Vormetric Protection for Teradata Database (VPTD)

Release Notes

- **Version: 6.4.0**
- **Date: April 7, 2020**

Caveats

Upgrading

When upgrading from a previous version of VPTD make sure to update the configuration using the following command:

```
/opt/vormetric/DataSecurityExpert/agent/pkcs11/teradata/bin/vormetric_local
_crypto_server -e
```

Warning! Failure to complete this step will cause the application to fail.

Re-registering to a different key manager

When re-registering the VPTD agent to a new key management server (DSM or KeySecure) follow these steps:

1. Stop the Cryptoserver.
2. Re-register to the new key manager.
3. Restart the Cryptoserver.

Warning! Failure to complete these steps will cause the application to fail.

Upgrading to VPTD from a prior version

We have observed unpredictable behavior related to Teradata UDF cache flushing during a VPTD upgrade. To defend against such unexpected behavior we recommend the following procedure for a VPTD upgrade:

1. Stop the Cryptoserver.
2. Drop existing UDFs using `DROP FUNCTION`.
3. Flush the UDF cache using **tpareset**.
4. Upgrade by invoking the `vptdxxx.bin` installation file.
5. Install the UDFs.
6. Change the configuration files as needed.
7. Start the Cryptoserver.
8. Flush the UDF cache by running **tpareset** three times.

New Features and Enhancements

Support for SafeNet KeySecure

This release adds support for using SafeNet KeySecure as a key manager (via its ICAPI crypto library) for encryption/decryption, in addition to the existing DSM key manager support.

Support for MultiLoad and FastExport

VPTD now supports the MultiLoad and FastExport Teradata utilities.

New datatype support

VPTD now includes new UDFs that support additional datatypes -- INT, BYTEINT, SMALLINT, DATE, TIME, and TIMESTAMP. New UDFs for standard CBC encryption and decryption add support for all of these datatypes. New UDFs for FPE and FF1 encryption/decryption have been added to support INT, BYTEINT, and SMALLINT datatypes.

Performance enhancements

VPTD operational performance has been enhanced.

Resolved Issues

There are no resolved issues in this release.

Known Issues

- **TER-339: Keys from old DSM are accessible after registration to new DSM**

  After re-registration to a new DSM, if the Cryptoserver is not restarted, the keys from the old DSM are accessible. To work around this issue, do not re-register to a DSM while the Cryptoserver is running, as described in the “Re-registration to a different DSM:” procedure under the “Caveats” section above.

- **TER-495: VPTD supports Unicode characters only up to code point 0xFFFF**

  VPTD supports Unicode characters up to 0xFFFF (that is, up to codepoint 65535).

  The character set range is specified in the `profiles.conf` file. An error message occurs when an FPE UDF call uses a begin/end character set range beyond 0xFFFF.

- **TER-512: No TLS on KeySecure and SSL on VPTD causes daemon to hang**

  When any No TLS interface mode is selected on a KeySecure server and VPTD is configured for SSL communication, the vormetric_local_crypto_server daemon start becomes blocked for an infinite time during initialization.

  For the correct configuration procedure, see the *VPTD Installation and Reference Guide* section “Configure NAE interface mode on KeySecure.”

Sales and Support

For support and troubleshooting issues:

- https://supportportal.thalesgroup.com
- (800) 545-6608

For Thales Sales:

- https://enterprise-encryption.vormetric.com/contact-sales.html
- sales@thalesesecurity.com
- (888) 267-3732

Notices and License

NOTICES, LICENSES, AND USE RESTRICTIONS

Vormetric, Thales, and other Thales trademarks and logos are trademarks or registered trademark of Thales eSecurity, Inc. in the United States and a trademark or registered trademark in other countries.

All other products described in this document are trademarks or registered trademarks of their respective holders in the United States and/or in other countries.

The software (“Software”) and documentation contains confidential and proprietary information that is the property of Thales eSecurity, Inc. The Software and documentation are furnished under license from Thales and may be used only in accordance with the terms of the license. No part of the Software and documentation may be reproduced, transmitted, translated, or reversed engineered, in any form or by any means, electronic, mechanical, manual, optical, or otherwise.

The license holder (“Licensee”) shall comply with all applicable laws and regulations (including local laws of the country where the Software is being used) pertaining to the Software including, without limitation, restrictions on use of products containing encryption, import or export laws and regulations, and domestic and international laws and regulations pertaining to privacy and the protection of financial, medical, or personally identifiable information. Without limiting the generality of the foregoing, Licensee shall not export or re-export the Software, or allow access to the Software to any third party including, without limitation, any customer of Licensee, in violation of U.S. laws and regulations, including, without limitation, the Export Administration Act of 1979, as amended, and successor legislation, and the Export Administration Regulations issued by the Department of Commerce, or in violation of the export laws of any other country.

Any provision of any Software to the U.S. Government is with "Restricted Rights" as follows: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277.7013, and in subparagraphs (a) through (d) of

the Commercial Computer-Restricted Rights clause at FAR 52.227-19, and in similar clauses in the NASA FAR Supplement, when applicable. The Software is a "commercial item" as that term is defined at 48 CFR 2.101, consisting of "commercial computer software" and "commercial computer software documentation", as such terms are used in 48 CFR 12.212 and is provided to the U.S. Government and all of its agencies only as a commercial end item. Consistent with 48 CFR 12.212 and DFARS 227.7202-1 through 227.7202-4, all U.S. Government end users acquire the Software with only those rights set forth herein. Any provision of Software to the U.S. Government is with Limited Rights. Thales is Thales eSecurity, Inc. at Suite 710, 900 South Pine Island Road, Plantation, FL 33324.

THALES PROVIDES THIS SOFTWARE AND DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT OF THIRD PARTY RIGHTS, AND ANY WARRANTIES ARISING OUT OF CONDUCT OR INDUSTRY PRACTICE. ACCORDINGLY, THALES DISCLAIMS ANY LIABILITY, AND SHALL HAVE NO RESPONSIBILITY, ARISING OUT OF ANY FAILURE OF THE SOFTWARE TO OPERATE IN ANY ENVIRONMENT OR IN CONNECTION WITH ANY HARDWARE OR TECHNOLOGY, INCLUDING, WITHOUT LIMITATION, ANY FAILURE OF DATA TO BE PROPERLY PROCESSED OR TRANSFERRED TO, IN OR THROUGH LICENSEE'S COMPUTER ENVIRONMENT OR ANY FAILURE OF ANY TRANSMISSION HARDWARE, TECHNOLOGY, OR SYSTEM USED BY LICENSEE OR ANY LICENSEE CUSTOMER. THALES SHALL HAVE NO LIABILITY FOR, AND LICENSEE SHALL DEFEND, INDEMNIFY, AND HOLD THALES HARMLESS FROM AND AGAINST, ANY SHORTFALL IN PERFORMANCE OF THE SOFTWARE, OTHER HARDWARE OR TECHNOLOGY, OR FOR ANY INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS, AS A RESULT OF THE USE OF THE SOFTWARE IN ANY ENVIRONMENT. LICENSEE SHALL DEFEND, INDEMNIFY, AND HOLD THALES HARMLESS FROM AND AGAINST ANY COSTS, CLAIMS, OR LIABILITIES ARISING OUT OF ANY AGREEMENT BETWEEN LICENSEE AND ANY THIRD PARTY. NO PROVISION OF ANY AGREEMENT BETWEEN LICENSEE AND ANY THIRD PARTY SHALL BE BINDING ON THALES.
Protected by U.S. patents:
6,678,828
6,931,530
7,143,288
7,283,538
7,334,124