Vormetric Data Security Platform

Vormetric Transparent Encryption for AWS

Getting Started Guide

Document Version 3

September 9, 2015
FAILURE OF ANY TRANSMISSION HARDWARE, TECHNOLOGY, OR SYSTEM USED BY LICENSEE OR ANY LICENSEE CUSTOMER. VORMETRIC SHALL HAVE NO LIABILITY FOR, AND LICENSEE SHALL DEFEND, INDEMNIFY, AND HOLD VORMETRIC HARMLESS FROM AND AGAINST, ANY SHORTFALL IN PERFORMANCE OF THE SOFTWARE, OTHER HARDWARE OR TECHNOLOGY, OR FOR ANY INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS, AS A RESULT OF THE USE OF THE SOFTWARE IN ANY ENVIRONMENT. LICENSEE SHALL DEFEND, INDEMNIFY, AND HOLD VORMETRIC HARMLESS FROM AND AGAINST ANY COSTS, CLAIMS, OR LIABILITIES ARISING OUT OF ANY AGREEMENT BETWEEN LICENSEE AND ANY THIRD PARTY. NO PROVISION OF ANY AGREEMENT BETWEEN LICENSEE AND ANY THIRD PARTY SHALL BE BINDING ON VORMETRIC.

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

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

Preface ......................................................................................... i
  Documentation Version Release Notes ........................................... i
  Scope ....................................................................................... i
  Intended audience ...................................................................... i
  Related documents .................................................................... ii
  Typographical Conventions ........................................................ ii
  Guide to Vormetric Documentation ............................................. iii
  Vormetric Data Security Platform—Overview ................................. vi
  Service updates and support information ..................................... vii
  Sales and Support ....................................................................... vii

1 Overview .................................................................................... 1
  What Vormetric Transparent Encryption for AWS does .................. 1
  What Vormetric Transparent Encryption for AWS is ...................... 1

2 DSM Administrators and Domains ............................................... 5
  Creating a DSM administrator ...................................................... 6

3 VTE Policies .............................................................................. 11
  Creating and viewing the data to be protected ............................... 12
  Creating a policy to control access to files .................................... 14
  Applying a policy to a GuardPoint ................................................ 25
  Editing a policy to allow limited access ........................................ 29

4 Auditing Data Access .................................................................. 37
  Modifying the current policy to audit file access ............................ 37
  Viewing the audit logs .................................................................. 38
Preface

This guide contains conceptual information and hands-on lab practice for the Vormetric Transparent Encryption for AWS (VTE).

Documentation Version Release Notes

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

<table>
<thead>
<tr>
<th>Document Version</th>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>9/10/13</td>
<td>Initial Release.</td>
</tr>
<tr>
<td>1.1</td>
<td>1/28/14</td>
<td>Removed instructions on connecting to instances using MindTerm. Suggested using PuTTY. Cleaned up minor issues. Fixed external hyperlinks.</td>
</tr>
<tr>
<td>3</td>
<td>9/9/15</td>
<td>Changed product name from Vormetric Data Firewall for AWS to Vormetric Transparent Encryption for AWS. Changed document numbering to whole numbers.</td>
</tr>
</tbody>
</table>

Scope

This document describes the most the basic and fundamental Vormetric Transparent Encryption for AWS concepts and procedures. More detailed information can be found in the DSM Administrators Guide. Contact cloudsupport@vormetric.com to get a copy.

Intended audience

The Getting Started Guide is intended for administrators who are responsible for data security in the Amazon cloud.

Assumptions

To complete the labs in this guide, requires the following:

- Experience creating Elastic Cloud Compute (EC2) instances in the AWS infrastructure.
- Experience using Linux.
• Installed either the Vormetric Transparent Encryption for AWS - 5 Client or the Vormetric Transparent Encryption for AWS - 30-day Free Trial with at least one DSM and one protected host in your AWS account.

• The Deployment Details of your DSM and protected hosts. This information was generated and displayed when you registered for the 30-day Free Trial or installed the 5-client product. See “Deployment Details information” on page 53.

Related documents

DSM Administrators Guide

Typographical Conventions

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

<table>
<thead>
<tr>
<th>Convention</th>
<th>Usage</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold regular font</strong></td>
<td>GUI labels, and options.</td>
<td>Click the <strong>System tab</strong> and select <strong>General Preferences</strong>.</td>
</tr>
<tr>
<td><strong>bold, monotype font</strong></td>
<td>commands, arguments, switches, options, variables, elements, properties, objects, parameters, events</td>
<td><code>session set appname=</code></td>
</tr>
</tbody>
</table>
| **regular monotype font** | Command and code examples, XML examples | Example: `session start
iptarget=192.168.253.102` |
Preface

Guide to Vormetric Documentation

Typographical Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Usage</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>italic regular font</td>
<td>GUI dialog box titles</td>
<td>The General Preferences window opens.</td>
</tr>
<tr>
<td></td>
<td>Non-literal symbols</td>
<td>myport, Failover.Port</td>
</tr>
<tr>
<td></td>
<td>File names, paths, and directories</td>
<td>/usr/bin/</td>
</tr>
<tr>
<td></td>
<td>URLs and names of protocols</td>
<td><a href="http://server.domain.com:90/">http://server.domain.com:90/</a></td>
</tr>
<tr>
<td></td>
<td>Text to be replaced</td>
<td>&lt;hostname&gt;</td>
</tr>
<tr>
<td></td>
<td>Emphasis</td>
<td>Do not resize the page.</td>
</tr>
<tr>
<td></td>
<td>New terminology</td>
<td>CDF (Carousel Definition Format)</td>
</tr>
</tbody>
</table>

**bold italics font**

Command line variable. # cd Vormetric_OracleTDE_Library_Path

“quotes”

File extensions

Attribute values

Terms used in special senses

“.js”, “.ext”

“true” “false”, “0”

“1+1” hot standby failover

Guide to Vormetric Documentation

Core documentation

*Page count does not include Table of Contents, Preface, Glossary or Index. Pictures includes blank pages.*

1. **Vormetric Transparent Encryption (VTE) Getting Started Guide** (~98 pages, 45% pictures). Read this first! Provides most of the general knowledge and procedures you need to protect your data with VTE.

   **Audience:** Anyone who wants to know about VTE and how to set it up.


   Use this to install the Data Security Manager.

   **Audience:** Administrator who installs security hardware and software.


   Use this to install agents on the hosts you want to protect.

   **Audience:** Administrator who installs security software on hosts with data to be protected.
4. **Vormetric Data Security (VDS) Platform Administrators Guide** (~304+ pages, 10% pictures). Refer to this book for detailed DSM Administrator procedures such as configuring the DSM for HA, installing license files, configuring host groups and so on. This book is divided into sections for DSM System Administrators, DSM Domain Administrators, DSM Security Administrators, VDS Host Administrators and Other Administrators.

**Audience:** DSM Administrators and anyone using the *Getting Started Guide* to set up VTE and needs additional instructions.

5. **Vormetric Transparent Encryption (VTE) Data Transformation Guide** (~85 pages, 20% pictures). Detailed information on 1) doing the initial encryption of your clear data, and 2) rekeying GuardPoints (key rotation).


**Audience:** Anyone interested in upgrading their DSM.

7. **Releases Notes for DSM, VTE Agents and other products** (~10 pages each). Lists compatible operating systems, browsers, hardware, resolved and known issues, and upgrade notes.

**Audience:** Anyone interested in upgrading their VDS products.

### Specialized documentation

1. **Vormetric Key Management (VKM) Configuration and Procedures Guide** (~60 pages, 15% pictures). Describes the *VDS Certificate and Key Vault, KMIP support, how to migrate the Oracle Database TDE MEK to the DSM, and how to encrypt the Microsoft SQL Server with TDE DEK with an asymmetric key stored in the DSM.*

2. **Vormetric Security Intelligence Configuration Guide** (~35 pages, 30% pictures). Use this to integrate your Vormetric Data Security Platform with the ArcSight ESM, Splunk, or IBM QRadar security information and event management (SIEM) systems.


6. **Vormetric Data Security Manager (DSM) Automation Reference** (~40 pages, 0% pictures). Describes the DSM Automation CLI (VMSSC) to the DSM. Allows you to automate deployments, script routine and repetitive tasks, and perform unattended batch processing. Advanced users only!
7. **Vormetric Data Security (VDS) Platform Web Services Description Language Reference** (~140 pages, 0% pictures). Describes the web services available in the VDS WSDL. Intended for experienced software developers with knowledge of web services.


### Searching through all the documents

Technical information for Vormetric products can be spread across many documents. Instead of searching through each individual document to find the information you need, you can use the following procedure to search all of the VTE documents with a single search in Windows (the same process should work for UNIX/Linux):

1. Copy all the .pdf files of a specific product into a single directory. For example, using the Vormetric Transparent Encryption:

   ```
   C:\Documents\PDFs\5.2.3>dir
   Admin_Guide_V1.pdf
   Agent_Install__Config_Guide_v2.pdf
   DSM_Automation_Reference_v1.pdf
   DSM_Install_Guide_v1.pdf
   Event__Log_Messages_Ref_v1.pdf
   GettingStarted_v1.pdf
   VSI_Reference_v1.pdf
   RN_DSM.pdf
   RN_Linux.pdf
   RN_RHEL7.pdf
   RN_UNIX.pdf
   RN_Windows.pdf
   VDSCompatibilityMatrix.pdf
   ```

2. Bring up Adobe Reader or Adobe Acrobat.

3. Open any pdf file from that directory: **File > Open > Select File**.

4. Click **Edit > Advanced Search**.

5. Under "Where would you like to search?" click "**All PDF Documents in**", then select the directory containing all the VTE PDF files. In this case, `C:\Documents\PDFs\5.2.3`

6. In the "What word or phrase would you like to search for?" enter the search phrase and click search.

   You can do this with any set of PDF files.
Vormetric Data Security Platform—Overview

The Vormetric Data Security (VDS) Platform protects data-at-rest, wherever it resides. The platform solves security and compliance issues with encryption, key management, privileged user access control, and security intelligence logging. It protects data in databases, files, and Big Data nodes across public, private, hybrid clouds and traditional infrastructures.

The platform consists of products that share a common, extensible infrastructure. At the heart of the platform is the Data Security Manager (DSM), which manages policies, keys, and the collection of security intelligence, all of which is managed and observed through your browser. In addition to the DSM, the Vormetric Data Security Platform consists of the following products:

- **Vormetric Transparent Encryption (VTE)** secures any database, file, or volume across your enterprise without changing the applications, infrastructure, or user experience.
- **Vormetric Application Encryption (VAE)** provides a framework to deliver application-layer encryption such as column-level encryption in databases or encrypt specific fields in files.
- **Vormetric Tokenization** replaces sensitive data in your database with unique identification symbols called tokens. This reduces the number of places that clear text sensitive data reside, and thus reduces the scope of complying with PCI DSS and corporate security policies.
- **Vormetric Key Management (VKM)** centralizes the storage and management of KMIP and Transparent Data Encryption (TDE) keys as well as Vormetric and non-Vormetric encryption keys and certificates.
• **Vormetric Security Intelligence** provides comprehensive logging combined with Security Information Event Management Systems (SIEM) to detect of advanced persistent threats and insider threats. In addition, the logs satisfy compliance and regulatory audits.

### Service updates and support information

Vormetric's Master Software License and Hardware Purchase Agreement ("MSLA") defines software updates and upgrades, support and services, and governs the terms under which they are provided. Any statements made in this guide or collateral documents that conflict with the definitions or terms in Vormetric's MSLA, shall be superseded by the definitions and terms of the MSLA. Any references made to “upgrades” in this guide or collateral documentation can apply either to a software update or upgrade.

### Sales and Support

For support and troubleshooting issues:

- help.vormetric.com
- Email questions to cloudsupport@vormetric.com.

For Vormetric Sales:

http://enterprise-encryption.vormetric.com/contact-sales.html

(888) 267-3732

sales@vormetric.com
Overview

Vormetric Transparent Encryption for AWS (VTE) protects your Amazon Web Services (AWS) data. The purpose of this guide is to present fundamental VTE concepts and hands-on labs for implementing VTE in AWS.

What Vormetric Transparent Encryption for AWS does

Vormetric Transparent Encryption for AWS protects data! VTE allows you to:

- Identify files and directories to protect.
- Specify who can access those files and block everyone else including system administrators.
- Identify the specific times when users can access that data.
- Define which executables can be used on those files (for example, Acrobat.exe, WINWORD.EXE, cat, tail, chmod0).
- Specify the processes that can and cannot be used on those files (for example, read, write, delete, copy, rename).
- Encrypt the files such that even if unauthorized users gain access to it, the data remains unusable.
- Efficiently create, store and manage the encryption keys used to encrypt data.
- Keep encrypted file’s metadata (file name, owner, size and so on) in clear text so IT administrators can carry out normal IT duties (for example, data back-up and restore).
- Activate auditing to see who accessed what files, when they were accessed, what executable were used, and what processes (read, write, copy and so on) were attempted.

What Vormetric Transparent Encryption for AWS is

VTE consists of a Data Security Manager (DSM) and one or more file system agents residing on the hosts that they protect (called protected hosts). The DSM is the central component of VTE, storing and managing host encryption keys, data access policies, administrative domains, and administrator profiles. The agents communicate with the DSM and implement the security
policies on their protected host systems. Communication between agents and the DSM is via SSL. The VTE Security Administrator’s job is to establish data access policies and the security infrastructure through the Management Console, a browser-based interface to the DSM.

In a traditional data center, the DSM is a security-hardened hardware appliance and the protected hosts are hardware servers. This is shown in **Figure 1**.

![Figure 1: Vormetric Transparent Encryption Architecture](image)

In AWS, the DSM and protected hosts are virtual machines in the AWS cloud (**Figure 2**).
**Figure 2:** VTE Architecture in the Amazon Cloud with protected hosts and clients

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

What Vormetric Transparent Encryption for AWS is
DSM Administrators and Domains

*DSM administrators* are different from *system administrators*. A system administrator is a person who is responsible for the upkeep, configuration, and reliable operation of computer systems. System Administrators generally have access to all the data on all the machines that they administer. A DSM administrator has no access to data or user accounts on any of the machines in a network. The DSM administrator’s sole responsibility is to provide data access to those who need it and block data access to those who don’t need it—including system administrators.

DSM administrators protect data by establishing data access policies, encrypting data, and auditing data access attempts. DSM administrators are assigned to *domains*, which are a group of one or more VTE-protected hosts.

**Figure 3:** Vormetric Transparent Encryption Domains

A newly installed DSM has a password-protected top-level *DSM System Administrator* account (to reiterate, *DSM System Administrator accounts* have no relationship to *system administrator accounts*). For each domain, the DSM System Administrator creates a single *DSM Domain Administrator* account. DSM Domain Administrators then create *DSM Security Administrators* who define policies, set up *GuardPoints* (directories to be protected), and do most of the actual data protection work. Having three levels of administrators and independent security domains, separates security duties such that no single individual can have, or provide, access to sensitive data.
There are three types of DSM administrators with no access to system data:

- **DSM System Administrators**: create or remove other DSM administrators of any type, change their passwords, create or remove domains, and assign a DSM Domain Administrator to each domain. The DSM System Administrator cannot perform any security procedures in any domain.

- **DSM Domain Administrators**: add or remove DSM Security Administrators to domains, and assign some or all of the following roles to each one:
  - **Audit**: Allow a DSM Security Administrator to generate and view logging data for file accesses.
  - **Key**: Allow a DSM Security Administrator to create, edit, and delete encryption keys.
  - **Policy**: Allow a DSM Security Administrator to create, edit, and delete policies. A policy is a set of rules that specify who can access which files with what executable during what times. Policies are described in more detail later.
  - **Host**: Allow a DSM Security Administrator to configure, modify, and delete hosts and host groups.
  - **Challenge & Response**: Generate a temporary password to give to a system user to decrypt cached encryption keys when there is no connection to the DSM.

DSM Domain Administrators cannot remove domains and cannot perform in any of the domain security roles.

- **DSM Security Administrators**: perform the data protection work specified by their roles. These roles, allow them to create policies, configure hosts, audit data usage patterns, apply GuardPoints and perform other duties.

The three administrator types can be combined into the following DSM hybrid administrators:

- **DSM Domain and Security Administrator**: This administrator can perform the tasks of DSM Domain and DSM Security Administrator.

- **DSM Administrator of type All**: This administrator can perform the tasks of all three of the DSM administrative types.

The VTE on AWS products have a domain called `awsdomain` and a DSM administrator of type `All` called `awsadmin`. The non-cloud VTE version only has a single Vormetric System Administrator called `admin` and no domain.

---

**Creating a DSM administrator**

This section describes how to create a DSM Domain and Security Administrator. You already have an DSM Administrator of type `All` called `awsadmin` that has permissions to set policies for all hosts and domains. However, it can be useful to create additional administrators to separate
security duties among them such that no one administrator has access to all VTE security.

1. **Retrieve the DSM and protected host detailed information.**

   When you first installed the DSM, the *Deployment details* were displayed for you to save to you could access them later. The public DNS name of the protected host(s) and the key pair used to instantiate the protected hosts were saved during installation. This information was also emailed to you. See “Deployment Details information” on page 53.”

2. **Open the Management Console.**

   a. Open a browser and go to the DSM URL (see *Deployment details*).

   ![Vormetric Data Security Management Console Login](image)

   b. Login as DSM System Administrator *admin* with the password from *Deployment details*.

   The VDS Summary Screen appears.

   ![Vormetric Data Security](image)

3. **List the administrators for this DSM.**

   a. Click *Administrators*.
This brings up the Administrators page.

VDS automatically creates `admin` by default, which cannot be deleted. The DSM installation process may also create an administrator of type `All` called `awsadmin`.

4. Create a new administrator of type Domain and Security Administrator.
   a. Click **Add**.

The **Add Administrator** pop-up appears.
b. Enter the following into the corresponding fields:

Login: SecurityAdmin-1
Description: Security Administrator
Password: Temp123!
Confirm Password: Temp123!
User Type: Domain and Security Administrator

NOTE: The first time you log in to the Management Console in a new DSM Administrator account, you will be prompted to change its password and you will not be allowed to use the same password that you entered here. If you have a specific password you want to use, do not enter it here as you will have to change it after your first login.

c. Click Ok.

The new Vormetric Administrator is created.
VTE Policies

The DSM administrator’s primary responsibility is to create policies that allow or deny access to specified users in specified directories called GuardPoints. A policy is a set of rules that must be satisfied before a user can access data in a GuardPoint.

Each time a user attempts to access data in a GuardPoint, the security rules ask:

- **What data is being accessed?** Are these files or folders protected?
- **Who is attempting to access protected data?** Is this user permitted to access this files and directory?
- **Which applications are authorized?** Is the executable used to access the data permitted on these files and directories?
- **When is the data being accessed?** What hours and days of the week can these files and directories be accessed?
- **How is the data being accessed?** What processes (read, write, delete, rename, and so on) are permitted on these files and directories?

When all the access rules in a policy match, VTE enables the policy’s effect. The effect specifies three things:

- Whether to permit or deny access
- Whether or not the data should be encrypted or decrypted for the specified user
- Whether or not to audit access attempts

A policy’s rules and effects allow you to specify that some users can have read/copy access, but not decrypting privileges. This allows system administrators to see the file's meta-data such as filename, size, and so on, and thus perform tasks such as backups and moves, while the data in the files remain in an encrypted state.
Creating and viewing the data to be protected

This section describes how to do the following:

- Create a new user called demo-user2 on your protected host.
- Create a directory called /vipdata2 and a text file called /vipdata2/helloworld.txt that can be viewed by all users including demo-user2.
- Create a policy allowing demo-user2 to view data in vipdata2, but block all others including root.

**NOTE:** Use the same protected host for all of the labs in this guide.

Creating and viewing the data to be protected

In this section you will create a simple text file on a protected host to demonstrate VTE data protection.

1. Connect to your protected host with an SSH client and log in as user root.

**NOTE:** Throughout this document you will be asked to log in as root. If you can’t log in as root, log in as ec2-user, then use the command `sudo su -` to switch to root. At other
times you may be asked to log on as ec2-user. If you don’t have permissions, just log in as root and complete the lab. Allowing and blocking access to user root is the main objective.

See “Connecting to Your Host with an SSH Terminal” on page 53 for details.

2. On the protected host, create a new user account called demo-user2 with a password.

You must be root to execute these commands.

```
[ec2-user@ec2-54-235-164-220 ~]# sudo su -
-bash-4.1# useradd demo-user2
-bash-4.1# passwd demo-user2
```

Changing password for user demo-user2.

New password:

Retype new password:

```
passwd: all authentication tokens updated successfully.
```

3. Create a directory called /vipdata2 and a simple text file called helloworld.txt.

a. __ Execute the following commands from the protected host command line as root:

```
-bash-4.1# mkdir /vipdata2
-bash-4.1# chmod 777 /vipdata2
-bash-4.1# cat > /vipdata2/helloworld.txt
This is a demo. Hello beautiful world!
(Press CTRL-D twice to save file)
-bash-4.1# chmod 777 /vipdata2/helloworld.txt
```

4. View the data as root and demo-user2.

a. __ Execute the following commands from the protected host command line as root:

```
-bash-4.1# ll /vipdata2
 total 4
-rwxrwxrwx. 1 root root 66 Jul 19 22:34 helloworld.txt
```

b. Create an SSH connection to your protected host as demo-user2 with PuTTY. Use the password you specified when you created demo-user2.

```
[demo-user2@ec2-54-235-164-220 ~]$ pwd
/home/demo-user2
[demo-user2@ec2-54-235-164-220 ~]$ more /vipdata2/helloworld.txt
This is a test. Hello beautiful world!
```

Both root and demo-user2 can view this file. This may be a security problem. Suppose you want root to have administrative privileges, but you don't want root to be able to view data in helloworld.txt. This problem is addressed in the next section.
Creating a policy to control access to files

A common use case for VTE is to remove the system administrator's (root) ability to see sensitive data within the system. In this section you will create a VTE policy on the /vipdata2 directory that allows demo-user2 full access to the data files while blocking root from all access.

A GuardPoint is a directory (and sub-directories) on which a policy is applied. A policy is a set of rules specified by a DSM Administrator that govern every I/O procedure performed in a GuardPoint’s directories.

1. Open the Management Console to your DSM using the information provided with your Deployment Details (see “Deployment Details information” on page 53).
   a. Open a browser and enter the DSM URL.
   b. Log in as awsadmin with the password from your DSM Details.
      The VDS Summary Screen appears:

2. Switch to a domain.
   To do any security work, you must be in a domain.
   a. Click Domains > Switch Domains
On a new system, you will have a domain called `awsdomain` that contains the protected hosts installed in your Vormetric-AWS system.

b. **Select the `awsdomain` radio button and then click Switch to domain.**

A domain is a host or group of host(s) on which a single administrator can set access policies. Before you switched to a domain, you had seven tab choices in the Management Console:

![Management Console with seven tab choices](image)

After switching to a domain, you have more tab choices:

![Management Console with additional tab choices](image)

The domain in which you are working is displayed in the upper right corner of the Management Console.

3. **View the hosts in this domain.**
a. Click **Hosts > Hosts**. The **Hosts** screen appears.

![Hosts screen](image)

4. Create a policy in your domain.

Creating access policies is the main work of security administrators.

a. Click **Policies > Manage Policies** to list the policies available to this domain.

![Policies screen](image)

In this example, there are no policies.

b. Click **Add Online Policy**.

The **Online Policy Computer** pop-up should appear:
The **Online Policy Composer**, a Java applet, starts automatically (above). If it doesn’t start, make sure that Java is installed on your system, enabled on your browser, and up-to-date. If the pop-up still doesn’t appear, you might have to bring up the **Java Control Panel** on your system, select the Security tab and lower the Security Level to **Medium**.

**Policies** control access to the file system. They consist of one or more file access **rules**. Each rule defines five file system I/O attributes:
Resource specifies the files and directories to which to apply this security rule.
User specifies users and user groups accessing the data.
Process specifies the executables that can operate on the data.
When specifies the time range in which the operation occurs.
Action specifies the type of user I/O access being made (for example, read, write, delete, or rename).
Effect specifies what happens when all the rules match.

Every time a user or application attempts a file access in a GuardPoint, that access attempt goes through each rule of the policy. If the file access attempt meets all the attributes in a rule, then the VTE enacts the Effect specified in that rule.

Attributes left blank specify a value of all. If User is blank, the rule applies to all users; if When is blank, the rule applies to all times; if Process is blank, the rules applies to all executables, and so on. Effect can never be blank. It must have at least a permit (allow access) or deny (deny access).

In this example, you will define a policy allowing demo-user2 to view files in /vipdata2, and block all other users including root. This policy requires the following three rules (some of this terminology will be new to you, but it will be described shortly after).

Rule 1 will specify that users in a User Group called User-access have full access with any process at any time. You will add demo-user2 to User-access.

Rule 2 will specify that users in the User Group Limit-access will have no access permissions with any executable at any time. You will add root and ec2-user to Limit-access.

Rule 3 will specify that all other users have no access permissions at all.

This policy allows complete access for users that are part of the user set User-access, and to denies access to all other users including root, who usually has access to everything.

Now, create Rule 1 as follows:

c. Click User.
The User Set List pop-up appears.

A User Set is a set of users to which this rule will apply. In this example you will add demo-user2 because you want that user to have access to files in the GuardPoint. Later you might want to add other users to this group so they too have access to files in the GuardPoint.

Click Add User Set.

The Add New User Set pop-up appears.

Type the name of the new user set, for example, User-access and click Add User.

The User Object pop-up appears.
__Type demo-user2 in the Uname field, click Add & Close. __
The Add New User Set pop-up returns.

__Click OK.__
The *User Set List* returns.

__Click Select__. The User attribute is set and you are returned to the *Policy Composer*.

__Click Effect.__
Add permit to Effects selected and click OK. This grants users in User-access full access to the GuardPoint. You are returned to the Policy Composer.

Click Add in the Policy Composer.

The new rule is displayed.

Rule 1 specifies that users in the group User-access have full access with any process at any time. Currently only demo-user2 is in User-access.

d. Create Rule 2.

Rule 2 specifies that users in the User Group Limit-access will have no access permissions with any executable at any time. You will add root to Limit-access.

Click Reset to clear the rule editor.

Now specify the users (root) for this rule:

Click User.

Click Add User Set.

Type in the name of the new user set, for example, Limit-access, then click Add User.

Type root in the Uname field and click Add & New.

Type ec2-user in the Uname field and click Add & Close. root and ec2-user will have limited file access.

Click OK in Add New User Set pop-up.

Make sure Limit-access is highlighted in the User Set List pop-up and click Select.
Leave blank **Resources**, **Process**, **When**, and **Action** because you want this rule to apply to all the resources (files) in a GuardPoint, to block all processes (executables), block all actions (read, write, rename, etc.), and apply at all times (when).

For **Effect**, you want to deny access to **root** and **ec2-user** access to files in the GuardPoint.

- Click **Effect**.
- Add **deny**.
- Click **OK**.
- Click **Add** to add Rule 2.

Rule 2 is added:

<table>
<thead>
<tr>
<th>No.</th>
<th>Resource</th>
<th>User</th>
<th>Process</th>
<th>Action</th>
<th>Effect</th>
<th>When</th>
<th>Allow Browsing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User-access</td>
<td>permit</td>
<td>off</td>
<td>deny</td>
<td>on</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Limit-access</td>
<td>deny</td>
<td>off</td>
<td>deny</td>
<td>on</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**e. Create Rule 3.**

**Rule 3** is a catch-all rule that applies to any user not applicable to the previous rules. It specifies that all other users have no access permissions with any executable. To create a catch-all rule, leave all the attributes blank and fill in an effect. For Rule 3, leave all attributes blank and add **Deny** to **Effect**:

- Click **Reset** to clear the rule editor.
- Click **Effect**.
- Add **deny**.
- Click **OK**.
- Click **Add** to add Rule 3.

**NOTE:** The order of the rules is important. Each time a user tries to access a GuardPoint, VTE runs the user information through the first rule. If all the attributes apply, then **Effect** is applied. If an attribute does not apply, then VTE goes to the next rule. This continues until a rule matches. Although the order of the rules is important, the order in which you create them is not, because you can change the order at the end by highlighting a rule and pressing the **Up** or **Down** buttons. The current rule order of the policy is appropriate.

**f. Save the policy.**
Click **Policy > Save** in the upper left corner.

The Save Policy pop-up appears.

Enter the **Policy** name.

Enter a **Description** if you want.

Click **OK**.

The policy, *basic-access-policy*, is saved.
Applying a policy to a GuardPoint

To limit data access, policies need to be applied to GuardPoints. A GuardPoint is a directory on which a policy is applied. In the previous section you created a policy called basic-access-policy in awsdomain. This policy can be applied to any directory in any host in awsdomain. In this section, you will apply this policy to /vipdata2 on the host in your domain.

1. **View the File System GuardPoints screen.**
   a. __Click Hosts > Hosts.
     
     ![Hosts screen](image)

     b. __Click on the protected host name in blue where you created the directory /vipdata2. The Edit Host screen appears.

     ![Edit Host screen](image)
c. Click the Guard FS tab.

There are no policies applied on this protected host:

2. Apply a policy to a GuardPoint.

   Apply the basic-access-policy to a GuardPoint at /vipdata2 on the protected host.
   a. From the Guard FS tab, click Guard.

   b. The Guard File System panel appears:
c. Set the attributes of the GuardPoint.
   - For **Policy**, choose **basic-access-policy**.
   - For **Type**, keep it as **Directory (Auto Guard)**.
   - For **Path**, enter `/vipdata2`. You can also click **Browse**, click the + box next to `/` to view the directories below it, and highlight the `/vipdata2` directory. This step specifies the directory to be protected by the policy.

   ![Remote File Browser](image)

   - Click **Ok**.
Click **Ok** to apply the policy to the GuardPoint on the host. The **Edit Host** panel appears. It may take a few seconds before the policy takes effect. A red status indicator means that the policy hasn’t taken effect.

Click **Refresh** until the **Status** turns **green**. When the Status is green the policy is activated and the GuardPoint is protected.

3. Test Guardpoint access to each of the users (**root**, **ec2-user**, and **demo-user2**).
   
   You must kill the existing SSH sessions and start new ones. If you can log in to **root** directly, don’t bother with logging in as **ec2-user**.
   
   a. **Log in directly as root** (if you can’t go to b:) and view the files at **/vipdata2**:

   ```bash
   -bash-4.1-# ls -l /vipdata2
   ls: cannot access /vipdata2: Permission denied
   -bash-4.1-# more /vipdata2/helloworld.txt
   /vipdata2/helloworld.txt: Permission denied
   ```

   b. **Log in as ec2-user, switch to root, and view the files at **/vipdata2**:

   ```bash
   [ec2-user@ec2-50-17-243-51 ~]# sudo su -
   -bash-4.1-# ls -l /vipdata2
   ```
Editing a policy to allow limited access

You can change the policies to limit data access in the GuardPoint by:

- Who can access the file.
- What file can be accessed (specific files, sub-directories, or wild card expressions, for example: *.pdf would be all Acrobat files).
- What application can open the files.
- What type of action can be performed (example: reads, writes, create file, and so on).
- When access can be attempted.

In this part of the demo, you will allow root and ec2-user to access the file helloworld.txt using only the Linux more command. root and ec2-user will not be able to access the file in any other way.

1. Log in to the Management Console.
   a. Log in as awsadmin and switch to the domain awsdomain as described in the previous section.

2. View the basic-access-policy.
   a. Click Hosts to list the protected hosts connected to the DSM.
b. Click on the host name containing /vipdata2 to bring up the Edit Host screen, then click the Guard FS tab.

c. Click the basic-access-policy policy.

The Online Policy Composer appears.
3. Change Rule 2 so that users in *Limit-access* can access `/vipdata2/helloworld.txt` with the Linux `more` command.
   a. __Double-click Rule 2 to edit root access control.__

<table>
<thead>
<tr>
<th>No.</th>
<th>Resource</th>
<th>User</th>
<th>Process</th>
<th>Action</th>
<th>Effect</th>
<th>When</th>
<th>Allow Browsing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User-access</td>
<td>permit</td>
<td>on</td>
<td>on</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Limit-access</td>
<td>deny</td>
<td>on</td>
<td>on</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>deny</td>
<td>on</td>
<td>on</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   b. __Add `more` to the Process Set.__

   __Click Process to define what executables can be used.__

   The Process Set List appears.
Click **Add Process Set.** The **Add New Process** set appears.

Type **linux_allow** or another name for the **Process Set**, then click **Add Process.**

The **Process Object** panel appears.
Enter more in the Baseline field, and click Add & Close.

The Add New Process Set panel appears with the new information.

Click OK. The Process Set List panel appears.
Highlight *linux_allow* and click **Select**.

A Process Set has been created with the single executable, *more*.

c. **Change Effect.**

__Click Effect in the Policy panel.** The Select Effects pop-up appears.

Double-click **deny** to remove the deny effect, then double-click **permit** and click **OK**.
Highlight Rule 2 and click Replace to replace the old Rule 2 with the new Rule 2.

d. Save the policy.

Select Policy > Save

The application of a new policy may take a few seconds to be effective.

e. Exit the policy editor.

4. Run cat and more commands on your ssh terminal as root or ec2-user.

Close and reopen your SSH connection to ec2-user.

Execute the following commands:

```
[ec2-user@ec2-50-17-243-51 ~]# cat /vipdata2/helloworld.txt
/vipdata/helloworld.txt: Permission denied
[root@ec2-50-17-243-51 ~]# more /vipdata2/helloworld.txt
This is a demo. Hello beautiful world!
```

```
[ec2-user@ec2-50-17-243-51 ~]# sudo su -
```
-bash-4.1# cat /vipdata/helloworld.txt
/vipdata/helloworld.txt: Permission denied
-bash-4.1# more /vipdata2/helloworld.txt
This is a demo. Hello beautiful world!
more is allowed. cat is not allowed.
Auditing Data Access

VTE allows you to audit every file access attempt in a GuardPoint. If this level of detail is unnecessary, you can specify audit activity by message type (policy evaluation, system administration, security administration), severity level (DEBUG, INFO, WARNING, ERROR, FATAL) and a number of other criteria. You can also filter by search words and source (DSM, Agent or both).

This demo shows how to generate audit records by modifying policies and how to view audit records.

Modifying the current policy to audit file access

In this demo, you implement auditing by adding the keyword, audit, to the policy rules in the Effect field of the Policy Composer. Each time a file access is attempted, and audit record is created.

1. **Login to the Management Console and view basic-access-policy.**

   After logging into the Management Console:
   - Click Domains > Switch Domains. Select the radio button for awsdomain and click Switch to Domain.
   - Click Hosts > Hosts. Click the blue host name.
   - Click Guard FS, then click basic-access-policy to bring up Policy Composer.
   - Examine the rules for basic-access-policy.

   To audit data access for each of these rules, add the keyword audit to the Effect field for each rule.

2. **Add the keyword audit to the Effect field for each of the basic-access-policy rules.**

   - Double-click Rule 1.
   - Click Effect in the Security Rules Panel.
   - Add audit to Effects selected, click OK, then click Replace.
Double-click Rules 2 and 3, and repeat the same procedures.
In the upper left corner, click Policy > Save. Enter a Policy Description if you want and click OK.

<table>
<thead>
<tr>
<th>No.</th>
<th>Resource</th>
<th>User</th>
<th>Process</th>
<th>Action</th>
<th>Effect</th>
<th>When</th>
<th>Allow Browsing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>User</td>
<td>access</td>
<td>permit</td>
<td>audit</td>
<td>on</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>User</td>
<td>access</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>User</td>
<td>access</td>
<td>permit</td>
<td>audit</td>
<td>on</td>
<td></td>
</tr>
</tbody>
</table>

3. Execute the cat command.
   ```bash
   # cat /vipdata2/helloworld.txt
   /vipdata2/helloworld.txt: Permission denied
   ```
   In the next section you’ll examine the audit logs.

### Viewing the audit logs

Once the `audit` keyword is added to the rules of a policy, VTE audits data access in the GuardPoint. This section explains how to read the audit records.

1. **Bring up the Logs page in the Management Console.**
   __Click Log > Logs

Management Console displays the audit logs.
Audit records contain the following fields:

- **ID**: Audit record number.
- **Time**: When the audit record was generated.
- **Severity**: The severity level of the audit record.
- **Source**: Where the audit was generated.
- **Message**: The body of the audit record.

Example audit message:

```
CGP2604E: [SecFS, 0] [ALARM] Policy[basic-access-policy]
User[root, uid=0, gid=0] Process[/bin/cat] Action[read_attr]
```

2. Filter specific messages.
   - Add a search word to the **Message Contains**: field.

For example, to show only messages with the word "DENIED," type **DENIED**. Only messages with the word DENIED appear.

3. Change the severity level of log records retrieved.
40

The audit logs displayed in the previous step only showed the DENIED file accesses. VTE did not display the PERMITTED accesses because the severity level was set too low. In this step, you raise the level so that you can see accesses that are permitted.

__Click Hosts > Hosts, then click the blue host name.__

__Click the FS Agent Log tab to display File System Agent log settings. The current Severity level for Policy Evaluation is set to ERROR.__

__Click the Severity Level pull-down for Policy Evaluation and select DEBUG.__

__Click Apply and OK.__

4. Test the new severity level.

__Start a command line shell on the protected host and look at the /vipdata2 files as root or ec2-user.__

```
[ec2-user@ec2-107-21-118-84 ~]$ cat /vipdata2/helloworld.txt
bash: /vipdata2/helloworld.txt: Permission denied
[ec2-user@ec2-107-21-118-84 ~]$ more /vipdata2/helloworld.txt
This is a demo. Hello beautiful world!
```

__In the DSM Management console bring up the logs by clicking Log > Logs. In the Logs page, click Go to refresh the log records. Examine the records. Note the cat and more commands that you ran as ec2-user.__
### Auditing Data Access

**Viewing the audit logs**

![Image of Vormetric Transparent Encryption for AWS Getting Started Guide v3](image-url)

<table>
<thead>
<tr>
<th>ID</th>
<th>Time</th>
<th>Severity</th>
<th>Source</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>233</td>
<td>2013-07-25</td>
<td></td>
<td>ec2-54-225-16b</td>
<td>CGP200ME: [SecDS, 0] [ALARM] Policy[basic-access-policy]</td>
</tr>
<tr>
<td>234</td>
<td>2013-07-25</td>
<td></td>
<td>ec2-54-225-16b</td>
<td>CGP20011: [SecDS, 0] [AUDIT] Policy[basic-access-policy]</td>
</tr>
<tr>
<td></td>
<td>2013-07-25</td>
<td></td>
<td>1.amazonaws.com/Reg/updata/helloworld.txt</td>
<td>Effect[DENIED Code (1U</td>
</tr>
</tbody>
</table>

**Go**
Encrypting Data

VTE can automatically encrypt your data so that if unauthorized users gain access to protected files, they can't read or access it. You can specify that some administrator users have read/write access to the file, but that the data itself remain encrypted and unreadable to those users. This allows administrators to manage files, but prevents them from viewing or using the content.

VTE encryption does the following:

- Encrypts data files using industry standard strong encryption routines.
- Manages, applies, and protects the encryption keys.
- Allows authorized users to access files transparently.

VTE encryption does not:

- Change the size of the files being encrypted.
- Change the names, owners, location, or any other non-file contents information.
- Change the file system operations that can be performed on the file.

VTE provides two ways to encrypt data:

1. Add an encryption rule to a GuardPoint policy, then copy files into that GuardPoint. File copied into the GuardPoint will be encrypted. Note that files already in the GuardPoint when the policy is changed are not encrypted. To encrypt files in a GuardPoint with this method, you must first move the files out of the GuardPoint, add the encryption rule, then move the files back into the GuardPoint.

2. Using a Vormetric utility called dataxform which encrypts files in a directory without having to move them in and out of the directory as is required in the first method.

This demo describes GuardPoint encryption. See the Vormetric Transparent Encryption (VTE) Data Transformation Guide for instructions on how to use dataxform.

Encrypting data within a GuardPoint

In this demo, you will do the following:

- Create a data encryption key.
- Move the data file /vipdata2/helloworld.txt to /demo-user2.
Encrypting Data within a GuardPoint

• Add an encryption rule to the GuardPoint policy.
• Move the data file back to /vipdata2.
• View the results of the encryption as various users.

1. Create a data encryption key.

To encrypt data you need an encryption key. You can use an existing key or you can create a new one. For this demo, you will create a new one.

a. Bring up the Agent Keys panel.
   __ Login to the Management Console as awsadmin.
   __ Switch to awsdomain: Domains > Switch Domains > select awsdomain > click Switch to Domain
   __ Bring up the Agent Keys page: Keys > Agent Keys > Keys

b. Click Add to bring up the Add Agent Key view.

   ![Add Agent Key View](image)

   ![Add Agent Key View](image)
__Enter the following values into the corresponding fields, and leave other fields as is:

Name: Demo-AES256
Description: AES 256 Key
Algorithm: AES256

__Click OK.

Your new key is created.

2. Move the file /vipdata2/helloworld.txt to the directory, /home/demo-user2.
   a. __Connect to your protected host with a standalone SSH Client and login as demo-user2.
   b. __Move the file:
      [demo-user2@ec2-50-17-243-22 ~]$ mv /vipdata2/helloworld.txt .
      [demo-user2@ec2-50-17-243-22 ~]$ ls
         helloworld.txt

3. Add an encryption key to the policy.
   a. Bring up the Policy pop-up
      __Log in to the Management Console as awsadmin.
      __Click Domains > Switch to Domains and switch to awsdomain
      __Click the Hosts > Hosts tab, then click on your protected host name.
      __Click the Guard FS tab.
      __Click the basic-access-policy policy.
   b. Add apply_key to the Effect of Rule 1.
      __Double-click Rule 1 to edit the policy rule for User-access.
Encrypting data within a GuardPoint

<table>
<thead>
<tr>
<th>No.</th>
<th>Resource</th>
<th>User</th>
<th>Process</th>
<th>Action</th>
<th>Effect</th>
<th>When</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User-access</td>
<td>User-access</td>
<td>permit</td>
<td>audit</td>
<td>permit</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Linux_allow</td>
<td></td>
<td></td>
<td>audit</td>
<td></td>
</tr>
</tbody>
</table>

**Click Effect.**

The **Select Effects** pop-up appears:

- **Add** `apply_key` to the **Effects selected** pane and click **OK**.

`apply_key` instructs the system to encrypt data that moves into the GuardPoint. Any data copied into a GuardPoint by anyone is encrypted. Any data accessed from the GuardPoint by a user in **User-access** will be unencrypted and readable. Users who are not in User-access can only get the data in an encrypted state.

- **Click Replace** to update Rule 1.
Encrypting data within a GuardPoint

The **Check Key Rule Requirement** pop-up appears.

![Check Key Rule Requirement](image)

This step allows you to specify a key to encrypt the data in a GuardPoint.

- Click **Yes** to create a key rule. You might be asked to commit your changes to security rule #1.

![Commit Changes](image)

- Click **Yes**.

The **Check Key Rule Requirement** pop-up may reappear. If so, click **Yes**.

The **Key Selection Rules** tab opens.

![Key Selection Rules](image)

- Click on the **Key** pulldown menu and select **Demo-AES256**.
Encrypting Data

Encrypting data within a GuardPoint

4. Encrypt the `helloworld.txt` by copying it into the GuardPoint.

`demo-user2` now has the `apply_key` effect in the GuardPoint. Any file copied into the GuardPoint will be encrypted to unauthorized users.

a. Log in to protected host as `demo-user2`, then copy `helloworld2.txt` from `/home/demo-user2` back to `/vipdata2`:

```
[demo-user@ec2-50-17-243-22 ~]$ mv helloworld.txt /vipdata2
[demo-user2@ec2-50-17-243-22 ~]$ ls /vipdata2
helloworld.txt
[demo-user2@ec2-50-17-243-22 ~]$ more /vipdata2/helloworld.txt
This is a demo. Hello beautiful world!
```

demo-user2 can only view the data in clear text.

b. Log in as `ec2-user` or `root` and try to view the file:

```
[ec2-user@ec2-50-17-243-51 ~]$ more /vipdata2/helloworld.txt
```

---

---

---
Encrypting data within a GuardPoint

ec2-user and root can only view the data in an encrypted state.
An encrypted file can be read by an authorized user, which in this example is demo-user2.
Unauthorized users will not be able to read the data in the file.

Give administrators read-write permission while protecting the data

It is useful to give your administrators read-write permissions so they can do file back-up and restores. However, you don’t necessarily want give them access to the file’s content. In this portion of the lab, we will give root and ec2-user read-write permissions, but keep the content encrypted.

1. Log in to the Management Console
   a. Open a browser and enter the DSM URL.
   b. Log in as awsadmin with the password from your DSM Details (see “Deployment Details information” on page 53).

2. Bring up the Policy pop-up
   __ Click Domains > Switch to Domains and switch to awsdomain
   __ Click the Hosts > Hosts tab
   __ Click on your protected host name.
   __ Click the Guard FS tab.
   __ Click the basic-access-policy policy.

3. Change the policy to allow root and ec2-user to copy and see the files in the GuardPoint, but not ever see the content of those files.
   __ Double-click Rule 2.
Encrypting Data

Encrypting data within a GuardPoint

__Delete linux_allow under Process. This removes the limitation of only using more command for users in the Limit-access User Set.

__Click the Action button and move read - read operations and write - write operations to the Action selected column. The allows any read and write operation to take place in the GuardPoint.

__Click OK.

__Click the Replace button on the Online Policy Composer.

__Save the Policy.

4. Test the policy.

a. __Connect to your protected host with a two SSH clients. Log in as demo-user2 in one client, and log in as root in the other. If you can’t log in as root, log in as ec2-user, then use the command sudo su - to switch to root.

See “Connecting to Your Host with an SSH Terminal” on page 53 for details.

b. As demo-user2, view and copy the file helloworld.txt to /tmp.

__Execute the following commands from the protected host command line:

[demo-user2@ec2-54-235-164-220 ~]$ more /vipdata2/helloworld.txt
This is a demo. Hello beautiful world!
[demo-user2@ec2-54-235-164-220 ~]$ cp /vipdata2/helloworld.txt /tmp/helloworld-DU2.txt
[demo-user2@ec2-54-235-164-220 ~]$ more /tmp/helloworld-DU2.txt
This is a demo. Hello beautiful world!

Note /tmp/helloworld-DU2.txt is now readable in clear text to anyone. For example:

-bash-4.1# more /tmp/helloworld-DU2.txt
This is a demo. Hello beautiful world!

c. __As user ec2-user or root, view and copy the file helloworld.txt to /tmp.
Encrypting Data

Encrypting data within a GuardPoint

login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Wed Jan 15 18:03:41 2014 from 12.104.149.40
[ec2-user@ec2-107-21-118-94 ~]$ sudo su -
-bash-4.1# more /vipdata2/helloworld.txt
?K.¿yÇdüRs¿È¿
-bash-4.1# cp /vipdata2/helloworld.txt /tmp/Helloworld-Root.txt
-bash-4.1# more !$
more /tmp/Helloworld-Root.txt
?K.¿yÇdüRs¿È¿
Root can copy the file, but cannot read it. Note that demo-user2 will not be able to read it either:
[demo-user2@ec2-54-235-164-220 ~]$ more /tmp/helloworld-Root.txt
?K.¿yÇdüRs¿È¿
For demo-user2 to read the file, it must be copied back into /vipdata2.
Encrypting Data

Encrypting data within a GuardPoint
Connecting to Your Host with an SSH Terminal

These demos require you to connect from your work machine to your protected AWS host via an SSH terminal program. There are many programs to choose from, but this document describes PuTTY for Windows and Linux machines, and Terminal for Mac OS X.

This appendix contains the following sections:

- “Deployment Details information” on page 53
- “Connecting to your protected host from Windows or Linux/UNIX using PuTTY” on page 54
- “Connecting to your protected host from Mac OS X” on page 57

Deployment Details information

You will need the following information to connect to your hosts with an SSH terminal:

- The downloaded the key and key path (location of the .ppk or .pem file) to access your protected host instances. For the Vormetric Transparent Encryption for AWS from the Amazon Marketplace product, this is the key pair you specified when you instantiated the protected hosts in AWS. For the 30-day Free Trial product, the .pem file was mailed to you in a .zip file along with the Deployment Details.

- The VTE on AWS Deployment Details for your installation. Depending on the product you are using, Deployment Details are accessed as follows:
  - If you installed the paid version of Vormetric Transparent Encryption for AWS from the Amazon Marketplace, then the Deployment Details are obtained by connecting to the DSM instance with an SSH session and logging in as ec2-user. Here’s an example:

  **Data Security Manager details**
  
  Management console URL is https://ec2-54-229-241-119.compute-1.amazonaws.com
  Management console internal URL is https://ip-10-1-0-202.ec2.internal
  System administrator credentials are admin / Yj3^KCFRhfb$ 
  ALL administrator credentials are awsadmin / Rx2%MSEK*bci@F
  CLI administrator credentials are cliadmin / FF8^95zaHk#B
Please download the agent install script from https://awsportal.vormetric.com/downloads/agent/5.1.1/install?lic_id=4PLEAQ6Y2CMQ9UY

- If you registered for the Vormetric Transparent Encryption for AWS 30-day Free Trial, your the Deployment Details and key file were emailed to you from Vormetric:

Vormetric Data Security Manager Instance
Access DSM via https:// ec2-54-221-227-112.compute-1.amazonaws.com
System administrator credentials are admin / Zh5@ewWxtG5q#
ALL administrator credentials are awsadmin / Qy9^yW9Yk]
CLI administrator credentials are cliadmin / Tn6[PCu)st$gl
SSH username: ec2-user / KEY_greg@claritysoftware.com_1383593105 key pair

Vormetric Files System Agent Instances:
- Protected host name/public DNS: Host-1/ec2-54-225-108-47.compute-1.amazonaws.com
- Protected host name/public DNS: Host-2/ec2-54-225-108-48.compute-1.amazonaws.com

Please use the username "ec2-user" and "KEY_greg@clarityworkssoftware.com_1383593105" key pair to connect to the Vormetric File System Agent instances.

Allocated Elastic IPs.
Following Elastic IPs have been allocated.
- 54.225.108.47
- 54.225.108.48
- 54.225.108.49

Please do not release or reuse them until all the Vormetric Free trial instances have been terminated.

IAM user:
VODUser_greg@clarityworkssoftware.com1383593108 has been created.
Please do not delete this user until all the Vormetric Free Trial instances have been terminated.

---

Connecting to your protected host from Windows or Linux/UNIX using PuTTY

Below are simple PuTTY login instructions. For more detailed information, see the AWS's Connecting to Linux/UNIX Instances from Windows Using PuTTY.

1. Download and install PuTTY on your Windows or Linux work machine.
   Go to [http://www.putty.org](http://www.putty.org) and download the version of PuTTY for your work machine.
2. If necessary, convert your .pem key file to a .ppk file using PuTTYgen.
CONNECTING TO YOUR HOST WITH AN SSH TERMINAL

Connecting to your protected host from Windows or Linux/UNIX using PuTTY

See Connecting to Linux/UNIX Instances from Windows Using PuTTY.

Figure 5: PuTTYgen

3. Bring up the PuTTY client on your work desktop.

Figure 6: PuTTY Configuration window

4. Make an SSH connection to your protected host or DSM.

Complete the following fields in the PuTTY client:

a. Enter the host name (from your Deployment Details) in the Host Name (or IP address) field, and under Connection type, select SSH. See “PuTTY Configuration window” on page 55.
b. Under Category, click the + icon next to SSH, select Auth, then enter the path to your .ppk file in the Private key file for authentication: field.

Figure 7: Entering Key file in PuTTY

c. Click Open.

An SSH terminal appears.

Figure 8: SSH terminal

NOTE: Depending on your AMI, you will log on to your protected hosts as ec2-user or root. Because you entered a .ppk file, no password will be required. If you are asked for a password, kill the terminal and reconnect as ec2-user or root (whichever user you didn’t log in as the first time).
5. You can open simultaneous SSH PuTTY sessions to your protected host by right-clicking on the PuTTY icon and selecting the recently created session.

![PuTTY, Recent Sessions pane](image)

**Connecting to your protected host from Mac OS X**

Mac OS X has a built-in terminal emulation program called *Terminal*.

1. **Start Terminal.**
   
   Click to the Mac *Applications* folder > *Utilities* folder > *Terminal*.

2. **Access the protected host.**
   
   At the *Terminal* command prompt, enter the following:
   
   ```
   # ssh <username>@<hostname>
   ```
   
   When prompted, enter the password. *Username, hostname* and *password* was sent to you in the Deployment Details email.

![Mac OS X SSH terminal](image)

**Figure 10:** Mac OS X SSH terminal

If you want to log in using a .pem file (a .ppk file won’t work), open a terminal window and enter the following:
ssh -i privatekeyname.pem user@my.server.com

The private key must have tight security settings otherwise SSH complains. Make sure only the user can read the key.

chmod go-rw privatekey.pem

To quit the session, type exit.

*Terminal* settings/preferences are at the top left of your screen, next to the Apple logo. Click on *Terminal > Preferences* to select various themes and settings.
GLOSSARY

access control
The ability of VDS to control access to data on protected hosts. Access can be limited by user, process (executable), action (for example read, write, rename, and so on), and time period.

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

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

administrator
See DSM administrator.

agent
A Vormetric software program that is loaded onto the host machine containing data to be protected. Vormetric agents implement the security policies that are defined and stored in the DSM. Vormetric Agents include the File Systems Agent, and Key Agents for Oracle Database TDE and Microsoft SQL Server.

Agent keys
Encryption keys used by the Vormetric agents. There are two categories of Agent Keys, Encryption Expert Agent keys and Key Agent keys. Encryption Expert Agent keys consist of keys for the File System Agent. Key Agent keys consist of keys for the Oracle Database TDE agent and Microsoft SQL TDE agent.

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

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

appliance
The DSM server. Often referred to as a DSM hardware appliance, which is a hardened DSM server provided by Vormetric, or as a DSM virtual appliance, which is the software version of the DSM to be deployed by the customers as a virtual machine.

(Vormetric) application encryption (VAE)
A library based on PKCS#11 that provides APIs for key management and cryptographic operations. Allows encryption of specific database fields and files. See VDS Application Encryption User Guide.

asymmetric key cryptography
See public key cryptographic algorithm.

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

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

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

Backup Agents
See Database Backup Agents.

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

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

challenge-response
The cryptographic algorithm used to gain access to the Management Console when the protected host is disconnected from the DSM. Host users must enter a new password each time a host password is required. When a host is configured with a dynamic password, host users can run a utility that displays a seemingly random string (the challenge), which they then give to a DSM administrator. The DSM administrator returns a counter-string (the response) that the host user must enter to decrypt guarded data. The host user has 15 minutes to enter the counter-string.

CIFS/SMB
Common Internet File System (CIFS)/Server Message Block (SMB). The Server Message Block (SMB) Protocol is a network file sharing protocol implemented in Microsoft Windows. CIFS is a version of SMB. The Vormetric NAS Proxy virtual appliance supports SMB/CIFS protocol through the Samba software.

Character device
See *Raw device*

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

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

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

**cryptographic signature**
See *signing files*.

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

**Data Security Manager (DSM)**
Also called the *Security Server or appliance*. A Vormetric server that acts as the central repository and manager of encryption keys and security policies. Receives instructions and configuration from administrators through a GUI-based interface called the Management Console. Passes information to and from the Vormetric agents. Available as a complete hardened hardware system (*DSM Appliance*) or as software solution to be installed on a UNIX box (*software-only DSM*).

**dataxform**
A utility to encrypt data in a directory.

**DB2**
A relational model database server developed by IBM.

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

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

**domains**
See *administrative domains*.

**Domain Administrator**
The second-level DSM administrator created by a DSM System Administrator. This administrator creates and assigns DSM Security Administrators to domains and assigns them their roles.
Domain and Security Administrator
A hybrid DSM administrator who is has the privileges of a DSM Domain Administrator and Security Administrator.

DSM
See Data Security Manager.

DSM administrator
A specialized administrative user with access to the DSM Management Console. There are five types of DSM administrators: System, Domain, Security, Domain-Security, and All.

DSM Automation Utilities
Also called VMSSC. A set of command line utilities installed with the File System Agent on protected hosts. These utilities can be used by advanced users to automate DSM processes that would normally be done with the Management Console. See the DSM Automation Reference for complete details.

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

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

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

EKM
See Encryption Key Management.

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

encryption agents
See Vormetric Transparent Encryption agent.

encryption key
A piece of information used in conjunction with a cryptographic algorithm that transforms plaintext into ciphertext, or vice versa during decryption. Can also be used to encrypt digital signatures or encryption keys themselves. An entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot. Any VDS policy that encrypts GuardPoint data requires an encryption key.
Encryption Key Management (EKM)
An API library specification provided by Microsoft that defines a software framework that allows hardware security module (HSM) providers like Vormetric to integrate their product with the Microsoft SQL Server.

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

file signing
See signing files.

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

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

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

GuardPoint
A GuardPoint is a location in the file system hierarchy, often a directory, where everything underneath has a Vormetric policy applied to it. It can be thought of as a UNIX mount point. The File System agent intercepts any attempt to access anything in the GuardPoint and uses policies obtained from the DSM to grant or deny the access attempt.

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

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

host system administrator
A host user with system administrator privileges.

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

**Key Agent**
A Vormetric agent required for the following features: Oracle Database TDE key management, Microsoft SQL Server TDE key management, KMIP, and Application Encryption (PKCS#11).

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

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

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

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

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

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

**KMIP**
Key Management Interoperability Protocol. A protocol for communication between enterprise key management systems and encryption systems. A KMIP-enabled device or client software can communicate with the DSM to manage encrypted keys.
Learn Mode
A DSM operational mode in which all actions that would have been denied are instead permitted. This permits a policy to be tested without actually denying access to resources. In the Learn Mode, all GuardPoint access attempts that would have been denied are instead permitted. These GuardPoint accesses are logged to assist in tuning and troubleshooting policies.

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

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

MEK
See Master encryption key.

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

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

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

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

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

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

policy
A set of security access and encryption rules that specify who can access which files with what executable during what times. Policies are created by DSM Security Administrators, stored in the DSM, and implemented on protected hosts by agents. See rule.

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

**protected host**
A host on which a Vormetric agent is installed to protect that host’s data.

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

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

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

**rekeying**
The process of changing the encryption keys use to encrypt data. Changing keys enhances data security and is a required to maintain compliance with some data security guidelines and regulations.

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

**RSA SecurID**
A hardware authentication token that is assigned to a computer user and that generates an authentication code at fixed intervals (usually 60 seconds). In addition to entering a static password, Management Console administrators can be required to input an 8-digit number that is provided by an external electronic device or software.
rule (for policies)
Every time a user or application tries to access a GuardPoint file, the access attempt passes through each rule of the policy until it finds a rule where all the criteria are met. When a rule matches, the effect associated with that rule is enforced. A rule consists of five access criteria and an effect. The criteria are Resource (the file/directories accessed), User (the user or groups attempting access), Process (the executable used to access the data), When (the time range when access is attempted) and Action (the type of action attempted on the data, for example read, write, rename and so on). Effect can be permit or deny access, decrypt data access, and audit access attempt. See policy.

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

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

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

Security Server
See DSM.

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

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

SMB/CIFS
Server Message Block (SMB)/Common Internet File System (CIFS). The Server Message Block (SMB) Protocol is a network file sharing protocol implemented in Microsoft Windows. CIFS is a version of SMB. The Vormetric NAS Proxy virtual appliance supports SMB/CIFS protocol through the Samba software.

Suite B mode
A set of publicly available cryptographic algorithms approved by the United States National Security Agency (NSA). These algorithms enhance security by adding up to 384-bit encryption to the communication between the Web browser and the DSM, the DSM and Agent, and between DSMs in HA environments.
Symmetric-key algorithm
Cryptographic algorithms that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption.

System Administrator
See VDS System Administrator.

System Administrator Reports
Reports available to DSM System Administrators. Such as Administrators, DSM Servers, Security Domains, and Executive Summary reports.

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

VAE
See Vormetric Application Encryption.

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

VMSSC
See DSM Automation Utilities.

Vormetric application encryption (VAE)
A library based on PKCS#11 that provides APIs for key management and cryptographic operations. It enables application-level encryption into existing corporate applications. For example, it allows encryption of specific database fields and files. Documented in the VDS Platform Application Encryption User Guide.

Vormetric Data Security Platform or VDS Platform
The overall name of the Vormetric data security product.

Vormetric Encryption Expert or VEE
Same as Vormetric Transparent Encryption (VTE). Vormetric Encryption Expert or VEE was the original name of the VTE agents. It is still used in the product GUI and installation scripts.

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

VMSSC or Vormetric Security Server Command Line Interface
See Vormetric DSM Automation Utility.

**Vormetric Transparent Encryption Agent or VTE**
Vormetric agents that are installed on protected hosts to implement data protection. VTE agents consists of the File Systems Agent.

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

**wrapper keys**
See key wrapping.

**WSDL**
Web Services Description Language.