Vormetric Transparent Encryption for AIX

Release Notes

Release 5.3.0

October 30, 2019

New Features and Improvements

Release 5.3.0 of Vormetric Transparent Encryption (VTE) for AIX adds new features, fixes known defects, and addresses known vulnerabilities.

New features

VTE 5.3.0 for AIX includes the following new features:

Security enhancements

Support for AES CBC-CS1

The AES-CBC-CS1 encryption is superior to the existing AES-CBC mode because it uses a unique and unpredictable (random) IV (initialization vector) generated for each individual file. The per-file IV object is generated only at file creation time. It is stored as file metadata.

“path_no_trust” authenticator

You can specify a path that is not to be trusted. No binaries on the path you name are trusted.

Updated GPFS native encryption support

Support for GPFS agent ends with VTE 5.3.0 for AIX. However, you can use the VTE 5.3.0 for AIX agent for access control using a KMIP solution. For information about KMIP, see the *DSM Administration Guide*.

Smart upgrade feature

You can initialize an upgrade, and defer it from taking effect until the next time you reboot your system.

Support for IBM POWER9 Clusters

The cluster capabilities of IBM POWER9 servers are compatible with VTE 5.3.0 for AIX.

Oracle 18c Support

VTE 5.3.0 for AIX supports Oracle 18c. See the *Vormetric Compatibility Matrix (VTE)* on the Official Documentation Page for details.

End of Support

The following products are no longer supported as of VTE 5.3.0 for AIX:

- IBM Spectrum Scale (also known as General Parallel File System – GPFS) is no longer supported. Spectrum Scale’s native encryption is available from Spectrum Scale version 4.2.1 (Advanced & Data Management editions only) onwards. You can still use the KMIP solution on the Vormetric Data Security Manager (DSM) for centralized key management for Spectrum Scale’s native encryption. The solution integration details can be found here:
  - https://www.ibm.com/support/knowledgecenter/en/STXKQY_5.0.0/com.ibm.spectrum.scale.v5r00.doc/bl1adv_encryptionenv_vormetric.htm
- AIX version 6.1. is no longer supported. IBM’s End of Support occurred on April 30, 2017. Please refer to https://www-01.ibm.com/support/docview.wss?uid=swg3y550416m84442g86 for additional information.
- IBM DB2 pureScale is no longer supported.

For a complete list of Operating system and framework version support, see the *Vormetric Compatibility Matrix (VTE)* on the Official Documentation Page.

Sales and Support

For support and troubleshooting issues:

- Log a ticket at https://supportportal.thalesgroup.com/
- or call 800-545-6608

For Vormetric Sales:

- http://enterprise-encryption.vormetric.com/contact-sales.html
- Email questions to sales@thalesesec.net or call 888-267-3732

Notices and License

Vormetric Transparent Encryption
Vormetric Transparent Encryption (VTE) 5.3.0
Release Notes v1
Copyright 2009 – 2019. Thales e-Security, Inc. All rights reserved.

NOTICES, LICENSES, AND USE RESTRICTIONS

Vormetric, Thales, and other Thales trademarks and logos are trademarks or registered trademark of Thales e-Security, 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 e-Security, 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