required by the evaluation level EAL2 + ALC_FLR.2 have been assigned a “PASS” verdict. Consequently, the laboratory Epoche & Espri S.L.U assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL2 + ALC_FLR.2, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

The TOE usage is recommended given that there are not exploitable vulnerabilities in the operational environment. The following usage recommendation is given:

- The fulfilment of the assumptions indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.

CERTIFIER RECOMMENDATIONS

Considering the evidences obtained during the instruction of the certification request of the product “HPE Operations Bridge Premium v2016.05 including: HPE Operations Manager i v10.11 Build 016.001.63210 Hotfix: QCCR8D53202_1011, HPE Operations Agent v12.01 Build 020 and HPE Operations Bridge Reporter v10.01 Build 953.00001”, a positive resolution is proposed.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OBR	Operations Bridge Premium
OC	Organismo de Certificación
SFR	Security Functional Requirement
TOE	Target Of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R4 Final, Sept. 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, Sept. 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, Sept. 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, Sept. 2012.

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

[ST] Hewlett Packard Enterprise Development LP HPE Operations Bridge Premium v2016.05 including HPE Operations Manager i v10.11, HPE Operations Agent v12.01, and HPE Operations Bridge Reporter v10.01 Security Target, v1.2, November 2017.