CipherTrust Transparent Encryption (CTE) for Linux

Release Notes

- **Release: 7.0.0.47**
- **Date: September 22, 2020**

New Features and Enhancements

Release 7.0.0.47 of CipherTrust Transparent Encryption (CTE) for Linux adds new features, fixes known defects, and addresses known vulnerabilities.

The major improvements to CTE for Linux in this release are:

- CTE-Efficient Storage on Linux now supports LVM, and a new use case describing this support has been added to the CTE-Efficient Storage chapter in the *CTE Agent for Linux Advanced Configuration and Integration Guide*.
- Learn mode is now available for CTE Cloud Object Storage (CTE COS) for Amazon S3 buckets (CTE COS S3).
- Audit Logging has been improved by adding the real userid and effective userid of the process and its ancestors when CTE generates an audit log entry for Guardpoint access. This helps to track the change of privileges across the process tree.
- The JSON file posted with the CTE binaries has been improved.
  - It now contains mappings of the product builds to Linux kernels.
  - It is now machine readable and can be used for automated deployments and compatibility checks.
- You can now specify the temporary directory that CTE will use to extract the installation files using `-t <temp_dir_path>` on the command line or the `TMPDIR` variable in the silent installation file.

Name Change to CipherTrust Transparent Encryption

Vormetric Transparent Encryption (VTE) is now called CipherTrust Transparent Encryption (CTE).

> **Note**
> Some of the names in the CTE suite still use "Vormetric".
> For example, the default installation directory is `/opt/vormetric/DataSecurityExpert/agent/`.

CTE and CipherTrust Manager Integration

Thales now offers two key managers that work with CTE:

- CipherTrust Manager, Thales's next generation key manager that supports most CTE for Linux features.
- The *Vormetric Data Security Manager* (DSM), Thales's legacy key manager that supports all CTE for Linux features.

Both key managers can be set up as either a security-hardened physical appliance or a virtual appliance, and both provide access to the protected hosts through a browser-based, graphical user interface as well as an API and a CLI. Thales recommends that you use the CipherTrust Manager unless you need a feature that is only supported by the DSM, as described below.

The CipherTrust Manager currently supports all CTE for Linux features *except* for the following:

- Container Security
- CTE-Efficient Storage
- CipherTrust InPlace Data Transformation
- CTE with Teradata Database Appliances

Support for these features will be included in future releases of the CipherTrust Manager.

For details about any of these features, see the *CTE Agent for Linux Advanced Configuration and Integration Guide*.

You must select one and only one key manager per host or host group. While you could have some hosts registered with a CipherTrust Manager and some registered with a DSM, you cannot have the same host registered to both a CipherTrust Manager and a DSM.

> **Note**
> For a list of CTE versions and supported operating systems, see the *Compatibility Matrix for CTE Agent with CipherTrust Manager* and the *Compatibility Matrix for CTE Agent with Data Security Manager*.

Upgrading Existing VTE Hosts to CTE 7.0.0.47

Currently, you can only upgrade a VTE for Linux host to CTE version 7.0.0.47 if you continue to use the DSM as your key manager. You cannot upgrade a VTE host to CTE and then register the upgraded CTE host with CipherTrust Manager. The migration path to CipherTrust Manager will be available in a future release.

CTE Documentation Set

The CTE Documentation Set has been expanded to include CipherTrust Manager and reorganized to make the information easier for customers to navigate. The CTE documentation set in version 7.0.0 includes the following books:

- *CTE Agent for Linux Quick Start Guide*
- *CTE Agent for Linux Advanced Configuration and Integration Guide*
- *CTE Agent for Windows Quick Start Guide*
- *CTE Agent for Windows Advanced Configuration and Integration Guide*
- *CTE Agent for AIX Installation and Configuration Guide*
- *CTE-Live Data Transformation with Data Security Manager*
- *CTE-Live Data Transformation with CipherTrust Manager*

- *Compatibility Matrix for CTE Agent with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent with Data Security Manager*
- *Compatibility Matrix for CTE Agent for AIX with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent for AIX with Data Security Manager*
- *Release Notes for CTE for Linux Version 7.0.0.47*
- *Release Notes for CTE for Windows Version 7.0.0.47*
- *Release Notes for CTE for AIX Version 7.0.0.11*

New Platform Support

- Ubuntu 20.04
- SLES 15 SP2

Resolved Issues

- **AGT-29113 — voradmin ldt attr delete removes attr on files while GuardPoint is active**

  In VTE version 6.3.1, if the GuardPoint path specified on the `voradmin ldt attr delete` command had a trailing `/` (slash), `voradmin` could not correctly determine whether or not the GuardPoint was an active LDT GuardPoint. Therefore, it would remove the LDT extended attributes on files even in active LDT GuardPoints.

  This issue has been fixed in the current release of CTE Agent and `voradmin` will no longer remove LDT extended attributes from files in an active GuardPoint.

- **AGT-28597— systemd failed to mount the filesystem for IDT and ESG GuardPoints**

  The fstab entry for an auto-mounted IDT or CTE-Efficient Storage GuardPoint must include the `x-systemd.wanted-by=` option. For details, see the "Auto Mount Options" section in the chapter for CTE-IDT or CTE-Efficient Storage in the *CTE Agent for Linux Advanced Configuration and Integration Guide*.

- **AGT-27201 [CS0962071] — VTE secvm crashes**

  In VTE 6.3.1, there are rare instances when secvm crashes. This has been fixed by providing the capability to eliminate a certain mode of virtual memory addressing by the Linux kernel.

- **AGT-29358: DD cmd does not fail properly on IDT device when device has reservation restrictions on write**

  For some versions of VTE 6.3.1, when running on Linux kernel version 4.4 or earlier, guarded raw devices (SECVM) may not properly propagate real errors from the underlying disk (storage device) back up to user space application.

  This issue has been fixed in this release of the CTE Agent.

- **AGT-29578: VTE uninstall leaves COS files behind / AGT-29281: Error: Credential store header is missing**

  For some versions of VTE 6.3.1, when VTE with VTE COS enabled is uninstalled, a VTE COS-related directory is not properly removed. Leaving this directory behind also results in a "Credential store header is missing" error.

  In this release of the CTE Agent, all CTE Agent directories are properly removed and the "Credential store header is missing" error no longer occurs.

- **AGT-29023 [CS0996021]: Various startup Issues with VTE and Hadoop reported when Hadoop is installed in a custom directory**

  Some versions of VTE 6.3.1 may encounter start up issues when Hadoop is installed in a non-default location.

  This issue has been fixed in this release of the CTE Agent by adding a `-g` option to the `config-hadoop.sh` script for the non-default path.

- **AGT-29024 [CS0996021]: VTE uninstall script also removes VAE folders**

  For some versions of VTE 6.3.1, if you have both VTE and VAE installed, when you uninstall the VTE Agent, the uninstaller also incorrectly deletes any VAE files in the VTE installation directory.

  This issue has been fixed in this release of the CTE Agent.

- **AGT-28931 [CS0994479]: VTE makes python3_check.sh world writable**

  For some versions of VTE 6.3.1, the VTE Agent assigned incorrect file permissions to the `python3_check.sh` file that allowed other users to write to that file (permission settings `rwxr-xrwx`).

  This issue has been fixed in this release of the CTE Agent and the file permissions are set to `rwxr-xr-x`.

- **AGT-28704 [CS0989919]: VTE generates recurring kernel error messages when deploying VTE with Linux container policies**

  For some versions of VTE 6.3.1, kernel error messages are raised when VTE is deployed with Docker containers in certain circumstances. The issue is related to an incorrect namespace used to generate some of the information for the VTE audit log messages, resulting in incomplete audit log entries and potentially flooding the kernel message buffers with "task does not exist" error messages.

  This issue has been fixed in this release of the CTE Agent.

- **AGT-28789 [CS0992250]: Hadoop fails to start with error after VTE upgrade**

  For some versions of VTE 6.3.1, there is an issue that causes Hadoop to fail to start when VTE is installed.

  This issue has been fixed in this release of the CTE Agent.

- **AGT-28919 — LDT hangs when rekeying an Oracle database that is performing Async Direct I/O**

  For some versions of VTE 6.3.1, there is a deadlock issue with rekeying an LDT GuardPoint on an Oracle database performing Async Direct I/O. This mode of I/O operation by Oracle may cause VTE to freeze access to the entire GuardPoint either when key rotation is first launched or when it is in the final completion stage.

  This issue has been fixed in this release of the CTE Agent

- **AGT-28668 [CS0986323]/AGT-28781 [CS0992751]: Oracle hangs on large insert job after upgrading VTE**

  For some versions of VTE 6.3.1, there is an incorrect recursive lock acquisition in VTE direct I/O read code path.

  This issue has been fixed in this release of the CTE Agent.

- **AGT-28725: The ownership of the AWS credential file changes after a credential is added using voradmin**

  For some versions of VTE 6.3.1, adding a chunk size by a non-root user changes the permissions of the AWS credential store. This prevents other non-root users from adding or deleting credentials and chunk sizes from the AWS credential store.

  This issue has been fixed in this release of the CTE Agent.

- **AGT-28451 [CS0980110] - Systems with Docker and CTE crashing**

  For some versions of VTE 6.3.1, there is a potential issue with mishandling of certain docker volume paths. This issue may have an adverse effect on other operations running on the system.

  This issue is fixed in this release of the CTE Agent.

- **AGT-28311 - Cannot disable an IDT-Capable or Efficient Storage GuardPoint in “Data transformation failed” state due to failure to transform data on such GuardPoints**

  For some versions of VTE 6.3.1, if an IDT-Capable or Efficient Storage GuardPoint enters the "Data transformation failed" state, the user cannot manually disable that GuardPoint until the host has been rebooted after the cause of the data transformation failure has been corrected.

  In this release of the CTE Agent, users can disable an IDT-Capable or Efficient Storage GuardPoint in the "Data transformation failed" state.

- **AGT-28330 [CS09817270] — Machine crashes after upgrading to 6.3.0.127**

  For some versions of VTE 6.3.1, if files are added to an LDT-protected GuardPoint while the GuardPoint is disabled, and then those files are truncated or changed by the user after the LDT GuardPoint has been re-eneabled, this may cause CTE to crash.

  It is extremely important that you do not allow anyone to access a guarded directory while the GuardPoint is disabled.

  The CTE Agent ignores such files if certain file attributes have changed.

- **AGT-27830 — Sparse data files may be corrupted with LDT**

  For some versions of VTE 6.3.1, LDT may not encrypt small sparse regions in files during initial data transformation. Sparse regions in CTE encrypted files are generally not encrypted as they are sparse. However, in some cases unaligned sparse regions must be encrypted, and LDT did not do so during initial data transformation. The discrepancy in encryption of small sparse regions results in corruption of data in those regions.

  This issue has been fixed in the current release of CTE Agent.

Known Issues

- **AGT-29799 — Object Set not defined error displays incorrectly after applying an In-place Data Transformation - Device policy to a GuardPoint**

  If you apply an In-place Data Transformation - Device policy to a GuardPoint, or if you rekey an ES GuardPoint or an IDT-Capable GuardPoint, the CTE Agent incorrectly logs one or more of the following messages: `No policy defined for [Object] set [_empty-0_]`, `[SecFS, 0] PID[pid] Object Set (_empty-0_) not defined` and `[SecFS, 0] PID[pid] Object Set (_empty-0_) used but not defined`. These messages can be safely ignored.

- **AGT-27047 — Restoring a file fails during lazy rekey transformation**

  If a GuardPoint is undergoing lazy rekey transformation and you attempt to restore a file from backup, accessing the file before the lazy rekey and restore operations have completed can lead to data inconsistencies in the target file.

  Make sure that all lazy rekey and restore operations have fully completed before you access the file.

Advisories

End of Support for Ubuntu 16.04

Thales announces the removal of support of Ubuntu 16.04 LTS operating system in CTE 7.0.0.47. This release will be the *last* version to support the Ubuntu 16.04 LTS operating system. Thales engineering and support will continue to provide new kernel validations and bug fixes for CTE 7.0.0 on Ubuntu 16 until the next CTE version is available.

We request our customers who have Ubuntu 16 environments protected by CTE to update those systems to newer, supported versions of Ubuntu.

End of Support for Red Hat Version 6

Thales announces the removal of support of the RHEL version 6 operating system in CTE 7.0.0.47. This release will be the *last* version to support RHEL version 6. Thales engineering and support will continue to validate RHEL 6 kernel patches for CTE on the 7.0.0 branch for critical security updates, and will fix any bugs raised through November of 2020, which corresponds to the end of Red Hat's Maintenance Support 2 (Product Retirement) phase.

We request our customers who have RHEL 6 environments protected by CTE to update those systems to newer, supported versions of RHEL.

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://cpl.thalesgroup.com/
- CPL_Sales_AMS_TG@thalesgroup.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.