THALES

Vormetric Data Security Platform

Vormetric Transparent Encryption for AIX

Installation and Configuration Guide

Release 5.3.0

OCTOBER 30, 2019

DOC V1

Vormetric Data Security Platform
Vormetric Transparent Encryption for AIX
Installation and Configuration Guide
Release 5.3.0

NOTICES, LICENSES, AND USE RESTRICTIONS

Vormetric, Thales, and other Thales trademarks and logos are trademarks or registered trademark of Thales e-Security, Inc. in the United States and a trademark or registered trademark in other countries.

All other products described in this document are trademarks or registered trademarks of their respective holders in the United States and/or in other countries.

The software (“Software”) and documentation contains confidential and proprietary information that is the property of Thales e-Security, Inc. The Software and documentation are furnished under license from Thales and may be used only in accordance with the terms of the license. No part of the Software and documentation may be reproduced, transmitted, translated, or reversed engineered, in any form or by any means, electronic, mechanical, manual, optical, or otherwise.

The license holder (“Licensee”) shall comply with all applicable laws and regulations (including local laws of the country where the Software is being used) pertaining to the Software including, without limitation, restrictions on use of products containing encryption, import or export laws and regulations, and domestic and international laws and regulations pertaining to privacy and the protection of financial, medical, or personally identifiable information. Without limiting the generality of the foregoing, Licensee shall not export or re-export the Software, or allow access to the Software to any third party including, without limitation, any customer of Licensee, in violation of U.S. laws and regulations, including, without limitation, the Export Administration Act of 1979, as amended, and successor legislation, and the Export Administration Regulations issued by the Department of Commerce, or in violation of the export laws of any other country.

Any provision of any Software to the U.S. Government is with "Restricted Rights" as follows: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277.7013, and in subparagraphs (a) through (d) of the Commercial Computer-Restricted Rights clause at FAR 52.227-19, and in similar clauses in the NASA FAR Supplement, when applicable. The Software is a "commercial item" as that term is defined at 48 CFR 2.101, consisting of "commercial computer software" and "commercial computer software documentation", as such terms are used in 48 CFR 12.212 and is provided to the U.S. Government and all of its agencies only as a commercial end item. Consistent with 48 CFR 12.212 and DFARS 227.7202-1 through 227.7202-4, all U.S. Government end users acquire the Software with only those rights set forth herein. Any provision of Software to the U.S. Government is with Limited Rights. Thales is Thales eSecurity, Inc. at Suite 710, 900 South Pine Island Road, Plantation, FL 33324.

THALES PROVIDES THIS SOFTWARE AND DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT OF THIRD PARTY RIGHTS, AND ANY WARRANTIES ARISING OUT OF CONDUCT OR INDUSTRY PRACTICE. ACCORDINGLY, THALES DISCLAIMS ANY LIABILITY, AND SHALL HAVE NO RESPONSIBILITY, ARISING OUT OF ANY FAILURE OF THE SOFTWARE TO OPERATE IN ANY ENVIRONMENT OR IN CONNECTION WITH ANY HARDWARE OR TECHNOLOGY, INCLUDING, WITHOUT LIMITATION, ANY FAILURE OF DATA TO BE PROPERLY PROCESSED OR TRANSFERRED TO, IN OR THROUGH LICENSEE'S COMPUTER ENVIRONMENT OR ANY FAILURE OF ANY TRANSMISSION HARDWARE, TECHNOLOGY, OR SYSTEM USED BY LICENSEE OR ANY LICENSEE CUSTOMER. THALES SHALL HAVE NO LIABILITY FOR, AND LICENSEE SHALL DEFEND, INDEMNIFY, AND HOLD THALES HARMLESS FROM AND AGAINST, ANY SHORTFALL IN PERFORMANCE OF THE SOFTWARE, OTHER HARDWARE OR TECHNOLOGY, OR FOR ANY INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS, AS A RESULT OF THE USE OF THE SOFTWARE IN ANY ENVIRONMENT. LICENSEE SHALL DEFEND, INDEMNIFY, AND HOLD THALES HARMLESS FROM AND AGAINST ANY COSTS, CLAIMS, OR LIABILITIES ARISING OUT OF ANY AGREEMENT BETWEEN LICENSEE AND ANY THIRD PARTY. NO PROVISION OF ANY AGREEMENT BETWEEN LICENSEE AND ANY THIRD PARTY SHALL BE BINDING ON THALES.

Protected by U.S. patents:
6,678,828
6,931,530
7,143,288
7,283,538
7,334,124

CONTENTS

PREFACE

This document describes how to install and configure Vormetric Transparent Encryption (VTE) to encrypt data.

SCOPE

This document describes how to install and configure VTE 5.3.0 for AIX agents on AIX platforms.

INTENDED AUDIENCE

This document 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:

- Log a ticket at https://supportportal.thalesgroup.com/
- or call 800-545-6608

For Vormetric Sales:

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

Overview

1

This document describes how to install and configure Vormetric Transparent Encryption for AIX (VTE) to protect data on a host computer. A computer protected with a VTE agent is referred to as a *protected host* in this document. VTE supports multiple operating systems and can be deployed on physical devices as well as virtual machines.

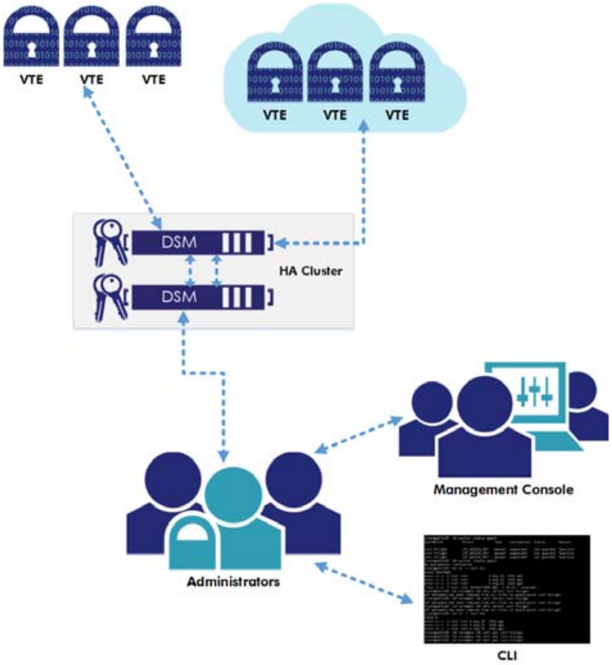
VTE Overview

The VTE solution consists of an appliance called the Data Security Manager (DSM), and one or more VTE agents installed on your protected hosts.

Thales provides the DSM as a security-hardened physical appliance or a virtual appliance. The DSM stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles.

The VTE agents communicate with the DSM and implement the security policies on the protected host systems. Protected hosts contain the data you want to protect. If connected to a NAS or SAN, the protected host has access to your data. Protected hosts can be on-site, in the cloud, or a hybrid of both.

Figure 1: Vormetric Transparent Encryption Architecture



In Figure 1, VTE agents protect hosts that may be physical or virtual machines. 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 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. In the following cases, VTE deviates from AIX lock semantics:

- 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.

AIX Agent Installation

2

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

- The *agent installer* or *host administrator* who uses these instructions to install and configure a VTE agent
- The DSM *administrator,* who, in some cases, adds hosts to the DSM database using the FQDN or the IP address

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 "Prerequisites" on page 5.

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.

Prerequisites

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

- "General setup information" on page 5
- "Determine your agent registration method" on page 5
- "Host name resolution" on page 6
- "Determine the installation method" on page 8
- "Determine the installation method" on page 8
- "Hardware Association (Cloning Prevention)" on page 9
- "One-way communication" on page 9
- "One-way communication" on page 9

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 (meaning 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 9 for more discussion.

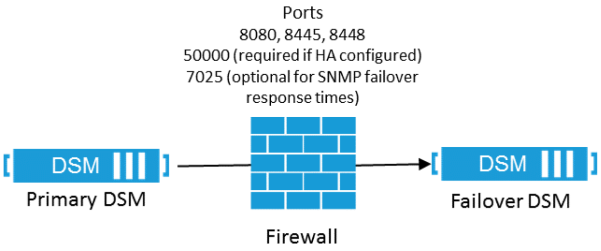
Use the following guidelines for hostname resolution:

- 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.

The following describes the communication direction and purpose of each protected host port you must open.

Table 1: Ports to Configure

Port	Protocol	Communication Direction	Purpose
	ICMP	All ICMP	Used for Ping
22	TCP	Management Console → DSM	CLI SSH Access
161	TCP/UDP	SNMP Manager → DSM	SNMP queries from an external manager
443	TCP	Browser → DSM DSM↔ DSM Agent → DSM	Redirects to either port 8445 or 8448 depending on the security mode. (8445 is used in compatible & RSA modes; 8448 is used in Suite B mode, for secure communication between DSMs in an HA cluster and for LDT registration.)
5432	TCP	DSM (HA node 1) ↔ DSM (HA node n)	HA information exchange.
5696	TCP	KMIP client → DSM	Allows communication between the KMIP client and DSMs
7025	TCP/UDP	DSM ↔ DSM	Uses SNMP to get HA node response time.

Table 1: Ports to Configure

Port	Protocol	Communication Direction	Purpose

8080	TCP	Agent → DSM
		DSM ↔ DSM
			Port 8080 is no longer used for registration, but you can manually close/open this legacy port for new deployment, for backward compatibility if you use previous versions of the agent and need to register to 8080. Default is on (open).
			Syntax
			`0001:system$ security legacyregistration`
			`[ on | off | show ]`

8443	TCP	Agent → DSM	RSA TCP/IP port through which the agent communicates with the DSM, in case 8446 is blocked. The agent establishes a secure connection to the DSM, through certificate exchange, using this port.
8444	TCP	Agent → DSM	RSA port via which the Agent log messages are uploaded to DSM, in case 8447 is blocked.
8445	TCP	Browser → DSM DSM ↔ DSM (fall back)	Management Console, VMSSC, and fall back for HA communication in case port 8448 is dropped.
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) and RSA
8448	TCP	Browser → DSM DSM ↔ DSM Agent → DSM	GUI Management during enhanced security using Elliptic Curve Cryptography (Suite B). Also for secure communication between DSMs in an HA cluster. Also used for communication between host with LDT host and DSM during Agent registration.
9004	TCP	DSM↔ network HSM	DSM communication with nShield Connect and its associated RFS
9005	TCP	DSM↔ remote admin	Used by Remote Administration Service process to accept connections from the Remote Administration Client.

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 11.

- **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 16.

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-6.2.0-110-rh6-x86_64.bin`
`vee-fs-6.2.0-110-rh6-x86_64.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 6 for the protected hosts and DSMs?	
Set “Determine the installation method” on page 8?	
Do you want “Hardware Association (Cloning Prevention)” on page 9?	
Is “One-way communication” on page 9 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-6.2.0-110-rh6-x86_64.binvee-fs-6.2.0-110-rh6-x86_64.bin -h

    [-d <dir>] [-e] [-i] [-h] [-m] [-s <file>] [-v] [-y] [-u]
      -d Install in specified directory
      -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)
      -u Upgrade VTE fs-agent on reboot
```

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

   ```
   ./vee-fs-6.2.0-110-rh6-x86_64.binvee-fs-6.2.0-110-rh6-x86_64.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 13.
- 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 RH-6

Shared secret : *********
Domain name : <assigned-domain-name-in-DSM>
Host Group : (none)
Host description : AIX RH-6
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 6 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 5	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-6.2.0-110-rh6-x86_64.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-6.2.0-110-rh6-x86_64.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.

VTE provides the host setting `protect` for this purpose. 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/etc/shadow
/etc/gshadow
```

The Protect setting supersedes the Audit setting if both tags are applied to the same file.

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

This VTE for feature does not require a matching DSM version. You can use a VTE for installation with a v5.x DSM. However, Thales highly recommends that you use the this VTE feature with a v6.x DSM. Although a VTE 6.x installation can use this protection feature with a v5.x DSM, audit messages are absent on the v5.0 DSM.

Package Installation

This section describes how to extract and run packages directly so that the Vormetric Agent installation integrates with the distribution software.

Caution: Do not use package installation for SUSE . Instead, use the typical installation (page 13) or the silent (unattended) installation (page 16).

To extract and run the RPM file

The VTE installation `bin` files contain the native packages and are extracted by running the `bin` file with the `-e` flag.

1. Log on to the host system as root and copy or mount the installation file to the host system.
2. Extract the RPM file. Type

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

Example: > ./vee-fs-6.2.0-110-rh6-x86_64.bin.bin -e

 Contents extracted.

> ls *rpm

 vee-fs-6.2.0-110-rh6-x86_64.bin.rpm
```

3. To start the installation using the RPM file, type

```
> rpm -ivh vee-fs-6.2.0-110-rh6-x86_64.bin.rpm {{this number will
change-will it be 6.0 or more digits?
```

4. Follow the prompts until installation and registration are complete.

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 .pkg file (Solaris)

1. Log on to the host system as root and copy or mount the installation file onto the host system.
2. Extract the .pkg file. Example:

```
: ./<product-version-build-system>.bin -e
Example: ./vee-fs-zone-5.2.4-7-sol11.bin
   Contents extracted.
> ls *pkg
   vee-fs-zone-5.2.4-7-sol11.pkg
```

3. Run pkgadd and follow the prompts.

   - If you are installing in a global zone for Solaris 10, use the following command (using -G):

```
> pkgadd -G -d ./vee-fs-zone-5.2.4-7-sol10.pkg vee-fs
```

   - If you are installing in a non-global zone for Solaris 10 or for Solaris 11 and higher, use the following command (without using -G):

```
> pkgadd -d ./vee-fs-zone-5.2.4-7-sol11.pkg vee-fs-zone
```

Caution: DO NOT register the host with the DSM when installing the agent in a non-global zone

To extract and run the .bff file on 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-5.3.0-13-aix71.bin -e
   Contents extracted.
# ls *bff
vee-fs-5.3.0-13-aix71.bff
```

3. Run installp and then follow the prompts.

```
> installp -aX -d vee-fs-5.3.0-13-aix71.bff vee.fs
```

To extract and run the .depot file (HP-UX)

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.

```
# cd /tmp
# ./vee-fs-5.3.0-9007-hp3-ia.bin -e
Contents extracted.
```

3. Run swinstall -s and follow the prompts

```
# swinstall -s /tmp/vee-fs-5.3.0-9007-hp3-ia.depot \*
```

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.

You can configure an upgrade to occur the next time the server restarts. See “Scheduled Upgrade” on page 25.

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.
- If you are installing agents in Solaris zones, the global zone and all the non-global zones should be up and running during installation. Install or upgrade the global zone first, followed by the non-global zones.

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-5.3.0-13-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.

Scheduled Upgrade

Scheduled upgrade allows you schedule an upgrade of the VTE agent to occur the next time the server on which an agent is installed reboots normally. Scheduled upgrade can minimize VTE service interruptions. Also, scheduled upgrade can reduce coordination issues in organizations where the security roles are separated. This section contains the following sections:

- “Scheduled upgrade prerequisites, notes, and error events” on page 26
- “Using the scheduled upgrade feature” on page 26
- “Performing an upgrade manually when an upgrade is already scheduled” on page 27

NOTE: Scheduled upgrade on reboot can be scheduled for VTE builds made available after the AIX 5.3.0 GA version. You cannot upgrade to the AIX 5.3.0 GA version using scheduled upgrade.

NOTE: Scheduled upgrade on reboot is not supported on HDFS nodes.

Scheduled upgrade prerequisites, notes, and error events

Keep in mind the following prerequisites for using scheduled upgrade, usage notes, and how scheduled upgrade behaves when errors occur.

- If a crash/power failure occurs before a user-initiated reboot, the scheduled upgrade runs when the system comes up after the crash/power failure.
- DSM connectivity is required during the scheduled upgrade process.
- All databases must be configured to automatically stop before VTE services stop during reboot/shutdown.
- Stopping and restarting the VTE agent does not trigger a scheduled upgrade.
- The installation binary used to run the scheduled upgrade is stored in `/var/tmp` until the scheduled upgrade runs. Ensure that no scheduled maintenance jobs periodically delete files in `/var/tmp`. All temporary files used by scheduled upgrade are removed following a successful scheduled upgrade.

Using the scheduled upgrade feature

Follow the steps below to enable scheduled upgrade.

If a scheduled upgrade has been enabled but has not run because the system wasn’t rebooted, you can override the existing scheduled upgrade with a newer VTE version by using the procedure described here with the newer installation binary.

1. Verify that the version of VTE you currently have installed is eligible for scheduled upgrade:

   ```
   $ vmd -v
   ```

   The version listed must be 6.2.1 or later.

2. Log in as root, change to the directory containing the installation binary, and run the binary with the `-u` scheduled upgrade option. For example:

   ```
   # ./vee-fs-5.3.0-13-aix71.bin -u
   ```

   The following upgrade confirmation is displayed:

   ```
   upgrade on reboot configured
   ```

NOTE: If syslog is properly configured, appropriate logs will be logged in syslog.

3. When you are ready, reboot the server.

   ```
   # reboot
   ```

   When the system restarts, the scheduled upgrade runs without any intervention needed.

4. After the system restarts, log in and run `vmd -v` to verify that the new version has been installed.

Performing an upgrade manually when an upgrade is already scheduled

If you change your mind, follow these steps to perform an upgrade manually when a scheduled upgrade is already enabled.

1. Log in as root, change to the directory containing the installation binary, and run the binary **without** the `-u` scheduled upgrade option:

   ```
   # ./vee-fs-5.3.0-13-aix71.bin
   ```

   The following warning is displayed:

   ```
   upgrade on reboot pending
   do you wish to continue [y/n]:
   ```

2. Enter “Y” to cancel the scheduled upgrade and proceed with an immediate installation. If you enter “N”, the scheduled upgrade remains enabled and occurs on the next reboot.

   If you enter “Y”, the binary runs and displays the license agreement.

3. When prompted, enter “Y” to accept the license or “N” to exit.

   After accepting the license agreement, the normal upgrade proceeds.

The scheduled upgrade is canceled and temporary files used by the scheduled upgrade are removed.

Special Cases for VTE Policies

3

This chapter describes some VTE-specific configuration tasks related to configuring policies in the DSM and contains the following sections:

- “More Information About Configuring VTE Policies” on page 28
- “Re-Signing Executable Files on Secfs GuardPoints” on page 28
- “Enable Automatic Signing for Host Settings (AIX)” on page 29

More Information About Configuring VTE Policies

This chapter describes some special cases that apply only to VTE agent policy configuration. See the DSM Administration Guide for general information about configuring polices. The following chapters in the DSM Administration Guide pertain specifically to the information in this chapter:

- “Creating and Configuring Signature Sets”
- “Configuring Hosts and Host Groups”
- “Configuring Policies”

Re-Signing Executable Files on Secfs GuardPoints

In previous versions, an issue affected signed executables in encryption policies. In these VTE versions, 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. So after each key rotation the host settings executables will no longer be authenticated, or the Signature Set policy rules that include those executables will no longer match them as expected. This problem occurred because VTE generated an SHA signature of the encrypted executable which changes after each key rotation. To work around these issues on these older VTE versions, the security administrator must manually re-sign each affected executable after each key rotation.

Starting with VTE release 5.2.7, the SHA signature is created from the unencrypted executable. This new SHA signature does not change with a key rotation.

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

1. Install the current release of the VTE agent. 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 the latest VTE release. Refer to the DSM Installation and Configuration Guide for information on how to perform a manual re-sign.
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 with VTE , there are no special steps if no signatures have been defined. New signatures will sign using the new method so it is not necessary to manually re-sign each affected executable after each key rotation.

NOTE: In previous releases, if the executable was in a GuardPoint protected directory, but was the same as an unguarded executable, the administrator could restrict only the guarded executable. With the change in , the unguarded executable matches the guarded executable with regards to policies.

Enable Automatic Signing for Host Settings (AIX)

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:

   ```
   AUTO_RESIGN_HOST_SETTINGS=TRUE
   ```

   Previously this setting was known as `RE_SIGN_HOST_SETTINGS`. As of VTE 5.3.0 and later, the attribute name is `AUTO_RESIGN_HOST_SETTINGS` as shown here.

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
```

Enabling the automatic regeneration of signatures exposes a potential security vulnerability for agents. When enabled, host setting binaries are re-signed 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.

Restricting access overrides from unauthorized identities

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**.

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" on page 32

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

- Verify 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 42.

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 42.

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 37.

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
60000000000D8000 01F27C42 40E75C23 5CE0202A C5F6465F
[..|B@.\#\. *..F_]
60000000000D8010 379BC9E1 B53A4016 E2DB2EF7 E2328706  [7....:@......2..]
60000000000D8020 CA2F30AD 522B4D21 99292639 004EBB34  [./0.R+M!.)&9.N.4]
60000000000D8030 A3896BE8 BD839D23 2204E19E 946C575C  [..k....#"....lW\]
60000000000D8040 4CE2218F 35E1B101 AF751A70 780E6D6E  [L.!.5....u.px.mn]
60000000000D8050 5E7E6A38 C600ED5F 929047C4 DF372A8E  [^~j8..._..G..7*.]
60000000000D8060 E103152D BA87CC03 11A7D963 9D72FCE1
[...-.......c.r..]
60000000000D8070 1EC6B48B 03EE869F 61D651F9 E7614957  [........a.Q..aIW]
```

```
60000000000D8080 810E0353 9C461F49 69569733 501D19EF  [...S.F.IiV.3P...]
60000000000D8090 B268002B 4F9457B6 BDB04AC5 D3D07446  [.h.+O.W...J...tF]
60000000000D80A0 FD9EE5E0 9B46CB66 30D10B22 F63AB77E  [.....F.f0..".:.~]
60000000000D80B0 6FF79075 4BBD1FAD 8F226188 7774300D  [o..uK...."a.wt0.]
60000000000D80C0 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.

5

Enhanced Encryption Mode

This chapter describes the enhanced AES-CBC-CS1 encryption mode for keys. It contains the following sections:

- "Compatibility" on page 46
- "Disk Space" on page 48
- "Encryption Migration" on page 48
- "File Systems Compatibility" on page 48
- "Using the new Encryption mode" on page 49
- "Exceptions and Caveats" on page 49
- "Best Practices" on page 50

The AES-CBC-CS1 encryption is superior to the existing AES-CBC mode because it uses a unique and unpredictable (random) IV (initialization vector) generated for each individual file. The per-file IV object is generated only at file creation time. It is stored as file metadata.

NOTE: AES-CBC-CS1 encryption does not require any additional license.

Table 4: Features Comparison

	AES-CBC	**AES-CBC-CS1**
Security Improvements		
Unique IV per-file	No	Yes
IV predicatibility	Yes	No
File System Support		
Local FS (AIX)	JFS2	JFS2
Remote FS (AIX)	NFS3/NFS4	NFS3/NFS4
Block Device Support (secvm)	Fully supported	No. When a policy contains a key with CBC-CS1 encryption mode, the guarding fails on the DSM, and an error message displays.

Compatibility

VTE 6.2.1 for Linux and Windows v5.3and later is backward compatible with and fully supports the existing AES-CBC mode, both for new and existing datasets, after the Agent is upgraded to VTE v5.3 or later.

Caution: AES-CBC-CS1 encryption is **only supported** with VTE v5.3.0 and later versions. A pre-v5.3 VTE host is incapable of supporting AES-CBC-CS1. On these earlier versions, attempting to guard using a policy containing an AES-CBC-CS1 key will fail.

- AES-CBC-CS1 encryption is supported for offline dataxform on VTE v5.3.0 environments.
- VTE hosts supporting AES-CBC-CS1 encryption can be added to host groups

Table 5: Data Transformation

	AES-CBC	AES-CBC-CS1
Offline data transformation	Supported	Supported

Difference between AES-CBC and AES-CBC-CS1

The two encryption modes are completely different from a file format standpoint.

- AES-CBC-CS1 encryption only applies to file system directories; AES-CBC encryption applies to both files and block devices.

NOTE: If you attempt to use an AES-CBC-CS1 key to guard a block device or partition, the guarding fails with an error reported on the DSM, similar to: Raw or Block Device (Manual and Auto Guard) Guardpoints are incompatible with Policy “policy-xxx" that contains a key that uses the CBC-CS1 encryption mode.”

IMPORTANT: AES-CBC-CS1 encryption is supported in AIX environments; as long as it is a local JFS2 or remote file system using NFS, the file formats will be compatible. It is possible that an encrypted file created with a specific AES-CBC-CS1 key on AIX cannot be read on a Linux or Windows local file system, even if that specific key were to be used, and vice versa.

- AES-CBC-CS1 uses cipher-text stealing to encrypt the last partial block of a file whose size is not aligned with 16 bytes.
- Each file encrypted with an AES-CBC-CS1 key is associated with a unique and random base IV.
- AES-CBC-CS1 implements a secure algorithm to tweak the IV used for each segment (512 bytes) of a file.

Disk Space

Files encrypted with AES-CBC-CS1 keys consume additional disk space in contrast to files encrypted with AES-CBC keys. This is because AES-CBC-CS1 encryption requires file IVs to be created and persistently stored -- in contrast to AES-CBC encryption which does not consume any additional disk storage.

Therefore, administrators need to plan and provision additional disk capacity prior to deploying AES-CBC-CS1 encryption.

Table 6: File size changes

	AES-CBC	AES-CBC-CS1
Local FS (AIX)	No change to file size. No extended attribute allocation	Extra 4KB allocation in the form of an embedded header per file. With VTE guarding enabled, file size expansion is hidden.
Remote FS (AIX)	No change to file size. No extended attribute allocation	Extra 4KB allocation in the form of an embedded header per file. With VTE guarding enabled, file size expansion is hidden.

Encryption Migration

You can use offline dataxform to:

- Transform data encrypted by AES-CBC to AES-CBC-CS1 and vice versa
- Transform AES-CBC-CS1 encrypted data to clear contents

File Systems Compatibility

On AIX, you can use AES-CBC-CS1 keys to guard currently supported file systems.

Local and Remote File Systems

AES-CBC-CS1 encrypted files on AIX local file systems can result in additional space consumption.

AES-CBC-CS1 files on AIX local or remote file systems such as JFS2 embed the IV in a 4K-byte header within the file. When these files are guarded, VTE masks the file header to applications and system utilities. The expanded file is only apparent when VTE guarding is disabled.

NOTE: The file system must have enough extra space to store the extra 4K bytes of the embedded header. You can run the following script in the GuardPoint to identify how much space to reserve before data transformation:

```
x=$(find . -type f | wc -l); y=$(echo "$x * 4 /1024" | bc); echo ${y}MB
```

On AIX, with AES-CBC-CS1 encryption, encrypted files on all file systems, both remote or local, have the same file format.

Storing Metadata

AES-CBC-CS1 encrypted files on AIX store the base IV of a file in the embedded header of the file.

To get the value of the base IV, type:

```
# voradmin secfs iv get <file-name>
```

NOTE: The base IV of a file is protected. It cannot be set/modified/removed by commands and applications. However, if a GuardPoint is unguarded, the files in the GuardPoint are no longer protected. An adversary can then corrupt the content of the files, as well as the IVs.

Using the new Encryption mode

Deploy the new encryption mode (AES-CBC-CS1) by using the new symmetric agent key type created in DSM 6.2.x or newer:

1. In the DSM, click **Keys > Agent Keys > Keys.**
2. Click **Add**.
3. In the Encryption Mode dropdown, select **CBC-CS1**.
4. In the Algorithm dropdown, select **AES128** or **AES256** to create an AES-CBC-CS1 key.
5. Add the key to your policy.

Exceptions and Caveats

Note the following when using AES-CBC-CS1 keys.

Guarding existing files without data transformation

You must convert an existing file with clear text through offline data transformation. If you do not transform the file, then after you guard using an AES-CBC key, the file displays garbled characters.

If you use an AES-CBC-CS1 key, access to the file is blocked with an I/O error.

Best Practices

The following are the recommended practices for deploying host groups with AES-CBC CS1 keys:

- In a host group, do not deploy policies associated with AES-CBC and AES-CBC CS1 keys unless all hosts are intended to run VTE 5.3 or later versions.
- If VTE 5.3 and older VTE versions are intended to be a part of the same host group, Thales recommends that you use policies without AES-CBC CS1 keys.

6

VTE for AIX Utilities

This chapter describes VTE for AIX utilities.

Thales provides a variety of utilities that an administrator can use to 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 7: `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:     7012404   5701814
```

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 7012404
```

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/vm
```

Display VTE Version Information

To display VTE version information, type:

```
# secfsd -version
```

System Response:

```
version:  5.3.0.7-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 8: 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=5.3.0.8
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
5.3.0.3
2018-10-31 16:47:43 ()
Copyright (c) 2009-2019, 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.

VTE for AIX version 5.2.7 introduced binaries that are signed with a signature that does not change with a key rotation. The security administrator must doonly one manual resigning after a key rotation. 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 the latest version of the VTE agent. (Starting with version 5.2.7, you can 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 administrator resigns the binaries.
3. Do not remove the old signatures on the DSM until all agents have been upgraded to at least VTE version 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. When all agents have been upgraded, 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 versions, 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.

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

Display the Installed Version

To display the installed VTE version, type:

```
# vmd -v
```

System Response:

```
Version 5
5.3.0.1
2018-02-13 10:37:40 (PDT)
Copyright (c) 2009-2018, Thales. 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.

NOTE:

7

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 71
- A host that has registered with the DSM; see “Configuring Concise Logging for a registered host” on page 72

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.