Vormetric Transparent Encryption (VTE) for Linux

Release Notes

- **Release: 6.3.1.38**
- **Date: June 2, 2020**

New Features and Enhancements

Release 6.3.1.38 of Vormetric Transparent Encryption (VTE) for Linux adds new features, fixes known defects, and addresses known vulnerabilities. For operating system and framework version support, see the *VTE Agent Compatibility Matrix*.

Support for IDT-Capable Devices

VTE offers InPlace Data Transformation (IDT) Capable Device GuardPoints on Linux. IDT-Capable GuardPoints allow you to guard devices by transforming the plain-text data to cipher-text on the host device, or by rekeying existing data using a new encryption key. The data transformation process is called InPlace Data Transformation (IDT). The term "IDT-Capable" refers to the data transformation capability available on IDT-Capable GuardPoints.

IDT-Capable GuardPoints use the DSM policy type "In-place Data Transformation - Device" that was introduced with DSM release 6.4.2. For details about IDT, see the IDT chapter in the *VTE Agent Installation and Configuration Guide*.

Support for VTE with Teradata Database Appliances

The principles behind VTE's IDT-Capable Device GuardPoints support can also be applied to Teradata Database platforms such as IntelliBase, IntelliFlex, and Teradata Data Warehouse platforms 2700, 2750, 2800, 6700, 6750, and 6800. VTE support for these platforms requires the following prerequisites:

- The minimum version of the SLES12 kernel installed in the nodes in your cluster must be `4.4.140-96.54.TDC-default`. For future releases of SLES12 kernel for Teradata clusters, see the VTE Release Notes for the version of VTE that you are using.

- The Parallel Upgrade Tool (PUT) component of Teradata (TDput) must be version `TDput-03.09.06.09` or higher.

- The Parallel Database Extensions (PDE) component of Teradata (ppde) must be version `ppde-16.20.53.07` or higher.

- The Teradata I/O Scheduler (tdsched) component must be version `01.04.02.02-1` or higher.

For details about using VTE with Teradata, see the Teradata chapter in the *VTE Agent Installation and Configuration Guide*.

New Platform Support

SLES 12 SP3 (Teradata kernel)

- 4.4.140-96.54.TDC-default (supported with 6.3.1.38)

Resolved Issues

- **AGT-28199 [CS0978443]: Installation on Oracle RAC agent displays an error message**

  Installing VTE on an unsupported kernel version correctly displays the message that VTE is not compatible with this kernel, however the install attempts leaves the modules in a failed state and blocks and future attempts to upgrade to the correct VTE version.

  VTE now makes sure that it automatically uninstalls cleanly if the kernel version is incompatible.

- **AGT-28310 [CS0980312]: Stale pointer error caused a system crash on NFS share**

  VTE attempted to access a file on an NFS share using a NULL pointer that led to a system crash.

  The current release of VTE makes sure that all file pointers are non-NULL before accessing files.

Sales and Support

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

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

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as "Thales") information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.

- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.