Guardium Data Encryption

Release Notes

- **Release: 6**
- **Version: 6.4.3.17026 (GDE 4.0.0.4)**
- **Date: October 16, 2020**
- **Document Version 1**

New Features and Enhancements

- **Change EXT_KID key parameter for migrations from RSA DPM**

  User has the option to make or prevent GDE Appliance from generating the EXT_KID attribute while creating, cloning, rotating or importing an agent key.

- **Host Group Navigation Improvement**

  Added a search box into the GDE GUI for hostgroups.

- **Host Update Improvements**

  You can now enable or disable "Registration Allowed" and "Communication Enabled" through the REST API using the host update method.

- **Multiple LDAP Forests**

  Prieviously, the GDE Appliance allowed for integration with one LDAP directory service. Now it allows for integration with multiple LDAP forests.

- **P11 asymmetric key wrap support**

  GDE Appliance now complies with the the PKCS11 specification so that keys can be wrapped as target asymmetric keys of any length and type using an RSA key. This on-demand manual extraction of GDE Appliance resident RSA key material provides for manual import into SAP Data Custodian.

- **Restful API can change appender's configuration setting**

  Using the REST API, users can change logging levels for a host.

- **Web Certificate to support SAN**

  Users can now use the Subject Alternative Name(s) in web certificates. It provides a structured method to define all of the domain names and IP addresses that are secured by the certificate. Defined options include: Email address, DNS name, IP address (IPv4, IPv6), Uniform resource identifier (URI), Object identifier (OID), Directory names or other names.

Resolved Issues

- **SRV-28725 [CS0959843]: GDE Appliance configured with DHCP renews hostname as your.name.here.com on reboot after upgrade**

  This has been resolved. Now, after rebooting, the hostname displays properly.

- **SRV-29117 [CS0977239:] GDE Appliance HA join fails with ERROR: Invalid command contains unsupported character [ha]**

  Fixed issue which prevented the user from using parenthesis in the password.

- **SRV-29329 [CS0981864]: GDE Appliance export logs not sorted by time**

  This has been fixed. You can now sort export logs by time.

- **SRV-29337 [CS0984383]: Unable to assign local administrator to a restricted domain**

  This has been fixed. The admins for the available domains now display correctly.

- **SRV-29432 [CS0984025]: LEEF/CEF/RFC5424 syslog format missing source IP info for failed login by valid user.**

  All syslogs now display the source IP address. The Source IP tag is appended in all of the syslog formats.

- **SRV-29436: Could not import AES key if there is an existing key name**

  Now, if the GDE Appliance imports a key and the key name already exists, it appends they key name with: _1

- **SRV-29438 [CS0990626]: GDE license file does not activate the KMIP Feature**

  Fixed issue so that the KMIP enabled option is activated in the UI.

- **SRV-29548 [CS0998510]: Vulnerabilities in GDE Appliance**

  Fixed SSL certificate issues.

Known Issues

- **SRV-14570: "Password Creation Method" and "Challenge Response" fields grayed out whenever the 'Key' option is checked**

  The Challenge and Response feature is not available for VAE, VKM, and VPTD agents, so therefore the Password Creation Method parameter does not apply. However, these fields are enabled on the UI for both of these agents.

- **SRV-18072: Arping fails for software GDE Appliance**

  Arping fails for GDE Appliance when the eth0 interface is renamed to en0 in RHEL 7+. Therefore, en0 should be available in arping under network diagnostics.

- **SRV-19930: AsymKey: During GenerateKeyPair, if Asym key template has CKA_END_DATE is set, it will be ignored and not set**

  Set the CKA_END_DATE using C_SetAttributeValue using the public key handle after calling GenerateKeyPair.

- **SRV-20104: A language does not display correctly in the GDE v3 Windows Enabler**

  Make sure that all necessary language packages are installed in your Windows system.

- **SRV-20105: GDE3 enabler -- canberra-gtk-module error fails to load on CentOS 7.2**

  Install the `libcanberra-gtk2.x86_64` package on your system.

- **SRV-20109: GDE3 enabler languages not showing correctly in ESXi CLI console**

  This is an ESXi issue.

- **SRV-22151: Expiration date does not change when x-deactivation-date is changed from the UI**

  Attributes should be modified from the client that utilizes the keys. Do not modify key attributes through the GDE Appliance UI. Changes may not be reflected in the table on the Agent > Keys page, or the operation may not complete.

- **SRV-22729: Europe/London Timezone showing BST instead of GMT+0**

  If the time zone is set to Europe/London time, which is marked as GMT +0:00, the actual time zone is British Summer Time marked as BST, which is an hour ahead during the summer. A workaround is to set the time to a GMT zone that does not use BST as follows:

  ```
  0001:dsm$ maintenance
  0002:maintenance$ gmttimezone set Europe/London
  Set timezone SUCCESS. Please restart server software to pick up
  the changes
  0002:maintenance$ time
  hour=18 min=26 sec=04 zone=BST
  Show system time SUCCESS
  0003:maintenance$ gmttimezone set Africa/Bamako
  Set timezone SUCCESS. Please restart server software to pick up
  the changes
  0004:maintenance$ time
  hour=17 min=30 sec=05 zone=GMT
  Show system time SUCCESS
  ```

- **SRV-24062: SSH key-based authentication changed after GDE Appliance upgrade**

  After setting up an initial ssh connection to a GDE Appliance server from a client machine, and saving that GDE Appliance server machine host key in `/etc/ssh/known_hosts` on the client machine, user upgrades the GDE Appliance. After upgrading, when user tries to establish an ssh connection with the GDE Appliance server from the same client machine, user finds that the host key has been changed.

- **SRV-26903: Prompted for smart card pin every minute or so while logged into GDE Appliance**

  This is a browser-related bug for Microsoft browsers. It is not a GDE Appliance bug. Try using a different browser, such as FireFox.

- **SRV-26985: Gencert fails on secondary nodes in the GDE Appliance cluster, but shows new identifier and creation date**

  Manually rotate the master key to solve this issue.

- **SRV-28360 | 29106: SNMP ports blocked on joining HA node**

  The workaround, to open the port, is to disable and enable SNMP manually in the GUI on the joining node. Go to (**System > SNMP > Configuration**) to toggle snmp off/on.

- **SRV-28560 [CS0938688]: Extreme slowness accessing Logs page after upgraded to 6.2.12050**

  Adjust the log file intake rate for the **Audit Log File Queue Size** from the Logging Settings page. (System > Log Preferences > Server)

Supported Agent Operating Systems & Applications

All of the compatibility information is now in a separate document. It is called the:

- <release_date>_DSM_VAE_VTS_VKM_VPTD_Compatibility_Matrix.pdf

Upgrade to Version 6.4.3.17026 (GDE 4.0.0.4)

Software Upgrade

Refer to the GDE Appliance Installation and Configuration Guide for details about how to upgrade your software. Thales strongly recommends that you backup your GDE Appliance configuration before you upgrade your GDE Appliance software.

GDE Appliance Browser Support

The GDE Appliance Web GUI supports the following browsers:

- Internet Explorer 10, 11
- Firefox
- Chrome

End of Life

- **SRV-27819: 3DES is no longer available for new key creation. However, GDE Appliance will continue to support legacy keys created with 3DES**
- **SRV-28176: The following CLI command has been deprecated:**

  ```
  0002:network$ ip diag
  ```

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
- 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.