Hewlett Packard Enterprise

Cloud Service Automation

FIPS 140-2 Compliance Statement

Software version: 4.70

Document release date: July 2016

Software release date: July 2016

Contents

Summary

The following Hewlett Packard Enterprise (HPE) Cloud Service Automation (CSA) components and elements comply with Level 1 Federal Information Processing Standard 140-2 (FIPS 140-2), which defines the technical requirements to be used by federal agencies when these organizations specify cryptographic-based security systems for protection of sensitive or valuable data:

- Cloud Service Management Console
- Marketplace Portal
- Password Utility Tool
- Marketplace Portal Password Utility Tool
- Content Archive Tool
- Component Tool
- Database Purge Tool
- Provider Configuration Tool
- Schema Installation Tool
- Identity Management Service

The compliance of these CSA elements with FIPS 140-2 is ensured by integrating FIPS 140-2 compliant, third party cryptographic module(s), using the module(s) as the only provider(s) of cryptographic services, and using FIPS-approved cryptographic functions, as applicable for CSA design, implementation, and operation.

Overview

This section describes the different elements that make up the CSA solution.

About Cloud Service Automation

CSA is a unique platform that orchestrates the deployment of compute and infrastructure resources and of complex multi-tier application architectures. CSA integrates and leverages the strengths of a hybrid cloud environment, which provides the ability to design and deploy enterprise-ready cloud services tailored to the business needs of your organization.

For details about how CSA implements FIPS 140-2 requirements, see the *Cloud Service Automation FIPS 140-2 Compliance Configuration Guide*.

Note: Only CSA installed with the following components is compliant with FIPS 140-2:

- Operating System – Microsoft Windows
- Database – Microsoft SQL Server (MS SQL)
- Java Runtime Environment – Oracle JRE

See the *Cloud Service Automation Solution and Software Support Matrix* for more information.

Cloud Service Management Console Web Application

The Cloud Service Management Console provides for the overall administration and configuration of the CSA system. The primary administration tasks are organized around the creation and configuration of organizations within the system.

Marketplace Portal Web Application

The Marketplace Portal delivers cloud-service catalogs to customers through an innovative, *enterprise-ready* design. In this design, users in each organization order services tailored specifically to their needs, and unless they have proper authorization, cannot access the service catalogs belonging to any other organization.

CSA Password Utility Tool

CSA's Password Utility tool is a standalone application used to encrypt sensitive data stored by CSA. This information includes:

- Seeded (CSA internal user) user credentials.
- Passwords as configured through the Cloud Service Management Console.

For details about the Password Utility tool, see the *Cloud Service Automation FIPS 140-2 Compliance Configuration Guide*.

Marketplace Portal Password Utility Tool

The Marketplace Portal Password Utility Tool is a standalone application used to encrypt passwords stored by the Marketplace Portal. For details about the Marketplace Portal Password Utility tool, see the *Cloud Service Automation FIPS 140-2 Compliance Configuration Guide.*

Content Archive Tool

CSA's Content Archive Tool is used to move various pieces of artifact information from one CSA installation to another.

For details about the Content Archive Tool, see the *CSA Content Archive Tool Guide.*

Component Tool

The component tool is run by the user after CSA installation to import the Operations Orchestration flows from the content packs that are installed with CSA. For details about the Component Tool, see the *Cloud Service Automation Configuration Guide*.

Purge Tool

The database purge tool is used to delete canceled, expired, failed, and retired subscriptions along with specific associated or referenced artifacts and entities from the CSA database. For details about the purge tool, see the *Cloud Service Automation Configuration Guide.*

Provider Configuration Tool

CSA's Provider Configuration Tool is a command line tool for reading (viewing), creating, updating and deleting service providers. For details about the Provider Configuration Tool, see the *Cloud Service Automation Provider Configuration Tool Guide*.

Schema Installation Tool

The CSA schema installation tool is used to upgrade the existing CSA database schema or install a fresh database schema without re-installing CSA. It is useful in the following situations:

- Installing the CSA database components onto the database if they were not installed during CSA installation.
- Upgrading the database schema if it was not upgraded during a CSA upgrade if, for example, the CSA upgrade failed.
- Dropping the existing schema and installing a fresh CSA database schema.

For details about the schema installation tool, see the *Cloud Service Automation Configuration Guide*.

Identity Management Service

The Identity Management service (IdM) provides authentication for CSA. CSA and the Marketplace Portal rely on the centralized IdM component to obtain authentication information. IdM works within the CSA Java Runtime Environment

(JRE) with all FIPS compliance components. IdM communicates with the Cloud Service Management Console and the Marketplace Portal through the HTTPS protocol to provide authentication and authorization services.

For details about how IdM implements FIPS 140-2 requirements, see the *Cloud Service Automation FIPS 140-2 Compliance Configuration Guide.*

Note: In this document, JRE or JVM refer to Oracle JRE or Oracle JVM respectively.

About FIPS 140-2

The Federal Information Processing Standards Publication (FIPS) 140-2, “Security Requirements for Cryptographic Modules,” was issued by the National Institute of Standards and Technology (NIST) in May, 2001. The FIPS 140-2 standard specifies the security requirements for cryptographic modules used within a security system that protects sensitive or valuable data. The requirements can be found in the following documents:

- SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

  http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
- Annex A: Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules

  http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf

---

Note: In this document, the abbreviation “FIPS” means “FIPS 140-2.”

FIPS 140-2 Compliant Module and Technologies

The benefits of using FIPS 140-2 compliant crypto modules is that the FIPS-approved crypto algorithms are deemed appropriate and that they perform the encrypt, decrypt, and hash functions correctly and in a FIPS-compliant manner.

Modes of Operation

CSA and its components can be configured and operated in the following two modes:

- FIPS-compliant mode: This mode supports FIPS 140-2 compliant cryptographic functions.
- Standard mode: This is a non-FIPS 140-2 compliant mode that uses existing or available cryptography without third-party FIPS-compliant 140-2 crypto modules.

FIPS 140-2 Compliant Third Party Modules

The Marketplace Portal component and the Marketplace Password Utility component are integrated with the third-party FIPS 140-2 compliant cryptographic module *OpenSSL FIPS Object Module v2.0.7*. When the Marketplace Portal is configured to operate in FIPS-compliant mode, its functions and procedures (such as SSL/TLS connections and encryption of stored sensitive data, which require cryptography such as secure hash, encryption, digital signature, and so on) use the cryptography services provided by the OpenSSL FIPS Object Module configured to run in FIPS mode.

All other CSA components are integrated with the third-party FIPS 140-2 compliant cryptographic module *RSA BSAFE Crypto-J version 6.1*. When CSA is configured to operate in FIPS-compliant mode, its functions and procedures (such as SSL/TLS connections and encryption of stored sensitive data, which require cryptography such as secure hash, encryption, digital signature, and so on) use the cryptography services provided by RSA BSAFE Crypto-J configured to run in FIPS mode.

Details about how to configure CSA and its components to conform to FIPS 140-2 appear in the following installation and configuration guides:

- *Cloud Service Automation Installation Guide*
- *Cloud Service Automation FIPS 140-2 Compliance and Configuration Guide*

FIPS Requirements

CSA can be run in FIPS mode in a standalone configuration.

CSA-Sensitive Data

CSA-sensitive data that requires FIPS-compliant encryption using RSA BSAFE Crypto-J is listed below.

- CSA seeded user credentials. There are internal users that are part of the CSA installation. The passwords of these seeded users are considered CSA-sensitive data.
- CSA transport user credentials and IdM transport user credentials. The Cloud Service Management Console has a REST web service interface. REST requests are authenticated using CSA's transport user credentials. In a typical CSA installation, the REST API is used by CSA to communicate with the Cloud Service Management Console. These passwords are stored in the following files: `applicationContext.properties, csa.properties, consumer-users.properties, provider-users.properties, idm-security.properties,` and `integrationusers.properties`. Transport user passwords are considered CSA-sensitive data.
- Access Point credentials. Every organization listed in the Cloud Service Management Console can be associated with an LDAP, SMTP, or one or more CSA Resource Provider access points. The access point passwords are stored in the CSA database and are considered CSA-sensitive data.
- The CSA server truststore contains third-party certificates that are implicitly trusted by CSA during secure communication. The CSA server truststore password is considered CSA-sensitive data. When run in FIPS mode, CSA does not use the default Java truststore.

Note: Data that does not compromise CSA-sensitive data as described above is not considered CSA-sensitive data.

Marketplace Portal-Sensitive Data

Marketplace Portal-sensitive data that requires FIPS-compliant encryption using the OpenSSL FIPS Object Module is listed below.

- IdM transport user credentials. The Marketplace Portal has a REST web service interface. REST requests are authenticated using IdM transport user credentials. In a typical CSA installation, the REST API is used by the Marketplace Portal to communicate with the Cloud Service Management Console. These passwords are stored in the `mpp.json` file. Transport user passwords are considered Marketplace Portal-sensitive data.
- Cookie password. This is the key used to encrypt the cookie that stores the user's organization name and the session ID to make the login persistent.
- Keystore password.
- List of third-party CA certificates (in PEM format or DER format) that the Marketplace Portal reads in that are implicitly trusted by the Marketplace Portal during secure communication.

Note: Data that does not compromise Marketplace Portal-sensitive data as described above is not considered Marketplace Portal-sensitive data.

FIPS Supported Configuration for CSA Data at Rest

When run in FIPS mode, CSA uses the following RSA BSAFE Crypto module FIPS certified algorithms for encryption and storage of CSA sensitive data:

- Supported Encryption Keystore format: PKCS 12
- Supported asymmetric algorithm for CSA Encryption Keystore: RSA (2048 (default); can be greater)
- Supported symmetric key algorithm used by CSA: AES (128-bit (default), 192-bit, and 256-bit key sizes)
- Supported Random Number Generation algorithm used by CSA for encryption is HMAC DRBG (128-bit)
- Supported hashing algorithm used by CSA: SHA256

FIPS Supported Configuration for Marketplace Portal Data at Rest

When run in FIPS mode, the Marketplace Portal uses the following OpenSSL FIPS Object Module FIPS certified algorithms for encryption and storage of sensitive data:

- Supported Encryption Keystore format : PBES2
- Supported symmetric key algorithm used by HPE MPP : AES256
- Supported Random Number Generation algorithm used by CSA for encryption : HMAC-SHA1

Data In Transit

When run in FIPS mode, CSA uses the FIPS-certified Cipher Suites provided by the RSA BSAFE Crypto module. The supported keystore and truststore format is PKCS 12.

When run in FIPS mode, the Marketplace Portal uses the OpenSSL FIPS Object Module for secure communication. The supported keystore and truststore format is PKCS 12.

TLS1.x (CSA)

All CSA component communications are secured with FIPS-compliant Transport Layer Security TLS1.0. It relies on FIPS 140-2 approved hash algorithms and symmetric and asymmetric ciphers provided by the RSA BSAFE Crypto module.

- TLS handshake, key negotiation and authentication provide data integrity and make use of secure hash, asymmetric key cryptography and digital signature.
- TLS encryption of data in transit provides confidentiality and makes use of symmetric cryptography.

TLS1.x (Marketplace Portal)

All Marketplace Portal component communications can be secured with FIPS-compliant Transport Layer Security TLS1.0. It relies on FIPS 140-2 approved hash algorithms and symmetric ciphers provided by the OpenSSL FIPS Object Module.

- TLS handshake, key negotiation and authentication provide data integrity and make use of secure hash, and digital signature.
- TLS encryption of data in transit provides confidentiality and makes use of symmetric cryptography.

To enable TLS1.0, you must:

- Add the proper settings to enable TLS1.0 in the Marketplace Portal mpp.json configuration file. For more information, see the “Configuring CSA” section in the *CSA FIPS 140-2 Compliance Configuration Guide*.

Secure Hash

CSA supports the secure hash algorithms supported by RSA BSAFE Crypto-J when run in FIPS-compliant mode. For details, see the FIPS compliance documentation provided by the RSA BSAFE Crypto-J module provider.

The Marketplace Portal supports the secure hash algorithms supported by the OpenSSL FIPS Object Module when run in FIPS-compliant mode. For details, see the FIPS compliance documentation regarding the OpenSSL FIPS Object Module at http://www.openssl.org/docs/fips/.

Digital Signature

CSA supports the secure digital signature algorithms supported by RSA BSAFE Crypto-J when run in FIPS-compliant mode. For details, see the FIPS compliance documentation provided by the RSA BSAFE Crypto-J provider.

The Marketplace Portal supports the secure digital signature algorithms supported by the OpenSSL FIPS Object Module when run in FIPS-compliant mode. For details, see the FIPS compliance documentation regarding the OpenSSL FIPS Object Module at http://www.openssl.org/docs/fips/.

CSA and FIPS 140-2

CSA is expected to operate on general-purpose systems with no additional physical security controls. The RSA BSAFE Crypto-J module and the OpenSSL FIPS Object Module installed on such platforms, provide compliance to Level 1 FIPS 140-2 compliant crypto services.

- For RSA BSAFE Crypto-J, install the Crypto-J module.
- For the OpenSSL FIPS Object Module, install the compiled NodeJS with OpenSSL with FIPS Object Module from the supported NodeJS in the %CSA_HOME%\node.js\ directory.

For instructions on installing the Crypto-J module and NodeJS, see “Preparing your environment” in the *CSA FIPS 140-2 Compliance and Configuration Guide.*

FIPS 140-2 Architecture

All CSA instances in a CSA deployment must be run in FIPS-compliant mode. CSA does not support a deployment architecture that contains a mix of CSA instances that run in FIPS and non-FIPS mode.

Standalone Configuration

The CSA JRE environment corresponds to the JRE being used by CSA components. This JRE must be configured using the RSA BSAFE JSafeJCE crypto library (as described in “Configuring CSA” in the CSA FIPS 140-2 Compliance Configuration Guide). For the Marketplace Portal, NodeJS is compiled with the OpenSSL FIPS Object Module v2.0.7.

Note: NodeJS version 0.10.29 is used for FIPS compliance. The OpenSSL version 1.0.1h is used by NodeJS.

You can deploy multiple Marketplace Portal instances in standalone mode.

Supported Platforms

See the *CSA Solution and Software Support Matrix* for more information.

Design Assurance

The following sections illustrate the design, operation, and use of the FIPS-compliant crypto components by CSA and by the Marketplace Portal when run in FIPS-compliant mode.

Key Management

All aspects of key management, such as random number and key generation, are provided by functions of the RSA BSAFE Crypto-J crypto module (for CSA) or the OpenSSL FIPS Object Module (for the Marketplace Portal) and thus meet FIPS 140-2 compliance requirements. The application-specific key management functions are identified below.

FIPS Compliance of CSA for Sensitive Data at Rest (Storage)

The following sections detail configuration and key management design used by the FIPS-compliant components of CSA.

Configuration of CSA

To configure FIPS-compliant components of CSA:

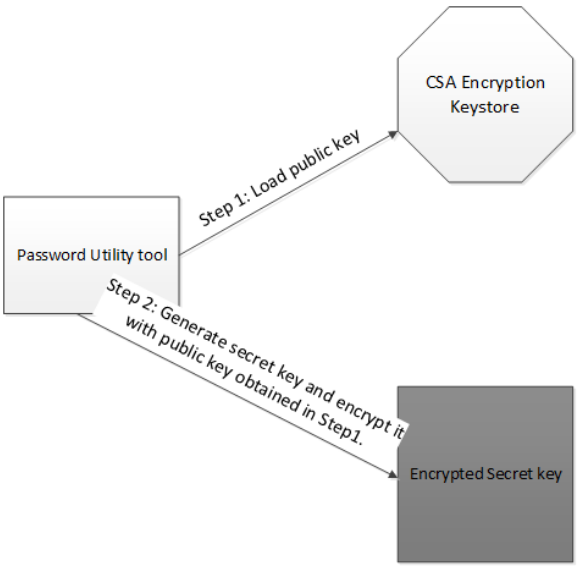
1. Create the CSA Encryption Keystore.
2. Create a file with a secret key in an encrypted form using the Password Utility tool or the Marketplace Portal Password Utility Tool as appropriate.

For additional details see the “Configuring CSA” section in the *CSA FIPS 140-2 Compliance Configuration Guide*.

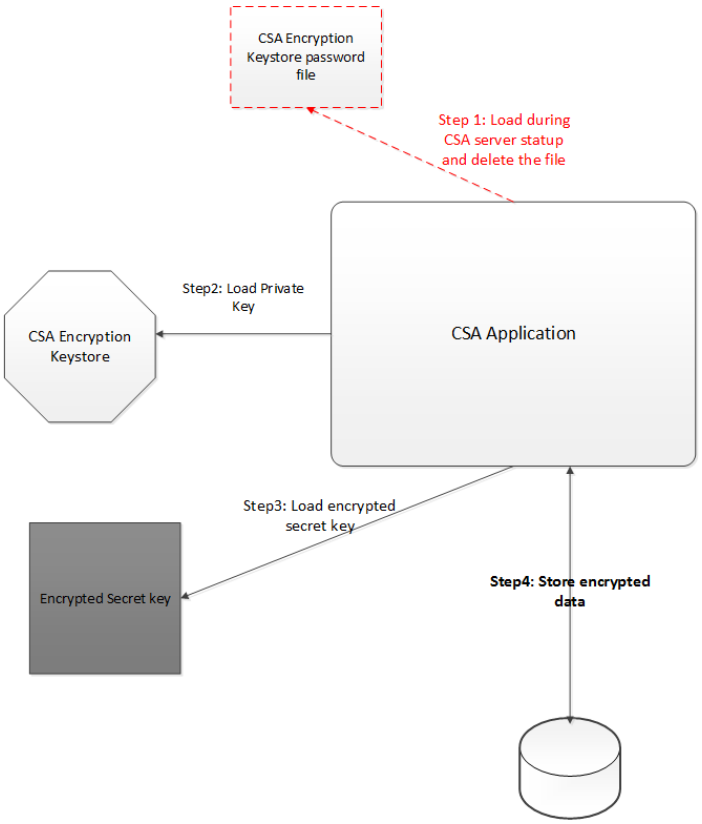
Key Management Design Used by CSA FIPS-Compliant Components

To perform key management using CSA FIPS-compliant components:

1. CSA Key Generation
    - The secret key is generated and stored in encrypted form by the Password Utility Tool. This tool uses the CSA Encryption keystore to encrypt the key. The crypto algorithms used are provided by the FIPS-certified RSA BSAFE provider.



2. CSA Encryption/Decryption Operation



- The secret key used by CSA is stored in a FIPS-compliant encrypted form. This key is loaded in encrypted form for encryption/decryption of CSA sensitive data. The location of the secret key has to be configured in the `csa.properties` file and the `idm-security.properties` file. See the *CSA FIPS 140-2 Compliance Configuration Guide* for details.

  The plain text password for the CSA Encryption keystore is loaded from a file during startup, and the file is deleted to ensure that the password for the encryption keystore is present only in the JVM memory of the CSA server.

  The administrator must recreate this file with the CSA encryption keystore password if the CSA server has to be restarted. The CSA server will fail to start up in FIPS mode if this file does not exist.

Usage

CSA uses the encrypted secret key to encrypt CSA sensitive data.

FIPS Compliance of CSA for Data in Transit

CSA supports only TLSv1.0 in FIPS compliance mode. As part of CSA configuration for FIPS, CSA requires the JRE to be configured to use the RSA BSAFE security provider in FIPS-certified mode for SSL (as mentioned in “Configuring CSA” in the *CSA FIPS 140-2 Compliance Configuration Guide*).

CSA Configuration

1. Create the keystore in PKCS 12 format.
2. Configure JBoss to support TLS v1.0.
3. Create and configure the CSA server Truststore. In FIPS mode, CSA will not use the default Java cacert truststore.

CSA SSL Operation and Usage

With the JRE configured to use the RSA BSAFE crypto provider in FIPS certified mode, the SSL cipher suites used by CSA will be the FIPS certified cipher suites of the RSA BSAFE provider. See “FIPS 140-2 Architecture” for details on the SSL components of CSA.

The third-party software components that CSA integrates with are expected to be set in FIPS-compliant mode in order to interact with CSA in a FIPS-compliant manner using SSL. The third-party components are:

- LDAP server of each organization configured in the Cloud Service Management Console
- Database instance used by CSA
- SMTP server

FIPS Compliance of the Marketplace Portal for Data in Transit

The Marketplace Portal supports only TLSv1.0 in FIPS compliance mode. As part of the Marketplace Portal configuration for FIPS, it requires the OpenSSL FIPS Object Module in FIPS certified mode for SSL (as mentioned in “Configuring CSA” in the *CSA FIPS 140-2 Compliance Configuration Guide*).

Marketplace Portal Configuration

1. Create the keystore in PKCS 12 format.
2. Configure NodeJS to support TLS v1.0.

Marketplace Portal SSL Operation and Usage

With NodeJS configured to use the OpenSSL FIPS Object Module in FIPS certified mode, the SSL cipher suites used by the Marketplace Portal will be the FIPS certified cipher suites of the OpenSSL FIPS Object Module. See “FIPS 140-2 Architecture” for details on the SSL components of the Marketplace Portal.

Security Governance and Policy

Physical security

The production servers on which CSA is installed must allow only users with valid credentials access to the system.

Configuration data security

CSA installation and configuration requires additional information such as credentials to access the database and the keystore password. These credentials, though confidential, are not considered CSA sensitive data, because:

- This data does not compromise the encrypted FIPS-compliant sensitive data stored by CSA that are configured by end users of CSA.
- This data is not exposed to the end users of CSA.
- This data cannot be read, updated, or modified remotely by third-party systems integrated with CSA.

The security policies mentioned below are required to be followed for these credentials to provide sufficient risk mitigation for these data points.

Datasource password for CSA

The datasource password is used by JBoss to connect to the CSA database server on behalf of CSA. When CSA is run in FIPS compliant mode, this value must be encrypted using the JBoss 7.1.1 vault functionality. See “Create a New Keystore and Truststore for Secure Communication” in the *CSA FIPS 140-2 Compliance Configuration Guide* for more information.

Keystore password for CSA

The keystore password is used by JBoss to access the keystore when initiating a secure connection. When CSA is run in FIPS compliant mode, this value must be encrypted using the JBoss 7.1.1 vault functionality. See “Create a New Keystore and Truststore for Secure Communication” in the *CSA FIPS 140-2 Compliance Configuration Guide* for more information.

Acronyms

AES
Advanced Encryption Standard.

CSA
CSA .

HMAC DRBG
Keyed-hash message authentication code deterministic random bit generator, which is a random number generation algorithm.

FIPS
Federal Information Processing Standard.

IdM
Identity Management component of CSA.

JBoss
JavaBeans Open Source Software Application Server, which is an application server that implements the Java Platform, Enterprise Edition.

JVM
Java Virtual Machine. CSA uses the JVM included in the Oracle Java Runtime Environment (JRE).

MPP
Marketplace Portal.

PKCS 12
Personal Information Exchange Syntax Standard #12.

REST
Representational State Transfer.

RSA
An algorithm for public-key cryptography. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman.

SMC
Service Management Console.

SSL
Secure Sockets Layer, which is the standard security technology for establishing an encrypted link between a web server and a browser.

TLS
Transport Security Layer.

References

CSA Installation Guide

CSA Configuration Guide

CSA FIPS 140-2 Compliance Configuration Guide

CSA Solution and Software Support Matrix

Send documentation feedback

If you have comments about this document, you can send them to clouddocs@hpe.com.

Legal notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted rights legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright notice

Trademark notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.

The OpenStack word mark and the Square O Design, together or apart, are trademarks or registered trademarks of OpenStack Foundation in the United States and other countries, and are used with the OpenStack Foundation's permission.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to the following URL and sign-in or register: https://softwaresupport.hp.com.

Select Manuals from the Dashboard menu to view all available documentation. Use the search and filter functions to find documentation, whitepapers, and other information sources.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your Hewlett Packard Enterprise sales representative for details.

Support

Visit the Hewlett Packard Enterprise Software Support Online web site at https://softwaresupport.hp.com.