CipherTrust Transparent Encryption (CTE) for Linux

Release Notes

- **Release: 7.2.0.128**
- **Date: February 04, 2022**

New Features and Enhancements

Release 7.2.0.128 of CipherTrust Transparent Encryption (CTE) for Linux adds new features, fixes known defects, and addresses known vulnerabilities.

LDT for NFS

- Live Data Transformation is now extended to network share deployments through a distributed architecture system, which allows users to encrypt data on NFS shares without any application downtime. CTE agents can support encryption of data workloads for both direct-attached storage and network shares with zero encryption downtime and automated key rotation capabilities, to meet compliance requirements, without disrupting business applications.

CTE Certificate Renewal

- CipherTrust Manager now supports automatic renewal of communication certificates with CipherTrust Manager. CTE Agent will attempt to renew the client certificates 60 days before their expiration date.

Cloudera

- CTE now supports Cloudera (CDP) 7.0 for RHEL 7.9 and RHEL 8.4.

CoSoSys Endpoint Protector

- CipherTrust Transparent Encryption is now compatible with CoSoSys Endpoint Protector v5.4.0.5 and subsequent versions.

Punch Hole Support for RHEL7 and RHEL 8

- CipherTrust Transparent Encryption now supports Punch Hole operations. This allows applications to free unused portions of the file and reclaim disk space.

Scheduled upgrade feature

- You can now schedule an upgrade with a custom binary extraction path directory for storing the temporary files it needs during the upgrade.

Improved Log Details

- Learn mode will now include process ancestor information in the Denied Message log entries.

Improved Host Settings

- The host/client settings entries are used to specify which binaries can be trusted by CTE to authenticate users.You can now use wild card settings and signature sets, in the host/client settings, to restrict access to unauthorized files.

Drop-in Files for systemd

- As an alternative to adding applications to the barrier file, you can use drop-in files to configure the `secfs-fs-barrier.service` file for dependency management using `systemd`. This eliminates the need to modify the `secfs-fs-barrier.service` file for configuring dependencies.

New Kernel Support

The following kernels are supported starting with the CTE v7.2.0 GA release:

Ubuntu 20.04.3

- 5.11.0-22-generic
- 5.11.0-25-generic
- 5.11.0-27-generic
- 5.11.0-34-generic
- 5.11.0-36-generic
- 5.11.0-37-generic
- 5.11.0-38-generic
- 5.11.0-40-generic
- 5.11.0-41-generic

Documentation Enhancements

- All CTE documentation is available at https://thalesdocs.com/ctp/cte/index.html.
- The CTE Compatibility Portal is now online.

> **Note:** The portal works best with Firefox and Chrome.

Resolved Issues

- **AGT-34207 [CS1069026]: AgentHealth script fails after registration**

  When the Agent Health script executes before registration and connection to the DSM succeeds, the script fails. For this situation, Thales added a new option `--w <value>` that allows a customer to add a retry operation in 10 second increments, with an upper limit of 1200 seconds (20 minutes).

  If the script completes in less than the timeout, it completes with a return of "0". If it does not complete, then it returns with an EAGAIN error which means that the DSM cannot connect with the agent.

- **AGT-36287 [CS1084169]: A compliance scan of port 7024 reported compliance issues with some TLS ciphers**

  New, compliant TLS ciphers were added to the software and non-compliant TLS ciphers were removed.

- **AGT-37466: Under heavy workloads, the syslog displays a `bad memhead` error message**

  The Syslog displayed the `bad memhead` error messages in `/var/log/messages`, under certain workloads, relating to CTE signature caches. This occurred when CTE detected freed memory and attempted to free it again.

Known Issues

CTE LDT

- **AGT-34000: Permission denied when removing secfs2 during upgrade to 7.2.0**

  When CTE is upgraded to v7.2.0 from a prior version, some warnings display at the end of the upgrade process. The warnings look similar to:

```
rm: cannot remove ‘/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/bin/secfs2’: Permission
denied
rm: cannot remove ‘/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/bin/secvm2’: Permission
denied
rm: cannot remove ‘/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/bin/.secfs2.mac’: Permission
denied
```

  This issue occurs because the newer product, v7.2.0, is installed first. This version protects the .sec directory. After this occurs, when the uninstall script of the older product is executed, the script then attempts to delete some files from the .sec directory, as part of the cleanup, resulting in permission denied warnings. Note that the order- of-execution of scripts is determined by the Linux distribution, so there is no way for Thales to change this order. This issue can be safely ignored.

- **AGT-36251: LDT disables read-ahead on files undergoing rekey on secondary hosts**

  As the result of disabling read-ahead, production workloads on secondary hosts may experience performance degradation if target files accessed for read/write are undergoing rekey. Performance degradation will persist during suspended rekey periods. This restriction will be relaxed during suspended periods in patch releases.

- **AGT-36269: Rekey does not continue when a secondary host crashes during active rekey**

  The primary CTE client stops rekeying GuardPoints when a secondary CTE client crashes during rekey. To enable the primary CTE client to resume rekey, you must remove the failed CTE client from the LDT GuardPoint Group.

  After reboot, if secfs services activate, and the GuardPoints are enabled on the failed CTE host, then you must disable the GuardPoints on all active secondary CTE clients. Stop secfs services on the failed host, and run the voradmin command on the primary host, to remove the failed host from the LDT GuardPoint Group for those GuardPoints.

  Following these steps, the failed host can now enable the GuardPoints and join the LDT GuardPoint Group as an active member. Failure to remove the host will result in failed attempts on the primary CTE client to send subsequent LDT messages to the members of the LDT GuardPoint Group. This can result in files not rekeying and possibly being flagged in rekey error status.

- **AGT-37206: If the majority of CTE clients fail in an LDT Communication Group, LDT cannot recover**

  The majority of the CTE clients must be fully operational for proper LDT operations across all LDT GuardPoint Groups.

  The LDT Communication Group requires that the majority of CTE clients are active, in order for the LDT Communication Group to work properly. If 50% or more CTE clients fail, then the LDT Communication Group cannot recover from that situation. To fix this issue, you must either:

  - Reboot all of the CTE clients in the entire LDT Communication Group.
  - For **Windows**, restart `secfsd` through the **Control Panel > Services** page on all of the CTE clients in the entire LDT Communication Group.
  - For **Linux**, `/etc/vormetric/secfs restart`does not work because it tries to unguard the GuardPointfirst, and then remains in that state because it cannot communicate with the LDT Communication Group. You have to reboot the Linux virtual machines to fix this issue. Once all nodes have been reset, the LDT Communication Group re-establishes the cluster.

    > **Note:** Thales will fix this in a subsequent patch.

- **AGT-37481: Cannot disable a GuardPoint after renaming a file while rekey suspended**

  You may fail when attempting to disable a GuardPoint if a partially rekeyed file is renamed while LDT is suspended. You will have to reboot the host to clear this condition.

- **AGT-37495: Primary CTE client hits assertion after crashing replica node**

  Reboot the CTE client on which the `secfsd-comm` process crashes. Reboot is required to re-establish the membership of the CTE client with the LDT GuardPoint Groups for GuardPoints enabled on the primary CTE client. Failure to reboot may force the primary CTE client to halt and not resume rekey until the membership of the CTE client with the LDT GuardPoint Group is re-established.

- **AGT-37500: Enable LDT Communication Group to recover from a secfsd crash**

  You must reboot the CTE client on which the `secfsd` process crashes. Reboot is required to re-establish the membership of the CTE client with the LDT GuardPoint Group for GuardPoints enabled on the CTE client. Failure to reboot may force the primary CTE client to halt and not resume rekey until the membership of the primary CTE client with the LDT GuardPoint Group s are re-established.

- **AGT-37505: After successfully installing the agent, the secfsd.log file displays an error message**

  The error is benign when displayed on CTE clients that are **not** using LDT over NFS/CIFS. On CTE clients that are using LDT over NFS/CIFS, the error resolves once the LDT Communication Group configuration has completed correctly.

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/encryption/contact-us
- 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.