

CipherTrust Transparent Encryption

CTE Agent for AIX with CipherTrust Manager

Installation & Configuration Guide

Release 7.2.0

Document Version 6

August 31, 2022



All information herein is either public information or is the property of and owned solely by Thales and/or its subsidiaries and affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as "Thales") information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any publicly accessible network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Copyright © 2009-2022 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Contents

Preface	8
The CTE Agent Documentation Set	8
Document Conventions	8
Typographical Conventions	8
Notes, Tips, Cautions, and Warnings	9
Sales and Support	10
Chapter 1: Overview	11
CTE Terminology	11
CTE Components	11
CTE Compliance with AIX Lock Semantics	12
How to Protect Data with CTE	12
Chapter 2: Getting Started with CTE for AIX	13
Installation Workflow	13
Additional Considerations	13
Tracking and Preventing Local User Creation	13
Restricted Mode	14
AIX Package Installation	14
Installing CTE with No Key Manager Registration	15
Configuring CTE for AIX with CipherTrust Manager	16
Installation Overview	16
Installation and Registration Options	16
Installation Method Options	16
Hardware Association (Cloning Prevention) Option	16
Installation Prerequisites	16
Recommendations and Considerations	17
Network Setup Requirements	17
Port Configuration Requirements	17
Communication with Key Manager	17
Interactive Installation on AIX	17
Before You Begin	17
Silent Installation on AIX	20
Guarding a Device with CipherTrust Manager	22
Access the CipherTrust Manager Domain	22
Create an Encryption Key	22
Create a Standard Policy	24
Create a GuardPoint	26

Chapter 3: Special Cases for CTE Policies	28
Restricting Access Overrides from Unauthorized Identities	28
Chapter 4: Using CTE with Oracle	29
CTE on Oracle ACFS Overview	29
Key Managers and SecVM	30
Host Groups and Identical Keys and Policies	30
Restrictions and Caveats	30
Oracle RAC ASM	30
Using CTE with an Oracle RAC ASM	30
Important ASM Commands and Concepts	30
Rebalancing Disks	30
Mapping Raw Devices	31
Checking Rebalance Status	31
Determining Best Method for Encrypting Disks	31
Online Method (No Application / Database Downtime)	32
Offline Method (Backup the DB)	32
General Prerequisites	32
Setup	32
Altering ASM_DISKSTRING on ASM	33
Specific Prerequisites	33
Establishing a Starting Point	33
The Importance of Device Mapping	33
Important Note about Raw Devices on AIX	33
About Oracle RAC ASM Raw Devices	34
When Not Using ASMLib	34
Devices using Raw Bindings	34
Multipath I/O Devices	34
Standard Devices	34
Consistent Naming of Devices across RAC Nodes	35
Oracle RAC ASM Multi-Disk Online Method	35
Checking for Space	35
Adding a Disk to the Diskgroup	35
Oracle RAC ASM Multi-Disk Offline Method (Backup/Restore)	36
Surviving the Reboot and Failover Testing	37
Failover Testing	37
Basic Troubleshooting Techniques	37
Verifying Database Encryption	37
Option 1	37

Option 2	38
Option 3	38
Chapter 5: Logs	40
Setting CTE Agent Logging Preferences	40
Audit Logs	42
Analyzing Audit log entries	42
File System Audit Log Effects Codes	42
Concise Logging	44
Using Concise Logging	44
Considerations	44
Configuring Concise Logging for CTE Clients or Client Groups with CipherTrust Manager	44
Chapter 6: Enhanced Encryption Mode	45
Compatibility	45
Difference between AES-CBC and AES-CBC-CS1	45
Disk Space	46
Encryption Migration	46
File Systems Compatibility	46
Storing Metadata	47
Using the AES-CBC-CS1 Encryption Mode in CM	47
Exceptions and Caveats	47
Best Practices for AES-CBC CS1 Keys and Host Groups	47
Chapter 7: Utilities for CTE Management	48
secfsd Utility	48
secfsd syntax	48
secfsd Examples	49
Display GuardPoint Information	49
Display GuardPoint Information in a Different Format	50
Display Host Settings	50
Display Key Status	50
Display Lock Status	51
Agent Security Configuration Protection	51
Display CTE Log Status	51
Display Applied Policies	52
Display CTE Process Information	52
Display CTE Version Information	52
Manually Enable a GuardPoint in CipherTrust Manager	52

seccsd and Raw Devices	53
vmsec Utility	53
vmsec Syntax	53
vmsec Examples	53
Display CTE Challenge String	53
Display CTE Status	54
Entering a Password	54
Display Kernel Status	54
Display CTE Build Information	55
Display Contents of Conf files	56
Configuring Dynamic Host Settings for AIX	56
Restricting Access Overrides with Client Settings	57
vmd utility	58
Syntax	58
Display the Installed Version	58
Agent Health Utility	58
The Agent Health check script	59
Agent Health Return Codes	59
Help	59
Return Codes	60
Wait Time	60
agentinfo Utility (Java version)	61
check_host Utility	61
check_host Syntax	62
register_host Utility	62
Displaying Information for Nested File Systems with the DF tool	62
User Space Utility	63
Initial cache miss	63
Cache expiration timeout	63
Cache stale timeout	63
Usage	64
Chapter 8: Upgrading CTE on AIX	65
Scheduling a CTE Agent Upgrade	65
Before You Begin	65
Using the Scheduled Upgrade Feature	65
Performing an Upgrade Manually When an Upgrade is Already Scheduled	66

Chapter 9: Uninstalling CTE from AIX	67
Considerations	67
Procedure	67

Preface

The CTE Agent for AIX with CipherTrust Manager provides information about advanced installation, configuration, and integration options for CTE for AIX.

The CTE Agent Documentation Set

The following guides are available for CTE Agent:

- *CTE Agent for Linux Quick Start Guide*
- *CTE Agent for Linux Advanced Configuration and Integration Guide*
- *CTE Agent for Windows Quick Start Guide*
- *CTE Agent for Windows Advanced Configuration and Integration Guide*
- *CTE Agent for AIX Installation and Configuration Guide*
- *CTE Data Transformation Guide*
- *CTE-Live Data Transformation with Data Security Manager*
- *CTE-Live Data Transformation with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent with Data Security Manager*
- *Compatibility Matrix for CTE Agent for AIX with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent for AIX with Data Security Manager*
- *Release Notes for CTE for Linux Version 7.2.0.126*
- *Release Notes for CTE for Windows Version 7.2.0.126*
- *Release Notes for CTE for AIX Version 7.2.0.56*

To access any of these guides for the latest releases of CTE Agent, go to <https://thalesdocs.com/ctp/cte/index.html>.

Document Conventions

The document conventions describe common typographical conventions and important notice and warning formats used in Thales technical publications.

Typographical Conventions

This section lists the common typographical conventions for Thales technical publications.

Table 3-1: Typographical Conventions

Convention	Usage	Example
bold regular font	GUI labels and options	Click the System tab and select General Preferences .
<i>bold italic monospaced font</i>	Variables or text to be replaced	https://< <i>Token Server name</i> >/admin/ Enter password: < <i>Password</i> >

Table 3-1: Typographical Conventions (continued)

Convention	Usage	Example
regular monospacedfont	<ul style="list-style-type: none">• Commands and code examples• XML examples	<code>session start iptarget=192.168.253.102</code>
<i>italic regular font</i>	GUI dialog box titles	The <i>General Preferences</i> window opens.
	File names, paths, and directories	<i>/usr/bin/</i>
	Emphasis	<i>Do not</i> resize the page.
	New terminology	<i>Key Management Interoperability Protocol (KMIP)</i>
	Document titles	See <i>CTE Agent for AIX with CipherTrust Manager</i> for information about CipherTrust Transparent Encryption.
quotes	<ul style="list-style-type: none">• File extensions• Attribute values• Terms used in special senses	"js", ".ext" "true" "false", "0" "1+1" hot standby failover

Notes, Tips, Cautions, and Warnings

Notes, tips, cautions, and warning statements may be used in this document.

A Note provides guidance or a recommendation, emphasizes important information, or provides a reference to related information. For example:

Note

It is recommended to keep tokenization keys separate from the other encryption/decryption keys.

A tip is used to highlight information that helps you complete a task more efficiently, such as a best practice or an alternate method of performing the task.

Tip

You can also use Ctrl+C to copy and Ctrl+P to paste.

Caution statements are used to alert you to important information that may help prevent unexpected results or data loss. For example:



CAUTION

Make a note of this passphrase. If you lose it, the card will be unusable.

A warning statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data. For example:



WARNING

Do not delete keys without first backing them up. All data that has been encrypted with deleted keys cannot be restored or accessed once the keys are gone.

Sales and Support

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

For support and troubleshooting issues:

- <https://supportportal.thalesgroup.com>
- (800) 545-6608

For Thales Sales:

- <https://cpl.thalesgroup.com/encryption/contact-us>
- CPL_Sales_AMS_TG@thalesgroup.com
- (888) 267-3732

Chapter 1: Overview

This document describes the installation and advanced configuration options for CTE for AIX, as well as detailed information about how to integrate CTE with Oracle.

CTE Terminology

The CTE documentation set uses the following terminology:

Term	Description
CTE	<p>CipherTrust Transparent Encryption is a suite of products that allow you to encrypt and guard your data. The main software component of CTE is the CTE Agent, which must be installed on every host whose devices you want to protect.</p> <div style="border: 1px solid black; padding: 5px;"><p>Note</p><p>This suite was originally called Vormetric Transparent Encryption (VTE), and some of the names in the suite still use "Vormetric".</p><p>For example, the default installation directory is <code>/opt/vormetric/DataSecurityExpert/agent/</code> for Linux and AIX, and <code>C:\Program Files\Vormetric\DataSecurityExpert\agent\</code> for Windows.</p></div>
CTE Agent	<p>The software that you install on a physical or virtual machine in order to encrypt and protect the data on that machine. After you have installed the CTE Agent on the machine, you can use CTE to protect any number of devices or directories on that machine.</p>
key manager	<p>An appliance that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles</p>
host / client	<p>In this documentation, host and client are used interchangeably to refer to the physical or virtual machine on which the CTE Agent is installed.</p>
GuardPoint	<p>A device or directory to which a CTE data protection and encryption policy has been applied. CTE will control access to, and monitor changes in, this device and directory, encrypting new or changed information as needed.</p>

CTE Components

The CTE solution consists of two parts:

- The *CTE Agent software* that resides on each protected virtual or physical machine (host). The CTE Agent performs the required data encryption and enforces the access policies sent to it by the *key manager*. The communication between the CTE Agent and the key manager is encrypted and secure.
After the CTE Agent has encrypted a device on a host, that device is called a *GuardPoint*. You can use CTE to create GuardPoints on servers on-site, in the cloud, or a hybrid of both.
- A *key manager* that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. After you install the CTE Agent on a host and register it with a key manager, you can use the key manager to specify which devices on the host that you want to protect, what encryption keys are used to protect those devices, and what access policies are enforced on those devices.

Note

For a list of CTE versions and supported operating systems, see the [CTE Compatibility Portal](#) or the *Compatibility Matrix for CTE Agent with CipherTrust Manager* and the *Compatibility Matrix for CTE Agent with Data Security Manager*.

All CTE documentation is available at <https://thalesdocs.com/ctp/cte/index.html>.

CTE Compliance with AIX Lock Semantics

CTE is compliant with AIX lock semantics. In the following cases, CTE 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.

How to Protect Data with CTE

CTE uses policies created in the associated key manager to protect data. You can create policies to specify file encryption, data access, and auditing on specific directories and drives on your protected hosts. Each GuardPoint must have one and only one associated policy, but each policy can be associated with any number of 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 applied when generating fine-grained audit trails.

A Security Administrator accesses the key manager through a web browser. You must have administrator privileges to create policies using either key manager. The CTE Agent then implements the policies once they are pushed to the protected host.

CTE can only enforce security and key selection rules on files inside a guarded directory. If a GuardPoint is disabled, access to data in the directory goes undetected and ungoverned. Disabling a GuardPoint and then allowing unrestricted access to that GuardPoint can result in data corruption.

Chapter 2: Getting Started with CTE for AIX

This chapter describes how to install CTE for AIX, register it with your selected key manager, and then create a simple GuardPoint on the protected host. It contains the following topics:

Installation Workflow	13
AIX Package Installation	14
Installing CTE with No Key Manager Registration	15
Configuring CTE for AIX with CipherTrust Manager	16

Installation Workflow

In order to install and configure CTE, you need to perform the following high-level tasks:

1. If you want to include the CTE Agent software with the AIX distribution files, see ["AIX Package Installation" on the next page](#).
2. If you want to install the CTE Agent without registering with a key manager, see ["Installing CTE with No Key Manager Registration" on page 15](#). However, you cannot protect any data on the host until it has been registered.
 - ["Configuring CTE for AIX with CipherTrust Manager" on page 16](#)
3. Create your policies, encryption keys, and GuardPoints using the selected key manager. For details, see:
 - ["Guarding a Device with CipherTrust Manager" on page 22](#).

Additional Considerations

The following sections describe some of the things to keep in mind when configuring CTE.

Tracking and Preventing Local User Creation

CTE audits any attempts to change user authentication files. It also allows you to prevent any change to user authentication files using the host settings `protect`. This includes, but is not limited to user creation, modification, and deletion, or to deny users.

- The `audit` setting is set to on by default. It logs access to the system credential files but does not prevent account modifications.
- The `protect` setting both audits and prevents local user account modifications. You must manually enable the `protect` setting for tracking and prevention of local user account creation.

The `protect` tag will prevent changes to the files mentioned below. In the absence of the `protect` tag in host/client settings, operations on these files are permitted. When a log entry is generated, it is tagged with an `[audit]` tag.

- `/etc/passwd`
- `/etc/group`
- `/etc/ssh/sshd_config`
- `/etc/ssh/sshrd`

Notes

- The first time you use the `protect` host setting, you must restart CTE. Subsequent files tagged with the `protect` setting do *not* require a restart.

Restricted Mode



CAUTION

If you install or upgrade in restricted mode, you cannot revert to unrestricted mode without uninstalling CTE.

You can install CTE in restricted mode. This mode prevents any user other than `root` from accessing the following directories:

- `/var/log/vormetric`
- `/opt/vormetric/DataSecurityExpert`

Restricted Mode also prevents non-`root` users from running the following utilities:

- `agenthealth`
- `agentinfo`
- `check_host`
- `register_host`
- `secfsd`
- `vmd`
- `vmsec`
- `voradmin`

Key Agents and Restricted Mode

- On systems where CTE is installed in restricted mode, you cannot install a key agent (pkcs11) or CipherTrust TDE Key Management.
- On systems where a key agent (pkcs11) or CipherTrust TDE are already installed, you cannot install CTE in restricted mode.

Restricted Mode Installation

To install in restricted mode, use the `-r` option.

```
# ./vee-fs-<release>-<build>-<system>.bin -r
```

For example:

```
# ./vee-fs-7.2.0.56-aix71.bin -r
```

Upgrade in Restricted Mode

The upgrade mode is the same as the installation mode.

AIX Package Installation

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

To extract and run the .bff file on AIX:

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-7.2.0.56-aix71.bin -e
Contents extracted.
# ls *bff
vee-fs-7.2.0.56-aix71.bff
```

3. Run `installp` and then follow the prompts.

```
# installp -aX -d vee-fs-7.2.0.56-aix71.bff vee.fs
```

- If you are going to register the system with a CipherTrust Manager, see ["Configuring CTE for AIX with CipherTrust Manager" on the next page.](#)

Installing CTE with No Key Manager Registration

The following procedure installs the CTE Agent on the host but does not register it with a key manager. You cannot protect any data on the host until the CTE Agent is registered with one of the supported key managers. For a comparison of the available key managers, see ["CTE Components" on page 11.](#)

1. Log on to the host where you will install the CTE Agent as `root`. You cannot install the CTE Agent without `root` access.
2. Copy or mount the installation file to the host system. If necessary, make the file executable with the `chmod` command.
3. Install the CTE Agent. A typical installation uses the following syntax:

```
# ./vee-fs-<release>-<build>-<system>.bin
```

For example:

```
# ./vee-fs-7.2.0.56-aix71.bin
```

To install the CTE Agent in a custom directory, use the `-d <custom-dir>` option. For example:

```
# ./vee-fs-7.2.0.56-aix71.bin -d /home/my-cte-dir/
```

Note: If possible, Thales recommends that you use the default directory `/opt/vormetric`.

To view all installer options, use the `-h` parameter. For example:

```
# ./vee-fs-7.2.0.56-aix71.bin -h
```

4. The Thales License Agreement displays. When prompted, type `y` and press Enter to accept.

The install script installs the CTE Agent software in either `/opt/vormetric` or your custom installation directory and then prompts you about registering the CTE Agent with a key manager.

```
Welcome to the CipherTrust Transparent Encryption File System Agent
Registration Program.
```

```
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: 7.2.0.56
```

```
In order to register with a Key Manager you need a valid registration
token from the CM.
```

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

5. Type `n` and press Enter to end the installation procedure without registering the CTE Agent with either key manager.

When you are ready to register the CTE Agent with a key manager, see :

- ["Configuring CTE for AIX with CipherTrust Manager" below](#)

Configuring CTE for AIX with CipherTrust Manager

This section describes how to install and configure CTE on AIX systems that you plan to register with a CipherTrust Manager.

Installation Overview

The installation and configuration process when you are using CTE with a CipherTrust Manager consists of three basic steps:

1. Gather the information needed for the install and set up your network as described in ["Installation Prerequisites" below](#).
2. Install CTE on the protected host as described in ["Interactive Installation on AIX" on the facing page](#) or ["Silent Installation on AIX" on page 20](#).
3. Register the protected host with CipherTrust Manager and make sure that they can communicate with each other. Registration can be done as part of the initial installation or at any point after the CTE Agent has been installed.

Installation and Registration Options

CTE provides the following installation and registration options. The options you choose determine the information you need to supply during the actual install procedure.

Installation Method Options

There are two methods for installing CTE on AIX platforms:

- **Typical:** Most common and recommended type of installation. Use this method for installing the CTE Agent on one host at a time. See ["Interactive Installation on AIX" on the facing page](#).
- **Silent:** Create pre-packaged installations by providing information and answers to a set of installation questions. Use silent installations when installing on a large number of hosts. See ["Silent Installation on AIX" on page 20](#).

Hardware Association (Cloning Prevention) Option

CTE's hardware association feature associates the installation of CTE with the machine's hardware. When enabled, hardware association prohibits cloned or copied versions of CTE from contacting the key manager and acquiring cryptographic keys. Hardware association works on both virtual machines and hardware clients.

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

Installation Prerequisites

This section lists the tasks you must complete, and the information you must obtain, before installing CTE.

Recommendations and Considerations

- Thales recommends that you install CTE in the default location.
- Make the installation root directory `/opt` a real directory. If `/opt` is a symlink, you **must** use the `-d` option to specify the installation directory, which must be a real directory.

For example:

```
# ./vee-fs-7.2.0.56-aix71.bin -d /home/hello/
```

- Ensure read/write permission is granted to other users accessing your shared resource.
- P8 Hardware Encryption is supported, but there is a required fix from IBM. If the required fix is not found, the installation defaults to Software Encryption for P8.
 - AIX 7.1 requires TL level 7100-04-04 or later.
 - AIX 7.2 requires TL level 7200-01-02 or later.

Network Setup Requirements

- The IP addresses, routing configurations, and DNS addresses must allow connectivity of the AIX system on which you plan to install CTE to the CipherTrust Manager. After the AIX system is registered as a client with the CipherTrust Manager, the client must be able to poll the CipherTrust Manager in case there are any changes to the encryption keys, policies, or GuardPoints.
- If the system is a virtual machine, the VM must be deployed and running.

Port Configuration Requirements

Communication with Key Manager

The default port for http communication between CipherTrust Manager and the CTE Agent is **443**. If this port is already in use, you can set the port to a different number during the CTE Agent installation.

Interactive Installation on AIX

The AIX typical install is an interactive script that asks you a series of questions during the installation. You can also install CTE using a silent installer which pre-packages the install information. This allows you to install CTE on a large number of hosts. (For more information, see "[Silent Install](#)" on page 1).

After you install CTE, you are prompted to register it immediately with a key manager. CTE must be registered with a key manager before you can protect any of the devices on the host. However, you may postpone the registration if you plan to register CTE later.

Note

Do not install CTE on network-mounted volumes like NFS.

Before You Begin

The following prerequisites must be met for CTE to install and register to CipherTrust Manager properly:

- CipherTrust Manager installed and configured. See [CipherTrust Manager Documentation](#) for more information.

- CipherTrust Manager must contain a Client Profile. See [Changing the Profile](#) for more information.
- CipherTrust Manager must contain a registration token. See [Creating a Registration Token](#).
- Optionally, the name of the host group you want this client to be a part of.

Procedure

1. Log on to the host where you will install the CTE Agent as `root`. You cannot install the CTE Agent without `root` access.
2. Copy or mount the installation file to the host system. If necessary, make the file executable with the `chmod` command.
3. Install the CTE Agent. A typical installation uses the following syntax:

```
# ./vee-fs-<release>-<build>-<system>.bin
```

For example:

```
# ./vee-fs-7.2.0.56-aix71.bin
```

To install the CTE Agent in a custom directory, use the `-d <custom-dir>` option. For example:

```
# ./vee-fs-7.2.0.56-aix71.bin -d /home/my-cte-dir/
```

Note: If possible, Thales recommends that you use the default directory `/opt/vormetric`.

To view all installer options, use the `-h` parameter. For example:

```
# ./vee-fs-7.2.0.56-aix71.bin -h
```

4. The Thales License Agreement displays. When prompted, type `y` and press Enter to accept.

The install script installs the CTE Agent software in either `/opt/vormetric` or your custom installation directory and then prompts you about registering the CTE Agent with a key manager.

```
Welcome to the CipherTrust Transparent Encryption File System Agent  
Registration Program.
```

```
Agent Type: CipherTrust Transparent Encryption File System Agent  
Agent Version: 7.2.0.56
```

```
In order to register with a Key Manager you need a valid registration  
token from the CM.
```

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

5. Enter `y` to continue with the registration process. The install script prompts you to enter the host name or IP address of the CipherTrust Manager with which you want to register CTE.

The default communication port is 443. If you want to specify a different communication port, enter it with the primary key manager host name in the format: `<hostName>:<port#>`

For example:

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

```
Please enter the primary key manager host name: 10.3.200.141:8445
```

```
You entered the host name 10.3.200.141  
Is this host name correct? (Y/N) [Y]: y
```

6. Enter the client host name when prompted.

Please enter the host name of this machine, or select from the following list.

```
[1] sys31186.qa.com
[2] 10.3.31.186
```

Enter a number, or type a different host name or IP address in manually:
What is the name of this machine? [1]: 2
You selected "10.3.31.186".

7. Enter the CipherTrust Manager registration token, profile name, host group and host description. If you omit the profile name, CipherTrust Manager associates the default client profile with this client.

```
Please enter the registration token: 12345
Please enter the profile name for this host: My-Profile
Please enter the host group name for this host, if any:
Please enter a description for this host: West Coast Datacenter server 5
```

```
Token           : 12345
Profile name     : My-Profile
Host Group      : (none)
Host description : West Coast Datacenter server 5
Are the above values correct? (Y/N) [Y]: Y
```

8. At the hardware association prompt, select whether you want to enable the hardware association feature (for details, see ["Hardware Association \(Cloning Prevention\) Option" on page 16](#)). The default is **y** (enabled):

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



WARNING

The registration token, profile name, client group name and name are case-sensitive. If any of these are entered incorrectly, the client registration will not succeed. If the registration fails, click Back in the installer and verify that the case is correct for all entries on this page.

9. CTE finishes the installation and registration process.

```
Generating key pair for the kernel component...done.
Extracting SECFS key
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
Enrolling agent with service on 10.3.200.141...done.
Successfully registered the CipherTrust Transparent Encryption File System Agent
with the
CipherTrust Manager on 10.3.200.141.

Installation success.
```

10. If you are using CipherTrust Manager version 2.2 or later, you can now use CipherTrust Manager to administer CTE on the client.

If you are using CipherTrust Manager version 2.1 or earlier, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Silent Installation on AIX

This section describes how to perform a silent (unattended) installation of the CTE on a single host. The silent 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 silent installation to install CTE on multiple hosts simultaneously.

The silent install method installs CTE on the host, and registers the host with the CipherTrust Manager you specify in the silent installation file.

Prerequisites

The following prerequisites must be met for CTE to install and register to CipherTrust Manager properly:

- CipherTrust Manager installed and configured. See [CipherTrust Manager Documentation](#) for more information.
- CipherTrust Manager must contain a Client Profile. See [Changing the Profile](#) for more information.
- CipherTrust Manager must contain a registration token. See [Creating a Registration Token](#).
- Optionally, the name of the host group you want this client to be a part of.

Procedure

1. Log on as an administrator to the host where you will install CTE.
2. Create a parameter file and store it on your system, or copy an existing file from another location. The file can contain any of the following parameters:

Required if you want to register CTE with a CipherTrust Manager.

The registration token for the CipherTrust Manager with which you plan to register this client. Required for registration.

Specifies the client profile in the CipherTrust Manager that will be associated with this client. If this value is omitted, the CipherTrust Manager uses the default client profile.

FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.

Use the IP address of the protected host instead of host name. Used when is not supplied.

Specifies the port number this CTE Agent should use.

when you want to associate this installation with the machine hardware for cloning prevention.

Example 1: Registering with CipherTrust Manager

The following example contains just the required information for registration with CipherTrust Manager. In this case, the client will be registered with the CipherTrust Manager using its IP address instead of its host name:

```
SERVER_HOSTNAME=Key-Mgmt-Server.example.com
REG_TOKEN=12345
PKCS11_PASSWORD=ClientAdminP@$w0rd
```

Example 2: Registering with CipherTrust Manager

The following example specifies the required registration information, adds a host name and description, and enables hardware association. In this case, the client will be registered with the CipherTrust Manager using its host name instead of the IP address:

```
SERVER_HOSTNAME=Key-Mgmt-Server.example.com
REG_TOKEN=12345
PKCS11_PASSWORD=ClientAdminP@$w0rd
AGENT_HOST_NAME=myagent.example.com
HOST_DESC="West Coast Server 12"
USEHWSIG=1
CERT_FIELD_PARAM="/C=US/ST=California/L=San Jose/O=Thales
eSecurity/OU=Vormetric/CN=localhost/emailAddress=admin@thalegroup.com"
SUBJECT_ALT_NAME_PARAM="DNS:www.thalesecurity.com,email:admin@thalesgroup.com"
```

3. Copy or mount the CTE installation file to the host system. The installation file is in the format `vee-fs-<release>-<build>-<system>.bin`.

4. Run the installer using the following syntax:

```
# ./vee-fs-<release>-<build>-<system>.bin [-d <custom-dir>] -s <install-file>
```

where:

- `-d <custom-dir>` is an optional parameter that specifies the installation directory for CTE. If you omit this parameter, CTE is installed in `/opt/vormetric/DataSecurityExpert/agent/`.
- `-s <install-file>` indicates that you want to install silently using the installation options file `<install-file>`

For example, if the installation options file is called `/tmp/unattended.txt`, you would enter:

```
# ./vee-fs-7.2.0.56-aix71.bin -s /tmp/unattended.txt
```

5. Verify the installation by checking CTE processes on the host:

- Run `vmd -v` to check the version of CTE matches that just installed.
- Run `vmsec status` to display CTE kernel status.
- Look at the log files in `/var/log/vormetric`, especially `install.fs.log.<date>` and `vorvmd_root.log`.

6. In CipherTrust Manager, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Guarding a Device with CipherTrust Manager

After you register a client with a CipherTrust Manager, you can create as many standard GuardPoints on the client as you need. These GuardPoints can protect an entire device or individual directories.

In order to guard a device or directory, you need to use the CipherTrust Manager Console to:

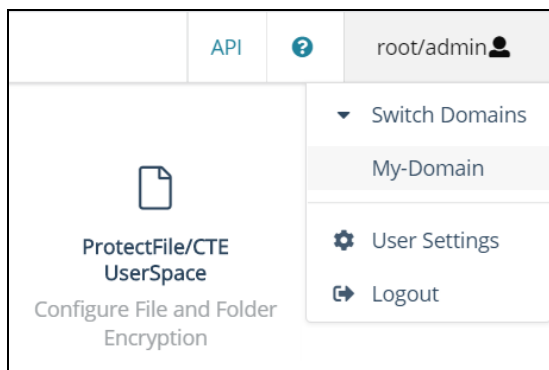
1. Access the CipherTrust Manager domain in which the client is registered.
2. Identify or create an encryption key that CTE will use to encrypt the data on the device or directory.
3. Identify or create a policy for the device or directory that specifies the access controls and the encryption keys to use for the device or directory.
4. Assign a GuardPoint to the device or directory.

The following example creates a simple policy and uses it to guard a directory on a registered client. For all of the following procedures, you must be logged into the CipherTrust Manager Console as a CipherTrust Manager Administrator, and you must be in the domain with which the client is registered.

For details about any of these procedures or the options for domains, encryption keys, policies, and GuardPoints, see the CipherTrust Manager documentation.

Access the CipherTrust Manager Domain

1. In a web browser, navigate to the URL of the CipherTrust Manager Console you want to use and log in with CipherTrust Manager Administrator credentials.
2. If the client you want to protect is registered to the default domain (root), proceed to ["Create an Encryption Key" below](#). If you need to change to a different domain, do the following:
 - a. In the top menu bar, click the user name **root/admin** on the right-hand side.
 - b. Select **Switch Domains**, then select the domain in which the client is registered.
 - c. The logged in user now shows the new domain name/user name.



Create an Encryption Key

Note

The following procedure is based on CipherTrust Manager version 2.2. If you are using a different version, see the CipherTrust Manager documentation for the version that you are using.

1. From the Products page in the CipherTrust Manager Console, click **Keys** in the left hand pane.

Tip: To navigate to the Products page from anywhere in the CipherTrust Manager Console, click the App Switcher icon in the top left corner.

- Above the Key table, click **Create a New Key**.
 - In the **Key Name** field, add a name for the key. This name must be unique. For example, Simple-Key.
 - In the **Key Usage** section, make sure **Encrypt** and **Decrypt** are selected.
 - Click **Create**. CipherTrust Manager displays the properties for the new key.
 - In the general options area, enable the **Exportable** option.
- You can also enable the **Deletable** option in this section if you want a CipherTrust Manager Administrator to be able to delete the key.

ID	2e58c582...61136313	Owner	Global	Object Type	Symmetric Key
UUID	e3ad9c3e...7fd47711	Created	05 Mar 2021, 05:13	Algorithm	AES
MUID	e3ad9c3e...f6333c9f	Last Modified	05 Mar 2021, 05:13	Size	256
KeyID	N/A	Exportable	<input checked="" type="checkbox"/>	Deletable	<input type="checkbox"/>

- In the **Key Access** section, do the following:
 - In the Search Groups box, type "cte".
If no groups are displayed, make sure the **Added Only** option is *disabled*.
 - Click the **All** check box for both the CTE Admins and CTE Clients groups.

KEY ACCESS

Key Owner

Search:

2 Results | 2 groups Added Only

Group	Read	Use	Decrypt	Encrypt	Sign	Sign/Verify	Export	All
CTE Admins	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CTE Clients	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- When you are done, click **Update**.

8. Click the **CTE** tab and set the following properties:
 - **CTE Versioned:** Specify whether the key is versioned. By default, the key is set as versioned.
For a standard policy, you should clear this check box. If you do not, the key will *not* appear in the keys list when you add the key rule to the standard policy.
 - **Persistent on Client:** Specify whether the key is stored in persistent memory on the client.
When the check box is selected, the key is downloaded and stored (in an encrypted form) in persistent memory on the client.
When the check box is left clear, the key is downloaded to non-persistent memory on the client. Every time the key is needed, the client retrieves it from the CipherTrust Manager. This is the default setting.
 - **Encryption Mode:** Encryption mode of the key. The options are:
 - CBC
 - CBC CS1
 - XTSEncryption using the XTS and CBC CS1 keys is known as enhanced encryption. For details, see the *CTE Agent for AIX Installation and Configuration Guide*.
- When you are done, click **Update**.

Create a Standard Policy

1. In the Applications page of the CipherTrust Manager Console, select the **Transparent Encryption** application.
2. In the sidebar on the Clients page, click **Policies**.
3. Click **Create Policy**. CipherTrust Manager displays the Create Policy Wizard.
4. On the General Info page, set the following options:

Field	Description
Name	A unique name for the policy. Make sure you use a name that is descriptive and easy to remember so that you can find it quickly when you want to associate it with a GuardPoint. This example uses "Simple-Policy".
Policy Type	The type of policy you want to create. In this example, we will create a Standard policy.
Description	A user-defined description to help you identify the policy later. For example: Standard policy for new GuardPoints
Learn Mode	Learn Mode provides a temporary method for disabling the blocking behavior of CTE policies. While useful for quality assurance, troubleshooting, and mitigating deployment risk, Learn Mode is not intended to be enabled permanently for a policy in production. This prevents the policy Deny rules from functioning as designed in the policy rule set. Ensure that the policy is properly configured for use in Learn Mode. Any Security Rule that contains a Deny effect must have Apply Key applied as well. This is to prevent data from being written in mixed states, resulting in the loss of access or data corruption. Apply Key will have no effect when combined with a Deny rule unless the policy is in Learn Mode.

Field	Description
Data Transformation	If you select Standard as the policy type, also select the the Data Transformation option to tell CTE that you want to change the current encryption key used on the data in the GuardPoint, or that you want to encrypt clear-text data for the first time. This option is only displayed for Standard policies.

When you are done, click **Next**.

5. On the Security Rules page, define the security rules that you want to use.

CipherTrust Manager automatically adds a default security access rule with an action of `key_op` and the effects `Permit` and `Apply Key`. This rule permits key operations on all resources, without denying user or application access to resources. This allows it to perform a rekey operation whenever the encryption key rotates to a new version.

To add additional security rules, click **Create Security Rule** and enter the requested information. For details about adding security rules, see the CipherTrust Manager documentation.

When you are done, click **Next**.

6. On the Create Key Rule page, click **Create Key Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click <code>Select</code> and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.
Current Key Name	Click Select to choose an existing key or create a new one. If the data has not yet been encrypted, select <code>clear_key</code> . Otherwise select the name of the non-versioned key that is currently being used to encrypt the data. In this example, select <code>clear_key</code> .
Transformation Key Name	Click Select to choose an existing versioned key or to create a new one. CTE uses the versioned key specified in this field to encrypt the data in the GuardPoint. If the data is currently encrypted, CTE decrypts it using the key specified in the Current Key Name field and re-encrypts it using the key specified in this field.

When you are done, click **Next**.

- On the Data Transformation page, click **Create Data Transformation Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.
Transformation Key Name	Click Select to choose an existing key or to create a new one. CTE uses the key specified in this field to encrypt the data in the GuardPoint. If the data is currently encrypted, CTE decrypts it using the key specified in the Current Key Name field and re-encrypts it using the key specified in this field. For this example, select the key Simple-Key you created in " Create an Encryption Key " on page 22.

When you are done, click **Next**.

- Click **Next**.
- On the confirmation page, review the information for the policy and click **Save**.

Create a GuardPoint

- Stop all applications that are accessing the device you want to protect. In this example, we are going to protect the following directories with the same policy and encryption key:
- In the Applications page of the CipherTrust Manager Console, select the **CTE** application.
- In the Clients table, click on the name of the client you want to protect.
- Above the GuardPoints table, click **Create GuardPoint**.

5. In the Create GuardPoint page:
 - a. In the **Policy** field, select the policy you created earlier.
 - b. In the Type field, select the type of device. You can guard a directory or a raw/block device. For this example, select **Auto Directory**.
 - c. In the **Path** field, enter the directories you want to protect with this policy or click **Browse** to select them from a explorer window.
If you want to enter multiple paths, put each path on its own line. For example:
 - d. Click **Create**.
 - e. If you want to use the same policy and GuardPoint type on another path, click **Yes** when prompted. Otherwise, click **No**. For this example, click No.

The CTE clients pull the GuardPoint configuration information from the CipherTrust Manager.

6. Type the following to transform the data:

```
# dataxform --rekey --print_stat --preserve_modified_time --gp <pathToGP>
```

When the data transformation has finished, applications can resume accessing the now-protected data. (See the “*CTE Data Transformation Guide*” for more information.)

Chapter 3: Special Cases for CTE Policies

This chapter describes some CTE-specific configuration tasks related to configuring policies in the key manager. It contains the following topics:

[Restricting Access Overrides from Unauthorized Identities](#) 28

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 CTE to not trust any authentication attempt performed by certain identities by assigning restricted users to a user shell that CTE 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.

CTE 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 in CipherTrust Manager:

1. In the CipherTrust Manager Applications Page, click **CTE > Clients**.
2. Click on an existing client name to edit the client.
3. Click **Client Settings** tab.
4. Add the following to the client settings:

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

For example:

```
|path_no_trust|/bin/ksh
```

The above example indicates that no process under the kshell executable will be authenticated.

5. Click **OK**.

Chapter 4: Using CTE with Oracle

This chapter describes how to install and configure CTE on Oracle RAC ASM, how to use an ASM Filter Driver as well as install and use CTE for AIX with Oracle Automated Storage Management (ASM™) Cluster File System (ACFS™). It contains the following topics:

CTE on Oracle ACFS Overview	29
Oracle RAC ASM	30
About Oracle RAC ASM Raw Devices	34
Oracle RAC ASM Multi-Disk Online Method	35
Oracle RAC ASM Multi-Disk Offline Method (Backup/Restore)	36
Surviving the Reboot and Failover Testing	37
Basic Troubleshooting Techniques	37

CTE on Oracle ACFS Overview

CTE enables data protection of Oracle Automatic Storage Management Cluster File System (Oracle 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

CTE 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 RAC

Oracle ACFS (File System)

Oracle ADVM (Volume Manager)

Oracle ASM (Storage Manager)

SecVM

On Oracle, ACFS is layered on ASM disks, which in turn are built on `secvbm` block devices. `secvbm` is a proprietary device driver that supports GuardPoint protection to raw devices. `secvbm` is inserted in between the device driver and the device itself.

Key Managers and SecVM

Server-side administrators must ensure that all `secvbm` 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 `seafs` layered on ACFS.
- Oracle ACFS encryption in conjunction with `secvbm` encryption might impact performance.

Oracle RAC ASM

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

Using CTE with an Oracle RAC ASM

You can apply CTE 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 CTE 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 CTE protection.
3. Add the disk back into the diskgroup.



CAUTION

If you drop a disk from an ASM diskgroup, then add it back to the diskgroup without cleanly wiping the disk, the ASM diskname will be corrupted. To avoid this problem, clear out the disk before you add it back to diskgroup. Example: `dd if=/dev/zero of=/dev/secvbm/dev/mapper/asmdg-asmlv002 bs=32k`

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:

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 CTE 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 CTE 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 CTE 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 CTE 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

Setup

- Verify that you have a current backup of the database
- Install and register CTE 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 CipherTrust Manager. 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 CTE.

Restarts can uncover issues in the RAC environment that are unrelated to CTE. To avoid issues after a CTE installation, Thales recommends that you restart each RAC node **AFTER** CTE is installed and **PRIOR** to establishing any GuardPoints. This may not be feasible in a single node configuration. However, by doing so, CTE 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, **CTE REQUIRES a block device for guarding.**

Notes

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

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

About Oracle RAC ASM Raw Devices

When Not Using ASMLib

Before starting the CTE implementation, investigate how the customer is using raw devices for their ASM configuration.

Devices using Raw Bindings

Typically, a device that uses a raw binding looks like the following to ASM:

```
/dev/raw/raw1
```

If the device is mapped this way, you must locate where the mapping is performed. Typically, you can find this in the following configuration file:

```
/etc/sysconfig/rawdevices
```

The underlying binding could be to either a **standard device** name or a **multipath I/O** device name. Either way, you must find where the bind commands are run so that you can modify them for SecVM.

Note

If raw bindings are in use, then typically no changes are needed for the `asm_diskstring`. Because the binding to the actual device is created through the `bind` command, locate where the binding occurs and change the binding to SecVM.

Multipath I/O Devices

Devices using multipath I/O are typically found with the name:

```
/dev/mapper/mpath1
```

Generally, when using multipath I/O, you create SecVM on the multipath device name.

Note

If you use multipath I/O devices in the ASM configuration to add its disk, you must modify the `asm_diskstring` parameter to include the `/dev/secvm/dev/*` path.

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/securevm/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;
```

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
```

DISKGROUP	DISK#	DISKNAME	TOTAL_MB	FREE_MB	PATH	HEADER_STATUS
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 CTE, 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 CipherTrust Manager, in the Host Group, apply a GuardPoint to the Raw Device: <rawDevice1Name>.
5. From **RAC Node 1**, to 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. For details, see "[Surviving the Reboot and Failover Testing](#)" on the facing page.

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.
2. 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.

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

4. # `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>`

5. On the CipherTrust Manager, in the Host Group, apply GuardPoints to the three raw devices:

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

6. On **RAC Node 1**, to display the status of the guarded disks, type:

```
# secfsd -status guard
```

7. 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>
```

8. 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.

9. On **RAC Node 1**, restore the database.
10. The system is now ready for a reboot and failover test. Go to the section "[Surviving the Reboot and Failover Testing](#)" below.

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 CTE 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

The 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.

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

1. On the CipherTrust Manager, 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 (this option is only for GPFS, which is not supported with CTE).
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, make sure the device names are the same across all nodes.
4. From ASM, make sure that the `asm_diskstring` parameter is modified to include the CTE devices and that the proper pathname is used, see "[Altering ASM_DISKSTRING on ASM](#)" on page 33.

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, double encrypted, 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
6000000000D8000 01F27C42 40E75C23 5CE0202A C5F6465F
[. . | B@ . \# \. * . . F _ ]
6000000000D8010 379BC9E1 B53A4016 E2DB2EF7 E2328706 [7 . . . . : @ . . . . . 2 . . ]
6000000000D8020 CA2F30AD 522B4D21 99292639 004EBB34 [ . / . 0 . R + M ! . ) & 9 . N . 4 ]
6000000000D8030 A3896BE8 BD839D23 2204E19E 946C575C [ . . k . . . . # " . . . . l W \ ]
6000000000D8040 4CE2218F 35E1B101 AF751A70 780E6D6E [ L . ! . 5 . . . . u . p x . m n ]
6000000000D8050 5E7E6A38 C600ED5F 929047C4 DF372A8E [ ^ ~ j 8 . . . _ . . G . . 7 * . ]
6000000000D8060 E103152D BA87CC03 11A7D963 9D72FCE1
[ . . . - . . . . . . . c . r . . ]
6000000000D8070 1EC6B48B 03EE869F 61D651F9 E7614957 [ . . . . . . . . a . Q . . a I W ]
6000000000D8080 810E0353 9C461F49 69569733 501D19EF [ . . . S . F . I i V . 3 P . . . ]
6000000000D8090 B268002B 4F9457B6 BDB04AC5 D3D07446 [ . h . + O . W . . . J . . . t F ]
6000000000D80A0 FD9EE5E0 9B46CB66 30D10B22 F63AB77E [ . . . . . F . f 0 . . " . : . ~ ]
6000000000D80B0 6FF79075 4BBD1FAD 8F226188 7774300D [ o . . u K . . . " a . w t 0 . ]
6000000000D80C0 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.

Chapter 5: Logs

This chapter contains the following sections:

Setting CTE Agent Logging Preferences	40
Audit Logs	42
Analyzing Audit log entries	42
File System Audit Log Effects Codes	42
Concise Logging	44

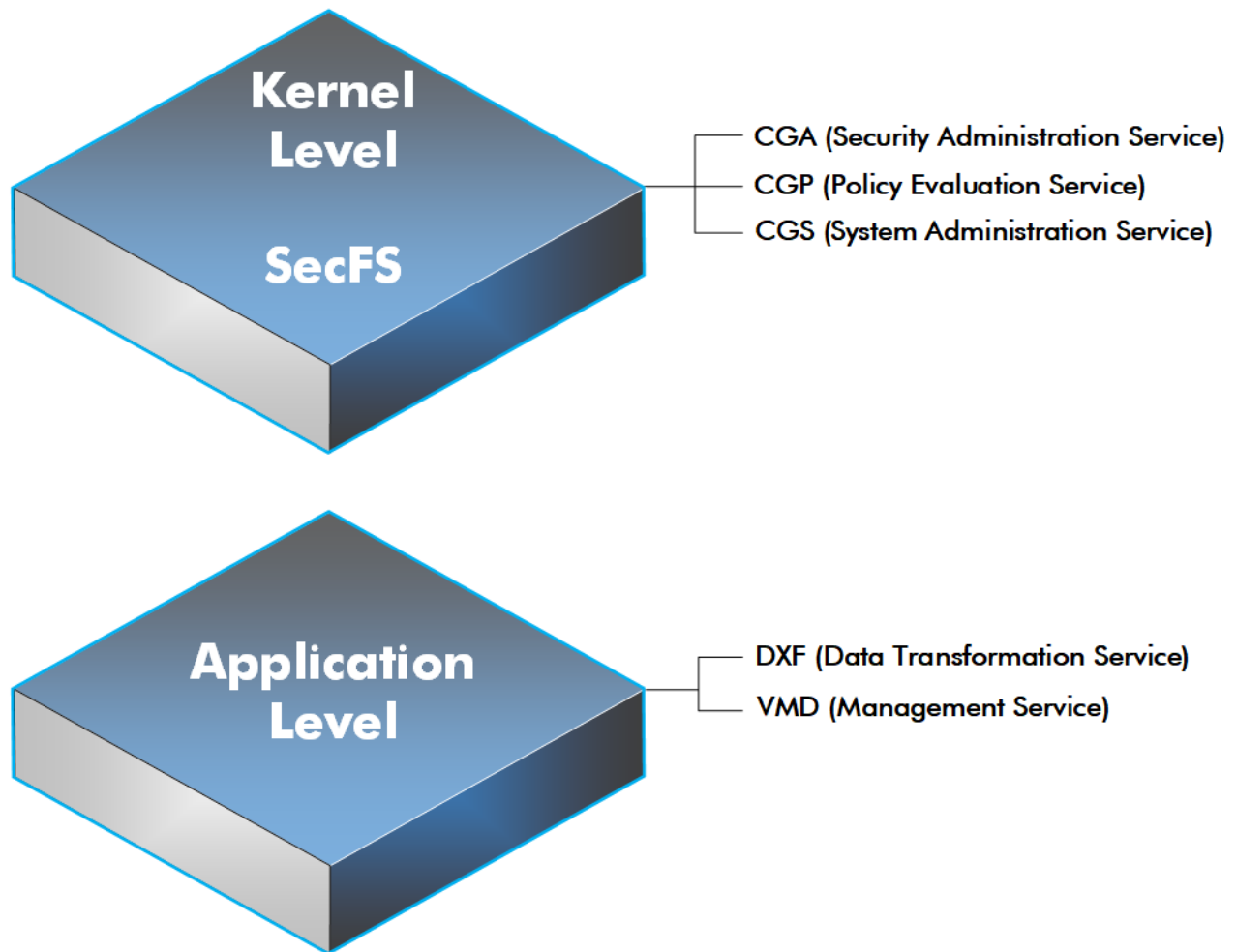
Setting CTE Agent Logging Preferences

You can configure the Agent process information that is entered into the Message Log. You can configure the process information globally, in which all the Agents that are added after the configuration change inherit the log attributes, while all current file system configurations remain intact. Alternatively, you can configure log attributes for individual Agent installations.

Always monitor log generation on new server and agent installations, and after changing logging preferences and options.

A variety of logging services are available and configured in the Log tab.

Logging Services



CTE log data may be sent to various different files such as:

- Sys log files, such as:

`/var/log/messages`

`/var/log/syslog`

Event log on

Note: The CM domain name can include spaces. However, Syslog does not allow spaces in header fields. Therefore, for Syslog purposes, the CTE client replaces the spaces with an underscore. For example: `My_Domain` instead of `My Domain`.

- CTE log files local to the agent, such as:

`/var/log/vormetric/vorvmd_root.log`

`C:\ProgramData\Vormetric\DataSecurityExpert\agent\log\vorvmd.log` (Windows)

- Uploaded to the Key Manager
- Uploaded to a Syslog server

Data Transformation log files are sent to:

- /var/log/vormetric/vordxf_path_usr.log

Audit Logs

Example audit log:

```
CGP2601I: [SecFS, 0] [AUDIT] Policy[allowAllOps_fs] User  
[root,uid=0,gid=0\root,bin,daemon,sys,adm,disk,wheel\] Process[/bin/cat] Action[write_  
app] Res[/opt/apps/apps1/doc/file2.txt] Key[aes128] Effect[PERMIT Code (1U,2U,3R,4M)]
```

Analyzing Audit log entries

The format of a File System Audit log entry is:

```
CGP2602I: [SecFS, 0] Level: Policy[policyName?] User[userID?] Process[command?] Access  
[whatIsItDoing?] Res[whatIsItDoingItTo?] Effect[allowOrDeny? Code (whatMatched?)]
```

Parameter	Description
Identifier	The TLA for the error message.
SECFS	Indicates that the message was generated by an Agent. You can enter <code>secfs</code> in the Search Message field in the Logs window to display the Agent policy evaluation and GuardPoint activity for all configured hosts.
Level	Indicates the importance of the message. For example, AUDIT indicates an informational message, whereas ALARM indicates a critical failure that you should not ignore.
Policy	Indicates the name of the policy that is being used to evaluate the access attempt.
User	Identifies the system user attempting to access data in the GuardPoint. It typically displays the user name, user ID, and group ID.
Process	Indicates the command, script, or utility being executed.
Access	Indicates what access is being attempted. Access may be <code>read_dir</code> , <code>remove_file</code> , <code>write_file_attr</code> , <code>write_app</code> , <code>create_file</code> , etc. These correspond to the Access methods that you configure in the policy. <code>Read_dir</code> corresponds to <code>d_rd</code> . <code>Remove_file</code> corresponds to <code>f_rm</code> , etc.
Res	Indicates the object/resource being accessed by the Process[].
Effect	Indicates the rule that matched and, based upon that rule, whether or not the CipherTrust Manager grants access. Access states may be either PERMIT or DENIED.

File System Audit Log Effects Codes

Codes are provided in the audit logs that identify actions by the policy enforcement engine. The code follows the number of the rule being processed.

Code	Definition
A	The Action component of a security rule failed to match.
M	All security rule components match and, unless overridden, the Effect for that security rule is applied.
P	The Process component of a security rule failed to match.
R	The Resource component of a security rule failed to match.
T	The time specified in the When component of a security rule failed to match.
U	The User component of a security rule failed to match.

Refer to the audit log example above:

- The first and second Security Rules fail because of a mismatch in the User component (1U, 2U).
- The third Security Rule fails because of a Resource component (3R) mismatch.
- All of the rules in the fourth Security Rule match (4M), and the actions defined in the policy, such as use an encryption key, are applied.

Concise Logging

Thales's standard operational logging sends audit messages for each file system operation 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.

Agent log data can be stored on the local host, sent to a syslog server, or uploaded to the Management Console. On an agent system, log entries can flood the local messages file or Event Log. Extreme logging can also affect network performance.

Concise Logging eliminates the following types of messages:

- Duplicate audit messages for each and every block read by the user or application. With Concise Logging, CTE only sends an audit message the *first* time a user or application performs a read/write activity. Subsequent read/write activity by that user or application is not logged.
- 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 CipherTrust Manager for the following:

- All registered hosts in all domains
- A host that has registered with the CipherTrust Manager.

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 CTE `secfs`.
- Enable and disable Concise Logging on the host. CTE 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 CipherTrust Manager level, it applies to all hosts in all domains, that are added to the CipherTrust Manager, 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 Concise Logging for CTE Clients or Client Groups with CipherTrust Manager

In CipherTrust Manager, when you create a Client Profile, you can select to Enable Concise Logging. Then, you can apply that Client Profile to a specific client, or to all clients in a Client Group. To enable Concise Logging, see the chapter *Managing Profiles* in the *CTE Administrator Guide*.

Chapter 6: Enhanced Encryption Mode

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

- Compatibility 45
- Disk Space 46
- Encryption Migration 46
- File Systems Compatibility 46
- Using the AES-CBC-CS1 Encryption Mode in CM 47
- Exceptions and Caveats 47
- Best Practices for AES-CBC CS1 Keys and Host Groups 47

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.

	AES-CBC	AES-CBC-CS1
Security Improvements		
Unique IV per-file	No	Yes
IV predictability	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 CipherTrust Manager, and an error message displays.

Compatibility

- Starting with VTE for AIX version 5.3, CTE is backward compatible with, and fully supports, the existing AES-CBC mode for both new and existing datasets.
- Starting with VTE for AIX version 5.3, CTE fully supports AES-CBC-CS1 encryption for offline data transformation on CTE AIX environments.
Versions of VTE prior to version 5.3 are *not* backwards compatible with AES-CBC-CS1 encryption. On these earlier versions, attempting to guard a device using a policy containing an AES-CBC-CS1 key will fail.
- Protected hosts supporting AES-CBC-CS1 encryption can be added to host groups.

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.

Notes

- 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 CipherTrust Manager, 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.”
- 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.

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

File Systems Compatibility

On AIX, you can use AES-CBC-CS1 keys to guard currently supported 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, CTE masks the file header to applications and system utilities. The expanded file is only apparent when CTE guarding is disabled.

Note

The file system must have enough extra space to store the extra 4K bytes of the embedded header.

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 AES-CBC-CS1 Encryption Mode in CM

When you create a key in CTE, you enable Encryption Mode by selecting CTE Key Properties. See *Creating a New Key* in the [Managing Policies](#) chapter in the [CTE Administrator Guide](#).

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 for AES-CBC CS1 Keys and Host Groups

In a host group, do not deploy policies associated with AES-CBC and AES-CBC CS1 keys unless all hosts are running VTE for AIX version 5.3 or CTE version 7.0.0 or later.

Chapter 7: Utilities for CTE Management

Thales provides a variety of utilities that augment the standard AIX utilities. This combination of tools helps administrators manage CTE. The following utilities are described in this chapter:

secfsd Utility	48
vmsec Utility	53
Restricting Access Overrides with Client Settings	57
vmd utility	58
Agent Health Utility	58
agentinfo Utility (Java version)	61
check_host Utility	61
register_host Utility	62
Displaying Information for Nested File Systems with the DF tool	62
User Space Utility	63

secfsd Utility

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

- GuardPoints defined in the *GuardPoints* 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 **GuardPoints** 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, CTE 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

Command	Description
<code>-help</code>	display <code>secfsd</code> options
Status Options	
<code>-status guard [-v -tree]</code>	list all GuardPoints
<code>-status keys</code>	show current encryption key state
<code>-status auth</code>	list authentication settings
<code>-status lockstat</code>	show CTE lock status

Command	Description
-status logger	list logging details
-status policy	list configured policies
-status plist	list protected processes
-status devmap	list guarded devices
Manual GuardPoint options	
-guard path [container ID]	manually guard path
-unguard path [container ID]	manually unguard path
Version option	
-version	list version of kernel module <code>secfs2</code>
Encryption Mode option information	
crypto	Displays the encryption modes that are supported.
Configuration Mode option information	
config <config_param> <value>	Displays the encryption modes that are supported.

secfsd Examples

Display GuardPoint Information

To display the GuardPoint paths, applied policies, policy type, and guard status, use the `secfsd -status guard` command. For example:

```
# 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
```

Column	Description
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 GuardPoints tab.
ConfigState	Guard status of the GuardPoint, as recognized by the key manager. It can be guarded or unguarded.

Column	Description
Status	Current guard status, as recognized by CTE. State can vary.
Reason	Additional information about the status, if any.

Notes

- Config State and Status can vary. As an example, if you apply a GuardPoint and someone is currently working in the GuardPoint, the policy cannot be applied at that time. In this case, the ConfigState is guarded and the Status is not guarded.
- When the user removes an auto-mounted GuardPoint from CipherTrust Manager, the CTE Agent is only deleted after the configured `autoofs` timeout expires. This timeout does not start until the GuardPoint is free.

Display GuardPoint Information in a Different Format

To display the same information in a block format, use the `secfsd -status guard -v` command. For example:

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

Display Host Settings

To display the SHA2 hash signature for each protected host setting, use the `secfsd -status auth` command. For example:

```
# secfsd -status auth
/bin/su 3E765375897E04C39AB17D4C755F50A35195535B6747DBA28DF9BD4AA672DFF9
|authenticator|/usr/sbin/sshd
98FC599D459EDEA52A60AB394B394803B5DAB96B53148DC608732DDA6777FA1A
/usr/sbin/in.rlogind 5C9A0EDD8BF54AE513F039476D21B3032507CF957AA0CB28C368EB8AB6E684FB
/bin/login 0D2EE0B995A30AE382B4B1CA5104715FC8902F457D283BDABAAD857B09259956
/usr/bin/gdm-binary 363780522E3CCF9ABF559F059E437743F9F97BBBB0EE85769007A464AD696BD1
/usr/bin/kdm BAD41BBCDD2787C7A33B5144F12ACF7ABC8AAA15DA9FDC09ECF9353BFCE614B5
```

Display Key Status

To display the status of CTE keys, use the `secfsd -status keys` command. For example:

```
# secfsd -status keys
Encryption keys are available
```

Display Lock Status

To display the status of CTE locks, use the `secfsd -status lockstat` command. For example:

```
# secfsd -status lockstat
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 CTE software, or change operating system files, the status of FS Agent Lock and System Lock must be false.

Agent Security Configuration Protection

The Agent lock directory, `/opt/vormetric/DataSecurityExpert/agent/secfs/.sec` contains secfs secret files, configuration files, host setting signatures, etc. Thales recommends protecting the directory whenever secfs is online.

Applying improved directory protection ensures that only CTE applications (`vmd`, `secfsd`, `voradmin`, etc.) can modify the `.sec` directory and the files in it. All users, including root, are denied read/write access to the files. They also do not have permissions to modify `conf` and `bin` directories, using other tools.

A new command has been created to protect the directory: `voradmin secfs config`

Syntax

```
# voradmin secfs config <configuration_parameter> <value>
```

Example

```
# voradmin secfs config pagecache_writeback 1
```

Previously, you would have had to use the following command to achieve the same results as the example above:

```
# echo 1 > /opt/vormetric/DataSecurityExpert/agent/secfs/.sec/conf/pagecache_writeback
```

Note

When CTE is upgraded to v7.2.0 from the previous release, it may display 'Permission Denied' warnings which display when files are removed from subdirectories of the `.sec` directory. You can ignore these warnings. They are harmless.

Display CTE Log Status

To display the status of CTE log service, use the `secfsd -status logger` command. For example:

```
# secfsd -status logger
Upload URL: https://vmSSA06:8444/upload/logupload,https://vmSSA07:8444/upload/logupload,
\
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 CTE certificate. CTE uses the certificate to authenticate CTE when it uploads the log data to the CipherTrust Manager.

Display Applied Policies

To display the policies that are applied to CTE, use the `secfsd -status policy` command. For example:

```
# secfsd -status policy
Policy: enc-audit
Type: ONLINE
```

Display CTE Process Information

To display CTE processes, use the `secfsd -status pslist` command. This command shows the process number associated with each CTE process. To show the details about a specific CTE process, use the `ps -fp <process #>` command, where `<process #>` is the process number from the `secfsd -status pslist` command.

For example:

```
# secfsd -status pslist
Protected pid list:      739    731
# ps -fp 739
UID      PID    PPID  C   STIME          TTY  TIME    CMD
root     739    1     0   11:04:56      -   0:00  /opt/vormetric/ \
        DataSecurityExpert/agent/vmd/bin/vmd
```

Display CTE Version Information

To display CTE version information, use the `secfsd -version` command. For example:

```
# secfsd -version
version: 7.2.0.56
```

Manually Enable a GuardPoint in CipherTrust Manager

To manually enable a GuardPoint on an AIX host:

1. Click **CTE > Clients > <clientName> GuardPoints**
2. Click **Create GuardPoint**.
3. In the Policy field, select a policy.
4. Set Type to **Manual Directory**.
5. Click **Browse** and enter the GuardPoint path.
6. Click **Create**.
7. Log onto the system hosting CTE as the root user.
8. To manually enable the GuardPoint, use the `secfsd -guard <path>` command. For example:

```
# secfsd -guard /opt/apps/etc
secfsd: Path is Guarded
```

9. To verify the change, use the `secfsd -status guard` command. For example:

```
# secfsd -status guard
GuardPoint      Policy              Type      ConfigState  Status      Reason
-----
/opt/apps/etc   allowAllOps_fs     manual    guarded      guarded     N/A
```

secfsd and Raw Devices

CTE only creates block devices. To display them, use the `ls -l /dev/secvm/dev` command. For example:

```
# ls -l /dev/secvm/dev
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 CTE on the host. On AIX hosts, the `vmsec` utility is located in:

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

vmsec Syntax

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

vmsec Examples

Display CTE Challenge String

To display a CTE password challenge string and enter the response string when the CipherTrust Manager is not network accessible, use the `vmsec challenge` command. This command displays a challenge string that you can send to your key manager administrator, who will then send you back the correct response information.

For example:

```
# vmsec challenge
Contact a Security Server administrator for a response.
Your hostname is host120.my.domain.com
Your challenge is: F5TL-42HU-5H6Y-EJCK
Response (part 1) -> 6B2T-Q3DV-5EK3-QOFD
Response (part 2) -> XBP5-LQXB-TDWA-SILG
Response (part 3) -> XSEA-CQB5-S6U5-3YWV
Response (part 4) -> KXRS-QYXB-BP74-C4RN
Success!
```

Contact your key manager administrator and give them the challenge string. The administrator will give you four response strings. Enter the first response string in the **Response (part 1)** field and press **Enter**, then enter the second, third, and fourth response strings in the same way. You have 15 minutes to enter the first response string.

Tip

If you are using CipherTrust Manager, the ability to change the contact string will be added in a future release. For CipherTrust Manager, the contact string says "Contact your CM administrator".

Display CTE Status

This utility shows you if CTE is configured and running. If it is not running, you might need to start it manually. To display CTE status, use the `vmsec checkinstall` command. For example:

```
# vmsec checkinstall
The kernel component is installed and running.
```

Entering a Password

To enter the CTE static host password, use the `vmsec passwd` command. For example:

```
# vmsec passwd
Please enter password:
OK passwd
```

To enter CTE static host password on the command line so you can specify it in a batch script, specify the password using the `-p` option. For example:

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

Display Kernel Status

To display the kernel status, use the `vmsec status` command. For example:

```
# vmsec status
FILE_FORMAT=2
FILE_GENERATED=08/27/2019 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=7.2.0.56
sdk_builddate=2019-08-19 15:16:46 (PDT)
coreguard_locked=false
system_locked=false
logger_upload_url=https://th1602-2114.qa.com:8447/upload/logupload,https://th1602-
```

```
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=2019-07-25 12:07:14.514
vmd_last_server_update_time=2019-07-25 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 CTE Build Information

To see the CTE build version, use the `vmsec version` command. For example:

```
# vmsec version
version 7
2020-07-31 10:03:59 (PDT)
Copyright (c) 2009-2022, Thales. All rights reserved.
```

Display Contents of Conf files

To display the contents of the `agent.conf` and `.agent.conf.defaults` files, use the `vmsec vmdconfig` command. For example:

```
# vmsec vmdconfig
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=7.2.0
VMSDK_AGENT_BUILD_ID=28
PREV_URLS=https://srv.my.thales.com:8443
syslog_appender_myhost name=dev.my.thales.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.thales.com:8443
STRONG_ENTROPY=false
```

Configuring Dynamic Host Settings for AIX

Previously, when host settings were changed, currently executing processes for the specified images were not modified. Only when a new process started would the changed host settings take effect. To make an already running process use the new host setting values, you had to terminate the process and restart it. The Dynamic Host Setting feature now permits the modified host settings take effect when the new entries are pushed from the CipherTrust Manager to the agent.

If the Dynamic Host Setting feature is enabled, then when a host setting is altered, all running processes with that signature are affected and their existing security attributes are modified to the new host settings parameters. Future actions by a process will contain authorization(s) derived from the new attributes. It is important to note that all descendent processes are affected by a process's host setting change. If an existing host setting entry is modified, the same situation occurs.

If an existing process did not have a host setting and one is applied, then all processes with that signature are updated with the new values. All of the existing descendent processes are affected by the changes. New child processes inherit the host setting parameters and authorizations.

In v7.2 of CTE, three new `vmadmin` commands are provided to enable, disable, and report the status of the Dynamic Host Settings:

- To turn on dynamic host settings, type:

```
# voradmin secfs config dhs_on 1
```

Note: You must restart the agent for this to setting to take effect.

- To turn off dynamic host settings, type:

```
# voradmin secfs config dhs_on 0
```

Note: You must restart the agent for this to setting to take effect.

- To report the state of the dynamic host settings, type:

```
# voradmin secfs config dhs_state
```

Note: State information is added to the `secfs.log` file.

- To immediately enable dynamic host settings without restarting the agent, type:

```
# voradmin cmd dhs_enable
```

Note: You must restart the agent for this setting to take effect. Perform this command after turning on DHS.

- To immediately disable dynamic host settings without restarting the agent, type::

```
# voradmin cmd dhs_disable
```

Note: Restarting the agent will enable it unless you turn the dynamic host settings off first.

Restricting Access Overrides with Client Settings

CTE host/client settings are the means by which an administrator configures user authorization. Users with root privileges, on Linux systems, have the unfettered ability to override all file access and execution permissions imposed by the system.

CTE access control allows you to restrict privileges of users, groups, application processes and binaries, including root users and `setuid` programs. By default, CTE agent **does NOT** trust any process as authenticated. Any attempt to access a resource, by any process, will therefore be flagged with a “User Not Authenticated” notification. The CTE agent must be instructed to trust the authenticator process progeny. For example, the `/usr/sbin/sshd` is a process that can be trusted to authenticate the user to the system and to CTE.

In some setups, when editing a host, system administrators can use the **host settings** > `|authenticator|` feature with `su` to change identities and gain access to restricted data. You can instruct CTE to not trust any authentication attempt performed by certain identities by assigning restricted users to a user shell that CTE 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.

CTE 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.

Note

Using `|trust|*` before a `|path_no_trust|` host setting no longer disables the `|path_no_trust|` host setting.

For example, the following host setting denies authentication for users accessing through `sshd`:

```
|trust|*  
|path_no_trust|/usr/sbin/sshd
```

To restrict access overrides in **CM**:

1. In the CM products page, click **Transparent Encryption > Clients**.
2. Click on an existing Client name to edit the host.
3. Click **Client Settings** tab.
4. Add the following to the 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 **Apply**.

vmd utility

The `vmd` utility displays CTE 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 CTE version

`-f` runs `vmd` in the foreground

Display the Installed Version

To display the installed CTE version, type:

```
# vmd -v
Version 7
7.2.0.56
2022-02-04 11:09:40 (IST)
Copyright (c) 2009-2022, Thales.. All rights reserved.
```

Agent Health Utility

The `agenthealth` utility validates:

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

- Tests if the agent can reach the GuardPoints
- CTE log directory resource status

This directory contains pending CTE log files for upload. This utility reports the size and number of pending files for upload. These text files are logs that contain vmd/SecFS information. They are regenerated whenever secfs restarts. If the number of files is unexpectedly large, this can indicate a problem.

The Agent Health check script

By default, the `agenthealth` script is installed in `/opt/vormetric/DataSecurityExpert/agent/vmd/bin`.

To run the `agenthealth` check script, type:

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

System Response

```
Checking for super-user privilege ..... OK
CipherTrust Agent installation ..... OK
CipherTrust policy directory ..... OK
Registration to server ..... OK
Kernel modules are loaded ..... OK
VMD is running ..... OK
SECFSD is running ..... OK
dsm4209.sjinternal.com is resolvable ..... OK
dsm4209.sjinternal.com port 8446 is reachable .... OK
dsm4209.sjinternal.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 ..... 2021-07-07 15:47:08.290
Checking available disk space ..... OK
Checking logging space ..... OK
    Log directory is "/var/log/vormetric"
    File system for log data is "/", 48G free (5% full)
    Log directory contains 9 of maximum 200 files (4% full)
    Log directory contains 1 of maximum 100 Mbytes used (1% full)
Testing access to /media ..... OK
Testing access to /usr/data/sub1 ..... OK
[root@agt4206 bin]#
```

Agent Health Return Codes

Previously, the agent health return codes were only available in `/var/log/vormetric/agenthealth.log`. Now, the following options are also available through the help pages:

Help

This agent health script checks various facets of the CipherTrust agent to make sure that everything is functioning properly. Results are also logged to `/var/log/vormetric/agenthealth.log`.

Syntax

```
# ./opt/vormetric/DataSecurityExpert/agent/vmd/bin/agenthealth --help
```

Return Codes

Use the return code option to get a list of the return codes and what they mean. The codes are returned if the Agent is not running.

Syntax

```
# ./opt/vormetric/DataSecurityExpert/agent/vmd/bin/agenthealth --return_codes
```

Response

Return Code	Definition
EPERM	User is not root.
ENOENT	One of the programs used in this script does not exist. See <code>/var/log/vormetric/agenthealth.log</code> for which program is missing.
ENOPKG	Agent software is not properly installed. Agent configuration directory is missing or corrupt. See <code>/var/log/vormetric/agenthealth.log</code> for more details.
EPROTO	Agent is not registered to a key manager. Register the agent to a key manager and try again. Try the wait option if the agent has never started correctly after registration. See <code>/var/log/vormetric/agenthealth.log</code> for more details.
EIO	Kernel modules are not loaded. To load a kernel module, type: <code>/etc/vormetric/secfs start</code>
ESRCH	VMD is not running. To start vmd manually, type: <code>/usr/bin/vmd</code>
SECFSD	Secfsd is not running. To start the secfsd manually, type <code>/usr/bin/secfsd</code>
EHOSTUNREACH	Unable to reach the Key Manager. Check network connectivity.
ECONNREFUSED	VMD is not listening. VMD did not finish initialization. See <code>/var/log/vormetric/vmd.log</code>
EWOULDBLOCK	VMD is attempting to connect to the Key Manager but has exceeded the designated wait time. Check <code>/var/log/vormetric/vmd.log</code> to fix any issues and retry.

Wait Time

Use `--w` to set a maximum wait time in seconds. The minimum is 10 seconds to test for the VMD to Key Manager initial contact. The default setting is 0, which means that there is no wait. Maximum is 1200 seconds.

Syntax

```
[root@agt4206 bin]# ./opt/vormetric/DataSecurityExpert/agent/vmd/bin/agenthealth --w <value>
```

Example

```
[root@agt4206 bin]# ./opt/vormetric/DataSecurityExpert/agent/vmd/bin//agenthealth --w 60
```

Response

```
Checking for super-user privilege ..... OK
CipherTrust Agent installation ..... OK
```

```
CipherTrust policy directory ..... OK
Registration to server ..... OK
Kernel modules are loaded ..... OK
VMD is running ..... OK
SECFSD is running ..... OK
dsm148.i.vormetric.com is resolvable ..... OK
dsm148.i.vormetric.com port 8446 is reachable ... OK
dsm148.i.vormetric.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 ..... 2021-08-18 10:34:56.665
Checking available disk space ..... OK
Checking logging space ..... OK
Log directory is "/var/log/vormetric"
File system for log data is "/", 29G free (23% full)
Log directory contains 1 of maximum 200 files (0% full)
Log directory contains 0 of maximum 100 Mbytes used (0% full)
```

If the customer did not use the wait time options, the output would look similar to the following:

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

```
Checking for super-user privilege ..... OK
CipherTrust Agent installation ..... OK
CipherTrust policy directory ..... OK
Registration to server ..... OK
Kernel modules are loaded ..... OK
VMD is running ..... OK
SECFSD is running ..... OK
Can communicate to at least one server ..... FAILED
For more information consult the log file /var/log/vormetric/agenthealth.log
```

agentinfo Utility (Java version)

The `agentinfo` utility collects system and CTE 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, (This section describes the Java version.)

The `agentinfo` utility is a Java Script 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 CTE 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 CipherTrust Manager during registration.

Run the `check_host` utility on a system that is hosting CTE 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[,name:port] | -r name
```

-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 CipherTrust Manager and the host, and to register CTE on the CipherTrust Manager. After the host is registered, you can configure CTE, apply GuardPoints, or perform database backups. Run the `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 CipherTrust Manager 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.

Displaying Information for Nested File Systems with the DF tool

When a file system mounts on top of another file system, the command `df -a` does not display the attributes for the covered file system.

On Linux environments, this is the expected behavior for any file system that is overlaid by another file system.

The `secfs` driver properly handles the call, which is made by the `statfs` system call, which is issued by the `df` tool. When the system call returns, its structures are correctly populated with the details of the nested file system. On examining the source of the `df` tool, it is found that when the `-a` switch is on, it nullifies the stats which are received for overlaid mounts. When the `-a` option is not enforced, the stats are maintained.

Issue the `df` command for a specific mount point, for example `df /xfs/nested-xfs` (where `/xfs` is a `secfs` GuardPoint). It works correctly.

User Space Utility

CTE has added a feature to improve the performance of the user cache lookup function, which contains information such as username and group name(s), plus timestamps and other supporting flags. It is mainly used during LDAP authentication. This feature improves lookup performance by allowing user-configurable values for lookup retries and user information refresh times. Performance can be impacted if authentication/ user lookups and timeout/ retries take a significant amount of time. Previously, these values were hard-coded. Now they are user-configurable.

The configuration options for this feature contain three new configuration parameters:

Initial cache miss

Initial check of access when no user information cache entry exists.

- **Default value:** 60 seconds
- **Default minimum:** 2 seconds
- **Default maximum:** 3600 seconds (1 hour)

To set this value, type:

```
# voradmin secfs config usrinf_miss_timeout <seconds>
```

Cache expiration timeout

Used when user information cache entry has not been used for the duration needed to trigger a refresh.

- **Default value:** 300 seconds (5 minutes)
- **Default minimum:** 60 seconds
- **Default maximum:** 86400 seconds (1 day)

To set this value, type:

```
# voradmin secfs config usrinf_expiry_timeout <seconds>
```

Cache stale timeout

When a cache entry has not been updated for the duration of the timeout, the entry will be considered inactive and removed.

- **Default value:** 300 seconds (5 minutes)
- **Default minimum:** 60 seconds
- **Default maximum:** 86400 seconds (1 day)

To set this value, type:

```
# voradmin secfs config usrinf_stale_timeout <seconds>
```

Usage

CTE uses the default values initially. If network errors occur and LDAP failure is observed (in system logs, look for timeout errors), then you have two options:

- If the network errors can be corrected in a short time, then the timeout values can remain unchanged.
- If not, set the expiration and stale timeout to large values. Then, reduce the initial timeout incrementally until the problem resolves.

Note: CTE must be restarted when a new timeout value is set, in order for the value to take effect.

Keep the new value until the problem is resolved. Then, once the network problems have been fixed, reset the timeout values back to the initial values.

Chapter 8: Upgrading CTE on AIX

This chapter describes how to upgrade an existing VTE for AIX host to CipherTrust Transparent Encryption (CTE) for AIX.

This chapter contains the following sections:

Scheduling a CTE Agent Upgrade 65

Scheduling a CTE Agent Upgrade

You can schedule an upgrade of the CTE Agent to occur the next time the server on which a CTE Agent is installed reboots normally. Scheduling an upgrade can minimize CTE service interruptions and reduce coordination issues in organizations where the security roles are separated.

Before You Begin

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.
- CipherTrust Manager connectivity is required during the scheduled upgrade process.
- All databases must be configured to automatically stop before CTE services stop during reboot/shutdown.
- Stopping and restarting the CTE 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

Note

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 CTE version by using the procedure described here with the newer installation binary.

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

```
$ vmd -v
```

The version listed must be version 5.3.0 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-7.2.0.56-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.

```
# shutdown -Fr
```

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

4. After the system is up and running, 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 want to upgrade without waiting for the system to reboot, 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. For example:

```
# ./vee-fs-7.2.0.56-aix71.bin
```

The following upgrade confirmation is displayed:

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

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 agreement 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.

Chapter 9: Uninstalling CTE from AIX

This chapter describes how to upgrade an existing VTE for AIX host to CipherTrust Transparent Encryption (CTE) for AIX.

This chapter contains the following sections:

Considerations	67
Procedure	67

Considerations

- The CTE Agent must be removed from the AIX host before the host is removed from the key manager with which it is registered.
- Database applications like DB2 and Oracle can lock the user space while they run. If the uninstall fails because a GuardPoint is in use, determine which applications are using the files in the GuardPoint and stop them. Then run the uninstall again.

Procedure

1. Stop any application from accessing files in the GuardPoint.
2. In the key manager with which this host is registered, do the following:
 - Decrypt any data you want to use after uninstall. After the CTE 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.

This decryption must be done on *every* GuardPoint on the host if you want to access all existing data on the host.
 - Make sure the Agent and System locks have been disabled for the host.
 - Thales recommends that you remove all GuardPoints from the host before you uninstall the CTE Agent.

Do not remove the host from the key manager yet.
3. Log on to the host as .
4. Remove the host record from the key manager.

THALES

Contact us

For office locations and contact information,
visit cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <

