THALES

Vormetric Data Security Platform

Transparent Encryption Agent Installation and Configuration Guide

Release 5.2.7

JANUARY 29, 2019
DOC V1

Vormetric Data Security Platform
Transparent Encryption Agent
Transparent Encryption Agent Installation and Configuration Guide
Release 5.2.7
January 29, 2019 Doc v1

NOTICES, LICENSES, AND USE RESTRICTIONS

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.

Contents

PREFACE

The *Transparent Encryption Agent Installation and Configuration Guide* describes how to install and configure Vormetric Transparent Encryption Agents (VTE Agents) (also known as File System (FS) Agents) on host machines. Once the agents are installed, data on that host can be protected.

Documentation Version History

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

Table 1: Documentation Version History

Software & Documentation Version	Date	Changes
5.2.6 v1	04/13/18	Added information for Oracle RAC with ASM and ASMLib.
5.2.7 v1	01/29/19	Added information on VTE compliance with AIX lock semantics, port configuration, and binary resigning.

SCOPE

This document describes how to install and configure VTE for AIX agents on AIX platforms.

INTENDED AUDIENCE

The *Transparent Encryption Agent Installation and Configuration Guide* is intended for system administrators who install and configure VTE on host machines.

Assumptions

This document assumes knowledge of network configuration. The system administrator must have root permissions for the systems on which VTE software is installed.

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in this guide or collateral documents that conflict with the definitions or terms in the License Agreement, shall be superseded by the definitions and terms of the License Agreement.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.

For support and troubleshooting issues:

- https://help.thalesesecurity.com/hc/en-us
- Email questions to support@vormetric.com or call 877-267-3247

For Thales Sales:

- http://enterprise-encryption.vormetric.com/contact-sales.html
- Email questions to sales@vormetric.com or call 888-267-3732

1 Overview

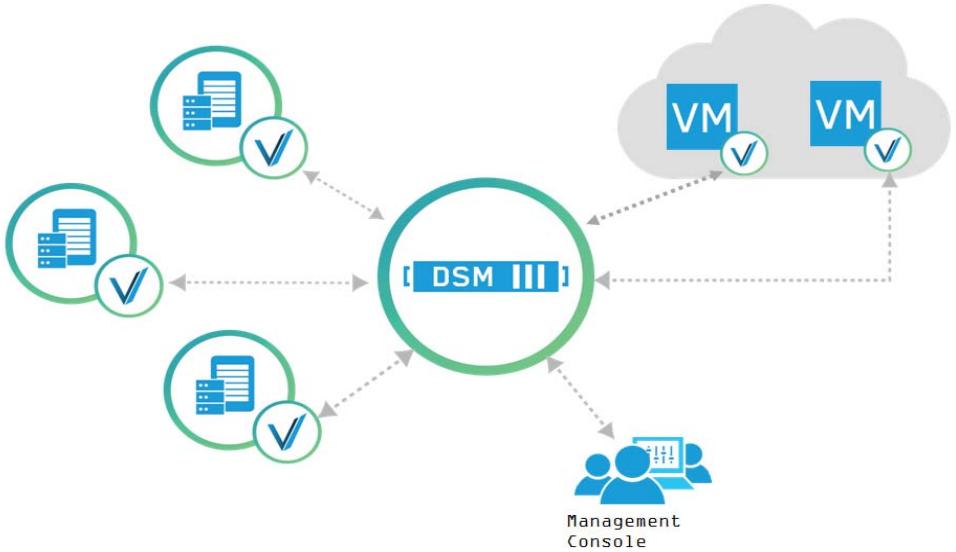
This document describes how to install and configure Vormetric Transparent Encryption (VTE) Agents (also called File System Agents) on host computers requiring data protection. These host computers are called *protected hosts*. VTE is supported in multiple operating system environments and can be deployed on physical devices as well as virtual environments.

VTE Overview

The VTE solution consists of a *Data Security Manager* (DSM) and one or more VTE agents residing on your *protected hosts*. Protected hosts contain your sensitive data. If connected to a NAS or SAN, the protected host has access to your sensitive data. Protected hosts can be on-site, in the cloud, or a hybrid of both.

The DSM is the central component of the VTE solution and is tasked with storing and managing data encryption keys, data access policies, administrative domains, and administrator profiles. Thales provides the DSM as either a security-hardened physical appliance or a virtual appliance. The agents communicate with the DSM and implement the security policies on their protected host systems.

Figure 1: Vormetric Transparent Encryption Architecture



In Figure 1, the *circled Vs* represent the VTE agents on protected hosts that may be physical or virtual machines. The *VMs* represent virtual machines in a cloud environment. Communication between agents and the DSM is encrypted and secure. DSM Administrators establish access and encryption policies through the *Management Console*, a browser-based, graphic-user-interface to the DSM.

VTE achieves security with complete transparency to end users with little impact to application performance. It requires no changes to your existing infrastructure and supports separation of duties between data owners, system administrators and security administrators.

What VTE does

Vormetric Transparent Encryption (VTE):

- Encrypts files and raw data
- Controls which users can decrypt and access that data
- Controls which processes and executables can decrypt and encrypt that data
- Generates fine-grained audit trails on those processes, executables, and users

With complete transparency to end users and applications, and with no changes to your existing infrastructure, VTE supports separation of duties and data access between data owners, system administrators, and Thales security administrators.

VTE protects data at rest. VTE can protect data residing on Direct Attached Storage (DAS), Network Attached Storage (NAS) or Storage Area Networks (SAN). This can be a mapped drive or mounted disk as well as through Universal Naming Convention paths.

VTE supports FIPS 140-2.

How to protect data with VTE

Data is protected by creating policies that specify file encryption, data access, and auditing on specific directories on your protected hosts. These directories are called *GuardPoints*. Policies specify whether or not the resting files are encrypted, who can access decrypted files and when, what level of file access auditing is desired, and so on.

Policies are created through the DSM GUI called the Management Console. Once the policies are created and pushed to protected hosts, the VTE agents implement those policies.

VTE compliance with AIX lock semantics

VTE is compliant with AIX lock semantics. There are cases, however, where VTE deviates from AIX lock semantics. Differences between AIX and guarded file locks are as follows:

- For a guarded file, an `fclear(2)` system call will block if the current process file location and specified `fclear` number of bytes overlaps an existing file lock.
- For a non-guarded file, the `fclear(2)`system call blocks only if the `fclear` number of bytes falls within the range limits of a specified file lock.

2 AIX Agent Installation

This chapter describes how to install and configure VTE on AIX systems. This process requires actions from two roles:

- The *Agent Installer* (also called the *Host Administrator*), who follows the instructions from this book
- The DSM *Administrator*

This chapter contains the following sections:

Installation Overview

The installation and configuration process consists of three basic steps:

1. Installing the agent on the protected host.
2. Adding the protected host FQDN or IP address to the DSM. This can be done manually by the DSM Administrator, or automatically using the Shared Secret Registration method.
3. Registering the protected host with the DSM so they can communicate with each other.

Before you can do these steps, complete "Pre-installation Tasks and Instructions" on page 6.

Assumptions

- The IP addresses, routing configurations, and DNS addresses allow connectivity of the DSM(s) to all hosts where VTE Agents are installed.
- If the protected host is a virtual machine, the VM is deployed and running.

Pre-installation Tasks and Instructions

This section lists tasks you must complete and information you must gather before installing VTE Agents:

General setup information

- Thales recommends that you install the agent in the default location.
- Do not install the Agents on network-mounted volumes such as NFS.

Determine your agent registration method

Protected hosts can be registered with the DSM using either the *Fingerprint method* or the default *Shared Secret method*.

- **The Fingerprint method**—Requires the DSM Security Administrator to add the fully qualified domain name (FQDN) or IP address of each protected host to the DSM before registering the agent.

  After registration, the installer of the agent passes the CA certificate to the DSM Security Administrator to verify that the protected host and DSM share valid certificates.

  If you choose the Fingerprint method, ask the DSM Administrator to add the FQDN or IP address of the protected host to the DSM before registering that host.

- **The Shared Secret method**—Requires the DSM Security Administrator to create a *shared secret* registration password—a case-sensitive string of characters—for auto-registering a host in a domain or host group.

  Agent Installers use the shared secret to add and register protected hosts to the DSM for a domain or host group. This method can automatically add host names or IP addresses to the DSM without the DSM Security Administrators having to do so, and there is no need to verify that the protected host and DSM share valid certificates. Multiple protected hosts can be added dynamically with a single shared secret password during the agent installation and registration process.

  If you choose the Shared Secret method, ask the DSM Administrator to create a shared secret for the domain or host group in which the new protected host will reside. Then, get the shared secret and the validity period (one hour, day, week, or month) and register within that period.

NOTE: There is a "**Require that hosts are first added**" checkbox in DSM Shared Secret creation page. If this box is checked, then the hosts must be manually added to the DSM.

Host name resolution

Host name resolution is how host names are mapped to an IP address. During this configuration process, enter either the FQDNs or IP addresses of your DSMs and protected hosts. If you use FQDNs, your protected hosts must be able to resolve their DSM hostnames, and the DSMs must be able to resolve their protected hosts (hosts registered in the DSM).

NOTE: The exception to the requirement of DSMs being able to resolve protected hostnames is if you approve of only agent-initiated communication between the DSM and the protected host. See "One-way communication" on page 10 for more discussion.

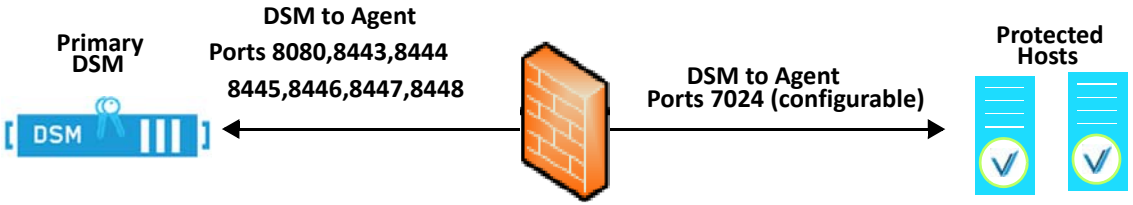
Use the following guidelines for hostname resolution:

- The Domain Name Service (DNS) is the preferred method of host name resolution. If you use DNS, use the DSM and host name FQDNs for the installation and configuration procedures in this chapter.
- If you do NOT use a DNS server, do one of the following on all of the DSMs and the protected hosts:
  - Have the DSM Security Administrator add an entry in the `/etc/hosts` file on the DSMs for each protected host. The administrator must use the DSM Admin CLI, and entries must be done on *each* DSM in an HA deployment since entries in the `/etc/hosts` file are not replicated across DSMs.
- Use the IP addresses of the DSMs and protected hosts.

Port configuration

If a protected host must communicate with a DSM through a firewall, open the ports in the firewall as shown in the following figure.

Figure 2: Ports to open between DSM and protected host



NOTE: See Table 1 to determine which of the above ports must be opened through the firewall.

Table 1 describes the communication direction and purpose of each protected host port you must open. For a complete list of ports required for the DSM, see the *VDS Administration Guide*.

Table 1: Ports to Configure

Port	Protocol	Communication Direction	Purpose
7024	TCP	DSM → Agent	Policy/Configuration Exchange
8080	TCP	Agent → DSM DSM ↔ DSM	Default TCP/IP port for HTTP that is used to exchange certificates between the DSMs in an HA configuration. Also, used once to do the initial certificate exchange between an agent host and DSM.
8443	TCP	Agent → DSM	TCP/IP port through which the agent communicates with the DSM. The agent establishes a secure connection to the DSM, via certificate exchange, using this port.
8444	TCP	Agent → DSM	Agent log messages uploaded to DSM.
8445	TCP	Agent → DSM	Used during initial certificate exchange between agent host and DSM over HTTPS. If not available, then port 8080 will be used instead.
8446	TCP	Agent → DSM	Configuration Exchange using Elliptic Curve Cryptography (Suite B)

8447	TCP	Agent → DSM	Agent uploads log messages to DSM using Elliptic Curve Cryptography (ECC)
8448	TCP	Agent → DSM	Used during initial certificate exchange between agent host and DSM over HTTPS. If not available, then port 8445 or port 8080 will be used instead.

The default port for communication between the DSM and the agent is 7024. If this port is already in use, set the port to a different number by specifying the new port during agent installation.

Port Usage in One Way Communications Mode

By default, polling from the agent host to the DSM when running in one-way communications mode uses HTTP via port 8080. If the agent is configured to use secure polling, then polling is performed using HTTPS via port 8448 (in suite B mode) or port 8445.

Determine the installation method

There are two ways to install the VTE Agents on AIX platforms:

- **Typical installation:** This is the most common and recommended type of installation. Use this method for installing the agent on one host at a time. See "Typical Install" on page 12.
- **Unattended installation:** Create pre-packaged installations by providing information and answers to a set of installation questions. Use unattended (sometimes called "silent install") installations when installing on a large number of hosts. See "Unattended (Silent) Install" on page 17.

Hardware Association (Cloning Prevention)

Thales's hardware association feature associates the installation of an agent with the machine's hardware. When enabled, hardware association prohibits cloned or copied versions of the agent from contacting the DSM and acquiring cryptographic keys. Hardware association works on both virtual machines and hardware hosts.

You can enable hardware association during the agent registration process. You can disable hardware association by re-running the registration program.

To verify if hardware association (cloning prevention) is enabled on an AIX host, on the command line enter the following:

```
cat /opt/vormetric/DataSecurityExpert/agent/vmd/etc/access
```

If you see `usehw:true`, then it's enabled. If you see `usehw:false`, it's disabled.

One-way communication

In some deployments, the agent may not be visible to the DSM through normal network communications. For example, when the host on which the agent is installed is:

- behind NAT
- behind a firewall
- not permanently connected to a communication channel to the DSM
- unable to resolve the host name to an IP address

In these situations, VTE can initiate agent-only communication to the DSM. This feature is called one-way communication and works by having the agent poll the DSM for any policy messages or changes, then downloading changes as required.

The downside of one-way communication is that the DSM cannot issue any queries to the agent. For example, the DSM Admin cannot browse GuardPoint directories or User IDs.

Agent Install Checklist

Use this table to verify prerequisites and collect the information you need for the installation.

Table 2: Agent Install Checklist

Checklist item	Status

Obtain the agent installation image from Thales. The format for VTE Agent file names is:
`vee-<agent_type-build-system>.bin`
Example:
`vee-fs-5.2.7.9-aix71.bin`	

Fully Qualified Domain Name (FQDN) of the DSM.	
IP address or Fully Qualified Domain Name (FQDN) of the host	
Administrator password for the host	
If using Shared Secret Registration, get from the **DSM Security Administrator**: 1) The shared secret password 2) Domain 3) Host group if applicable 4) A description for the host.	
If using the Fingerprint Registration ask **DSM Administrator** to add the host to the **DSM** and check the **Registration Allowed** check box. After checking the fingerprint, select the **Communication Enabled** check box.	
Resolved "Host name resolution" on page 7 for the protected hosts and DSMs?	
Set "Determine the installation method" on page 9?	
Do you want "Hardware Association (Cloning Prevention)" on page 9?	
Is "One-way communication" on page 10 required?	
Synchronize host clock to DSM clock.	
Set network subnet mask on the host (unless you are using one-way communication)	
Preferred DNS Server (if using FQDNs):	

Typical Install

This section describes the typical install and registration process of the VTE Agent on an AIX system.

Typically, you will register the agent with the DSM as part of the installation process; however you may postpone registration if you have a specific plan to register the agent later.

The data on the host is not protected until you set a GuardPoint. Communication to the DSM (and retrieval of any policies and keys) cannot happen until you register the agent on the DSM, and enable communication between the agent and the DSM.

NOTE: Do not install VTE (FS) Agents on network-mounted volumes like NFS.

Before you begin

Verify with the DSM Security Administrator that all hosts where you will install the agent with the fingerprint method have been added to the DSM with the following functionality enabled:

- Registration Allowed
- Communication Enabled

NOTE: If registration appears to hang, verify that the DSM and agent can communicate with each other over the network.

NOTE: If you will be installing agent(s) using the shared secret method, you do not need to have the host(s) added to the DSM before installation. The hosts can be added to the DSM later.

Installation

NOTE: The VTE for AIX installation file is shown as an example.

1. Log on to the host where you will install the agent. You must have root access.
2. Copy or mount the installation file to the host system. If necessary, make the file executable with the `chmod` command.
3. Start the installation. The syntax for the installation utility can be displayed with `-h`.

Example:

```
./vee-fs-5.2.7.9-aix71.bin -h

[-d <dir>] [-e] [-i] [-h] [-m] [-s <file>] [-v] [-y]
-d Install in specified directory (option not supported on Ubuntu)
-e Extract to the current working directory; don't install
-h This help message
-m Display a manifest of the contents
-i Install only (don't register)
-s <file> Register using silent mode; file has environment vars
-v Verbose
-y Answer YES to installation questions (for registration use -s)
```

4. The Thales License Agreement displays. Enter '**Y**' and **Enter** to accept.

```
./vee-fs-5.2.7.9-aix71.bin

Do you accept this license agreement? (Y/N) [N]: Y
```

The installation proceeds.

5. The VTE agent is installed on the host, but not yet registered. The following prompt appears:

```
Welcome to the Vormetric Encryption Expert File System Agent
Registration Program.

Agent Type: Vormetric Encryption Expert File System Agent
Agent Version: X.X.X.XX

In order to register the Vormetric Encryption Expert File System Agent
with a Vormetric Data Security Server:
    1) you must know the host name of the machine running the
       Security Server (the host name is displayed on the
       Dashboard window of the Management Console), and
    2) unless you intend to use the 'shared secret' registration method,
       the agent's host machine must be pre-configured on the
       Security Server as a host with the 'Reg. Allowed'
       checkbox enabled for this agent type on the Hosts window
       of the Management Console.
Do you want to continue with agent registration? (Y/N) [Y]:
```

6. You now have three choices:

- Register the agent now using the *Shared Secret* method. See "To register the agent using the Shared Secret Registration method" on page 14.

- Register the agent now using the *Certificate Fingerprint* method. See"Registering the agent using the Certificate Fingerprint method" on page 15.
- Register the agent later by entering N. Use the command `register_host` at `/opt/vormetric/DataSecurityExpert/agent/vmd/bin/` to register without the installation program.

To register the agent using the Shared Secret Registration method

1. Verify that the DSM Administrator created a shared secret for the domain or host group in which the new protected host will reside.
2. Enter Y when you see the following prompt:

   ```
   Do you want to continue with agent registration? (Y/N) [Y]: Y
   Please enter the primary Security Server host name:
   ```
3. Enter the DSM FQDN and then Y. Ask the DSM Administrator to get this from the dashboard of the DSM Management Console.

   Example: `dsm1490.i.vormetric.com`

   ```
   You entered the host name dsm1490.i.vormetric.com
   Is this host name correct? (Y/N) [Y]: Y
   ```
4. You are prompted for the protected hostname:

   ```
   Please enter the host name of this machine, or select from the following
   list. If using the "fingerprint" registration method, the name you
   provide must precisely match the name used on the "Add Host" page of the
   Management Console.

   [1] host14.i.example.com
   [2] Host-AIX-14.i.example.com
   [3] 10.3.14.90
   [4] 192.168.122.

   Enter a number, or type a different host name or IP address in manually:
   What is the name of this machine? [1]: 1
   ```
5. Enter the protected hostname. This hostname must match the name used on the **Add Host** page of the Management Console (adding the hostname is not needed for the shared secret method). You are prompted for the registration method:

   ```
   You selected "host14.i.example.com".
   Would you like to register to the Security Server using a registration
   shared secret (S) or using fingerprints (F)? (S/F) [S]: S
   ```
6. Enter S (Shared Secret). You are prompted for the following information (examples are in italics—use your own system information):

```
What is the registration shared secret?
Please enter the domain name for this host: <assigned-domain-name-in-DSM>
Please enter the host group name for this host, if any:
Please enter a description for this host: AIX

Shared secret : *********
Domain name : <assigned-domain-name-in-DSM>
Host Group : (none)
Host description : AIX
Are the above values correct? (Y/N) [Y]:y
```

7. If the Shared Secret information is correct enter Y. You are prompted for whether or not you want to enable hardware association (see "Hardware Association (Cloning Prevention)" on page 9).

```
It is possible to associate this installation with the hardware of this
machine. If selected, the agent will not contact the DSM or use any
cryptographic keys if any of this machine's hardware is changed. This
can be rectified by running this registration program again.
Do you want to enable this functionality? (Y/N) [Y]:
```

8. Enter **Y** or **N**. If everything is working, the install program will generate certificate signing requests and the signed certificates will be generated. Unlike the fingerprint method, the fingerprints will not be displayed for verification:

9.
```
Generating certificate signing request for the kernel component...done.
Signing certificate...done.
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
Successfully registered the Vormetric Encryption Expert File System
Agent with the primary
Vormetric Data Security Server on dsm1490.i.vormetric.com.
Installation success.
[root@host14 Downloads]#
```

10. Verify the installation by checking agent processes on the protected host:

    a. Run `vmd -v` to check the version of the agent.

    b. Run `secfsd -status pslist` to display agent processes.

    c. Look at the log files `/var/log/vormetric/install.fs.log.<date>` and `/var/log/vormetric/vorvmd_root.log`

Registering the agent using the Certificate Fingerprint method

1. Enter Y when you see the following prompt:

```
Do you want to continue with agent registration? (Y/N) [Y]: Y
Please enter the primary Security Server host name:
```

2. Enter the DSM FQDN and then Y. Ask the DSM Administrator to get this from the dashboard of the DSM Management Console.

   Example: `dsm1490.i.vormetric.com`

   ```
   You entered the host name dsm1490.i.vormetric.com
   Is this host name correct? (Y/N) [Y]: Y
   ```

3. You are prompted for the protected hostname:

   ```
   Please enter the host name of this machine, or select from the following
   list. If using the "fingerprint" registration method, the name you
   provide must precisely match the name used on the "Add Host" page of the
   Management Console.

   [1] host14.i.example.com
   [2] Host-AIX-14.i.example.com
   [3] 10.3.14.90
   [4] 192.168.122.

   Enter a number, or type a different host name or IP address in manually:
   What is the name of this machine? [1]: 1
   ```

4. Enter the protected hostname. This hostname must match the name used on the **Add Host** page of the Management Console. You are prompted for the registration method:

   ```
   You selected "host14.i.example.com".
   Would you like to register to the Security Server using a registration
   shared secret (S) or using fingerprints (F)? (S/F) [S]: F
   ```

5. Enter F (fingerprints), as shown in the previous step.

   ```
   It is possible to associate this installation with the hardware of this
   machine. If selected, the agent will not contact the DSM or use any
   cryptographic keys if any of this machine's hardware is changed. This
   can be rectified by running this registration program again.
   Do you want to enable this functionality? (Y/N) [Y]:
   ```

6. Enter **Y** or **N**. If everything is working, the install program will generate certificate signing requests and list the fingerprint of the EC (elliptic curve) CA (Certificate Authority) certificate:

   ```
   The following is the fingerprint of the EC CA certificate. Please verify
   that it matches the fingerprint shown on the Dashboard page of the
   Management Console. If they do not match, it can indicate an unsuccessful
   setup or an attack.

   A5:6D:4B:DE:1C:ED:F7:E5:8C:C7:F3:21:58:31:F2:27:15:C5:8C:C9

   Do the fingerprints match? (Y/N) [N]:
   ```

NOTE: If you get the error message *File System component service stopped 'Couldn't resolve hostname',* it means the DSM host name could not be resolved by the protected host. See "Host name resolution" on page 7 to fix.

7. This fingerprint must match the certificate on the DSM dashboard. This is done to verify that nobody is intercepting and modifying traffic between the DSM and agent. Verify this match with the DSM Administrator, then enter **Y**. The agent fingerprint for the host displays:

   ```
   The following is the fingerprint for this agent on this host.
   Please verify that it matches the fingerprint shown for this host on the
   Edit Host window of the Management Console.

   01:FE:F9:37:93:36:F7:74:DD:D5:5D:EA:C8:4A:9B:9C:D0:58:73:8C

   Successfully registered the Vormetric Encryption Expert File System
   Agent with the primary Vormetric Data Security Server on
   dsm1490.i.vormetric.com.
   ```

8. Verify with the DSM Administrator that the agent fingerprint matches with the fingerprint shown for this host on the **Edit Host** window of the Management Console. the agent is installed and registered.
9. Verify the installation by checking agent processes on the protected host:

   a. Run `vmd -v` to check the version of the agent.

   b. Run `secfsd -status pslist` to display agent processes.

   c. Look at the log files in `/var/log/vormetric/install.fs.log.<date>` and `/var/log/vormetric/vorvmd_root.log`.

Unattended (Silent) Install

This section describes how to do an unattended (sometimes called "silent") installation of the VTE Agent on a single host. The unattended installation automates the installation process by storing the answers to installation and registration questions in a separate file that you create. You can also use the unattended installation to install agents on multiple hosts simultaneously. We recommend doing a typical install before doing an unattended install so you can do the actual manual steps.

Before you begin

The unattended install method installs the agent on the host, and registers the host with the DSM you specify in the silent installation file.

For the Fingerprint Registration method, the DSM Administrator must add all hosts on which you will install agents to the DSM. The following functionality must be enabled:

- Registration Allowed
- Communication Enabled

For the Shared Secret Registration method, hosts may not need to be added to the DSM beforehand but can be added later.

Create the unattended installation file

The following table shows the required and optional environment variables to be entered in the unattended installation file. You can store this file anywhere on your system, and access it by using the `-s` option in the install command.

Table 3: Register host options for unattended install

Variable	Description	Required?
SERVER_HOSTNAME	FQDN of DSM	Yes
AGENT_USEIP	Uses IP address instead of host name	No
AGENT_HOST_PORT	The port number for the VTE (FS) agent (vmd). Ignored for other agents.	No
AGENT_HOST_NAME	FQDN of this agent's host	Yes, if HOST IP is being registered.
STRONG_ENTROPY	Use `/dev/random` on AIX. Set to '1' if desired	No
ONEWAY_COMMS	Set to '1' when agent-initiated-only communication is required	No
USEHWSIG	Associate hardware to keys+certs. Set to '1' if desired.	No (default: false)
SHARED_SECRET	Specifies the passphrase for a shared secret registration. See "Determine your agent registration method" on page 6	Yes
HOST_DOMAIN	Specifies domain for the shared secret. Required if using Shared Secret method.	Yes
HOST_GROUP	Specifies the optional host group for the shared secret.	No
HOST_DESC	Specifies a host **Description** on the **Hosts** page of the DSM Management Console. Works only with SHARED_SECRET.	No

Unattended Install with Shared Secret Registration method

1. Create a parameter file and store it on your system. Here is an example file containing the FQDN of the DSM and the FQDN of the host on which you will install the VTE Agent. In this example, the file is called `unattended.txt`.

   Example:

   ```
   SERVER_HOSTNAME=DSM.example.com
   AGENT_HOST_NAME=AIX6.example.com
   SHARED_SECRET=Shallacl12345#
   USEHWSIG=1
   HOST_DESC="AIX"
   ```

2. Log on as an administrator to the host on which you will install the agent.
3. Copy or mount the installation file to the host system.
4. Start the installation. Type

   `./vee-<`*`product-version-build-system`*`>.bin` `-s <`*`dir`*`>/unattended.txt`

   Example: `./vee-fs-5.2.7.9-aix71.bin -s /tmp/unattended.txt`

   Sample output:

   ```
   Welcome to the Vormetric Encryption Expert File System Agent
   Registration Program.

   Agent Type: Vormetric Encryption Expert File System Agent
   Agent Version: 5.2.6.20

   Generating certificate signing request for the kernel component...done.
   Signing certificate...done.

   Generating EC certificate signing request for the vmd...done.
   Signing certificate...done.

   Generating EC certificate signing request for the vmd...done.
   Signing certificate...done.

   Successfully registered the Vormetric Encryption Expert File System
   Agent with the primary

   Vormetric Data Security Server on DSM.example.com.

   Installation success.

   [root@host15101 Downloads]#
   ```

5. Verify the installation by checking agent processes on the protected host:

   a. Run `vmd -v` to check the version of the agent.

   b. Run `secfsd -status pslist` to display agent processes.

   c. Look at the log files `/var/log/vormetric/install.fs.log.<date>` and `/var/log/vormetric/vorvmd_root.log`.

Unattended Install with Fingerprint Registration method

1. Create a parameter file and store it on your system. Here is an example file containing the FQDN of the DSM and the FQDN of the host on which you will install the VTE Agent. In this example, the file is called `unattended.txt`.

   Example:

   ```
   SERVER_HOSTNAME=DSM.example.com
   AGENT_HOST_NAME=AIX.example.com
   ```

2. Log on as an administrator to the host on which you will install the agent.
3. Copy or mount the installation file to the host system.
4. Start the installation. Type

   `./vee-<product-version-build-system>.bin` `-s <dir>/unattended.txt`

   Example: `./vee-fs-5.2.7.9-aix71.bin -s /tmp/unattended.txt`

   Sample output:

   ```
   Welcome to the Vormetric Encryption Expert File System Agent Registration
   Program.

   Agent Type: Vormetric Encryption Expert File System Agent

   Agent Version: 5.2.6

   Generating certificate signing request for the kernel component...done.

   Signing certificate...done.

   Generating EC certificate signing request for the vmd...done.

   Signing certificate...done.

   Generating EC certificate signing request for the vmd...done.

   Signing certificate...done.

   The following is the fingerprint of the CA certificate. Please verify
   that it matches the fingerprint shown on the Dashboard page of the
   Management Console. If they do not match, it can indicate an unsuccessful
   setup or an attack.

   8C:6A:DB:4F:79:7B:D0:7F:A7:94:02:98:9D:9A:D5:3E:EA:B4:ED:7C


   The following is the fingerprint for this agent on this host. Please
   verify that it matches the fingerprint shown for this host on the Edit
   Host window of the Management Console.

   D9:0E:B5:FF:51:F8:8F:2F:C9:F1:B0:74:5C:09:5B:45:BF:DA:01:9E
   ```

5. Verify the installation by checking agent processes on the protected host:

   a. Run `vmd -v` to check the version of the agent.

b. Run `secfsd -status pslist` to display agent processes.

c. Look at the log files `/var/log/vormetric/install.fs.log.<date>` and `/var/log/vormetric/vorvmd_root.log`.

Unattended upgrade

In a unattended upgrade, you do not need an answers file because it inherits those settings from the existing install. Simply use the **-y** flag so that the installer answers 'yes' to the license agreement and upgrade.

Tracking and Preventing Local User Creation

VTE tracks attempts to change user authentication files. This includes, but is not limited to user creation, modification, and deletion.

All VTE versions enable detection and prevention of user accounts on the local host. You can deploy any 5.x or 6.x DSM for protection of the AIX host.

The `|protect|` host setting both monitors and prevents local user account creation. You must manually enable the `|protect|` setting for tracking and prevention of local user account creation.

You can tag the following files with protect:

```
/etc/passwd
/etc/group
/etc/security/passwd
```

NOTE: If you go from not using protected files to using protected files (using the `|protect|` host settings), you will need to restart VTE.

AIX Package Installation

This section describes how to install AIX packages directly so that the VTE Agent installation integrates with AIX distribution software. The VTE installation `bin` files contain the native packages and are extracted by running the `bin` file with the `-e` flag.

Before you begin

Before you can register an agent with the DSM, the DSM Security Administrator must add the host to the DSM with the following functionality enabled:

- Registration Allowed
- Communication Enabled

To extract and run the .bff file (AIX)

NOTE: P8 Hardware Encryption is supported. To support this, an ifix from IBM is required for the initial release. If the ifix version required is NOT found, the installation defaults to software encryption for P8.

1. Log on to the host system as root and copy or mount the installation file onto the host system.
2. Extract the package files.

```
# ./vee-fs-5.2.7.9-aix71.bin -e
   Contents extracted.
# ls *bff
vee-fs-5.2.6-22-aix71.bff
```

3. Run installp and then follow the prompts.

```
> installp -aX -d ./vee-fs-5.2.7.9-83-aix71.bff vee.fs
```

Uninstalling Agents

This section describes how to uninstall an agent on an AIX host.

Before Removing Agents from an AIX host

Consider the following before removing an agent from a host machine.

- Stop all applications from running on locations where GuardPoints are installed.
- Before you remove the agent, decrypt any data you want to use after uninstall. Once the agent software is removed, access to data is no longer controlled. If data was encrypted, it will remain encrypted. If decrypted or copied out of the GuardPoint, the data is visible as clear text.

- The DSM Administrator must evaluate the current GuardPoints in the *Guard FS* tab to avoid data loss or compromise.
- The DSM Administrator must remove **System Locked** and **FS Agent Locked** settings for this host (if set).
- All GuardPoints must be removed.
- The AIX agent must be removed from the host before the host is removed from the DSM.
- Database applications like DB2, and Oracle, can lock the user space while they run. If agent installation fails because a GuardPoint is in use, determine which applications are using the GuardPoints and stop them. Then run the uninstall again.
- Commands like `fuser` and `lsof` might not reveal an active GuardPoint because they detect active usage, not locked states. Although it may appear that a GuardPoint is inactive, it may be in a locked state. Under this condition, software removal may fail and an error like the following may be displayed:

  ```
  /home: device is busy.
  ```

To remove Agents from an AIX host

1. Stop any application accessing files in the GuardPoint.
2. Log on to the host as root with system administrator privileges.
3. Change directory to an unguarded location (for example, `/..`)

Caution: Do not change (`cd`) into the `/opt/vormetric` directory or any directory below `/opt/vormetric`. If you are in `/opt/vormetric`, or any directory below `/opt/vormetric`, the package removal utility may fail and return the following message:

```
...
You are not allowed to uninstall from the /opt/vormetric
directory or any of its sub-directories.
Agent uninstallation was unsuccessful.
```

4. Start the uninstall. Type

   ```
   # /opt/vormetric/DataSecurityExpert/agent/vmd/bin/uninstall

   Would you like to uninstall the vee-fs package? (Y/N) [Y]: Y
   Success!
   ```

Upgrade

This section describes the generic instructions for upgrading VTE Agents. For specific instructions, refer to the release notes for the agent.

General upgrade information

- Check that no one is using the directory before making it a GuardPoint. Instruct users to save their work, to close applications that are running in the directory, and to exit the directory. Then make a backup of all files in that directory before installing an agent (GuardPoint) over that directory.

To upgrade an agent

1. Stop any application accessing files in the GuardPoint.
2. Log on to the host where you will upgrade the VTE Agent. You must have root access.
3. Copy or mount the installation file onto the host system.
4. Start the upgrade. Type:

   ```
   # ./vee-<product-version-build-system>.bin
   ```

   Example: `vee-fs-5.2.7.9-aix71.bin`
5. Type 'y' and press **Enter** to accept the Vormetric License Agreement. The upgrade proceeds.
6. Follow the prompts. During an upgrade, the following message is displayed:

   ```
   Upgrade detected: this product will be stopped and restarted.
   Do you wish to proceed with the upgrade? (Y/N) [Y]: y
   Installation success.
   ```
7. Type "Y" or press **Enter** to complete the upgrade. You will not do the registration steps since the agent is already registered with the DSM.

Using VTE with Oracle

This chapter describes how to install and configure VTE on Oracle RAC ASM, as well as install and use VTE for AIX with Oracle Automated Storage Management (ASM™) Cluster File System (ACFS™).

It contains the following sections:

VTE on ACFS Installation Overview

VTE enables data protection of ACFS on `secvm` volumes as part of the Oracle ASM stack. Oracle ACFS configured with `secvm` block devices is intended for use solely by the Oracle RAC application set to store related Oracle generated data such as:

- Oracle-generated related database files:
  - database datafile
  - control files
  - redo log files
  - archive log files
- Oracle-generated database backup files:
  - hot/cold
  - rman
  - datapump exports
- Oracle-generated database TDE local wallet files

NOTE: VTE on ACFS only provides encryption. It does not provide access control.

For other files such as manually created shell scripts that require staging in a shared storage device, use other shared storage setups such as Veritas shared storage or share NFS mount.

Oracle ACFS Stack

Oracle RAC
Oracle ACFS (File System)
Oracle ADVM (Volume Manager)
Oracle ASM (Storage Manager)
SecVM
Block Devices

On both Oracle 11gR2 and Oracle 12c databases, ACFS is layered on ASM disks, which in turn are built on `secvm` block devices.

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

DSM Security Administrators and SecVM

Server-side administrators must ensure that all `secvm` guards for an Oracle cluster use the same policies for encryption and access control.

Host Groups and Identical Keys and Policies

Thales recommends that you deploy host groups to ensure that identical policies and keys are applied on all nodes of the ACFS cluster. This is faster and less error-prone.

Restrictions and Caveats

- Thales does not support `secfs` layered on ACFS.
- Oracle ACFS encryption in conjunction with `secvm` encryption might impact performance

Oracle RAC ASM

This section describes how to install and configure VTE on an Oracle RAC ASM.

Using VTE with an Oracle RAC ASM

You can apply VTE when the Oracle DB is active or inactive. If you choose to use it while the Oracle DB is active, it eliminates any downtime. You can apply VTE during low volume traffic time frames. If you choose to use this option, then use the **rebalance** function of ASM. This allows you to:

1. Migrate data off of a disk so that it can be dropped/removed from a **Diskgroup.**
2. Apply VTE protection.
3. Add the disk back into the diskgroup.

Important ASM Commands and Concepts

Rebalancing Disks

When you drop/remove a disk from the diskgroup, it is important to apply the proper value for the power setting for rebalance and to use the **WAIT** command.

Example ASM Command:

```
SQL> ALTER DISKGROUP <DiskGroupName> DROP DISK <diskName>
REBALANCE POWER 8 WAIT;
```

- The **rebalance** command moves the data off of the disk that you are removing from the diskgroup, distributing the data across the remaining DISKS.
- The **power** setting is a number from 1 to 11. It determines how much processing power is dedicated to the **rebalance**, versus normal operations. Unless the encrypting occurs during heavy traffic volume, the minimum value you should use is 6. Otherwise, consult the customer's DBA for the proper setting. An appropriate value to start with is 8.

Mapping Raw Devices

You can map raw devices for this configuration using:

- **EMC PowerPath**

  If using EMC PowerPath then the device names are similar to the following: `/dev/hdiskpowerXX`.

When browsing the DSM through the local host, you cannot find Power Path devices. You must manually input the paths. The guarded disk names are prepended with: `/dev/secvm`.

Checking Rebalance Status

The **Wait** command is very important when ASM performs a rebalance. When you specify **`wait`**, the command prompt does not display until all of the data is rebalanced and migrated off of the disk. If you do not specify wait, the command prompt returns immediately, and you must issue the following ASM command to check the status of the rebalance:

```
SQL> select * from v$asm_operation;
```

This command returns information about the:

- State
- Current power level
- Current amount rebalanced
- Estimated work until completion
- Rate
- Estimated minutes
- Any error codes

NOTE: It is highly recommended that you always specify the **WAIT** command when performing a **Drop Disk** with Rebalance. If it is not specified, ASM may prematurely release the disk, thereby allowing VTE to place a GuardPoint on the disk before the rebalance completes. This action may corrupt the data.

Oracle cautions against this issue:

Caution: The `ALTER DISKGROUP...DROP DISK` statement returns before the drop and rebalance operations complete. Do not reuse, remove, or disconnect the dropped disk until the `HEADER_STATUS` column in the `V$ASM_DISK` view for this

disk changes to FORMER. You can query the V$ASM_OPERATION view to determine the amount of time remaining for the drop/rebalance operation to complete. For more information, refer to the *Oracle Database SQL Language Reference* and the *Oracle Database Reference*.

Determining Best Method for Encrypting Disks

A diskgroup can contain one or multiple disks. You must determine if the diskgroup contains enough disks and free space for encryption. If the diskgroup contains only one disk, or multiple disks but not enough free space, then you must use the **Offline** (backup/restore) method for encryption.

If the diskgroup contains more than one, you can use the **Online** (rebalancing) method. During rebalancing, additional disks allow for migrating data from the original disk so that it can be encrypted, added back into the diskgroup, and then migrated back to the source disk. Therefore, if the customer does not want to permanently add extra disks, they can add disks temporarily, just for rebalancing.

In general, once you have completed the initial setup for the operating system with which you are working, for both ASM or ASMLib, the high-level process is the same for applying VTE protection to raw devices and using them.

Online Method (No Application / Database Downtime)

Typically, when using the online method, follow these steps:

1. Make an ASM disk available for protection by either removing a disk from an existing diskgroup, or allocating a new disk.
2. Apply VTE encryption to the disk.
3. Add each protected disk to the diskgroup.
4. Restart the nodes and the failover test.
5. Repeat the previous steps for each disk in the diskgroup.

Offline Method (Backup the DB)

Typically, when using the offline method, follow these steps:

1. Backup the database.
2. Make an ASM disk available for protection by either removing a disk from an existing diskgroup, or allocating a new disk.

3. Stop the Oracle database.
4. Delete the diskgroup.
5. Apply VTE encryption to the disk.
6. Recreate the diskgroup.
7. Add the protected disk to the diskgroup.
8. Restart the nodes and the failover test.
9. Repeat the previous steps for each disk in the diskgroup.

General Prerequisites

Follow these guidelines for best results.

Setup

- Ensure that you have a current backup of the database
- Install and register VTE agents on **all** RAC node Hosts
- Create a **Host Group** and add all RAC node hosts as members
- Create an encryption key for the Oracle RAC Database / Application
- Create an Oracle policy using the proper encryption key

NOTE: If the raw device mappings for the disk(s) are **not** identical across all nodes in the RAC, then you cannot use a Host Group for managing the GuardPoint within the DSM. You **must** apply the GuardPoint to each Host individually. This is typically not optimal, as a Host Group is the most effective and consistent way to manage GuardPoints for Oracle RAC environments.

Altering ASM_DISKSTRING on ASM

ASM uses the `asm_diskstring` setting to identify the path where ASM will attempt to locate available disks to use. If you are using device names when adding the disk, you must modify the string to include the path to SecVM.

1. To retrieve the `ASM_DISKSTRING` setting, type:

   ```
   SQL> SHOW PARAMETER ASM_DISKSTRING
   ```

2. To modify the setting, type:

```
SQL> ALTER SYSTEM SET ASM_DISKSTRING='/dev/*', '/dev/secvm/dev/*';
```

Where the path added is the path to SecVM.

Specific Prerequisites

Establishing a Starting Point

In many production environments, you may find that it has been a very long time since the RAC nodes have had the services restarted or have been completely rebooted. This can result in a lack of understanding of the actual state of the RAC cluster and its ability to survive a reboot on its own, prior to installing VTE.

Restarts can uncover issues in the RAC environment that are unrelated to VTE. To avoid issues after a VTE installation, Thales recommends that you restart each RAC node **AFTER** VTE is installed and **PRIOR** to establishing any GuardPoints. This may not be feasible in a single node configuration. However, by doing so, VTE is installed but inactive, and you can ensure that the platform is in a workable state prior to getting started.

The Importance of Device Mapping

It is important to use device naming and mapping in a multi-node RAC configuration. Verify the device names to ensure that the disks are mapped to the same disks on each RAC node before applying any GuardPoints. Thales **recommends** that RAC nodes use the same device names across all nodes. If they do not match, then problems can occur.

If the RAC nodes use the same device names, use a Host Group to create GuardPoints. If they do not match, do not use a Host Group to create GuardPoints. Set them up independently on each Host.

Important Note about Raw Devices on AIX

In general, raw devices are created as either character or block mode devices. Any I/O performed on character devices is non-buffered, while I/O on block devices is buffered and performed in defined block sizes (that is, 4K bytes).

While the Oracle documentation for using ASM with raw devices indicates that you can use either character or block devices**, VTE REQUIRES a block device for guarding.**

NOTE: Attempting to apply a GuardPoint on a character device that ***does not*** have a corresponding block device may result in a GuardPoint that never encrypts data. The status of the GuardPoint never shows as guarded.

NOTE: WebUI does not support browsing for the character devices. You would need to manually paste the name into the WebUI.

Once guarded, VTE creates both a character and block mode version of the guarded device. Oracle ASM can use either device.

About Oracle RAC ASM Raw Devices

Standard Devices

In many cases the ASM configuration may be using plain device names, like the following:

```
/dev/hdisk1
```

NOTE: If you use standard device names in the ASM configuration to add a disk, you must modify the `ASM_DISKSTRING` parameter to include the `/dev/secvm/dev/*` path.

Consistent Naming of Devices across RAC Nodes

As previously stated, if the raw device mappings for the disk(s) are **NOT** identical across all nodes in the RAC, then you **CANNOT** use a Host Group and you **MUST** apply the GuardPoints to each Host individually. This is typically NOT optimal, as a Host Group is the most effective way to manage an Oracle RAC environment.

Oracle RAC ASM Multi-Disk Online Method

Performing encryption with the online rebalancing method requires sufficient free space to allow the drop of the largest ASM disk.

Checking for Space

In the Oracle system, use the following commands to check for available disk space:

1. Check total free space in the disk group:

```
SQL> SELECT name, free_mb, total_mb, free_mb/total_mb*100 as
percentage    FROM v$asm_diskgroup;
```

System Response:

```
NAME                            FREE_MB   TOTAL_MB PERCENTAGE
------------------------------ ---------- ---------- ----------
DATA                                     7       2109 .331910858
```

2. Check individual ASM disk size and usage:

```
SQL> select a.name DiskGroup, b.disk_number Disk#, b.name
DiskName, b.total_mb, b.free_mb, b.path, b.header_status FROM
v$asm_disk b, v$asm_diskgroup a where a.group_number (+)
=b.group_number order by b.group_number, b.disk_number, b.name
```

System Response:

```
DISKGROUP  DISK# DISKNAME   TOTAL_MB    FREE_MB PATH  HEADER_STATU
---------- ---------- ------------- ---------- ---------- ---------
DATA   0 DATA_0000           1874       1273
/dev/oracleasm/disks/DATA3     MEMBER

DATA   1 DATA_0001           1992        608
/dev/oracleasm/disks/DATA4     MEMBER

DATA   3 DATA_0003            117          0
/dev/oracleasm/disks/DATA2     MEMBER

       0 DATA_ENC_0000        109         28
/dev/oracleasm/disks/DATA1_ENC MEMBER
```

Adding a Disk to the Diskgroup

Using the Online Method assumes that there is enough free space in the diskgroup so that you can drop/remove a disk, protect it with VTE, and then add it back into the diskgroup.

To add the disk to the diskgroup:

1. Open a terminal session on both RAC Nodes.
2. On **RAC Node 1**, on the ASM, remove the disk from the disk group, type.

   SQL> **ALTER DISKGROUP <*diskGroupName*> DROP DISK <*diskName*> REBALANCE POWER 11 WAIT;**
3. On both **RAC Node 1** and **2** type:

   ```
   # chown oracle:oinstall /dev/<rawDevice1Name>
   ```

   ```
   # chmod 660 /dev/<rawDevice1Name>
   ```
4. On the DSM, in the Host Group, apply a GuardPoint to the Raw Device: ***<rawDevice1Name>***
5. From **RAC Node 1**, display the status of the guarded disks, type:

   # secfsd -status guard
6. On both **RAC Node 1 and 2** type:

   # chown oracle:oinstall **/dev/secvm/dev/*<rawDevice1Name>***

   # chmod 660 **/dev/secvm/dev/*<rawDevice1Name>***
7. From **RAC Node, on the ASM,** add the protected disk to the disk group:

   SQL> **ALTER DISKGROUP *<diskGroupName>* ADD DISK /dev/secvm/dev/*<rawDevice1Name>* NAME *<disk1Name>*;**

   The disk is now added to the diskgroup and ready for use.
8. The system is now ready for a reboot and failover test. Go to the section "Surviving the Reboot and Failover Testing" on page 36.

Oracle RAC ASM Multi-Disk Offline Method (Backup/Restore)

Using the Offline Method assumes that there is not enough free space in the diskgroup.

1. Open a terminal session on both RAC Nodes.

   On RAC Node 1, on the ASM, type the following to remove the disk group. **SQL> DROP DISKGROUP *<diskGroupName>* FORCE INCLUDING CONTENTS;**

NOTE: Make sure that the disk is removed before guarding the raw devices.

2. On both **RAC Node 1** and **2** type:

```
# chown oracle:oinstall /dev/<rawDevice1Name>
# chmod 660 /dev/<rawDevice1Name>
# chown oracle:oinstall /dev/<rawDevice2Name>
# chmod 660 /dev/<rawDevice2Name>
# chown oracle:oinstall /dev/<rawDevice3Name>
# chmod 660 /dev/<rawDevice3Name>
```

3. On the DSM, in the Host Group, apply GuardPoints to the three raw devices:

```
<rawDeviceName1>
<rawDeviceName2>
<rawDeviceName3>
```

4. On **RAC Node 1**, perform the following:

   a. Display the status of the guarded disks, type:

```
# secfsd -status guard
```

5. On both **RAC Node 1** and **2**, type:

```
# chown oracle:oinstall /dev/secvm/dev/<rawDeviceName1>
# chmod 660 /dev/secvm/dev/<rawDeviceName1>
# chown oracle:oinstall /dev/secvm/dev/<rawDeviceName2>
# chmod 660 /dev/secvm/dev/<rawDeviceName2>
# chown oracle:oinstall /dev/secvm/dev/<rawDeviceName3>
# chmod 660 /dev/secvm/dev/<rawDeviceName3>
```

6. From **RAC Node 1**, **on the ASM**, add the protected disk to the disk group, type:

```
SQL> ALTER DISKGROUP <diskGroupName> ADD DISK
/dev/secvm/dev/<rawDeviceName1> NAME <diskName1>;

SQL> ALTER DISKGROUP <diskGroupName> ADD DISK
/dev/secvm/dev/<rawDeviceName2> NAME <diskName2>;

SQL> ALTER DISKGROUP <diskGroupName> ADD DISK
/dev/secvm/dev/<rawDeviceName3> NAME <diskName3>;
```

   The disks are now added to the diskgroup and ready for use.

7. On **RAC Node 1**, restore the database.
8. The system is now ready for a reboot and failover test. Go to the section "Surviving the Reboot and Failover Testing" on page 36.

Surviving the Reboot and Failover Testing

Failover Testing

Confirm that everything is functional:

- Ensure that the GuardPoints are all operational.
- Ensure that you receive valid results when you query the database.
- Verify that the load order ensures that VTE starts before ASM .

Once verified, you can start the failover testing for each RAC Node.

1. Reboot the RAC Node 1 and monitor the startup.
2. Once the restart is clean, reboot RAC Node 2 and monitor the startup.

Basic Troubleshooting Techniques

Following are some of the most common configuration issues that prevent the Oracle ASM configuration from working properly.

If you encountering errors similar to:

- ORA-15075: disk(s) are not visible cluster-wide
- ORA-15032: not all alterations performed

This could be the result of improper settings for the I/O layer, meaning that your disks are not properly configured, etc.

Perform the following tasks to verify that the settings are correct:

1. On the DSM **WebUI**, in the Host Group that was created for the RAC cluster, verify that the host group for this configuration does **NOT** have the Cluster Group option set (it is only for GPFS).

2. Ensure that the GuardPoints for the block devices are set at the Host Group level. This ensures that each node receives identical GuardPoints.
3. Verify that the GuardPoints are active on all nodes. When the GuardPoints are set, go to each node and verify that they are set and guarded, using the WebUI or the **`secfsd –status guard`** command. If they do not guard correctly:
   - The device names are not the same across all nodes
4. From ASM, make sure that the `asm_diskstring` parameter is modified to include the VTE devices and that the proper pathname is used, see "Altering ASM_DISKSTRING on ASM" on page 30.

Verifying Database Encryption

Option 1

The best way to verify the state of the data, without impacting anything in the existing environment, is to use the Oracle `kfed` command. You can run this command against the native path of the existing GuardPoints and make sure it returns with valid header information. If it returns valid information with the GuardPoint in place, then this confirms that the data is properly encrypted. If it returns with invalid header information, then that indicates that the data is either clear, or not in the expected encrypted state. The syntax for running this command would look similar to the following but will vary based on your environment.

```
# /app/oracle/grid/product/11.2.0/grid/bin/kfed read
/dev/<diskName>
```

If the location is properly encrypted, following is an example of the viewable output:

```
# /app/oracle/grid/product/11.2.0/grid/bin/kfed read
/dev/<diskName>
```

System Response:

```
kfbh.endian:                          1 ; 0x000: 0x01
kfbh.hard:                          242 ; 0x001: 0xf2
kfbh.type:                          124 ; 0x002: *** Unknown Enum
***
kfbh.datfmt:                         66 ; 0x003: 0x42
kfbh.block.blk:              1088904227 ; 0x004: blk=1088904227
```

```
kfbh.block.obj:              1558192170 ; 0x008: file=8234
kfbh.check:                  3321251423 ; 0x00c: 0xc5f6465f
kfbh.fcn.base:                932956641 ; 0x010: 0x379bc9e1
kfbh.fcn.wrap:               3040493590 ; 0x014: 0xb53a4016
kfbh.spare1:                 3806015223 ; 0x018: 0xe2db2ef7
kfbh.spare2:                 3794962182 ; 0x01c: 0xe2328706
600000000000D8000 01F27C42 40E75C23 5CE0202A C5F6465F
[..|B@.\#\. *..F_]
600000000000D8010 379BC9E1 B53A4016 E2DB2EF7 E2328706
[7....:@......2..]
600000000000D8020 CA2F30AD 522B4D21 99292639 004EBB34
[./0.R+M!.)&9.N.4]
600000000000D8030 A3896BE8 BD839D23 2204E19E 946C575C
[..k....#"....lW\]
600000000000D8040 4CE2218F 35E1B101 AF751A70 780E6D6E
[L.!.5....u.px.mn]
600000000000D8050 5E7E6A38 C600ED5F 929047C4 DF372A8E
[^~j8..._..G..7*.]
600000000000D8060 E103152D BA87CC03 11A7D963 9D72FCE1
[...-.......c.r..]
600000000000D8070 1EC6B48B 03EE869F 61D651F9 E7614957
[........a.Q..aIW]
600000000000D8080 810E0353 9C461F49 69569733 501D19EF
[...S.F.IiV.3P...]
600000000000D8090 B268002B 4F9457B6 BDB04AC5 D3D07446
[.h.+O.W...J...tF]
600000000000D80A0 FD9EE5E0 9B46CB66 30D10B22 F63AB77E
[.....F.f0.."..:.~]
600000000000D80B0 6FF79075 4BBD1FAD 8F226188 7774300D
[o..uK...."a.wt0.]
600000000000D80C0 A809B6FB E1F1C80B B5760E68 9747D97D
[.........v.h.G.}]
KFED-00322: Invalid content encountered during block traversal:
[kfbtTraverseBlock][Invalid OSM block type][][124]
```

Option 2

The second option to verify the state of the data is to use the dd command. This requires you to specify some blocks and write it out to a file. After this completes, read the file using the strings command. You can do this while the device is in use. In the example below some sectors are skipped and it only dumps 10000 counts.

For example:

```
# dd if=/dev/asm_data2p1 of=/tmp/dd2.out skip=1047 count=10000
```

Option 3

The third option to verify the state of the data without impacting the existing environment is to use the strings command.

NOTE: The strings command cannot read a busy or large device.

You can run this command against the native path (`/dev/<deviceName>`) of the existing GuardPoints (`/dev/secvm/dev/<deviceName>`). By executing the strings command against the native path **`strings /dev/devicename | more`**, this does not go through the SecVM device and therefore is not be decrypted. If it is encrypted the output should contain illegible text.

4 Installation for GPFS and pureScale

The Vormetric Encryption for GPFS (VTE Agent) enables you to secure files and devices under the control of the IBM General Parallel File System (GPFS™) in AIX environments.

NOTE: In 2015, IBM rebranded GPFS as IBM Spectrum Scale™.

The VTE agent supports application workloads that require GPFS for shared file access. Refer to the compatibility matrix for system requirements supporting specific application workloads. Some restrictions apply on usage of GPFS features on GuardPoints.

This chapter contains the following sections:

VTE for GPFS

This section describes the architecture of VTE within the GPFS subsystem, and its integration with other AIX technologies for proper operation of VTE in a cluster environment. This section

also explains how to prepare your system for installing and configuring the agent and how to administer the agent and protect resources within the GPFS environment.

VTE agent performs cluster-wide management of policies and GuardPoints over GPFS on distributed hosts belonging to a GPFS cluster. As policy information for GuardPoints or access control is defined or updated for a cluster on the DSM, this same information is also managed and applied to GuardPoints on each member of the cluster, ensuring cluster-wide consistency and access to the same policy information.

Data Security Manager (DSM)

The DSM provides cluster host group functionality to administer policies across a GPFS cluster. A cluster host group is a variation of a host group. Some restrictions apply to cluster host groups that don't apply to host groups. For instance, membership in a GPFS cluster mandates membership of the same hosts to a cluster host group. It also mandates that member hosts cannot belong to other cluster host groups or host groups. Hosts that belong to the same GPFS cluster share GuardPoint(s) and policies.

NOTE: Do not mix GPFS GuardPoints and non-GPFS GuardPoints.

NOTE: The DSM administrator must use cluster host groups for GPFS clusters to accommodate the separation of GuardPoints as required.

The DSM Administrator applies strict rules to enable GuardPoints on GPFS. Those restrictions include:

- A host in a cluster host group can be a member of only one GPFS cluster and one cluster host group.
- Before a host can be added to a cluster host group, it's verified that the host is not a member of a host group or a member of another cluster host group. If the host is already a member of such groups, the DSM refuses to add the host to the designated cluster host group.
- GPFS GuardPoints must be defined within a cluster group.

Data corruption will occur when accessing files within a GuardPoint on an unregistered host or a host that has not been added to the cluster host group on the DSM. However, a host can belong to a cluster host group and/or registered with the DSM before it is added to a GPFS cluster. The rule is that a host added to a GPFS cluster must be registered with the DSM and belong to a cluster host group before mounting GPFS file systems with GuardPoints on the host.

NOTE: Do NOT mix GuardPoints over GPFS and non-GPFS file systems. GuardPoints are supported only over GPFS file systems.

RSCT (Reliable Scalable Clustering Technology)

RSCT is an IBM clustering and communications technology that provides a scalable and reliable framework for clustering application clients running on multiple hosts. RSCT provides the communication infrastructure between VTE agents across a cluster of GPFS nodes for high availability.

Peer Domain and Clustering

RSCT provides support for peer domains. A peer domain is a cluster of hosts configured for high availability. GPFS clustering is not based on RSCT peer domain and it uses its own private clustering infrastructure.

The VTE agent integrates with RSCT to support clustering of VTE agent instances running on a cluster of hosts under GPFS. Clustering multiple instances requires cluster-wide management of security policies and GuardPoint operations across the hosts under GPFS cluster management. The VTE agent for GPFS creates the peer domain, called VormetricDomain, on each node of a GPFS cluster.

Through the peer domain, the VTE agent can join running instances of the agent on multiple host members of the GPFS cluster. Although RSCT supports multiple peer domains on a host, only one peer domain can be active and the same peer domain must be active on the members of a cluster. Make sure that other distributed products active on your hosts do not create and enable a peer domain before installing the VTE agent.

NOTE: Contact Thales customer support if your system runs other cluster services that may depend on peer domains. To determine if a peer domain is installed and online on your system, run the command `lsrpdomain`. If there is no output, then there is no peer domain on your system. The following example shows Vormetric Domain active on each member of a GPFS cluster.

```
# /usr/sbin/rsct/bin/lsrpdomain
Name OpState RSCTActiveVersion MixedVersions TSPort GSPort
VormetricDomain Online 3.2.1.1 Yes 12347 12348
```

VTE Agent for GPFS

A VTE agent operates on each host in a GPFS cluster. The agents operate as a single distributed solution across the hosts in a cluster, using the components described in the following sections.

VMD (Vormetric daemon)

The VMD is a component of the VTE agent. It communicates with the DSM for local caching of policy and GuardPoint information on a managed host. It also performs cluster-wide policy management with other VMD instances in the cluster for approval or rejection of policies and GuardPoints information before caching such information on each host. Other components of the VTE agent rely on the VMD for cluster-wide operations. With VMD running on all the hosts that belong to a GPFS cluster, each VMD instance participates in cluster-wide policy propagation when changing or applying policies and GuardPoints. VMD also enables distributed operations such guard and unguard on GuardPoints. Nodes without a running VMD instance cannot participate in cluster-wide operations.

When the VMD instance starts up on each host in the cluster, it joins the cluster of VTE agents as described by the `VormetricDomain` peer domain. The VTE agent creates the peer domain on participating members of the GPFS cluster during agent installation. However, installation of VTE agent in DB2 v10.5 Cluster Application environments does not create `VormetricDomain`. Instead, the agent relies on the peer domain created by DB2 for operation of DB2 pureScale. The VTE agent operates in cluster mode in clusters configured with `VormetricDomain` or DB2 specific peer domain.

VMD instances communicate with one another through Group Services of RSCT. Group Services enables each VMD instance to be aware of the membership status of other VMD instances in the cluster. As stated earlier, the cluster consists of hosts that belong to the `VormetricDomain` peer domain, or DB2 specific peer domain.

When VMD instances establish a cluster, they operate as a cohesive system for application and propagation of security policies on GuardPoints and cluster-wide guard or unguard operations. If an active VMD instance departs or fails, the remaining active instances declare the departed or failed VMD a non-participant member, and as such, exclude it from the cluster-wide operations.

Clustered mode refers to policy and GuardPoint management operations specific to GPFS clusters. As stated previously, management operations on the DSM define the operating mode of the VMD per GuardPoint. GuardPoints defined under cluster host groups are identified to the VMD as clustered objects that belong to GPFS whereas GuardPoints defined outside of cluster host groups are non-cluster objects that don’t belong to GPFS clusters. VMD operates only in non-GPFS mode if the VTE agent for GPFS is not selected during installation. GuardPoints identified as clustered objects are managed and processed in a cluster-wide manner.

secfs

`secfs` is a layered file system that enables and disables GuardPoints on native or cluster file systems. Using GuardPoints, `secfs` enforces access control policies and encryption on GuardPoints at a file level granularity. Policy and GuardPoint information is provided to the `secfs` module on a per-host basis from the DSM through the local VMD module. Because VMD operates in a cluster-wide cohesive manner, policy and GuardPoint information is always consistent across active members of the GPFS cluster.

Because the `secfs` module supports GPFS and non-GPFS file systems, GuardPoint administration is always performed in a cluster-wide manner over GPFS. This means that a manual GuardPoint enabled on one host also enables the GuardPoint on other members of the GPFS cluster where VMD is active.

secvm

`secvm` is a layered device driver with two modes of operation depending on which device it is layered on. The first mode is the default mode in which `secvm` driver enforces policies and guards devices that have been configured on the DSM. The second mode is specific to GPFS. In this mode, the `secvm` layered devices are NSD devices of GPFS. The NSD type of `secvm` layered devices is `secvmdisk`, rather than `hdisk`. Layering `secvm` over existing NSD devices of a GPFS file system requires changing the NSD type of file system NSD devices from `hdisk` to `secvmdisk` type through the GPFS `mmcommon` utility. The NSD type `secvmdisk` is a new NSD type that GPFS supports as of GPFS 3.5.0.22 or higher. GPFS file systems composed of only `secvmdisk` NSD devices can be under the management of the VTE agent for access control and encryption. A GPFS file system with any number of GuardPoints must be composed of only `secvmdisk` NSD devices.

Operational Details

This section describes the operation and interaction between the various components of the VTE agent.

Cluster Policy Management

Cluster policy management is a cluster-wide operation that applies and maintains consistent policies and GuardPoints across members of the GPFS cluster. The VMD instances participate in policy propagation upon receipt of updated policy and GuardPoint information from the DSM. Cluster policy management guarantees approval of updated policy information by all nodes, or the policy information is rejected.

Primary Cluster Policy Manager

The VMD instance on one of the hosts in a cluster performs cluster-wide GuardPoint and policy management. This host is designated as the primary Cluster Policy Manager (CPM). References to primary role designation are made in terms of hosts or VMD in this document. A cluster must have one host designated as the Primary CPM.

As each VMD instance in the cluster receives and processes policy and GuardPoint information changes from the DSM, the designated primary VMD/host engages other running VMD instances in the cluster for approval or rejection of the information change. If all instances share the same policy information, the change is approved and atomically applied to all active nodes of the cluster. Otherwise the change is rejected.

Secondary Cluster Policy Manager

Although not mandatory, a second host as the secondary CPM for your cluster is strongly recommended. The secondary CPM host assumes the primary CPM role if a primary CPM host fails or is removed from the cluster. Other agents in a cluster assume a Member role, which is non-primary and non-secondary. Designation of a host to primary, secondary, or member role is done when the agent is installed.

Best practices for CPM role designation

Implement the following best practices for designation of CPM role to members of your cluster:

- Designate the first host in a cluster on which the VTE agent is installed to the primary CPM role for the cluster. A cluster must have one host designated as primary. This practice is mandatory.
- Hosts do not require additional CPU or memory for assuming primary or secondary CPM roles.
- Clusters with 2 nodes should not designate a host to secondary CPM role. This practice avoids splits in the cluster as the result of network connection failure between the two nodes of the cluster.
- Although not mandatory, it is strongly recommended that you designate a host as the secondary CPM in clusters with 3 or more hosts. Other agents in a cluster assume Member roles.
- If the designated primary host must be shut down when there is no secondary designation, consider designation of another host to the secondary CPM before the primary host is brought down. The secondary CPM will assume the primary role as soon as the primary node is shut down. Refer to the section on CPM role promotion.
- In the absence of primary and secondary CPM hosts, avoid policy or GuardPoint changes to your cluster on the DSM. Under these conditions, the cluster does not have a primary CPM to orchestrate and commit policy or GuardPoint changes to the hosts across your cluster.

- Use the `voradmin` utility to alter designation of primary or secondary CPM hosts on your cluster.

CPM role promotion and demotion

Hosts in your cluster can be promoted or demoted to a CPM role as necessary. The `voradmin` utility supports limited administrative tasks for CPM role promotion or demotion. The following rules apply:

- Promotion or demotion of a host to primary or secondary CPM role is rejected if your cluster already holds the same role designation.
- If an existing role designation in your cluster is not wanted, demote the existing designation before applying the new designation.
- Demotion of primary to secondary is not allowed. The primary host can only be demoted to member role.
- Before removing a host that holds the primary CPM role, consider designation/promotion of another host to the secondary CPM role before removing the designated primary host.
- Be sure that there are no policy changes on the DSM while your cluster has no host designated to primary or secondary roles.
- Designating a different host to primary role should be done after demotion of the current primary and secondary to member roles to avoid the secondary taking over the primary role.
- The designated secondary CPM will automatically be promoted to the primary role if the current primary is demoted to member role, fails, or leaves the network.
- A new role designation fails if it would duplicate an existing role in a cluster.
- Hosts can be promoted or demoted to any CPM role as other hosts are removed or added to the cluster.

Cluster-wide policy propagation process

Cluster-wide policy propagation is a two-phase commit protocol for applying policy and GuardPoints to all hosts in a cluster. Policies for non-cluster hosts or GuardPoints are excluded in the cluster-wide policy propagation. The process for policy update is described in the following steps:

1. The DSM pushes policies to each host in the cluster upon availability of each host.
2. Each host receives policies and waits for the next policy propagation process across the cluster. Only the host (the VMD process) designated to the primary CPM role takes action in response to the policies received from the DSM.

3. The primary CPM host initiates a 2-phase commit proposal for other hosts to vote on approval of the pushed policies to all hosts. A unique hash code representing the most recent policy pushed to the primary is provided in the commit proposal to each host.
4. Any host not having the exact same policy code specified in the commit proposal rejects the cluster-wide policy commit proposal. Hosts having the same policy hash code approve the proposal. If all hosts approve, the policy goes into effect on all hosts, otherwise the policy is discarded on all hosts.

Installing the VTE Agent for GPFS

This section provides an overview of how to install and configure the VTE agent on the GPFS hosts, then describes the install procedure in detail. If you are installing in a pureScale system, see "VTE for pureScale" on page 54.

Installation overview

Following is a list of high-level steps for installing the VTE Agent for GPFS in the order in which they should be executed.

1. On the DSM, add hosts from the GPFS cluster to the DSM.
2. On the DSM, create a GPFS cluster host group by selecting GPFS (the other option is HDFS).
3. On the DSM, add the hosts to the cluster host group.
4. Install the VTE Agent on the primary CPM.
5. Install the VTE Agent on the rest of the hosts in the cluster.
6. Verify that the list of hosts with the VTE agent is all cluster host members and GPFS cluster members.
7. On the DSM, add GuardPoints to the cluster host group.

Pre-installation checklist

1. Verify the following environment is installed:
   a. AIX 6.1 at TL5 or higher
   b. RSCT 2.5.5.0 file sets or higher
   c. GPFS 3.5.0.22 or higher

NOTE: GPFS must be shut down when installing, upgrading, or uninstalling the VTE agent.

2. Determine how you want to name the hosts: FQDN, host name, or IP address.
   - If FQDN, verify that DNS is configured and resolving host names on the DSM.
   - If host name, use the host CLI command to link IP addresses with host names, or edit `/etc/hosts` directly.
3. Follow the best practices as described in "Best practices for CPM role designation" on page 46 to determine the host in the GPFS cluster on which you will install the VTE agent. Installation on the primary creates VormetricDomain, which is required for installing the agent on the other hosts in the cluster.
4. Designate a host in the GPFS cluster as the secondary Cluster Policy Manager. The rest of the hosts in the cluster will be members.

Configure the DSM

This section describes the steps for installing the VTE agent for GPFS.

To add hosts to the DSM

1. Log on to the DSM as type Security Administrator with Host role permissions, or type All with full administrator privileges.
2. Switch to the domain that will contain the host. Click **Domain > Switch Domains**, and then select the domain you want and click **Switch to Domain**.
3. Select **Hosts > Hosts** in the menu bar. The **Hosts** window opens.
4. Click **Add**. The **Add Host** window opens.
5. In **Host Name**, enter the IP address or FQDN. This is the name that will be used when the certificate is generated.
6. In **Password Creation Method**, select **Manual**.

NOTE: Do not use **Generate** as the **Password Creation Method**.

7. Enter a host password, and confirm it.
8. Optional: In the **Description** field, enter an identifier for this host group. The maximum number of characters is 256.
9. For **Registration Allowed Agents**, select **FS**.
10. Select the license type you will use on this host. Options are **Perpetual**, **Term**, and **Hourly**.
11. Click **Ok**. The **Hosts** window opens.

12. Click on the hostname of the host you just added. The **Edit Host** window opens.
13. Under the **General** tab, in the **Agent Information** area, select **Communication Enabled** in the FS agent row.

NOTE: Be sure that communication is enabled on your DSM for your GPFS agent installation. Do NOT use one-way communication for GPFS—ensure that this checkbox is empty (unchecked) on your DSM. Ensure that all networking connectivity is working between the DSM and the host where the agent will be installed before doing the installation.

14. The **Certificate Fingerprint** column. (This should be empty.)
15. Click **Ok**. The **Hosts** window opens.
16. Repeat steps 4 through 15 for all the hosts in the cluster.

To add a cluster host group

1. Select **Hosts > Host Groups** in the menu bar. The **Host Groups** window opens.
2. Click **Add**. The **Add Host Group** window opens.
3. In **Host Group Name**, enter the name for the host group. This field is mandatory. The maximum number of characters is 64.
4. Select **Cluster Group**, and then select **GPFS**.
5. Optional: Add a **Description** to identify this cluster host group. The maximum number of characters is 256.
6. Click **Ok**. The **Host Groups** window opens.

To add a host to the cluster host group

1. In the **Name** column of the **Host Groups** window, click the name of the host group you just created. The **Edit Cluster Host Group** window opens.
2. Select **FS Agent Communication Enabled**.

NOTE: Be sure that communication is enabled on your DSM for your GPFS agent installation. Do NOT use one-way communication for GPFS—ensure that this checkbox remains empty (unchecked) on your DSM. Ensure that all networking connectivity is working between the DSM and the host after agent registration.

3. Click the **Member** tab, and then click **Add**. The **Edit Cluster Host Group - Add Host** window opens.

4. In the **Select** column, select the hosts to add to the cluster host group.
5. Click **Ok**.

Install the VTE Agent on a GPFS host

This section describes how to install the VTE agent on an existing GPFS host.

NOTE: GPFS must be shut down when installing, upgrading, or uninstalling the VTE agent.

When you have fulfilled the following, you are ready to install the VTE Agent.

1. You have added all the hosts from the GPFS cluster to the DSM.
2. You have created a cluster host group on the DSM.
3. You have added the hosts to the cluster host group.

To install the agent on the primary CPM

1. SSH to the host that is designated as the primary CPM or member. Log on as root.
2. Copy or mount the VTE agent installer to the host system. The naming format of the installer is:

   `vee-<product-version-build-system>.bin`

   Example:

   `vee-fs-5.2.7.8-aix71.bin`
3. Execute the installer. Type:

   `#./vee-<product-version-build-system>.bin`
4. At the License Agreement prompt, type `Yes`.
5. At the prompt, "`Is this a GPFS Installation?`", type `Yes`.
6. At the pureScale installation prompt, type `N` for no.
7. At the role of this host prompt, type **`Primary`**.
8. At the prompt, type **Y**, to run the agent registration process. You must know the host name of the machine running the DSM and the agent's host machine must be pre-configured on the DSM.

To install the agent on the secondary CPM and members

1. SSH to the host that is designated as the secondary CPM. Log on as root.
2. Copy or mount the VTE agent installer to the host system. The naming format of the installer is:

```
vee-<product-version-build-system>.bin
```

Example:

```
vee-fs-5.2.7.8-aix71.bin
```

3. Execute the installer. Type:

```
#./vee-<product-version-build-system>.bin
```

4. At the License Agreement prompt, type **Yes**.
5. At the prompt, "`Is this a GPFS Installation`?", type **Y** for yes.
6. At the pureScale installation prompt, type **N** for no.
7. At the role of this host prompt, type **Secondary**. If you have already installed a secondary, type **Member**.
8. At the prompt, provide the FQDN of the primary CPM for this installation. Use the hostname of the primary CPM.
9. At the prompt, confirm the name of the Primary CPM.
10. At the prompt, type **Y**, to run the agent registration process. You must know the host name of the machine running the DSM and the agent's host machine must be pre-configured on the DSM.
11. When you have installed the agent on all hosts, and registered agents on all the hosts, verify cluster membership of the `VormetricDomain` to match GPFS cluster members. To verify, the list of hosts reported in the output of the command `lsrpnode` must match the members of the GPFS cluster. Type:

```
# /usr/sbin/rsct/bin/lsrpnode -i
```

Add GuardPoints

This section describes how to add GuardPoints to a host group.

When you have fulfilled the following, you are ready to add GuardPoints.

1. You have added all the hosts from the GPFS cluster to the DSM.
2. You have created a cluster host group on the DSM.
3. You have added the hosts to the cluster host group.
4. You have installed and registered agents on all the hosts in the cluster.

Once installed, the VTE agent is active on the entire cluster. Although GuardPoints can be activated now, the agent will not encrypt data under the GuardPoint unless all NSD devices are assigned to an NSD of type `secvmdisk`.

Best practice for GuardPoint administration for GPFS

- Cluster environments impose timely requirements for availability of file systems, and subsequently, GuardPoint resources. Policy information for GuardPoints must be available to all hosts across the cluster before any host tries to mount a file system. This high-availability requirement is not always achievable with GuardPoints configured for auto-guard.
- The manual-guard option allows the DSM administrator to delegate administration of a GuardPoint to the managed host mounting the file system and prevent hosts trying to mount a file system before the GuardPoint is enabled.

NOTE: Be sure that the file systems with GuardPoints are composed of only `secvmdisk` type NSD devices.

To add GuardPoints to a cluster host group

Before adding GuardPoints:

- Be sure that all file systems consist of `secvmdisk` type NSD devices. Run the **`mmlsnsd -x`** command to check the type.
- To convert any disk to `secvmdisk` type, run the `mmcommon` utility ("Adding a disk to GPFS with GuardPoints" on page 66).
- Be sure to use the manual-guard option when creating a GuardPoint as described in "Best practice for GuardPoint administration for GPFS" on page 53.

1. Log into the Management Console as an administrator of type **Security Administrator** with Host role permissions or type **All**.
2. Click **Hosts > Host Groups**. The **Host Groups** window opens.
3. In the **Name** column, click the name of the **Host Group**. The **Edit Cluster Host Group** window opens to the **General** tab.
4. Click the **Guard FS** tab. This tab displays the applied policies, the host groups to which the policies are being applied, and their enforcement status.
5. Click **Guard**. The **Guard Host Group File System** window opens to enable you to select the desired File System Agent policy and apply it to the desired GuardPoint as follows:
   - **Host to Browse**—Click **Select** to choose the host (the host where you will apply the GuardPoint).
   - **Policy**—Select the desired policy from the drop down list.
   - **Type**—Select the Directory (Manual Guard) option from the drop down list.

- **Path**—Click **Browse**; the **Remote File Browser** window opens. Select the path where the GuardPoint will be applied. Confirm that the selected directory is under a GPFS file system, as you are configuring a GuardPoint under a cluster host group. Click **Ok**.

6. Click **Ok** in the **Guard Host Group File System** window.

VTE for pureScale

This section provides an overview of how to install and configure VTE agent in a DB2 pureScale environment. A pureScale cluster consists of host members with shared access to a common database. The file system providing shared access to the database on each member is GPFS. Your DB2 installation is configured as a system managed or user managed file system. User managed implies that it is a user, not DB2, managing GPFS file system space for database. In both configurations, you must configure GuardPoints for manual guard administration.

If you are not installing VTE agent to protect your GPFS file system under DB2 pureScale, see "Installing the VTE Agent for GPFS" on page 48.

Pre-Installation checklist

1. For installation of the VTE agent, determine how you want to name the hosts: FQDN, host name, or IP address.
   - If FQDN, verify that DNS is configured and resolving host names on the DSM.
   - If host name, use the host CLI command to link IP addresses with host names, or edit `/etc/hosts` directly.
   - If using IP addresses, be sure to select an IP address during agent installation.
2. Designate primary CPM role, and designate secondary CPM role, if applicable.

Installation overview - pureScale

This overview describes the high-level steps that should be followed when installing the VTE Agent for DB2 pureScale, in the order they should be executed.

- Follow IBM/DB2 guidelines for installing and configuring the pureScale software on your cluster.
- Install the VTE agent on all DB2 members and Caching Facility (CF) nodes of your cluster.
- Follow the guidelines for designation of a host as primary and/or secondary CPM role, as described in "Best practices for CPM role designation" on page 46. Designate primary CF node

to primary CPM role and secondary CF to secondary CPM. If your cluster does not have a secondary CF, do not designate a DB2 member node to secondary CPM role.

- Choose the manual-guard option to configure GuardPoints on the DSM.
- Be sure to enter **yes** to the question: "`Is this an install of vee.fs on a DB2 pureScale cluster node?`" when installing the VTE Agent. A '**no**' response would configure the VTE agent without joining the existing cluster established when pureScale was installed and configured on your cluster.

The following steps must be followed to install the VTE Agent in your pureScale cluster.

1. On the DSM, add hosts from the GPFS cluster to the DSM.
2. On the DSM, create a cluster host group for your pureScale cluster.
3. On the DSM, add the hosts to the cluster host group.
4. Install the VTE Agent on the primary CPM.
5. Install the VTE Agent on the rest of the hosts in the cluster.
6. Upon completion of installing VTE agent on your cluster, be sure that members of your cluster host group on the DSM, the cluster of VTE agents, and the pureScale cluster, are the same hosts. Refer to "VTE Agent administration utility – voradmin" on page 71 to determine how to examine the membership status of the VTE agent cluster.
7. Migrate your GPFS file systems for file system encryption.
8. On the DSM, add GuardPoints to the cluster host group.

Configure the DSM

This section describes the steps for installing the VTE Agent for GPFS with pureScale.

Before you install the VTE Agent on each host, add the host members of your pureScale cluster to the DSM, and then add them to a cluster host group on the DSM. Hosts must be configured for VTE (File System) Agents and added to the DSM manually. They cannot be added in batch mode.

1. Log on to the DSM as type Security Administrator or an administrator of type All.
2. Switch to the domain that will contain the host. Click **Domain > Switch Domains**, and then select the domain you want and click **Switch to Domain**.
3. Select **Hosts > Hosts** in the menu bar. The *Hosts* window opens.
4. Click **Add**. The *Add Host* window opens.
5. In **Host Name**, enter FQDN of the new host. This is the name that will be used when the certificate is generated.

6. In **Password Creation Method**, select **Manual**. The *Host Password* and *Confirm Host Password* fields appear.
7. Enter a host password, and confirm it.
8. Optional: In the **Description** field, describe this host.
9. For **Registration Allowed Agents**, select the **Key** check box.
10. In the **License Type** list, select the license type you are using on this host. Options are **Perpetual**, **Term**, and **Hourly**.
11. Click **Ok**. The *Hosts* window opens.
12. Click on the hostname of the host you just added. The *Edit Host* window opens.
13. Under the **General** tab, in the *Agent Information* area, select **Communication Enabled** in the FS agent row.

NOTE: The **Certificate Fingerprint** column should be empty.

14. Click **Ok**. The *Hosts* window opens.

To add a cluster host group

1. Select **Hosts > Host Groups** in the menu bar. The *Host Groups* window opens.
2. Click **Add**. The *Add Host Group* window opens.
3. In **Host Group Name**, enter the name for the host group. This field is mandatory. The maximum number of characters is 64.
4. Select **Cluster Group**, and then select **GPFS**.
5. Optional: Add a **Description** to identify this cluster host group. The maximum number of characters is 256.
6. Click **Ok**. The **Host Groups** window opens.

To add a hosts to the cluster host group

1. In the **Name** column of the *Host Groups* window, click the name of the host group you just created. The *Edit Cluster Host Group* window opens.
2. Select **FS Agent Communication Enabled**.
3. Click the **Member** tab, and then click **Add**. The *Edit Cluster Host Group - Add Host* window opens.
4. In the **Select** column, select the hosts to add to the cluster host group.
5. Click **Ok**.

Install the VTE agent for pureScale

To install VTE Agent, At this point, your pureScale cluster is down and ready for installing the VTE Agent.

1. Put the pureScale cluster in maintenance mode.
2. Follow instructions in "Install the VTE Agent on a GPFS host" on page 51 to install VTE Agent on each member of pureScale cluster. Be sure to enter '**yes**' to the question of installing VTE agent for pureScale, and be sure to install the agent on the primary CF node first, next on the secondary CF if present, and finally on DB2 members.
3. Exit pureScale maintenance mode.
4. When the installation of the VTE Agent is finished, the VTE Agent cannot detect the cluster membership of the hosts in the pureScale cluster.

   a. Restart the VMD process on each node of the pureScale cluster to enable each VTE Agent instance to detect the cluster membership.
   Follow these steps as root administrator.
5. Run the `voradmin` command to verify cluster membership of the pureScale node as viewed by the VTE agent:

```
# voradmin cluster status
```

Migrate the database for File System encryption

Migrate the database after installing the VTE agent on all hosts and before you apply the GuardPoints and policies.

To migrate the database

1. Shut down the DB2 database.
2. Shut down GPFS on the entire cluster.
3. Convert the NSD type of disks that belong to the file systems that will have GuardPoints: The example below shows conversion of a file system device called `dbfs`:

```
mmcommon changeNSD –disk-type secvmdisk –f dbfs
```

4. Set the DSM policy for `dataxform` in the cluster host group.
5. Restart GPFS and mount the file systems.
6. Run `dataxform` from clear to encrypt from any one node.

7. After `dataxform` is done, remove the `dataxform` policy and set the encryption policy on the GuardPoints enabled under the cluster host group on the DSM.

NOTE: You must manually enable the GuardPoints.

8. Start DB2 database on all nodes sequentially. Your pureScale cluster is secure.

Sample install output

Following provides sample output of the pureScale environment before installing the VTE agent and the actual steps while installing the agent. The pureScale cluster used below is a 3-node cluster with one CF and 2 DB2 members. The hostname of the CF node in this example is `cf_host`.

```
# ./vee-fs-5.2.7.8-aix71.bin
...
Do you accept this license agreement? (Y/N) [N]: y
New VTE Agent Install
Is this a GPFS cluster install? (Y/N) [N]: y
Checking OS levels
Checking for GPFS
***** Checking for DB2 pureScale Installation *****
Is this an install of vee.fs on a DB2 pureScale cluster node? (Y/N) [N]: y

     ***** Configuring the Vormetric Encryption Agent for GPFS *****

 Please enter the role that this host will perform
 Valid roles are "primary", "secondary" or "member".
 You may enter "p" for "primary", "s" for "secondary".
 The default role (blank or "m") is "member".
 role [m]: p

 Role is "primary".

 Is this correct?
 Enter "Y" (or blank) for yes, "N" for no (and try again),
 or anything else to exit this installation
```

```
 (Y/N) [Y]: y

***** Installing on Host fslpar912 as a primary host *****
+-----------------------------------------------------------------------------+
                    Pre-installation Verification...
+-----------------------------------------------------------------------------+
Verifying selections...done
Verifying requisites...done
Results...

SUCCESSES
---------
 File sets listed in this section passed pre-installation verification
 and will be installed.

 Selected File sets
 ------------------
 vee.fs 5.2.6.20                            # Vormetric Encryption Expert ...

 << End of Success Section >>

+-----------------------------------------------------------------------------+
                   BUILDDATE Verification ...
+-----------------------------------------------------------------------------+
Verifying build dates...done
FILESET STATISTICS
------------------
    1 Selected to be installed, of which:
        1 Passed pre-installation verification
 ----
    1 Total to be installed

+-----------------------------------------------------------------------------+
                         Installing Software...
+-----------------------------------------------------------------------------+
```

```
installp: APPLYING software for:
        vee.fs 5.2.6.20

Finished processing all file sets. (Total time: 15 secs).

+-----------------------------------------------------------------------------+
                                Summaries:
+-----------------------------------------------------------------------------+

Installation Summary
--------------------
Name                        Level           Part        Event       Result
-------------------------------------------------------------------------------
vee.fs                      5.2.7.8         USR         APPLY       SUCCESS
vee.fs                      5.2.7.8        ROOT        APPLY       SUCCESS
Configuring with PRIMARY role

Callbacks are already registered.

Starting the Vormetric Agent
Starting the Vormetric Encryption Expert File System Agent.
Stopping the vmd...already stopped
Stopping the secfsd...done
Kernel extension agent/secfs/.sec/mod/secfs2 was successfully loaded,
kmid=a141f000
Kernel extension agent/secfs/.sec/mod/secvm was successfully loaded,
kmid=a14ae000
Starting the secfsd...done
Starting the vmd...not yet registered; not starting
Stopping sshd
Restarting sshd
Encryption Expert File System Agent started.
Tivoli Systems Automation (TSA) support script for has been installed or
updated.
Please review README in /secfs/TSA for more information.
```

```
Welcome to the Vormetric Encryption Expert File System Agent
Registration Program.

Agent Type: Vormetric Encryption Expert File System Agent
Agent Version: 5.2.7.8

In order to register the Vormetric Encryption Expert File System Agent
with a Vormetric Data Security Server:
    1) you must know the host name of the machine running the
       Security Server (the host name is displayed on the
       Dashboard window of the Management Console), and
    2) unless you intend to use the 'shared secret' registration method,
       the agent's host machine must be pre-configured on the
       Security Server as a host with the 'Reg. Allowed'
       checkbox enabled for this agent type on the Hosts window
       of the Management Console.

Do you want to continue with agent registration? (Y/N) [Y]: y

Please enter the primary Security Server host name: dsm-1.com

You entered the host name dsm-1.com
Is this host name correct? (Y/N) [Y]: y

Please enter the host name of this machine, or select from the following
list. If using the "fingerprint" registration method, the name you provide
must precisely
match the name used on the "Add Host" page of the Management Console.

[1] host-1.com
[2] 10.3.59.12

Enter a number, or type a different host name or IP address in manually:
What is the name of this machine? [1]: 2
```

```
You selected "10.3.59.12".

Would you like to register to the Security Server using
a registration shared secret (S) or using fingerprints (F)? (S/F) [S]: f

It is possible to associate this installation with the hardware of this
machine. If selected, the agent will not contact the DSM or use any
cryptographic keys if any of this machine's hardware is changed. This
can be rectified by running this registration program again.
Do you want to enable this functionality? (Y/N) [Y]: y

Generating certificate signing request for the kernel component...done.
Signing certificate...done.
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.

The following is the fingerprint of the EC CA certificate.
Please verify that it matches the fingerprint shown on the Dashboard
page of the Management Console. If they do not match, it can indicate an
unsuccessful setup or an attack.

EA:6D:01:09:43:D6:73:0B:BC:E4:68:4C:F2:3B:92:4D:FB:77:B8:67
Do the fingerprints match? (Y/N) [N]: y

The following is the fingerprint for this agent on this host.
Please verify that it matches the fingerprint shown for this host on the
Edit Host window of the Management Console.

FB:4D:10:52:CD:20:22:55:50:B3:2C:9C:A1:B7:D5:2B:16:41:C0:17

Successfully registered the Vormetric Encryption Expert File System Agent
with the primary
```

```
Vormetric Data Security Server on dsm-1.com.
Installation success.
```

System Administration Tasks

This section provides a high level overview of the tasks a system administrator must perform to install, configure and maintain VTE agent in a GPFS cluster environment.

Adding a host to your GPFS cluster

When you add a host to your GPFS cluster for installing the VTE agent, the host is added to the peer domain enabled on your cluster. The administration tasks are divided between DSM and GPFS. You do not need to shut down GPFS or unmount your file systems on any member of your cluster until you mount GPFS file systems with GuardPoints on the new host.

1. On the DSM, define a host entry for the new host and add the host entry to the cluster host group for the GPFS cluster.
2. Install and add the new host to your GPFS clusters. Do not mount your file systems on the newly added host until GuardPoints are enabled on the new host.

NOTE: Mounting and accessing a file system on a node not installed with the VTE Agent will result in corruption if the file system is mounted with GuardPoints enabled on other nodes.

3. Install the VTE agent on the new host. Register the host with the DSM at the end of the install.

   Upon successful registration, the VTE agent on the host is enabled and ready for operation.
4. Verify cluster membership of the VTE agent to match GPFS cluster members. To verify, the list of hosts reported in the output of the `lsrpnode` command must match the members of GPFS.

```
# /usr/sbin/rsct/bin/lsrpnode -i
```

NOTE: Before starting the application on the newly added node, mount your GPFS file systems. The GuardPoints configured on your GPFS file system will automatically be enabled on the new host upon mounting each GPFS file system. Once the GuardPoints are enabled, you can start your application service on the new host.

Removing a host from your GPFS cluster

Before removing a node from your GPFS cluster, you must disable the active GuardPoints on the host to be removed.

- The GuardPoints on your GPFS cluster must be configured for manual guarding.
- Disable GuardPoints by running the `secfsd` command on the host to be removed.

Use the `-local` option of the `secfs` command to keep the GuardPoints enabled on other members of your cluster, as follows:

```
# mount | grep secfs
# /usr/bin/secfsd -unguard <GuardPoint Path> -local
```

The next step is to unmount your GPFS file systems and then shut down GPFS on the host being removed. After shutdown you can remove the installed file set of the VTE agent by typing:

```
# /opt/vormetric/DataSecurityExpert/agent/vmd/bin/uninstall
```

NOTE: Removal of the VTE agent does not remove the `VormetricDomain` peer domain from the host.

NOTE: `VormetricDomain` is not available in the DB2 pureScale environment.

In a non-DB2 pureScale environment, you can manually remove the host from the peer domain by running the **`rmrpnode`** command. The **`rmrpnode`** command must be run on one of the remaining hosts in your cluster to remove the host from the peer domain. Run the **`lsrpnode`** command to identify a preferred node in your cluster. A host entry with the value '**`Yes`**' in the **Preferred** column is a preferred node.

```
# /usr/sbin/rsct/bin/lsrpnode -P
```

On the preferred host, you can remove the host from the peer domain. Assuming host2 is the host being removed from the cluster, run the following command on the group leader host:

```
# /usr/sbin/rsct/bin/rmrpnode host2
```

Shutting down or unmounting GPFS file system with GuardPoints

System administers have full control over operations on GuardPoints configured for manual-guard under cluster host group.

GuardPoints on a file system must be unguarded before unmounting the file system; otherwise GPFS fails to unmount the file system due to busy status. Similarly, shutting down GPFS in presence of active GuardPoints forces GPFS to force-unmount file systems with active GuardPoints. A forced unmount on a file system with active GuardPoints forces the VTE agent to deactivate GuardPoints regardless of application activities on GuardPoints.

NOTE: Disable GuardPoints using `secfsd -unguard`, before unmounting the file system.

Details about GuardPoint activation and deactivation are described in the following sections

To remove manual GuardPoints from the host

1. SSH to the host and log in with root privileges.
2. Type the following command followed by the GuardPoint path to deactivate the GuardPoint on all members of the GPFS cluster.

```
# /usr/bin/secfsd -unguard <GuardPoint path>
secfsd: Path is Unguarded
```

The GuardPoint is deactivated on all active GPFS hosts where the GuardPoint is applied.

Removing GuardPoints from a host group on the DSM

GuardPoints assigned and configured on the DSM can be permanently removed.

To unguard GuardPoints

Unguarding GuardPoints on the DSM permanently removes the shared GuardPoint from all members in the cluster host group. It does not delete the policy from the DSM. To reapply the policy, reapply the guard operation to the cluster host group.

1. Log into the Management Console as an administrator of type **Security Administrator** with **Host** role permissions or type **All**.
2. Select **Hosts > Host Groups** in the menu bar. The *Host Groups* window opens.
3. Click the host group in the **Name** column. The *Edit Cluster Host Group* window opens to the **General** tab.
4. Click the **Guard FS** tab. This tab displays the applied policies, the host groups to which the policies are being applied, and their enforcement status. Nothing is displayed if this is a new installation or no policies are applied.
5. Select the GuardPoint you would like to unguard.
6. Click **Unguard**.
7. The GuardPoint is removed from the list of those displayed for the Host Group.

Adding a disk to GPFS with GuardPoints

Before you add a disk to a file system device, the NSD type of the device must be configured. A file system with GuardPoints is composed of NSD devices of `secvmdisk` type only; and as such adding a new disk to a file system with a GuardPoint requires adding a new device of `secvmdisk` type.

Preferred Method

When adding a new NSD device, you can specify a `secvm` device instead of the native device. Specifying a `secvm` device allows it to be added to a guarded GPFS file system without shutting down GPFS.

The following example shows how you can create a new `secvm` NSD device, `nsd1`, from `hdisk1`.

1. Check that `hdisk1` has a corresponding `secvm` device. Type:

   ```
   ls -l /dev/secvm/dev/hdisk1 OR voradmin secvmdisk status
   ```

   If there is no `secvm` device, add one with '`voradmin secvmdisk add /dev/hdisk1`' (Refer to "Adding a new disk to a GPFS file system under a pureScale cluster" on page 70 for further details)

2. Create a stanza file with the `secvm` device,

   ```
   secvm/dev/hdisk1:::dataAndMetadata:-1:nsd1
   ```

3. Pass the stanza file into `mmcrnsd`

   The `mmcrnsd` utility will create a new `secvmdisk` type NSD from the stanza file and it will be ready to be used in a guarded GPFS file system.

Alternate Method

The `mmcommon` utility enables you to change the NSD type of the device to add to your file system from `hdisk` to `secvmdisk`. Run the `mmcommon` utility to change the NSD type of a device before adding the free device to your file system:

```
# /usr/lpp/mmfs/bin/mmcommon changeNSD --disk-type secvmdisk -d <NSD device
name>
```

4. Before running the `mmcommon` command, you must shut down GPFS.

Removing a Disk With GuardPoints from GPFS

Deletion of a device from a file system frees the device in the same NSD type as it was added to the file system. Run `mmdeldisk` to remove the device from your file system. You can choose to keep the device in NSD type `secvmdisk`, or change the type back to `hdisk`. To change the NSD type to `hdisk`, do the following:

1. Unguard manual GuardPoints using `secfsd -unguard` on any host of the cluster.
2. Shut down GPFS across the cluster.
3. Run `/usr/lpp/mmfs/bin/mmdeldisk` to remove the device from file system.
4. Run the `/usr/lpp/mmfs/bin/mmcommon` utility on the NSD device removed from file system.

   ```
   # /usr/lpp/mmfs/bin/mmcommon changeNSD --disk-type hdisk -d <NSD device name>
   ```
5. Run `/usr/lpp/mmfs/bin/mmlsnsd -X` to verify the NSD type of the device is changed to hdisk. Verify that the NSD type is `hdisk` and the device path is not `/dev/secvm/dev` in the output of `mmlsnsd –X`.
6. Restart GPFS.

Removing the VTE Agent from your cluster

1. Unguard all active GuardPoints and then shut down GPFS before uninstalling the VTE agent. Run the following command to compile a list of active GuardPoints.

   ```
   # mount | grep secfs
   ```
2. Use the following command to shut down any of the GuardPoints shown in the list:

   ```
   # /usr/bin/secfsd -unguard <GuardPoint path>
   ```
3. Unmount your GPFS file systems on all the hosts in your cluster.
4. Shut down GPFS on all hosts.
5. Remove the VTE agent from each node of your cluster. On each node, type:

   ```
   # /opt/vormetric/DataSecurityExpert/agent/vmd/bin/uninstall
   ```
6. After removing the VTE agent, remove the hosts from the peer domain, VormetricDomain peer domain. To remove a host from the peer domain, run the `lssrc` command on any member of your cluster to determine the host known to be the Group Leader of the peer domain. Type:

   ```
   # /usr/bin/lssrc -ls IBM.ConfigRM | grep GroupLeader
   ```
7. On the host identified as the Group Leader, run `/usr/bin/rmprnode` for each member of your GPFS cluster. This command removes a host from the peer domain. Type:

   ```
   # /usr/bin/rmrpnode <list of host names separated by a space>
   ```

   For example, assuming host1 is group leader and the VTE agent was removed on host2 and host3 as part of uninstalling the agent, run the following on host1.

   ```
   # /usr/bin/rmrpnode host2 host3
   ```
8. Compile list of NSD devices of type `secvmdisk`. Type:

   ```
   # /usr/lpp/mmfs/bin/mmlsnsd -X | grep secvmdisk
   ```
9. Change the NSD devices configured as `secvmdisk` to `hdisk`. Type:

```
# /usr/lpp/mmfs/bin/mmcommon changeNSD --disk-type hdisk -d <secvmdisk type
NSD>
```

10. Terminate registration of the agent with GPFS for delivery of notification. Type:

```
# /usr/lpp/mmfs/bin/mmdelcallback secfsMount,secfsPreMount,secfsPreUmount
```

11. On the host identified as group leader, remove the peer domain. Type:

```
# /usr/bin/rmrpdomain VormetricDomain
```

12. After removing the VTE agent from your cluster, remove the cluster host group on the DSM and start GPFS.

Reconfigure GPFS file systems to host GuardPoints

Before you can enable GuardPoints on GPFS, you must configure the GPFS file systems to host GuardPoints. Whether you wish to enable one or all GPFS file systems for guarding, you must shut down GPFS to prepare the file systems selected for GuardPoints. Preparing a file system for GuardPoints requires changing the NSD type for devices assigned to the file system from `hdisk` to `secvmdisk`.

Follow these steps to change the NSD type for the file systems you plan to guard:

1. Shut down GPFS across the entire cluster.
2. For each file system selected for hosting GuardPoints, run the `mmcommon` command to change the NSD type to `secvmdisk`.

   For example, a GPFS NSD device `dbfs` can be reconfigured by typing:

```
# /usr/lpp/mmfs/bin/mmcommon changeNSD --disk-type secvmdisk –f dbfs
```

3. Restart GPFS on your cluster.
4. Run the `mmlsnsd –X` command to verify successful conversion from `hdisk` to `secvmdisk`. To verify, the list of devices in the output of the `mmlsnsd -X` command for the reconfigured file system must show a device path to `secvm` devices (i.e., `/dev/secvm/dev/hdisk5`) and NSD type `secvmdisk`.

NOTE: Make sure your file system consists of devices with NSD type `secvmdisk` before enabling GuardPoints. Without `secvm` devices, encryption will not be done on data under your GuardPoints on the file system. Do not mix NSD types. A file system with mix of `hdisk` and `secvmdisk` NSD types may result in data corruption.

Administration tasks in pureScale

Adding a host to a pureScale cluster

Before you can add a host to a pureScale environment, all current DB2 members must have the VTE agent installed.

To add a host to a pureScale cluster

1. Install AIX on the new host and upgrade it to the required TL.
   a. Mount the GPFS file systems.
   b. Follow the IBM procedure for installing GPFS on the new host and adding the host to the GPFS cluster.
   c. Follow the IBM/DB2 procedure for adding a new host to your pureScale cluster. The DB2 cluster is now online with the new host as a cluster member.
2. Register the host with the DSM.
   a. Configure the host and the cluster host group on the DSM to include the new host. See "To add hosts to the DSM" on page 49 and "To add a host to the cluster host group" on page 50
3. Install the VTE agent on the new host. See "Install the VTE Agent on a GPFS host" on page 51
4. Restart VMD to detect cluster membership established by pureScale installation. Use the following command:

   ```
   /etc/rc.d/init.d/secfs restart
   ```

5. Verify that the agent has joined other agent instances in the DB2 cluster. Type:

   ```
   # /usr/bin/voradmin cluster list
   ```

6. Designate Primary/Secondary Cluster Policy Management, if necessary. The Primary and Secondary CPM role designations should be assigned to CF nodes by typing:

   ```
   /usr/bin/voradmin cluster <promote|demote>
   ```

7. Verify the current policy and GuardPoints are applied on this host. Type:

   ```
   /usr/bin/voradmin cluster policy
   ```

8. Verify the GuardPoints are available on all nodes including the one that was just added.
9. Start a DB2 instance. Type:

   ```
   su – <db2_instance_owner>
   db2start
   exit
   ```

10. Verify that the host is in the DB2 cluster. Type:

    ```
    db2cluster -cm -list -host -state
    ```

Deleting a host from a pureScale cluster

For maintenance or other reasons, you may need to remove a node from the pureScale cluster.

To remove an existing node from pureScale

1. Follow IBM DB2 procedures for removing a node from your pureScale cluster.
2. On the DSM, remove the host entry from the cluster host group. Removing the host from the cluster host group disables the GuardPoints on the host being removed.
3. Clean up the GPFS file system. See "Removing a Disk With GuardPoints from GPFS" on page 66.
4. Remove pureScale according to IBM documentation.
5. Clean the Global Registry V record GPFS_CLUSTER according to IBM documentation.
6. After complete removal of pureScale, remove the VTE Agent. Type:

```
# /opt/vormetric/DataSecurityExpert/agent/vmd/bin/uninstall
```

Adding a new disk to a GPFS file system under a pureScale cluster

Before you add a new disk to the GPFS file system under pureScale management, the disk must configured as a `secvm` layered device. Use voradmin command with option `secvmdisk` add to configure an `hdisk` device as a `secvm` layered device.

```
voradmin secvmdisk add <disk-name>
```

Use `voradmin secvmdisk` status to verify the device configuration as a `secvm` layered device:

```
# voradmin secvmdisk status
GPFS   Mounted      Secvm Disk
------------------------------
Yes    Yes     /dev/secvm/dev/hdisk1
Yes    Yes     /dev/secvm/dev/hdisk2
```

Using the `db2cluster` command you can add the disk to the GPFS file system under pureScale management. Be sure to use the `secvm` device name for the device in the `db2cluster` command for adding the device. For example, the following command adds the `secvm` layered device for `hdisk2` to the GPFS file system device named `db2fs`:

```
# db2cluster -add -filesystem db2fs -disk /dev/secvm/dev/hdisk2
```

Utilities Specifically for Use with GPFS

VTE Agent administration utility – voradmin

The `/usr/bin/voradmin` utility is an administrative tool that enables system administrators to examine the status of the VTE agent operations in a cluster. Proper operation of `voradmin` relies on the availability of the `vmd` daemon process. Without `vmd` running the `voradmin` utility hangs indefinitely.

An administrator can examine status of policy propagation, node membership, and NSD devices configured as `secvmdisk` type. The syntax for running the `voradmin` utility is as follows:

```
# /usr/bin/voradmin [secvmdisk <options> | [cluster <options>]
```

With secvmdisk option, a user can do the following:

```
# /usr/bin/voradmin secvmdisk [add | remove] [device list | -f DiskListFile]
```

The `secvmdisk add` option configures one or more devices as `secvm` layered devices. A device configured as a `secvm` layered device can be added to GPFS as a `secvmdisk` NSD device. GPFS NSD discovery process can discover devices of `hdisk` and `secvmdisk` types. The device list is a space separated list of `hdisk` devices. If the device list is too long, you can use the `-f` option to provide a file name containing the list of devices separated with a space.

The `secvmdisk remove` option removes a list of `secvm` layered devices that are no longer in use in GPFS. Before you detach a device from your cluster you must remove the control of the device from `secvm`.

With a cluster you have the following options:

```
# /usr/bin/voradmin cluster [ policy [-l] | status ]
[ [ promote | demote ] [ primary | secondary] ]
```

The `cluster policy` option outputs a message indicating the status of policy propagation in your cluster. One of the following messages will be displayed depending upon approval of each member for policy propagation. A policy propagation process is initiated when the primary CPM designated node receives new policy information from the DSM:

`Policy Hash Values not synced` when members do not agree on the pushed policy

`Policy Hash Values are synced` when members all agree on the pushed policy

Using the `-l` option with cluster policy displays two hash values. One hash value labeled as `Pushed`, represents the last policy pushed from the DSM to the host. The other value is labeled `Applied`, representing the current policy in effect on all instances of the agent in the cluster. When `Pushed` and `Applied` values are the same, the VTE agent on all hosts of your cluster agree on the current value in effect in the cluster.

The `cluster status` option outputs the status of membership of each instance in the cluster. The output consists of multiple lines with each line providing the membership status of each

instance of the VTE agent. In addition, each line displays the host name, the host ID, the designated CPM role, the state of membership, and extended status of the membership, if available, for each node. The states are described below:

- `INIT` — the instance has initialized its connection to RSCT
- `JOINING` — the instance is in the process of joining the cluster
- `JOINED` — thee instance has joined the cluster
- `PAUSING` — the instance is in the process of resetting self
- `PAUSED` — the instance has reset self without changing CPM role designation
- `ERROR` — the instance has encountered an unrecoverable error, refer to the log
- `LEFT` — the instance has departed from the cluster
- `ACTIVE` — the instance is an active member of the cluster
- `REJECTED` — the instance rejected the last cluster-wide policy propagation

The extended status of the membership may be blank or provide one of the following statuses. Extended status is provided if the instance is in a `JOINED` state:

- `PAUSING` — the instance is in the process of resetting self
- `PAUSED` — the instance has reset self without changing CPM role designation
- `LEAVING` — the instance is in the process of departure from the cluster
- `ROLECHGDCPM` — the role designation has been changed on this instance
- `ERROR` — the instance has encountered an unrecoverable error, refer to the log
- `NORESP` — the instance has not been timely responsive to RSCT
- `ETIME` — the instance has timed out on its last operation
- `AWAITING PRIMARY` — the instance is waiting for primary node to join and delegate its CPM role to the cluster

The CPM role designation to each instance will be display as follow:

- `PRIMARY` — the instance is the designated `PRIMARY` in cluster
- `SECONDARY` — the instance is the designated `SECONDARY` in cluster
- `MEMBER` — the instance is not primary, nor secondary

One of the instances designated as `MEMBER` may be labeled with (g). This is a label identifying the instance that may become responsible for passing down information on active GuardPoints to newly joined instances in the cluster. This information is internal to VTE agents.

In the output of `voradmin` cluster status the `hostname` proceeded with '*'is the host running the `voradmin` command.

Specifying `-t <seconds>` and `-c <count>` with cluster status displays the membership status of each for the specified number of times, count, in the specified seconds interval.

VTE GuardPoint Administration Utility – secfsd

The `secfsd` utility can operate in cluster mode on GuardPoints under GPFS file systems. By default, the `secfsd` utility does cluster-wide guard or unguard operations on GPFS-based GuardPoints. Cluster-wide operation of `secfsd` relies on the availability of the `vmd` daemon. Without the `vmd` daemon running, the `secfsd` utility fails and hangs for the cluster-wide guard or unguard operation.

An attempt to guard or unguard a GuardPoint initiates a cluster-wide request from the local `secfsd` process to other `secfsd` instances running on the other hosts in your cluster. Each `secfsd` process performs a local guard or unguard on the specified GuardPoint. When the local operation is complete, local access to the GuardPoint is blocked until the GuardPoint is guarded on all participating hosts in a cluster-wide guard/unguard operation. If any host fails to guard or unguard the specified GuardPoint, the operation fails on all nodes.

If the cluster-wide effect of a `secfsd` guard or unguard operation is not desired, you must specify `-local` for local guard or unguard operation. The syntax is as follow:

```
# /usr/bin/secfsd –[guard | unguard] <guard-point> [-local]
```

mmcommon Command

Use the GPFS `mmcomman` command to configure or change NSD type of GPFS NSD devices. You can configure or change the NSD type of a single NSD device or all NSD devices that to a GPFS file system. The usage of `mmcommon` for NSD type configuration is as follows:

```
# mmcommon changeNSD --disk-type <NSD type> -a | -F | -f <FS Device> | -d <NSD
device list>
```

Specify `secvmdisk` to assign `secvmdisk` NSD type to the specified device(s). Use `-a` to change the NSD type for all devices added to GPFS.

- Use `-F` to change the NSD type for all free devices.
- Use `-f` to change the NSD type to the specified type, following `-disk-type`, for all NSD devices belonging to the specified file system. The file system device name is specified after `-f`.
- Use `-d` to change the NSD type to the specified type, following `-disk-type`, for all NSD devices listed after `-d`. The NSD device list is a comma separated NSD device list.

For example, the following command changes the NSD type to `secvmdisk` for all NSD devices assigned to the `dbfs` file system:

```
# mmcommon changeNSD --disk-type secvmdisk -f db2fs
```

VTE for AIX Utilities

This chapter describes VTE for AIX utilities.

Thales provides a variety of utilities that an administrator can use to help manage VTE. These utilities reside in storage until summoned by the administrator.

The following utilities are described in this chapter:

secfsd utility

The `secfsd` utility displays the following attributes of VTE:

- GuardPoints defined in the *Guard FS* tab
- Authentication parameters defined in the *Host Settings* tab
- Lock status set by enabling FS Agent Locked and System Locked
- Web destination and SSL certificate for uploading log entries
- Policies applied in the **Guard FS** tab
- Status of required processes (`secfsd` and `vmd`)
- Version of `secfs`

The `secfsd` utility is also used to mount GuardPoints for `Directory (Manual Guard)`. Normally, VTE automatically mounts the `secfs` file system when you

apply a GuardPoint to a directory. On AIX, the `secfsd` utility is located in `<install_dir>/secfs/.sec/bin` and a symbolic link to this file is placed in `/usr/bin/secfsd`.

secfsd syntax

Table 4: `secfsd` Syntax

Command	Description
`-help`	display `secfsd` options
Status Options	
`-status guard [-v]`	list all GuardPoints
`-status keys`	show current encryption key state
`-status auth`	list authentication settings
`-status lockstat`	show VTE lock status
`-status logger`	list logging details
`-status policy`	list configured policies
`-status pslist`	list protected processes
`-status devmap`	list guarded devices
Manual GuardPoint options	
`-guard path [-local]`	manually guard path
`-unguard path [-local]`	manually unguard path
Version option	
`-version`	list version of kernel module `secfs2`

Examples

Updating status file

To create or update the `/var/log/vormetric/statusfile` file, type:

```
# secfsd -status
```

VTE does not remove the file after a configuration change. It updates when you run any of the `secfsd -status` commands.

Display GuardPoint-related information

To display the GuardPoint paths, applied policies, policy type, and guard status, type:

```
# secfsd -status guard
```

System Response

```
# secfsd -status guard
GuardPoint     Policy           Type          ConfigState   Status    Reason
----------     ----------      -----         -----------   ------     -----
/opt/apl/lib   allow AllOps_fs  local         guarded       guarded     N/A
/dev/sdb       watchaccess_rd   rawdevice     guarded       guarded     N/A
/dev/sdc       watchaccess_rd   manualrawdevice guarded      guarded     N/A
/dev/sdd       watchaccess_rd   manualrawdevice unguarded    not guarded
Inactive
/opt/apl/tmp   MSSQL00123        manual       unguarded     not guarded
Inactive
```

GuardPoint	Full path of the GuardPoint.
Policy	Name of the policy applied to the GuardPoint.
Type	Can be local, automount, manual, raw device, or manual raw device. Configured in the Guard FS tab.
ConfigState	Guard status of the GuardPoint, as recognized by the DSM. It can be guarded or unguarded.
Status	Current guard status, as recognized by VTE. State can vary.

Display GuardPoint-related information in a different format

To display the same information in a different format, include the `-v` argument, type:

```
# secfsd -status guard -v
```

System Response:

```
GuardPoint: 1
        Policy:         allowAllOps_fs
        Directory:      /opt/apps/apps1/tmp
        Type:           local
        ConfigState:    guarded
        Status:         guarded
        Reason:         N/A
GuardPoint: 2
        Policy:         allowAllRootUsers_fs
        Directory:      /opt/apps/apps1/lib
        Type:           local
        ConfigState:    guarded
        Status:         guarded
        Reason:         N/A
GuardPoint: 3
        Policy:         allowAllOps-winusers1_fs
        Directory:      /opt/apps/apps1/doc
        Type:           local
        ConfigState:    guarded
        Status:         guarded
        Reason:         N/A
```

Display host settings

Use the `auth` argument to display the SHA2 hash signature for each VTE host setting, type:

```
# secfsd -status auth
```

System Response:

```
|authenticator|/usr/sbin/tsm
2FB799BE9E0277EC3FAA1ABA1CB5AA559B394C4FB41D4DDF28B50619F14AFDE2

|authenticator|/usr/sbin/sshd
2C55C2ECEF8DD08C406C89F1436E5223B98F42AC857B6E56B4AF2C89844F7D45

|realfsid|/usr/bin/mksysb
233CACCF96C41CA7CF0E437DAC9C69E1AAFB70769103D26FEE21C6ECB40E8726
```

The host setting and hash value are also displayed in `/var/log/vormetric/statusfile` Display Key Status

To display the status of VTE keys, type:

```
# secfsd -status keys
```

System Response:

```
Encryption keys are available
```

Display Lock Status

To display the status of VTE locks, type:

```
# secfsd -status lockstat
```

System Response:

```
FS Agent Lock: false
System Lock: false
```

The value is **true** if the lock is applied. The value is **false** if the lock is not applied. **System Lock** corresponds to **System Locked** in the *Host* window. **FS Agent Lock** corresponds to **FS Agent Locked** in the *Host* window.

NOTE: Before you upgrade, remove VTE software, or change operating system files, the status of FS Agent Lock and System Lock must be false.

Display VTE Log Status

To display the status of VTE log service, type:

```
# secfsd -status logger
```

System Response:

```
Upload URL:
https://vmSSA06:8444/upload/logupload,https://vmSSA07:8444/upload/l
ogupload,https://vmSSA05:8444/upload/logupload

Logger Certificate directory:
/opt/vormetric/DataSecurityExpert/agent/vmd/pem
```

This command sequence returns the URL to which the log service sends log data. It also returns the directory that contains the VTE certificate. VTE uses the certificate to authenticate VTE when it uploads the log data to the DSM.

Display Applied Policies

To display the policies that are applied to VTE, type:

```
# secfsd -status policy
```

System Response:

```
Policy: allowAllOps_fs

Type: regular

Policy: allowAllRootUsers_fs

Type: regular

Policy: allowAllOps-winusers1_fs

Type: regular
```

Display VTE processes

To display VTE processes, type:

```
# secfsd -status pslist
```

System Response:

```
Protected pid list:     739   731
```

Display Detail about VTE processes

The example displays the process PID numbers for the `vmd` and `secfsd` processes. The `ps` commands show the processes for those PIDs.

```
# ps -fp <process #>
```

Example

```
# ps -fp 739
```

System Response:

```
      UID        PID     PPID   C    STIME    TTY  TIME CMD
    root  7012404        1   0 11:04:56      -  0:00
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/vmd
```

Display VTE Version Information

To display VTE version information, type:

```
# secfsd -version
```

System Response:

```
version:  5.2.7.8-aix71-powerpc
```

Manually Enable a GuardPoint

To manually enable a GuardPoint on a AIX host:

1. Click **Hosts > Hosts > *<hostName>*** > **Guard FS.**
2. Click **Guard**.
3. In the Policy field, select a policy.
4. Set Type to **Directory (Manual Guard)**.
5. Click **Browse** and enter the GuardPoint path.
6. Click **OK**.
7. Log onto the system hosting VTE as the root user.
8. Verify the change, type:

```
# secfsd -status guard
```

System Response:

```
GuardPoint    Policy         Type   ConfigState Status     Reason
----------    ------         ----   ----------- ------     ------
/opt/apps/etc allowAllOps_fs manual unguarded  not guarded Inactive
```

Verifying a GuardPath

Verify that a GuardPath is guarded, type:

```
# secfsd -guard <path>
```

For example:

```
# secfsd -guard /opt/apps/etc
```

System Response:

```
secfsd: Path is Guarded
```

secfsd and raw devices

VTE for AIX creates block and character devices.

To display them, type:

```
# ls -l /dev/secvm/dev
```

System Response:

```
brw-------    1 root     system       38,  1 Jan 29 16:37 hdisk1
brw-------    1 root     system       38,  2 Jan 29 16:37 hdisk2
crw-------    1 root     system       38,  3 Jan 29 16:37 rhdisk1
crw-------    1 root     system       38,  4 Jan 29 16:37 rhdisk2
```

vmsec utility

The vmsec utility allows you to manage security aspects of VTE on the host. On AIX -hosts, the vmsec utility is located in:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/vmsec
```

vmsec syntax

Table 5: vmsec Syntax [options]

`checkinstall`	Show vmd kernel status
`challenge`	Enter the dynamic host password
`vmdconfig`	Display the vmd configuration
`hwok`	Report status of hardware signature
`passwd [-p <password>]`	Enter the static host password
`version`	Display VTE version

Examples

Display VTE Challenge String

To display a VTE password challenge string and enter the response string when the DSM is not network accessible, type:

```
# vmsec challenge
```

System Response:

```
Contact the help desk at 1-800-555-1212 for response generation.
Your host name is "Host120" Your challenge is: HPTQ-ZYLK
Response -> IHFY-W7WG-PDAO-QKKQ
```

The contact information is configured in the DSM Management Console (Domains > Manage Domains) *Add Domain* window. Contact the DSM administrator and give them the challenge string. The DSM administrator will give you the response string. Enter the response string in the **Response** field and press **Enter**. You have 15 minutes to enter the response string.

Display VTE Status

This utility shows you if VTE is configured and running. If it is not running, you might need to start it manually.

To display VTE status, type:

```
# vmsec checkinstall
```

System Response:

```
The kernel component is installed and running.
```

Entering a Password

To enter VTE static host password, type:

```
# vmsec passwd
```

System Response:

```
Please enter password:
OK passwd
```

To enter VTE static host password on the command line so you can specify it in a batch script, type:

```
# vmsec passwd -p myPass123
```

System Response:

```
OK passwd
```

Display Kernel Status

To display the kernel status, type:

```
# vmsec status
```

System Response:

```
FILE_FORMAT=2
FILE_GENERATED=10/27/2017 18:54:10
SA_QOS_STATUS=0
SA_HOST_CPU_UTIL=0
GP_1_Policy=27
GP_1_Dir=/gp
GP_1_lock=1
GP_1_type=1
GP_1_gtype=manual
GP_1_opt=gtype=2,policy=27,lock=1,type=1,dir=/gp/
GP_1_config_state=unguarded
GP_1_status=not guarded
GP_1_statuschk_tm=0-00-00 00:00:00
GP_1_config_op_retry_cnt=0
GP_1_config_op_attempt_tm=0-00-00 00:00:00
GP_1_flags=0
GP_1_reason=Inactive
GP_1_usage=free
TOTAL_GP=1
KEYS_AVAILABLE=TRUE
sdk_version=5.2.6.22
sdk_builddate=2017-10-17 15:16:46 (PDT)
coreguard_locked=false
system_locked=false
logger_upload_url=https://thl602-
2114.qa.com:8447/upload/logupload,https://thl602-
2116.qa.com:8447/upload/logupload
logger_cert_dir=/opt/vormetric/DataSecurityExpert/agent/vmd/pem
hostname_for_logging=vmd
QOS_PAUSED=false
vmd_STRONG_ENTROPY=false
vmd_URL=https://thl602-2114.qa.com:8446
vmd_SRV_URLS=https://thl602-2114.qa.com:8446, https://thl602-
2116.qa.com:8446
```

```
vmd_PRIMARY_URL=https://thl602-2114.qa.com:8446
vmd_SUPPORTS_F8P=TRUE
vmd_SUPPORTS_CR256=TRUE
vmd_RANDHP=TRUE
learn_mode=false
concise_logging=false
vmd_listening_port=7024
vmd_initialization_time=2017-10-25 12:07:14.514
vmd_last_server_update_time=2017-10-25 12:12:04.747
policy_name_27=aes256
policy_version_27=0
policy_keyvers_27=0
policy_type_27=ONLINE
policies=27
logger_suppression_VMD=SUPPRESS
logger_intervaltime_VMD=600
logger_repeat_max_VMD=5
logger_suppression_POL=SUPPRESS
logger_intervaltime_POL=600
logger_repeat_max_POL=5
CONFIG_SA_1=27
TOTAL_CONFIG_SA=1
SA_1_NAME=27
SA_1_ALIAS=aes256
SA_1_TYPE=0
SA_1_REF=1
SA_1_HIP_REG_TIME=0
SA_1_FLAGS=1
TOTAL_SA=1
TOTAL_AUTH=0
AUTHBIN_1=|authenticator|/usr/sbin/sshd
B92A3D7EEF67B82230F7F76097D65159FCF5722A4154A249EFDC22C20F1B572C
AUTHBIN_2=|authenticator|/bin/login
4F210D1B83ACD79B006BCF7DB247ED002A45FC892C42720390BFA6AE21AEA8DC
TOTAL_AUTHBIN=2
```

Display VTE Build Information

For AIX, type:

```
# vmsec version
version 5, Service Pack 2
2018-12-17 20:41:51 ()
Copyright (c) 2009-2018, Vormetric.  All rights reserved.
```

Display Contents of Conf files

To display the contents of the `agent.conf` and `.agent.conf.defaults` files, type:

```
# vmsec vmdconfig
```

System Response:

```
appender_syslogdest_Syslog_Appender_0=127.0.0.1
VMSDK_AGENT_CONFIG_FILE=/opt/vormetric/DataSecurityExpert/agent/vmd
/etc/agent.conf
appender_layout_Syslog_Appender_0=Syslog_Layout
VMSDK_AGENT_VERSION=5.2.6.0
VMSDK_AGENT_BUILD_ID=28
PREV_URLS=https://srv.my.vormetric.com:8443
syslog_appender_myhost name=dev.my.vormetric.com
VMD_PORT=7024
...
...
appenders=Upload_Appender, File_Appender, Syslog_Appender_0
layouts=Upload_Layout, File_Layout, Syslog_Layout, Simple
CONNECT_TIMEOUT=180000
URL=https://srv.my.vormetric.com:8443
STRONG_ENTROPY=false
```

Binary Resigning

Any executable that is part of either a Host Setting or Signature set, and resides in a GuardPoint that uses an encryption policy, will use different signatures in the case

of a key rotation using Offline Data Transformation. The result is that the Host Settings binaries will no longer be authenticated, or the Signature Set policy rules will no longer trigger for those binaries. To prevent these issues, the Security Administrator must manually resign each affected binary after each key rotation.

As of VTE release 5.2.7, binaries are now signed with a signature that does not change with a key rotation. The Security Administrator will need to do one manual resigning. After that, there is no longer a need to resign after each key rotation.

If upgrading or installing a new machine using the same signature sets that you used previously, do the following:

1. Install release v5.2.7of the VTE agent (which contains the ability to generate unencrypted signatures of binaries inside GuardPoints). The previous signatures will be used until the next key rotation.
2. Before the next key rotation, the Security Administrator must resign the binaries.
3. Do not remove the old signatures on the DSM until all agents have been upgraded to VTE release 5.2.7 (which has the ability to generate unencrypted signatures on binaries inside GuardPoints). Refer to the DSM Installation and Configuration Guide for information on how to do a manual resign.
4. After all agents have been upgraded, then you can remove the old signatures.

If you are installing the VTE agents for the first time, there are no special steps, if no signatures have been defined. The agent will sign using the new method.

NOTE: In previous releases, if the binary was in a GuardPoint protected directory, but was the same as an unguarded binary, the Administrator could restrict to only the guarded binary. With this change, the unguarded binary is now unrestricted. This means that if a user uses the unguarded binary and its SHA matches the guarded binary, it will now match as if it was the guarded binary.

Enable Automatic Signing for Host Settings

A new feature of VTE blocks automatic re-signing of the host settings. Some users may have established procedures for updating system software. The user created these procedures based on their assumption that restarting the `vmd` will generate new signatures when signed software is updated. This is no longer true. To restore this behavior for updating system software, you must disable this new feature.

Disabling on AIX

1. Change to the directory where the `agent.conf` file resides. For example, type:
   ```
   # cd /opt/vormetric/DataSecurityExpert/agent/vmd/etc/
   ```
2. Edit the `agent.conf` file.
3. Change or add the following line:
   ```
   RE_SIGN_HOST_SETTINGS=TRUE
   ```
4. Save your changes and exit the file.
5. Restart the vmd to set the changes, type:
   ```
   # /etc/rc.d/init.d/secfs restart
   ```
6. Type the following to verify that the Host settings is set to true:
   ```
   # vmsec vmdconfig
   ```

Warning! Enabling the automatic regeneration of signatures exposes a potential security vulnerability for agents. When enabled, host setting binaries are resigned when it receives a push from the DSM. If an attacker were to replace a binary with a Trojan, and then force a push from the DSM by, for example, restarting the agent, VTE could generate a signature for the malicious binary and pass it to the kernel.

Restricting access overrides from unauthorized identities

<AGT-5571> <DOCSJ-730> <AGT-15309><AGT-14552>For 5.2.6 & 6.0.3

In some setups, system administrators can use the host settings > |authenticator| feature with su to change identities and gain access to restricted data. Now, you can instruct VTE to not trust any authentication attempt performed by certain identities by assigning restricted users to a user shell that VTE can block from authenticating other processes.

Any executable path that is marked with a `|path_no_trust|` host setting marks the process, and all child processes, as not trusted. Non-trusted processes are treated as "User Not Authenticated" to prevent access on user-based policies.

VTE prevents overrides from other host settings authenticators, using the `|path_no_trust|` status. If a user runs the su command from a non-trusted shell, that new shell is still marked as `|path_no_trust|`, even if `|authenticator|/usr/bin/su` is specified in the host-settings. The `|path_no_trust|` feature overrides any and all authenticators under host settings.

To restrict access overrides:

1. At the DSM management console, click **Hosts > Hosts**.
2. Click on an **existing** Host name to edit the host.
3. Click **Host Settings** tab.
4. Add the following to the host settings:

   `|path_no_trust|`*<path of the binary>*

   Example

   `|path_no_trust|/bin/ksh`

   The above example indicates that no process under the kshell executable will be authenticated.
5. Click **OK**.

vmd utility

The vmd utility displays VTE software version information.

The vmd utility is located in `/opt/vormetric/DataSecurityExpert/agent/vmd/bin` and a symbolic link to this file is placed in `/usr/bin/vmd`.

Syntax

```
vmd [OPTIONS...]
```

`-h`	show utility syntax
`-v`	display VTE version
`-f`	runs vmd in the foreground

Display the Installed Version

To display the installed VTE version, type:

```
# vmd -v
```

System Response:

```
Version 5
5.2.7.8
2018-12-17 20:41:51 ()
Copyright (c) 2009-2018, Vormetric.  All rights reserved.
```

agenthealth utility

The agenthealth utility validates:

- Super-user privilege
- VTE Agent installation
- VTE registration to DSM Server
- VTE processes/modules that are running
- Available disk resources
- Current GuardPoints

  Tests if the agent can reach the GuardPoints

The Agent health check script

To run the Agenthealth check script, type:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/agenthealth
```

System Response:

```
Checking for super-user privilege ..............  OK
Vormetric Agent installation ...................  OK
Vormetric policy directory .....................  OK
Registration to server .........................  OK
Kernel modules are loaded ......................  OK
```

```
VMD is running ..................................... OK
SECFSD is running .................................. OK
dsm602-33-101.qa.com is resolvable ................. OK
dsm602-33-101.qa.com port 8446 is reachable ....... OK
dsm602-33-101.qa.com port 8447 is reachable ....... OK
dsm602-63-183.qa.com is resolvable ................. OK
dsm602-63-183.qa.com port 8446 is reachable ....... OK
dsm602-63-183.qa.com port 8447 is reachable ....... OK
Can communicate to at least one server............. OK
VMD is listening on port 7024...................... OK
Time of last update from server.................... 2018-02-13
20:25:37.446
Checking available disk space...................... OK
Checking logging space ............................ OK
    Log directory is "/var/log/vormetric"
    File system for log data is "/", 32G free (17% full)
    Log directory contains 2 of maximum 200 files (1% full)
    Log directory contains 1 of maximum 100 Mbytes used (1% full)
Testing access to /ofx-fs1 ........................ OK
Testing access to /gp1 ............................ Access denied as
per policy
```

agentinfo utility

The `agentinfo` utility collects system and VTE configuration data. The `agentinfo` utility is used to take a configuration snapshot of the system that you will send to Thales Customer Support to debug an issue.

On AIX-systems, the utility executes data-gathering functions, such as `mount`, `df`, `station`, `oslevel`, and many more. The `agentinfo` utility is a text file. You can open it in a text editor to see specific functions.

The `agentinfo` utility displays status information on the screen and outputs the results to a compressed tar file. The compressed tar file name format is

`ai.<os_name_ver>.qa.com.tar.gz` and it is located in the current working directory.

To create an agentinfo file, type:

```
# /opt/vormetric/DataSecurityExpert/agent/vmd/bin/agentinfo
```

check_host utility

If a VTE software installation fails during the certificate generation and exchange stage, use the `check_host` utility to list the network addresses for the host. The utility checks network interfaces, `/etc/hosts`, DNS, and so on, to compare, test, and evaluate possible addresses for the host, and weights them based upon their network efficiency. FQDNs are the most preferred and stand-alone IP addresses are the least preferred. Some applications, such as silent-mode installation, use `check_host` to determine the best host address to submit to the DSM during registration.

Run the `check_host` utility on a system that is hosting VTE to display available network host names, FQDNs, and IP numbers for the host.

Type:

```
# /opt/vormetric/DataSecurityExpert/agent/vmd/bin/check_host
```

check_host Syntax

```
check_host [-h | -i | -a] [-s name] [-l name:port]
```

-h	Print the best host name for this machine
-i	Print the best IP address
-a	Print all the host names and IP addresses
-s	The name of the server (optional hint)
-r	The name of the server for name resolution checks
-l	The name and port of the server for listening checks

register_host utility

Use the `register_host` utility to create certificate requests, exchange certificates between the DSM and the host, and to register VTE on the DSM. After the host is registered, you can configure VTE, apply GuardPoints, or perform database backups. Run the AIX register_host utility in text mode on a terminal window.

Caution: The default host registration timeout is 10 minutes. If the host is unable to reach the DSM within the allotted period because of an extremely slow network connection, set the `REGISTER_HOST_TIMEOUT` environment variable to extend the registration timeout. The variable value is an integer expressed in seconds. You might also have to extend the default TCP timeout.

Concise Logging

This section describes Concise Logging and selective filtering.

This chapter contains the following sections:

Overview of Concise Logging

Thales's standard operational logging sends audit messages for each file system operation. An audit message is sent each time a file is opened, read, updated, or written. Thales's standard logging can generate high volumes of log data. Most of these messages might not be useful or required by security administrators to monitor file system activity on the system.

Concise Logging allows you to focus on relevant audit messages and important actionable messages, such as errors and warnings. It can eliminate the repetitive and less important audit messages generated by read and write activity on a file, reading and writing directory attributes, and other file system activity.

Concise Logging eliminates the following types of messages:

- Audit messages for each and every block read by the user or application. It sends only one audit message for each read/write activity.
- Audit messages that read the attributes, read the basic information of file-set attributes, and other event-based messages.
- Audit messages for directory open, read directory attributes, and directory close.

Using Concise Logging

You can enable and disable the Concise Logging option from the DSM. You can configure Concise Logging for the following:

- All registered hosts in all domains; see "Do not use Learn mode with Concise Logging." on page 96
- A host that has registered with the DSM; see "Configuring Concise Logging for a registered host" on page 97

Considerations

- Concise Logging changes the set of log messages that are sent to Security Information and Event Management (SIEM) software systems. If this results in loss of data required for customer reports, then disable Concise Logging.
- Concise Logging is only supported by VTE.
- Enable and disable Concise Logging on the host. VTE applies it to all GuardPoints and for all users on the host for which it is selected. There is no finer-grained control, such as per-GuardPoint, user, or message type.
- When you enable this setting at the DSM level, it applies to all hosts in all domains, that are added to the DSM, but does not apply to any existing hosts. Hosts added after this setting is enabled inherit this setting. The default global setting is off.
- Do not use Learn mode with Concise Logging.

Configuring global Concise Logging

You can enable or disable Concise Logging at any time. The DSM controls the function. Any change in the Concise Logging is reflected on any newly registered hosts and their domains.

To configure global Concise Logging:

1. Login to the DSM with System Admin privileges.
2. Click **System > Log Preferences**. Your system may contain multiple log tabs.
3. Click on a **Log** tab.
4. In the Duplicate Message Suppression Settings field, click **Enable Concise Logging**.
5. Click **Apply**.

6. Repeat steps for any other logs, as appropriate.

The host sends the following message after the administrator has enabled Concise Logging for an individual host:

```
DAO00821: Administrator “voradmin” updated Security Server
configuration “Concise Logging Enabled” from “true” to “false”.
```

Configuring Concise Logging for a registered host

You can enable Concise Logging for a host after you have registered it with the DSM. Hosts that are added to the DSM after enabling Concise Logging inherit the global settings from the DSM. This setting can be customized at any time.

To enable Concise Logging on the DSM for a registered host:

1. Log into your host with DSM security admin privileges.
2. Select the host that you would like to customize.
7. Select a **Log** tab.
8. In the Duplicate Message Suppression Settings, click **Enable Concise Logging**.
9. Click **Apply**.

After you enable or disable Concise Logging, VTE generates a log message to record that event:

```
"[CGA] [INFO] [CGA3201I] [11/11/2016 10:57:18] Concise
logging enable

"[CGA] [INFO] [CGA3202I] [11/11/2016 10:57:27] Concise
logging disabled
```

GLOSSARY

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 hardware appliance*, which is a hardened DSM server provided by Vormetric, or 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. Available as a complete hardened hardware system (*DSM Appliance*) or as software solution installed on a UNIX box (*software-only DSM*).

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 or third-party vault 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.

Key Vault
A Vormetric product that provides passive key vaulting. It securely stores symmetric and asymmetric encryption keys from any application and tracks key expiration dates.

KMIP
Key Management Interoperability Protocol. A protocol for communication between enterprise key management systems and encryption systems. A KMIP-enabled device or client software can communicate with the DSM to manage encrypted keys.

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**".

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, KMIP device 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.

Vormetric Vault
A virtual vault to store 3rd-party encryption keys, certificates and other security objects.

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.