IBM® Guardium Data Encryption

Installation & Configuration Guide

Release 3.0.0.2

IBM Guardium Data Encryption 3.0.0.2 is the same product as Vormetric Data Security (VDS) Release 6.1.0.   VDS Release 6 consists of Data Security Manager and Vormetric Agents.

Vormetric Data Security Platform

Installation and Configuration Guide

Release 6

Version 6.1.0

Documentation v1
September 6, 2018

Vormetric Data Security Platform
Installation and Configuration Guide
v3.0.0.2 for IBM GDE
Vormetric Data Security Manager

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

Thales Data Security includes a restricted license to the embedded IBM DB2 database. That license stipulates that the database may only be used in conjunction with the Thales Vormetric Security Server. The license for the embedded DB2 database may not be transferred and does not authorize the use of IBM or 3rd party tools to access the database directly

Table of Contents

Preface

The *Data Security Manager*DSM Troubleshooting Guide describes how to install and configure the GDE appliance. This document is intended for system administrators who install the GDE appliance and connect it to a network.

DOCUMENTATION VERSION HISTORY

The following table describes the documentation changes made for each document version.

Documentation Changes

Document Version	Date	Changes
GDE 3.0b v1	12/14/2017	GDE 3.0b release is the same as DSM release v6.0.2-patch. This release addresses several security issues.
GDE 3.0.0.1 v1	07/02/2018	GA release of GDE 3.0.0.1. The GDE 3.0.0.1 release is the same as DSM release v6.0.3. This release introduces support for nShield Connect Integration, Automatic registration of LDT/Docker hosts,and Bring Your Own Encryption Keys (BYOK).
GDE 3.0.0.2 v1	08/24/2018	GA release of GDE 3.0.0.2. The GDE 3.0.0.2 release is the same as DSM release v6.1.0. V6000 and virtual appliances can now be HSM-enabled by connecting them to an nShield Connect appliance.

ASSUMPTIONS

This documentation assumes that you have knowledge of your computer network as well as network configuration concepts.

For more information about what’s new in this release, refer to the *GDE v3.0.0.2 Release Notes*. Refer to the *GDE Administrators Guide* for how to administer your GDE Appliance and to the various agent guides for information about Vormetric Data Security Agents.

SERVICE UPDATES AND SUPPORT INFORMATION

The license agreement that you have entered into to acquire the Thales products (“License Agreement") defines software updates and upgrades, support and services, and governs the terms under which they are provided. Any statements made in this guide or collateral documents that conflict with the definitions or terms in the License Agreement, shall be superseded by the definitions and terms of the License Agreement. Any references made to “upgrades” in this guide or collateral documentation can apply either to a software update or upgrade.

SALES AND SUPPORT

For support and troubleshooting issues:

- http://help.thalesesecurity.com
- http://support.vormetric.com
- support@thalesesecurity.com
- (877) 267-3247

For Thales Sales:

- http://enterprise-encryption.vormetric.com/contact-sales.html
- sales@thalesesec.net
- (408) 433-6000

Installing & Configuring GDE

1

This chapter describes how to install the IBM Guardium Data Encryption (GDE) virtual appliance as a standalone, primary, or failover server.

Overview

The the IBM GDE virtual appliance helps you protect structured and unstructured data and meet compliance requirements. It provides centralized encryption key and policy management to simplify data security management.

In conjunction with the GDE appliance, VTE/VAE/VTS/VPTD agents enable data-at-rest encryption and the collection of security intelligence logs without re-engineering applications or infrastructure.

Installation Process

The installation process includes the following steps:

1. Download the CI9V9EN.tar file from the IBM Passport website and extract the files. The tarball contains the following files:
   - GDE_PreReq_Download_Credential.bin
   - GDE_3.0.0.2.bin
   - GDE_README.txt
2. Run the GDE_PreReq_Download_Credential.bin file to generate the credentials required to log on to the Thales eSecurity website and download the GDE Appliance OVA file.

NOTE: The GDE_PreReq_Download_Credential.bin must be run in a Linux GUI. Console (CLI) mode is not supported.

3. Run the enabler; GDE_3.0.0.2.bin, to extract a license for the GDE appliance. You will need to upload this license once the GDE appliance is deployed and configured.

4. Deploy the OVA file on your ESXi server.
5. Configure the appliance.

Extract the GDE appliance license

1. Run the enabler file (GDE_3.0.0.2.bin) downloaded from the IBM Passport website. The file must be run on a RedHat or CentOS 6/7 system. To run the file type the following at the prompt:

   ```
   ./GDE_3.0.0.2.bin
   ```
2. Select a language to display the instructions and the EULA, by entering a number that corresponds to that language.
3. Accept the default location to install the license, or follow the on-screen instructions to save it to another location. Press ENTER to continue.
4. Accept the license agreement.
5. The license will be saved on your system in the default location or to the one you specified.

Make sure you can access the system on which you have saved the license from the GDE appliance. You will need to upload this license file to start using the appliance.

Installing the GDE Appliance

This section describes the steps to build a GDE appliance.

System Requirements

- VMware ESXi v5.5 or later with v9 hardware or later
- VMware vSphere Client
- GDE virtual appliance OVA file

These instructions assume the IP address, routing configuration, and DNS addresses for the GDE, appliance allow connectivity to all hosts where the Vormetric Agents are installed.

Hardware Requirements

The hardware hosting the virtual machine must meet the following requirements:

Table 1: Virtual machine hardware requirements

	Number of Agents			
	1 to 10	**11 to 50**	**51 to 250**	**Over 250**
Number of CPUs	2	4	4	6
RAM (in GB)	4	8	12	16
HD (in GB)[a]	250	250	250	above 250

a. The disk size change was introduced in v5.3.1, however you can still use "thin" provision to minimize storage utilization.

Installation Plan

1. Assemble configuration information using the checklist, see "GDE Appliance Installation Checklist".
2. Complete the pre-configuration tasks described here "Installation and Pre-Configuration tasks", if applicable.
3. Deploy the GDE appliance as described here, "Deploying the GDE Appliance".
4. Setup initial and basic configurations as described here, "Configure the appliance".
5. Verify Web access as described here, "Verify web access".

GDE Appliance Installation Checklist

Table 2: Installation Checklist

REQUIREMENT	VALUE
Software requirements	
DSM - Virtual Machine file from Support.	
Hardware requirements for Virtual Machine	
1 virtual socket, 4 cores per socket	
4GB memory	
2 virtual NIC cards	
250GB virtual disk	
Network Information	
eth0—dhcp by default.	IP address netmask default gateway (optional)
eth1—this comes configured with a default IP address 192.168.10.1. We recommend that you retain this configuration in the event that you need a recovery option to access the appliance.	IP address netmask default gateway (optional)
bond0—this interface is used when the eth0 and eth1 interfaces are aggregated into a single logical interface for load balancing./fault tolerance. If configured, the bond0interface supersedes the eth0 and eth1 interfaces, and must be used to access the GDE appliance.	IP address netmask default gateway (optional)
Primary GDE appliance Hostname: FQDN	
Failover GDE appliance Hostname: FQDN	
Domain Name Server (DNS) addresses - up to 3 plus optional DNS search domains.	
NTP server FQDN or IP address (if applicable)	
Certificate Information	
GDE appliance Hostname: FQDN	
Name of your organizational unit	
Name of your organization	

Name of your city or locality. Must be fully spelled out, no abbreviations.	
Name of your state or province. Must be fully spelled out, no abbreviations, e.g., California *not* CA	
Two-letter country code	

Installation and Pre-Configuration tasks

Host name resolution

You can map a host name to an IP address using a Domain Name Server (DNS). DNS is the most preferred method of host name resolution. If you are not using DNS, you need to modify the */etc/hosts* file on the GDE appliance or identify a host using only the IP address. If you're using the GDE appliance in a high availability (HA) configuration, you need to modify the */etc/hosts* file on each cluster node. Additionally, you must modify the */etc/hosts* file on *each* protected host (hosts on which the file encryption agents are installed) making sure to add an entry for all GDE appliance nodes (if using HA).

Port configuration

If a GDE appliance must communicate with a device behind a firewall, you must open various ports in the firewall.

The following table lists the communication direction and purpose of each port you must open.

Table 3: Ports to configure

Port	Protocol	Communication Direction	Purpose
22	TCP	Management Console → GDE	CLI SSH Access
443	TCP	Browser → GDE	TCP port used to browse the GDE appliance URL without specifying the port. By default it redirects to 8445. If you switch to "suite b" mode, then it redirects to 8448.
161/7025	TCP/UDP	SNMP Manager → GDE GDE ↔ GDE	SNMP queries from an external manager and to get failover node response times.

Table 3: Ports to configure

8080	TCP	Agent → GDE GDE ↔ GDE	Port 8080 is no longer used for registration, but you can manually close/open this legacy port for new deployment, forbackward compatibility if you use previous versions of the agent and need to register to 8080. **Syntax** `# security legacyregistration [ on | off | show ]`
8443	TCP	Agent → GDE	Fallback RSA TCP/IP port through which the agent communicates with the GDE, in case 8446 is blocked. The agent establishes a secure connection to the GDE appliance, via certificate exchange, using this port.
8444	TCP	Agent → GDE	Fallback RSA port via which the Agent log messages are uploaded to GDE, in case 8447 is blocked.
8445	TCP	Browser → GDE GDE ↔ GDE (fallback)	Management Console, VMSSC, and fallback for RSA HA communication in case port 8448 is blocked.
8446	TCP	Agent → GDE	Configuration Exchange using Elliptic Curve Cryptography (Suite B).
8447	TCP	Agent → GDE	Agent uploads log messages to GDE using Elliptic Curve Cryptography (Suite B).
8448	TCP	Browser → GDE GDE ↔ GDE	GUI management during enhanced security using Elliptic Curve Cryptography (Suite B). Also for secure communication between GDE appliances in HA clusters.
50000	TCP	GDE (primary) → GDE (failover)	HA information exchange
Host port to open			
7024	TCP	GDE → Agent	GDE appliance uses this port to push policy and/or configuration updates to the host on which the Agent is installed.

Access the Command Line Interface (CLI)

The CLI commands are used to configure the appliance. The commands are grouped into the following categories or *submenus*. Entering ? on the CLI command line lists those categories:

```
0000:dsm$ ?
network      Networking configuration
system       System configuration
hsm          HSM configuration
maintenance  System maintenance utilities
```

```
ha            HA configuration
ipmi          IPMI configuration
user          User configuration
exit          Exit
```

To enter a submenu, enter a name or just the first few letters of the name. To display the commands for that submenu, enter a ?. For example, the submenu `maintenance` is used to provide maintenance utilities:

```
0001:dsm$ main
0038:maintenance$ ?
showver       Show the installed VTS version
ntpdate       Set ntp services
date          Set system date
time          Set system time
gmttimezone   Set system time zone
diag          OS diagnostics
up            Return to previous menu
exit          Exit
```

Every command has usage and example input. Type the command without a value:

```
0039:maintenance$ ntpdate
usage: ntpdate {sync | add SERVER_ADDRESS | delete SERVER_ADDRESS | on |
off | show }
0040:maintenance$ date
month=Mar day=17 year=2015
Show system date SUCCESS
0041:maintenance$ time
hour=11 min=11 sec=36 zone=PDT
Show system time SUCCESS
0042:maintenance$ gmttimezone
usage: gmttimezone {list|show|set ZONE_NAME}
0043:maintenance$ diag
usage: diag [log [ list | view LOG_FILE_NAME] | vmstat | diskusage |
hardware | osversion | uptime ]
0044:maintenance$
```

You must enter the submenu to execute the submenu commands. For example, the reboot command is in the system submenu, so you would enter system, then enter reboot. To return to the main level when finished, enter up.

A complete description of the CLI commands can be found in the *Administrators Guide*.

Deploying the GDE Appliance

This section describes how to deploy the OVA file to create the appliance. The GDE appliance uses static IP addresses and cannot be assigned an address by DHCP.

1. Open the VMware vSphere Client.
2. Click **File > Deploy OVF template**.
3. Click **Browse** and locate the OVA file. Select the file and click **Next**. The *OVF Template Details* page appears.

   The file name format for the OVA file is *Vormetric DSM - Virtual Appliance<version>.OVA*
4. Click **Next**. The *Name and Location* page opens.
5. Type in a name for the Virtual Appliance and then click **Next**. The *Storage* page opens.
6. Select a destination for the Virtual Appliance and then click **Next**. The *Disk Format* page opens.

   Select the type of provisioning based on the storage characteristics for your system. The options are:

   - **Thick Provisioned Lazy Zeroed**: creates the VM and allocates all the blocks for the VM but doesn’t zero them.
   - **Thick Provisioned Eager Zeroed**: creates the VM, allocates and zeros all the blocks.
   - **Thin Provision**: creates the VM with just the header information, but it does not allocate or zero blocks.

   In the following example, we use **Thick Provisioned Lazy Zeroed**.
7. Select **Thick Provisioned Lazy Zeroed** and click **Next**. The *Ready to Complete* window opens.
8. Click **Finish** to deploy the Virtual Appliance. This takes a few minutes.
9. At the message **Completed Successfully**, click **Close**. The main screen of the vSphere Client appears.
10. In the left pane, select the Virtual Appliance you just created and then click the power on icon in the tool bar. It takes about a half hour to provision the VM and build the appliance.
11. To watch the output as the installation progresses, click the Console tab and click inside the console window. When the installation is finished, continue to the next section.

Configure the appliance

This section describes how to configure network settings, NTP, Time Zone and Date/Time, and the hostname. It describes how to configure a bonded NIC device type should you choose to use this feature. It also describes how to generate a certificate authority (CA), add console administrators, and verify Web access.

If you are setting up the GDE appliance in a high availability (HA) deployment, the appliance designated as the failover is configured as a standalone appliance, the same procedure as described here, and then converted to a failover server. For more about HA, refer to the *Administrators Guide*.

Configure network settings

1. Access the GDE appliance CLI and log in with the default login and password:

```
Login: cliadmin
Password: cliadmin123
```

2. The Thales EULA is displayed, type ‘y’ to accept and press **Enter**.
3. When prompted, type in a new password and press **Enter**. Reconfirm your password.

Warning! Do not lose this password.

4. Navigate to the *network commands* menu. Type,

```
0000:dsm$ network
```

5. Add an IP address for the GDE appliance. Type,

NOTE: We recommend that you retain the default eth1 IP address configuration in the event that you need a recovery option to access the GDE appliance.

```
0001:network$ ip address init <IP address>/<subnet mask (e.g. 16 or 24)>
dev eth0/eth1
```

Example: `ip address init 192.168.10.2/16 dev eth1`

IPv6 Example: `ip address init fa01::3:15:130/64 dev eth1`

NOTE: If you are connected via eth0 and you choose to configure eth0 with a new IP address, you will be disconnected at this step. Reconnect on the new IP address.

6. (Optional) You may choose to configure the eth0 interface instead of retaining the default IP address 192.168.10.1, if for example, you want the GDE appliance to communicate with agents on a different subnet, or access the Management Console from a different subnet. To configure an IP address for eth0, type,

   ```
   0001:network$ ip address init <eth0 IP address>/<subnet mask (e.g., 16
   or 24)> dev eth0
   ```

   Example: `ip address init 192.168.10.3/16 dev eth0`

   IPv 6 Example: `ip address init fa01::3:15:130/64 dev eth0`

   The following warning is displayed:

   ```
   WARNING: Changing the network ip address requires server software to be
   restarted.
   Continue? (yes|no) [no]:
   ```

   Type ‘yes’ to continue with the IP address configuration.

7. Add the IP address for the default gateway. Type,

   ```
   0001:network$ ip route add default table main.table dev [eth0 or eth1]
   via <IP address for the default gateway>
   ```

   Example: `ip route add default table main.table dev eth0 via 192.168.1.5`

   IPv 6 Example: `ip route add default table main.table dev eth0 via fa01::3:15:120`

8. Verify interface settings. Type,

   ```
   ip address show
   ```

9. Verify route settings. Type,

   ```
   ip route show
   ```

10. If you are using DNS, set the primary DNS server for the GDE appliance. Type,

    ```
    dns dns1 <ip address for dns server 1>
    ```

11. If you have a second or third DNS server, set them for the GDE appliance. Type,

    ```
    dns dns2 <ip address for dns server 2>
    ```

12. If you want to set the search domain, type,

    ```
    dns search <search_domain>
    ```

13. Show the DNS settings. Type,

    ```
    dns show
    ```

14. Return to the main menu. Type,

    up

Configure a bonded NIC device

This section describes how to aggregate the two NICs on the GDE appliance into a single logical interface to provide load balancing and/or fault tolerance. The bonded NIC device is called `bond0`.

On the virtual appliance, you must configure at least two NICs and define them as `eth0` and `eth1` in order to enable the bond0 device type. Any additional physical/virtual NICs are ignored. For virtual appliances where only one network connector is configured for a virtual machine, the `bond0` interface cannot be enabled—the network interface itself can be up but, no IP address can be assigned to it.

The NIC bonding setting is system specific. If it is to be used for all nodes in a cluster, it must be enabled on all nodes individually.

1. Access the GDE appliance CLI and login with your login credentials. If this is the first time you are logging in, then you will be required to accept the license agreement and change the default password, see "Configure network settings".
2. Navigate to the network commands menu;

   ```
   0000:dsm$ network
   0001:network$
   ```

3. Enable the bonded NIC;

   ```
   0001:network$ ip address init <ip_address>/<subnet_mask> dev bond0
   ```

   Example: `ip address init 1.2.3.4/16 dev bond0`

In the event that a bonded NIC is being configured after the initial configuration, or after the GDE appliance has been upgraded, if you want to reuse an IP address that was originally assigned to `eth0` or `eth1`, then you must delete that address from `eth0` or `eth1` first, and then reassign it to the `bond0` interface.

4. Add a default gateway for the `bond0` device;

   ```
   0001: ip route add default table main.table dev bond0 via
   <gateway_ip_address>
   ```

   Example: `ip route add default table main.table dev bond0 via 1.2.7.8`

If a `bond0` interface is configured after setting up the `eth0` and/or `eth1` interfaces, and it is configured with an IP address that is on the same subnet as a default gateway, that gateway configuration continues to apply. However, if you configure `bond0` with an IP address on a different subnet, you will have to reconfigure the default gateway.

5. You can change the bonding driver mode based on your requirements. There are seven modes available from 0-6. See "Bonding driver modes" for more information. Note however, that only the default options are available with each of the modes and these options cannot be changed.

   When the mode option is specified the speed option cannot be specified (i.e. the options mode and speed are mutually exclusive). In other words, bond0 does not take the speed option and both eth0 and eth1 don't take the mode option. However, the MTU and up/down options can still be used for the bond0 device.

   To set or change the mode type,

   ```
   0002:network$ ip link set bond0 mode <mode>
   ```

   Example: `ip link set bond0 mode 2`

   To see what mode is currently in use type,

   ```
   0002: network$ ip link show bond0
   ```

6. To disable or break up a bonded NIC type, you can use either the delete or flush command. Delete will only delete a specific IP address (multiple can be assigned) and flush will clear all assigned IP addresses.

   ```
   0003:network$ ip address delete <ip_address>/<subnet_mask> dev bond0
   ```

   or

   ```
   0003:network$ ip address flush bond0
   ```

   Routes that are associated with this bonded NIC device will also be deleted.

Bonding driver modes

The modes specify the bonding policies. The following modes are supported (see Table 4 below), but none of the options for the modes are configurable and take the default values for those modes, except for the `miimon` setting. The `miimon` setting specifies the MII link monitoring frequency in milliseconds, which determines how often the link state of each slave is inspected for link failures. The `miimon` setting has a value of 100 instead of the default value of 0.

Table 4: Bonding driver modes

Mode	Name	Description	Load-balancing	Fault tolerance
0	balance-rr	Round-robin policy. Transmit packets in sequential order from the first available through the last. This is the default mode for the bonded NICs.	Yes	Yes
1	active-backup	Active-backup policy: Only one slave in the bond is active. A different slave becomes active if, and only if, the active slave fails. The bond's MAC address is externally visible on only one port (network adapter) to avoid confusing the switch.	No	Yes

Mode	Name	Description	Load-balancing	Fault tolerance
2	balance-xor	XOR policy: Transmit based on the selected transmit hash policy. The default policy is a simple [(source MAC address XOR'd with destination MAC address) modulo slave count].	Yes	Yes
3	broadcast	Broadcast policy: transmits everything on all slave interfaces.	No	Yes
4	802.3ad	IEEE 802.3ad Dynamic link aggregation. Creates aggregation groups that share the same speed and duplex settings. Utilizes all slaves in the active aggregator according to the 802.3ad specification.	Yes	Yes
5	balance-tlb	Adaptive transmit load balancing: channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave.	Yes	Yes
6	balance-alb	Adaptive load balancing: includes balance-tlb plus receive load balancing (rlb) for IPV4 traffic, and does not require any special switch support. The receive load balancing is achieved by ARP negotiation. The bonding driver intercepts the ARP Replies sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of one of the slaves in the bond such that different peers use different hardware addresses for the server.	Yes	Yes

Configure NTP, time zone, date, time

You must have the correct time set on your GDE appliance(s) as this will affect system functions such as agent registration, log timestamps, high availability cluster synchronization, and certificate exchange. Although configuring an NTP server is not mandatory, it is strongly recommended.

1. Navigate to the *maintenance commands* menu. Type

   ```
   maintenance
   ```

2. Show the current ntpdate settings. Type

   ```
   ntpdate show
   ```

3. Add a new ntpdate server. Type

   ```
   ntpdate add <IP address/Hostname for the ntpdate server>
   ```

   Repeat this step for each ntpdate server.

4. Activate the ntpdate server connection. Type

```
ntpdate on
```

5. Show the current timezone settings. Type

```
gmttimezone show
```

6. Set the country and city where the GDE appliance resides. Type

```
gmttimezone set <country/city>
```

7. Set the date. (If you used `ntpdate synch`, this step is not necessary.) Type

```
date <mm/dd/yyyy>
```

8. Set the time. (If you used `ntpdate synch`, this step is not necessary.) Type

```
time <hh:mm:ss>
```

   Where *hh* is 00 to 23.

9. Verify your settings. Type

```
time
date
```

10. Return to the main menu. Type

```
up
```

Configure the hostname

1. Navigate to the *system* menu. Type,

```
0001:dsm$ system
```

2. Show the current setting. Type,

```
0002:system$ setinfo show
```

   The default host name in the output is *your. name.here*.

3. Set the hostname. You must enter the fully qualified domain name for the GDE appliance. Type,

```
0003:system$ setinfo hostname <FQHN>
```

   Example:

```
0003:system$ setinfo hostname securityserver.company.com
```

Generate the Certificate Authority

1. Generate a new certificate authority for the GDE appliance. Type

```
security genca
```

2. A warning is displayed, informing you that all agents and peer node certificates will need to be re-signed after the CA and server certificate have been regenerated, and the GDE appliance server software will be restarted. Type ‘yes’ to continue, the default is ‘no’.
3. Enter the FQDN of this appliance, the name displayed in ‘This Security Server host name [FQDN of the GDE appliance]’, should be correct if you entered the host name information in the previous sections correctly. Press **Enter** to accept the name.
4. Next, enter the information required to generate the certificate. Answer the prompts:

   a. What is the name of your organizational unit? []:

   b. What is the name of your organization? []:

   c. What is the name of your City or Locality? []:

   d. What is the name of your State or Province? []:

   e. What is your two-letter country code? [US]:
5. Once the certificate is signed, return to the main menu. Type

   ```
   up
   ```

Add CLI administrators (optional)

With separation of duties for good security practices, CLI administrators can only log into the CLI and administer the GDE appliance. Management Console administrators can only log on to the Management Console to administer the GDE appliance.

1. Navigate to the *users commands* menu. Type

   ```
   user
   ```
2. Add an administrator. Type

   ```
   add <administrator name>
   ```
3. When prompted, enter a password. The password criteria are:
   - Does not have repeating characters
   - Uses at least 1 upper and 1 lower case character
   - Uses at least 1 special character
4. Return to the main menu. Type up

Verify web access

The Management Console is a Web-based GUI used for day-to-day security and administration tasks. Open a browser and confirm access over HTTPS to either the GDE appliance hostname (if configured in DNS) or the IP address defined in "Configure network settings" on page 15.

Example URL:

```
https://securityserver.vormetric.com
```

If the URL doesn't work because, for example, port 443 is blocked by a firewall, specify port 8448.

Example:

```
https://securityserver.vormetric.com:8448
```

or specify port 8445. Example

```
https://securityserver.vormetric.com:8445
```

If the link still does not work, make sure all the necessary ports are open, see Table 3, "Ports to configure," on page 11.

The first time you connect to the appliance via a web browser, a self-signed certificate is used by default. Your browser will display a warning about the SSL certificate, follow the instructions on your browser to continue with the default self-signed certificate. You can configure the GDE appliance to use third party signed certificates after you have logged in for the first time. Refer to the *GDE Administrators Guide*, chapter 6 for procedures to do this.

The default user name and password to log on to the GDE appliance the for first time are; `admin` and `admin123`. You will be prompted to reset the password. The password criteria are:

- Does not have repeating characters
- Uses at least 1 upper and 1 lower case character
- Uses at least 1 special character

Upload a license file

The first time you log on to the GDE appliance, the dashboard displays "License file not found," and all you will see are the *Dashboard* and *System* tabs. You need to click **System**, select **License**, and then **Upload the license file**.

Upload the license file that you extracted from the enabler package.

After uploading your license file, all the other tabs for which you have licenses are displayed.

Upgrading GDE Appliance Software

2

If you are using GDE Release 2.0, you cannot upgrade directly to GDE release 3.0.0.2. At a minimum, you must use GDE 2.0 release 2h and migrate from it to GDE 3.0.0.2. This chapter contains instructions for migrating data from GDE 2.0 release 2h to GDE 3.0.0.2. You can upgrade to GDE 3.0.0.2 from the following GDE versions:

- GDE 3.0
- GDE 3.0 release 3b
- GDE release 3.0.0.1

Migrating to a GDE 3.0 Appliance

You can upgrade your GDE appliance by backing up your current GDE appliance configuration and restoring it to a fresh installation of the new GDE appliance software.

The following tasks must be done to upgrade via a backup of the current installation configuration:

1. "Backup the current configuration"
2. "Install and configure a GDE appliance"
3. "Restore backup to new GDE appliance"
4. "Configure additional appliances as required"

Backup the current configuration

A backup is a snapshot of a GDE appliance configuration. When a backup is restored, the GDE appliance Management Console will contain and display the same information captured at the time the backup was originally made.

Create or import a wrapper key

GDE appliance backup files are encrypted with a wrapper key to keep them secure. This wrapper key must be created, or imported from a previous create operation, before creating a backup. The same wrapper key used to encrypt a backup is also required to restore that backup. For additional security, wrapper keys can be broken up into key shares—pieces of a wrapper key. These key shares can then be divided amongst two or more custodians, such that each custodian must contribute their key share in order to assemble a complete wrapper key. This is also referred to as split key knowledge or M of N configuration.

For example you can break up the wrapper key amongst a total of five custodians and set the minimum number of required custodians at two. When the wrapper key is required, at least two of the custodians must contribute their key share in order to assemble a complete wrapper key. The wrapper key must be created by an administrator of type System or All.

1. Log on to the Management Console as an administrator of type *System Administrator* or *All*.
2. Select **System > Wrapper Keys** from the menu bar.
3. In the *Wrapper Keys* window, select **Operation > Create**, then click **Apply** to create the wrapper key.
4. Select **System > Backup and Restore > Manual Backup and Restore** from the menu bar.

   A confirmation message also displays on this tab, stating that the wrapper key exists. You can now proceed with creating a backup.
5. Click **Backup** tab and select **Ok**.

NOTE: Some Browsers will automatically save and download the file. Some will display a Save as dialog.

6. Click **Save** in the File Download dialog box, if your browser displays one.
7. Save the file to a secure location that you are sure will still be accessible if the server fails.

   By default, the file name will be in the format: backup_config_<dsm server name>_yyyy_mm_dd_hhmm.tar. Where <dsm server name> is the FQDN of the DSM that is being backed up.
8. Return to the **System > Wrapper Keys** menu option and select **Operation > Export** to export key shares.
9. Set a number for both the **Minimum Custodians Needed** and the **Total Number of Custodians**.

   This setting splits the wrapper key value among multiple custodians. If only a single administrator is to control the wrapper key, enter a value of 1 in both fields.
10. Select the GDE appliance administrators who will serve as custodians for the wrapper key shares.

    Administrators of type *System Administrator* and *All* are listed. You can select any of these administrators, with the exception of the default initial log-on administrator *admin*, as a custodian.
11. Click **Apply** on the bottom right hand corner.

    If you have selected more than one custodian, each of them is given a share of the wrapper key. The wrapper key share is displayed on their **Dashboard** page, beneath the fingerprint for the CA, when they log into the Management Console. The generated wrapper key, or key shares, are exported and are visible on the **Dashboard**, beneath the fingerprint for the CA. The **Wrapper Key Share** displayed on the *Dashboard* is a toggle. Click **Show** to display the wrapper key share value. Each administrator must see a unique wrapper key share displayed on the dashboard beneath the fingerprint for the CA.

12. On the Dashboard, click **Wrapper Key Share** string to hide the value and display 'Show'.
13. Ensure the administrator(s) or wrapper key custodian(s) securely store a copy of this key or key share. This is required, as part of their role in a GDE appliance restore operation.

NOTE: Do NOT lose the wrapper key used to create the backup. You cannot restore the backup without the wrapper key that was used to create it.

14. Create a backup of the GDE appliance configuration after the wrapper key has been created.

Create a backup

1. Log on to the Management Console as an administrator of type *System Administrator* or *All*.
2. Select the **System > Backup and Restore** menu option. The *Manual Backup and Restore* page opens.
3. Click the **Backup** tab and then click **Ok**.
4. Click **Save** in the **File Download** dialog box. Save the file to a secure location that you are sure will still be accessible if the server fails. By default, the file name will be in the format:

   ```
   backup_config_<gde server name>_yyyy_mm_dd_hhmm.tar
   ```

   Where <*gde server name*> is the FQDN of the GDE appliance that is being backed up.
5. Save the backup to a secure location. Access to the backup should be limited to only a few employees and should be audited.

Install and configure a GDE appliance

In order to ensure the continuity of your GDE deployment, you must configure the new GDE 3.0 appliance with the same hostname as the GDE 2.0 appliance that is being migrated. You can assign a new IP address to the new GDE 3.0 appliance, however you must ensure that the hostname resolution method in use is correspondingly updated.

NOTE: A change in the GDE appliance hostname will cause a cause a conflict when you restore the backup of the old GDE appliance that is being migrated, if you are using a third party SSL certificate.
You will have to upload a new third party certificate with the new GDE appliance hostname.

If you configure the new GDE 3.0 appliance with the same hostname and IP address, you must take the old appliance off the network, otherwise any registered agents will try and communicate with both the old and the new GDE appliance and cause conflicts in your system.

If you configure a new GDE 3.0 appliance and give it a new hostname, and agents that were registered with the earlier GDE 2.0 appliance backup will have to re-register with the new GDE appliance. Refer to the *VTE Agent Installation and Configuration Guide* for detailed procedures to re-register agents.

For procedures to install and configure a GDE appliance, see "Installing the GDE Appliance".

Restore backup to new GDE appliance

The GDE appliance backup is restored via the Management Console.

1. Locate the backup that is to be restored
2. Log on to the Management Console as an administrator of type *System Administrator* or *All*.

NOTE: If you already have the Wrapper Key imported, skip to Step 7.

3. Import wrapper keys. Select **System > Wrapper Keys** from the menu bar.
4. Select **Import** from the **Operation** pull-down menu. Click **Add**.
5. If key shares have created from the wrapper key, paste a Key Share value from one previously stored with a custodian into the **Key Share** text field and click **Ok**.

   Repeat steps 5 and 6 for each administrator selected as a key custodian if you have chosen to have more than one custodian for the wrapper key. A key share must be imported for at least as many as were specified by the Minimum Number of Custodians value when the wrapper key was exported.
6. Click **Apply** to finish importing the wrapper key.
7. Restore the backup file. Select **System > Backup and Restore** from the menu bar.
8. Select the **Restore** tab.
9. Click **Browse**. Locate and select the backup file to restore.
10. Click **Ok**. The restored file uploads and the GDE appliance disconnects from the Management Console. The restore operation takes up to 30 minutes to complete.

    If the browser has not refreshed automatically after the restore operation, you must manually refresh the browser to log back on to the Management Console.

    If you were using a third party SSL certificate, this certificate will now also be restored as part of this operation. See "Verify web access" on page 21 for more details.

11. Log back on to the Management Console as an administrator of type *System* or *All*. Verify that the configuration is restored correctly

Your GDE appliance is now migrated to the new version.

Upload a license

As part of the process of configuring a new GDE 3.0 appliance, you will have already uploaded the GDE 3.0 license. However, once you restore a backup of the earlier GDE version, you will need to upload the license once again. Follow the steps to upload the license as described here, "Upload a license file".

Migrate a High Availability Configuration

To migrate a GDE 2.0 high availability deployment to GDE 3.0. Your current GDE 2.0 must be at release 2h. Refer to the GDE 2.0 release 2h documentation for instructions on how to upgrade to release 2h.

The procedure to migrate an HA deployment is as follows:

1. Log on to the primary and backup the GDE configuration, see "Backup the current configuration"
2. Configure a new appliance as described here, "Install and configure a GDE appliance". If you plan to configure the new appliance with the same FQDN and IP address, you must turn off the old appliance *before* bringing up the new appliance, otherwise any registered agents will try and communicate with both GDE appliances and cause conflicts in your system.
3. Restore the backup taken in step 1 to the newly configured GDE 3.0 appliance as described here, "Restore backup to new GDE appliance".

Configure additional appliances as required

To serve as failover nodes, as described in step 2 above. Convert these designated GDE appliances to failover server as described below:

1. Log on to the Management Console of the primary GDE node as an administrator of type *System*, or *All*.
2. Click **High Availability** in the menu bar. The *High Availability Servers* window opens.
3. The license must be installed on the primary node before HA can be configured.
4. Click **Add**. The *Add Server* window opens.
5. In **Server Name** field, enter the host name or FQDN of the server that is to be converted to a failover node. Click **Ok**.

That server is now listed in the High Availability Servers table with the role of **Failover**.

6. Log on to the CLI of the failover server, and access the High Availability sub-menu, at the prompt type:

```
 # ha
```

7. At the HA menu, type:

```
 # convert2failover
```

   Example:

```
0002:ha$ convert2failover
WARNING: We will now convert this server to failover server.
Please make sure the primary server is running and has this server on its
failover server list.
This may take several minutes.
Continue? (yes|no)[no]:
```

8. Type **yes** to continue and then follow the prompts:

   a. Type the host name or FQDN of the primary server.

   b. Type the name of an administrator of type System Administrator or All, configured on the primary node.

   c. Type the same administrator’s password.

   d. Press **Enter** to use the default name for the local host. Do not change this name.

9. Enter the certificate information and type **yes** to continue. The installation utility create the certificate, completes the installation process, and starts the server.
10. On the Management Console of the primary node, click the **Dashboard** tab. Match the fingerprint from the output on the failover node with the EC CA fingerprint on the Dashboard.
11. Click **High Availability** on the main menu. In the row for the failover node, the **Registered** check box should be selected.

After configuring the failover, you need to configure replication from the primary to the failover:

1. In the **Selected** column, select the failover node.
2. Click **Config Replication**. A dialog box opens, prompting you to continue.
3. Click **Ok**. The **Configured** check box for the failover node should be enabled after configuration completes.

   You will have to wait for the operation to complete and for the status to turn green, before you can verify the configuration changes.

4. Verify that the failover node configuration completed successfully. Check the *High Availability Servers* window on the primary node.

5. Repeat step for each failover node.

After all the failovers have been configured and replication is complete, the migration of your HA deployment is complete.

Troubleshooting

3

This section describes some troubleshooting procedures for your appliance.

Loss of Connection

If you have created GuardPoints and for some reason the appliance cannot be reached, the GuardPoints will continue to function with no issues. However, if the system is rebooted, the agent cannot access its configuration from the appliance and the GuardPoints cannot use the encryption key to encrypt or decrypt data unless you are using a cached-on-host key. Challenge and response and manual passwords are good way to provide business continuity in these situations.

Is the Management Console accessible?

1. Try to open a web browser with the correct address to the appliance (example: https://192.168.10.11:8445 or 8448 for Suite B mode).
2. Check if the appliance is a trusted site in your web browser's Security Options.
3. Netcat or Telnet to the GDE appliance and see if it's listening on port 8445. (8448 for Suite B mode.)

Check whether Agent communication ports are open from the UI

1. Use the Network Diagnostic checkport tool in the Management Console (or CLI) to check those ports.
2. Refer to the DSM Installation and Configuration guide for information about ports that need to be configured.

Glossary

G

access control
The ability of Vormetric Transparent Encryption (VTE) to control access to data on protected hosts. Access can be limited by user, process (executable), action (for example read, write, rename, and so on), and time period. Access limitations can be applied to files, directories, or entire disks.

admin administrator
The default DSM administrator created when you install the DSM. Admin has DSM System Administrator privileges and cannot be deleted.

Administrative Domain
(domains). A protected host or group of protected hosts on which an DSM administrator can perform security tasks such as setting policies. Only DSM administrators assigned to a domain can perform security tasks on the protected hosts in that domain. The type of VTE tasks that can be performed depends on the type of administrator. See also “**local domain**”.

administrator
See “**DSM Administrator and types**”.

Agent utilities
A set of utilities installed with the VTE agents and run on protected hosts. These utilities provide a variety of useful functions such as gathering protected host and agent configuration data, registering agents on the DSM, and encrypting data on the protected host.

All Administrator, **Administrator of type All**
The DSM Administrator with the privileges of all three administrator types: *System*, *Domain* and *Security*.

appliance
The DSM server. Often referred to as a *DSM virtual appliance*, which is the software version of the DSM to be deployed by the customers as a virtual machine.

asymmetric key cryptography
See *public key cryptographic algorithm.*

asymmetric key pair
A public key and its corresponding private key used with a public key algorithm. Also called a key pair.

authentication
A process that establishes the origin of information, or determines the legitimacy of an entity's identity.

authorization
Access privileges granted to an entity that convey an "official" sanction to perform a security function or activity.

block devices
Devices that move data in and out by buffering in the form of blocks for each input/output operation.

catch-all rule
The last policy rule that applies to any GuardPoint access attempt that did not fit any of the other rules in the policy.

certification authority or CA
A trusted third party that issues digital certificates that allow a person, computer, or organization to exchange information over the Internet using the public key infrastructure. A digital certificate provides identifying information, cannot be forged, and can be verified because it was issued by an official trusted agency. The certificate contains the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate-issuing authority (CA) so that a recipient can verify that the certificate is real. This allows others to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. The CA must be trusted by both the owner of the certificate and the party relying upon the certificate.

challenge-response
When a protected host is disconnected from the DSM, the GuardPoint data is not accessible to users. Challenge-response is a password-based procedure that allows users to gain access to their GuardPoint data during disconnection. Users run a utility, `vmsec challenge`, a seemingly random string (the challenge) is displayed. The user calls this in to their DSM Security administrator. The administrator returns a counter-string (the response) that the host user must enter to decrypt guarded data.

Character device
See ***"raw device."***

ciphertext
Data in its encrypted form. Ciphertext is the result of encryption performed on plaintext using an algorithm, called a cipher.

cleartext or plaintext
Data in its unencrypted form.

cryptographic algorithm
A computational procedure that takes variable inputs, including a cryptographic key, and produces ciphertext output. Also called a cipher. Examples of cryptographic algorithms include AES, ARIA, and DES.

cryptographic key
See "**encryption key**."

cryptographic signature
See “**signing files**.”

Database Encryption Key (DEK)
A key generated by Microsoft SQL when TDE is enabled.

Data Security Manager (DSM)
Sometimes called the *Security Server* or *appliance*. A Vormetric server that acts as the central repository and manager of encryption keys and security policies. Receives instructions and configuration from administrators through a GUI-based interface called the *Management Console*. Passes and receives information to and from VTE Agents.

dataxform
A utility to encrypt data in a directory. Short for “data transform.”

DB2
A relational model database server developed by IBM.

Decryption
The process of changing ciphertext into plaintext using a cryptographic algorithm and key.

Digital signature
A cryptographic transformation of data that provides the services of origin authentication, data integrity, and signer non-repudiation.

domains
See *administrative domains*.

Domain Administrator
The second-level DSM administrator created by a DSM *System Administrator*. The DSM *Domain Administrator* creates and assigns DSM *Security Administrators* to domains and assigns them their security “**roles**”. See “**DSM Administrator and types**”.

Domain and Security Administrator
A hybrid DSM administrator who is has the privileges of a DSM Domain Administrator and Security Administrator.

DSM
See ***“Data Security Manager (DSM).”***

DSM Administrator and types
Specialized system security administrators who can access the Vormetric DSM Management Console. There are five types of DSM administrators:

> *DSM System Administrator* - Creates/removes other DSM administrators of any type, changes their passwords, creates/removes, domains, assigns a Domain Administrator to each domain. Cannot do any security procedures in any domain.

Domain Administrator - Adds/removes DSM Security Administrators to domains, and assign roles to each one. Cannot remove domains and cannot do any of the domain security roles.

Security Administrator - Performs the data protection work specified by their roles. Different roles enable them to create policies, configure hosts, audit data usage patterns, apply GuardPoints, and so on.

Domain and Security Administrator - Can do the tasks of DSM Domain and Security Administrators.

All - Can do the tasks of all three of the DSM administrative types

DSM Automation Utilities
Also called VMSSC. A set of command line utilities that is downloaded and installed separately on the protected host or any networked machine. These utilities can be used by advanced users to automate DSM processes that would normally be done with the Management Console. See the *DSM Automation Reference* for complete details.

DSM CLI
A command line interface executed on the DSM to configure the DSM network and perform other system-level tasks. See the *DSM Command Line Interface* documentation

DSM CLI Administrator
A user who can access the DSM CLI. DSM CLI Administrators are actual system users with real UNIX login accounts. They perform tasks to setup and operate the DSM installation. They do not have access to the Management Console.

DSM database
A database associated with the DMS containing the names of protected hosts, policies, GuardPoints, settings, and so on.

DSM System Administrator
The highest level of DSM administrator. This administrator creates/removes other DSM administrators of any type, creates/removes domains, and assigns a Domain Administrator to each domain. The DSM System Administrator cannot perform any security procedures in any domain or system. This administrator is not related to computer or network system administrators.

EKM
See "**Extensible Key Management (EKM)**."

Encryption
The process of changing plaintext into ciphertext using a cryptographic algorithm and key.

encryption agent
See *Vormetric Transparent Encryption agent*.

encryption key
A piece of information used in conjunction with a cryptographic algorithm that transforms plaintext into ciphertext, or vice versa during decryption. Can also be used to encrypt digital signatures or encryption keys themselves. An entity with knowledge of the key can reproduce or reverse the operation, while an entity

without knowledge of the key cannot. Any VDS policy that encrypts GuardPoint data requires an encryption key.

Extensible Key Management (EKM)
An API library specification provided by Microsoft that defines a software framework that allows hardware security module (HSM) providers to integrate their product with the Microsoft SQL Server.

failover DSM
A secondary DSM that assumes the policy and key management load when a protected host cannot connect to the primary DSM or when a protected host is specifically assigned to the failover DSM. A failover DSM is almost identical to the primary DSM, having the same keys, policies, protected hosts, and so on.

FF1
See “Format Preserving Encryption (FPE)”.

FF3
See “Format Preserving Encryption (FPE)”.

file signing
See *signing files*.

File Key Encryption Key (FKEK)
The key used to encrypt the file encryption key that is used to encrypt on-disk data, also known as a wrapper key.

FKEK
See “File Key Encryption Key (FKEK)”

File System Agent
A Vormetric software agent that resides on a host machine and allows administrators to control encryption of, and access to, the files, directories and executables on that host system. For example, administrators can restrict access to specific files and directories to specific users at specific times using specific executables. Files and directories can be fully encrypted, while the file metadata (for example, the file names) remain in cleartext. Also called the “**VTE Agent**”.

Format Preserving Encryption (FPE)
An encryption algorithm that preserves both the formatting and length of the data being encrypted. Examples of such algorithms used by Vormetric include FF1 and FF3, both of which are approved by NIST. Vormetric’s **FPE tokenization format** uses the FF3 algorithm.

FQDN
Fully qualified domain name. A domain name that specifies its exact location in the tree hierarchy of the Domain Name Server (DNS). For example: `example.vormetric.com`.

GPFS
General Parallel File System is a high-performance shared-disk clustered file system developed by IBM.

GuardPoint
A location in the file system hierarchy, usually a directory, where everything underneath has a Vormetric data protection policy applied to it. The File System Agent intercepts any attempt to access anything in the GuardPoint and uses policies obtained from the DSM to grant or deny the access attempt. Usually, depending on the policies, data copied into a GuardPoint is encrypted, and only authorized users can decrypt and use that GuardPoint data.

Hardware Security Module or HSM
A tamper-resistant hardware device that stores keys and provides stringent access control. It also provides a random number generator to generate keys. The DSM Appliance can come with an embedded Hardware Security Module.

host locks
Two Management Console options, **FS Agent Locked** and **System Locked,** that are used to protect the File System Agent and certain system files. File System Agent protection includes preventing some changes to the File System Agent installation directory and preventing the unauthorized termination of File System Agent processes.

host password
This is not a regular login or user password. This is the password entered by a host system user to unlock a GuardPoint when there is no DSM connection. This password decrypts cached keys when the DSM is not accessible. The host must also be configured with **Cached on Host** keys. See "**challenge-response**".

initial test policy
A first data security policy applied to a GuardPoint that is used to gather directory access information so DSM Security Administrators can create a permanent operational policy. The initial test policy encrypts all data written into the GuardPoint; decrypts GuardPoint data for any user who access it; audits and creates log messages for every GuardPoint access; reduces log message "noise" so you can analyze the messages that are important to you for tuning this policy; is run in the "**Learn Mode**" which does not actually deny user access, but allows you to record GuardPoint accesses.

After enough data is collected, the DSM Security Administrator can modify the initial test policy into an operational policy.

Key Agent
A Vormetric agent that provides an API library supporting a subset of the PKCS#11 standard for key management and cryptographic operations. It is required for the following products: Vormetric Key Management (VKM), Vormetric Tokenization, Vormetric Application Encryption (VAE), Vormetric Cloud Encryption Gateway (VCEG). Sometimes called the *VAE Agent*.

key group
A key group is a collection of asymmetric keys that are applied as a single unit to a policy.

key management
The management of cryptographic keys and other related security objects (for example, passwords) during their entire life cycle, including their generation, storage, establishment, entry and output, and destruction.

key template
A template that lets you quickly add agent keys by specifying a template with predefined attributes. You can define specific attributes in a template, then you can call up the template to add a key with those attributes.

key shares
When data is backed up or exported from VTE (for example, symmetric keys or DSM database backups), they can be encrypted in a wrapper key needed to restore the exported data on the new machine. Wrapper keys can be split and distributed to multiple individuals. Each split piece of the wrapper key is called a *key share*. Decrypting the data requires that some specified number of the individuals that received key shares contribute their key share to decrypt the data.

key wrapping
A class of symmetric encryption algorithms designed to encapsulate (encrypt) cryptographic key material. The key wrap algorithms are intended for applications such as protecting keys while in untrusted storage or transmitting keys over untrusted communications networks. Wrapper keys can be broken up into *key shares*, which are pieces of a wrapper key. Key shares are divided amongst two or more *custodians* such that each custodian must contribute their key share in order to assemble a complete wrapper key.

Learn Mode
A DSM operational mode in which all actions that would have been denied are instead permitted. This permits a policy to be tested without actually denying access to resources. In the Learn Mode, all GuardPoint access attempts that would have been denied are instead permitted. These GuardPoint accesses are logged to assist in tuning and troubleshooting policies.

Live Data Transformation (LDT)
A separately licensed feature of Vormetric Transparent Encryption (VTE) that allows you to transform (encrypt or decrypt) or rekey GuardPoint data without blocking use or application access to that data.

local domain
A DSM domain in which DSM administration is restricted to Domain Administrators or Security Administrators assigned to that domain. To access a local domain in the Management Console, a DSM administrator must specify their local domain upon login.

Management Console
The graphical user interface (GUI) to the DSM.

Master encryption key (MEK)
The encryption key for Oracle Database used to encrypt secondary data encryption keys used for column encryption and tablespace encryption. Master encryption keys are part of the Oracle Advanced Security Transparent Data Encryption (TDE) two-tier key architecture.

MEK
See *Master encryption key.*

Microsoft SQL Server
A relational database server, developed by Microsoft.

Microsoft SQL Transparent Data Encryption (MS-SQL TDE)
Microsoft SQL Server native encryption for columns and tables.

multi-factor authentication
An authentication algorithm that requires at least two of the three following authentication factors: 1) something the user knows (for example, password); 2) something the user has (example: RSA SecurID); and 3) something the user is (example: fingerprint). VTE implements an optional form of multi-factor authentication for Management Console users by requiring DSM administrators to enter the token code displayed on an RSA SecurID, along with the administrator name each time the administrator logs on to the Management Console.

multitenancy
A VTE feature that enables the creation of multiple local domains within a single DSM. A local domain is a DSM domain in which DSM administration is restricted to Domain Administrators or Security Administrators assigned to that domain. This allows Cloud Service Providers to provide their customers with VTE administrative domains over which the customer has total control of data security. No other administrators, including CSP administrators, have access to VTE security in a local domain.

offline policy
Policies for Database Backup Agents. *Online policies* are for the File System Agent.

one-way communication
A VTE feature for an environment where the DSM cannot establish a connection to the agent, but the agent can establish a connection to the DSM. For example, the protected host is behind a NAT so protected host ports are not directly visible from the DSM, or the protected host is behind a firewall that prohibits incoming connections, or the protected host does not have a fixed IP address as in the cloud. When an agent is registered with one-way communication, changes made for that protected host on the DSM are not pushed to the protected host, rather as the protected host polls the DSM it will retrieve the change.

online policies
Policies for the File System Agent. *Offline policies* are for Database Backup Agents.

policy
A set of security access and encryption rules that specify who can access which files with what executable during what times, and whether or not those files are encrypted. Policies are created by DSM Security Administrators, stored in the DSM, and implemented on protected hosts by a File system Agent. See “**rule (for policies)**”.

policy tuning
The process of creating a simple Learn Mode policy that allows any protected host user to access a GuardPoint; to examine who accesses the GuardPoint, what executables they use, and what actions they require; and to modify the policy such that it allows the right people, using the right executable, performing the right action to do their job, and prevent anyone else from inappropriate access.

process set
A list of processes that can be used by the users in a user set associated with a policy rule.

protected host
A host on which a VTE Agent is installed to protect that host’s data.

public key cryptographic algorithm, public key infrastructure
A cryptographic system requiring two keys, one to lock or encrypt the plaintext, and one to unlock or decrypt the ciphertext. Neither key can do both functions. One key is published (*public key*) and the other is kept private (*private key*). If the lock/encryption key is the one published, the system enables private communication from the public to the unlocking key's owner. If the unlock/decryption key is the one published, then the system serves as a signature verifier of documents locked by the owner of the private key. Also called asymmetric key cryptography.

raw device
A type of block device that performs input/output operations without caching or buffering. This results in more direct access.

register host
The process of enabling communication between a protected host and the DSM. Registration happens during agent installation. Before registration can happen, the host must be added to the DSM database.

rekeying
The process of changing the encryption keys used to encrypt data. Changing keys enhances data security and is a requirement to maintain compliance with some data security guidelines and regulations. Also called *key rotation*.

roles
A set of Management Console permissions assigned to DSM Security Administrators by DSM Domain Administrators. There are five roles: *Audit* (can generate and view logging data for file accesses), *key* (can create, edit, and delete keys), *Policy* (can create, edit, and delete policies), *Host* (can configure, modify, and delete protected hosts and protected host groups), and *Challenge & Response* (can generate a temporary password to give to a protected host user to decrypt cached encryption keys when connection to the DSM is broken).

RSA SecurID
A hardware authentication token that is assigned to a computer user and that generates an authentication code at fixed intervals (usually 60 seconds). In addition to entering a static password, Management Console administrators can be required to input an 8-digit number that is provided by an external electronic device or software.

rule (for policies)
Every time a user or application tries to access a GuardPoint file, the access attempt passes through each rule of the policy until it finds a rule where all the criteria are met. When a rule matches, the *effect* associated with that rule is enforced. A rule consists of five access criteria and an effect. The criteria are Resource (the file/directories accessed), User (the user or groups attempting access), Process (the executable used to access the data), When (the time range when access is attempted) and Action (the type of action attempted on the data, for example read. write, rename and so on). *Effect* can be permit or deny access, decrypt data access, and audit access attempt. See *policy*.

secfs

1) The File System Agent initialization script. 2) An acronym for Vormetric Secure File System agent. It generally refers to the kernel module that handles policies (locks, protected host settings, logging preferences) and keys, and enforces data security protection.

secvm

A proprietary device driver that supports GuardPoint protection to raw devices. `secvm` is inserted in between the device driver and the device itself.

Security Administrator

The third-level DSM administrator who does most of data protection work like creating policies, configuring protected hosts, auditing data usage patterns, applying GuardPoints and other duties. The privileges of each Security Administrator is specified by the roles assigned to them by the Domain Administrator. See *roles*. See “**DSM Administrator and types**”.

Security Server

See “**DSM**”.

separation of duties

A method of increasing data security by creating customized DSM administrator roles for individual DSM administrators such that no one administrator has complete access to all encryption keys in all domains of all files.

signing files

File signing is a method that VTE uses to check the integrity of executables and applications before they are allowed to access GuardPoint data. If file signing is initiated in the Management Console, the File System Agent calculates the cryptographic signatures of the executables that are eligible to access GuardPoint data. A tampered executable, such as a Trojan application, malicious code, or rogue process, with a missing or mismatched signature, is denied access. Also called *cryptographic signatures*.

Suite B mode

A set of publicly available cryptographic algorithms approved by the United States National Security Agency (NSA). These algorithms enhance security by adding up to 384-bit encryption to the communication between the Web browser and the DSM, the DSM and Agent, and between DSMs in HA environments.

Symmetric-key algorithm

Cryptographic algorithms that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption.

System Administrator (DSM)

See “**DSM Administrator and types**”.

Transparent Data Encryption (TDE)

A technology used by both Microsoft and Oracle to encrypt database content. TDE offers encryption at a column, table, and tablespace level. TDE solves the problem of protecting data at rest, encrypting databases both on the hard drive and consequently on backup media.

user set

A named list of users on which a policy rule applies.

VAE Agent

See “**Key Agent**”.

VDE Agent

Vormetric agent installed on a protected host to implement disk encryption. See *Vormetric Disk Encryption (VDE)*.

vmd

Acronym for Vormetric Daemon, vmd is a process that supports communication between the DSM and kernel module.

VMSSC or Vormetric Security Server Command Line Interface

See *DSM Automation Utilities*.

Vormetric Application Encryption (VAE)

A product that enables data encryption at the application level as opposed to the file level as is done with VTE. Where VTE encrypts a file or directory, VAE can encrypt a column in a database or a field in an application. VAE is essentially an API library for key management and cryptographic operations based on PKCS#11. See the *Vormetric Application Encryption Installation and API Reference Guide*.

Vormetric Cloud Encryption Gateway (VCEG)

Vormetric product that safeguards files in cloud storage environments, including Amazon Simple Storage Service (Amazon S3) and Box. The cloud security gateway solution encrypts sensitive data before it is saved to the cloud storage environment, then decrypts data for approved users when it is removed from the cloud.

Vormetric Data Security Platform or VDS Platform

The technology platform upon which all other Vormetric products—Vormetric Transparent Encryption (VTE), Vormetric Application Encryption (VAE), Vormetric Key Management (VKM), Vormetric Cloud Encryption Gateway (VCEG), Vormetric Tokenization Server (VTS), Vormetric Key Management (VKM), and Vormetric Protection for Teradata Database—are based.

Vormetric Encryption Expert or VEE

Earlier name of the Vormetric Transparent Encryption (VTE) product. It may sometimes appear in the product GUI or installation scripts.

Vormetric Key Management (VKM)

Vormetric product that provides a standards-based platform for storing and managing encryption keys and certificates from disparate sources across the enterprise. This includes Vormetric encryption keys, 3rd-party software keys and so on.

Vormetric Protection for Teradata Database
Vormetric product that secures sensitive data in the Teradata environment.

Vormetric Security Intelligence
Vormetric product that provides support for Security Information and Event Management (SIEM) products such as ArcSight, Splunk and QRadar. Provides solutions that monitor real-time events and analyze long-term data to find anomalous usage patterns, qualify possible threats to reduce false positives, and alert organizations when needed. Documented in the VDS Platform Security Intelligence User Guide.

Vormetric Tokenization Server (VTS)
Vormetric product that replaces sensitive data in your database (up to 512 bytes) with unique identification symbols called tokens. Tokens retain the format of the original data while protecting it from theft or compromise.

Vormetric Transparent Encryption or VTE
Vormetric product that protects data-at-rest. Secures any database, file, or volume without changing the applications, infrastructure or user experience.

VTE Agent
Vormetric agents that are installed on protected hosts to implement data protection. See “**File System Agent**”.

wrapper keys
See “**key wrapping**”.

WSDL
Web Services Description Language.