GUARDIUM DATA ENCRYPTION

Release Notes for Guardium Data Encryption

Version: GDE v4.0.0.2 (DSM 6.4.0.15031)

Date: December 23, 2019

New Features and Enhancements

Cloud Object Storage Encryption

GDE now provides encryption and protection for data that resides in the Amazon S3 buckets running in the AWS cloud environment. (Available with VTE 6.3.0)

DHCP

Admin can allow/disallow static DNS settings when a network uses a DHCP server.

Disabling All Administrators in a Domain

All/Sys Admins can prevent Domain Administrators from being able to disable all administrators in a domain.

Efficient Storage Device for IDT

Modified Efficient Storage GuardPoints for use as IDT GuardPoints for a specific customer. IDT is used for the offline transformation of ESG devices that already contain user data.

Encryption Key Protection

VTE can encrypt keys that are cached in kernel memory. (Available with VTE 6.3.0)

LDAP

You can now configure the duration for which the GDE tries to connect to the LDAP server. The limits have been raised: [maximum time: 600s].

Additionally, the maximum number of LDAP records that can be imported is now 1 million.

Luna

You can now attach a Luna HSM to the V6000 and virtual GDEs.

Smart Card

The GDE now supports using Smart Cards for access control.

Switch Hosts

An administrator can change the host source from a network DNS server to the local `/etc/hosts` file to improve performance.

Resolved Issues

- **SRV-24789 [Zen 77604]:** GDE **log not registering any SSH logins or disconnected sessions**

  Rebooting the GDE solved the issue.

- **SRV-28059 [CS0 926242]: Vulnerabilities in 6.1.0.9229 and 6.2.0.12050**

  Vulnerabilities have been fixed.

- **SRV-15064 [Zen 25308]: Cannot import the EC Cert, the public keys or digital signatures do not match**

  This has been fixed. Now a mixed web certificate is allowed, i.e. one with an ECC key and RSA signature.

- **SRV-26850 [Zen 93630]: LDAP login and case sensitivity problem**

  Added a feature in the General Preferences > Password section: **Ignore Login Username Case**. When enabled, user names are case **in**sensitive. Hence, lower and upper case letters are treated the same. Disable this control to make login names case sensitive.

- **SRV-27543 [Zen 100506]:** GDE **KMIP license is not enforced**

  This has been fixed. The license is now enforced.

- **SRV-27891 [CS0 923385]: Host Group list follows random sorting order**

  Converted Host Group name header to sortable table header. Added sorting capability on name column. Default ordering is ascending, which toggles upon clicking name header.

- **SRV-28156: Failed to restore** GDE **configuration with different Luna HSMs**

  After restoring the configuration to a GDE, run the command: `HSM > Luna add` on that GDE.

- **SRV-28295: Nodes are not joining to the HA cluster**

  When trying to join nodes in wide geographic areas, DNS and other network factors become obstacles. By adding a whitelist to each joining node, the operation improves.

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-19825:** GDE **DHCP does not configure NTP server**

  Configuring the NTP server manually works.

- **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-20532: Getting 'Operation Not Complete' error after login to GDE Appliance**

  This error occurs intermittently. This seems to happen on systems with an excessive amount of VAE keys. It has no impact on functionality.

- **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: GDE Appliance - 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-25645 [Zen 84735]: x-key-state attribute is present, but expired after upgrade to 6.1.0**

  Key state is not supported for non-versioned keys so the x-key-state does not affect users.

- **SRV-26154: Cannot create** GDE **HA cluster on AWS with static public IP address**

  For AWS deployments, you must manually add an entry for every other node in the HA cluster to `/etc/hosts`. Note that the hosts file will already contain an entry for the GDE from which you are working. In the CLI menu, switch to the network menu and type:

```
0001:network$ host add <HOST_NAME> <IP_ADDRESS>
```

Example:

```
0001:network$ host add dsmHA1.compute.amazonaws.com 192.68.10.1
```

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

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

- **SRV-26967: Support Smart Card authentication for RESTful API**

  Currently, you can only authenticate the smart card through the GUI.

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

  You can now manually rotate the master key to solve this issue.

- **SRV-28065:** GDE **cannot discern between the two styles used for the Cloud Object Storage GuardPoints**

  Use only one GuardPoint style:

  - **Path style**: https://s3.amazonaws.com/vte-repository
  - **Virtual host style**: https://vte-repository.s3.amazonaws.com

Supported Agent Operating Systems & Applications

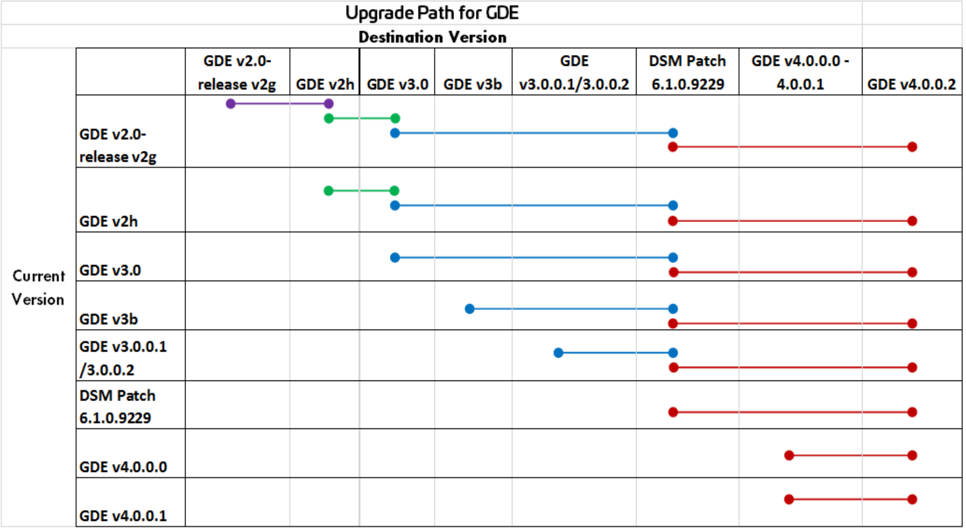
All of the compatibility information is now in a separate document. It is called the:

- ***<release_date>*_DSM_VAE_VTS_VKM_VPTD_Compatibility_Matrix.pdf**

Upgrade to Version 4.0.0.2

Software Upgrade

The following illustration describes the paths for upgrading from your current version to your destination version.



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 Browser Support

The GDE Appliance Web GUI supports the following browsers:

- Internet Explorer 10, 11
- Firefox
- Chrome

Hypervisor Support

The GDE Appliance can be installed on the following hypervisors:

- VMware 6.0 or higher
- Microsoft Hyper-V 2012R2, 2016 and 2019
- KVM
- SLES 12 SP3 with Xen v4.9

End of Life

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

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

Sales and Support

Technical Support

- https://supportportal.thalesgroup.com/csm

Sales

- **Email questions to** sales@thalesgroup.com **or call 888-267-3732**

Notices and License

Vormetric Data Security Platform
Vormetric Data Security Manager 6.4.0.15031
Release Notes v1