

Privacy DAM Manager demo guide

Copyright: TOVADATA

1. Product Overview

1.1. Introduction: What is a Privacy DAM?

As the personal data controller's responsibility for the protection of personal data becomes more important, the need for a way for the data controller to view and control personal data processing activities is increasing.

Privacy DAM makes the accesses to the database, which is the storage of personal information, into APIs, manages the processing type, processing purpose, and authority for individual APIs, and provides the status and analysis report on the results of individual API calls. Via Privacy DAM, the DPO(Data Protection Officer), a person in charge of personal information protection, can understand and respond to information processing activities with ease.

- Control of accesses to personal information storage (DB) through APIs
- Inspect and control the purpose and role of data processing per personal data handlers
- Provides a dashboard for API call status and analyzed reports

This Privacy DAM Manager is a part of the Privacy DAM solution. The Privacy DAM solution consists of a Privacy DAM Manager and Privacy DAM API Processors. A Privacy DAM Manager controls the data accessing APIs including a creation of new data accessing APIs and an activation/deactivation of data accessing APIs. It also manages who can call APIs and on what purpose the API can be called. The Privacy DAM API Processors are the actual worker processes that perform the SQL process according to the defined via a Privacy DAM Manager. The Privacy DAM API Processors are not included in this AMI. If you are interested in it, please contact the TOVADATA sales representatives. (sales@tovadata.com)

1.2. Prerequisites and Requirements

■ Prerequisites

The Privacy DAM Manager AMI is completely self-contained. You don't need to install any additional software to run and evaluate the Privacy DAM Manager. Basic AWS skills related with creating and managing EC2 instances are sufficient to deploy Privacy DAM Manager on AWS. In addition, basic Linux CLI familiarity

are preferred during the initial deployment for running some CLI commands.

- **Requirement**

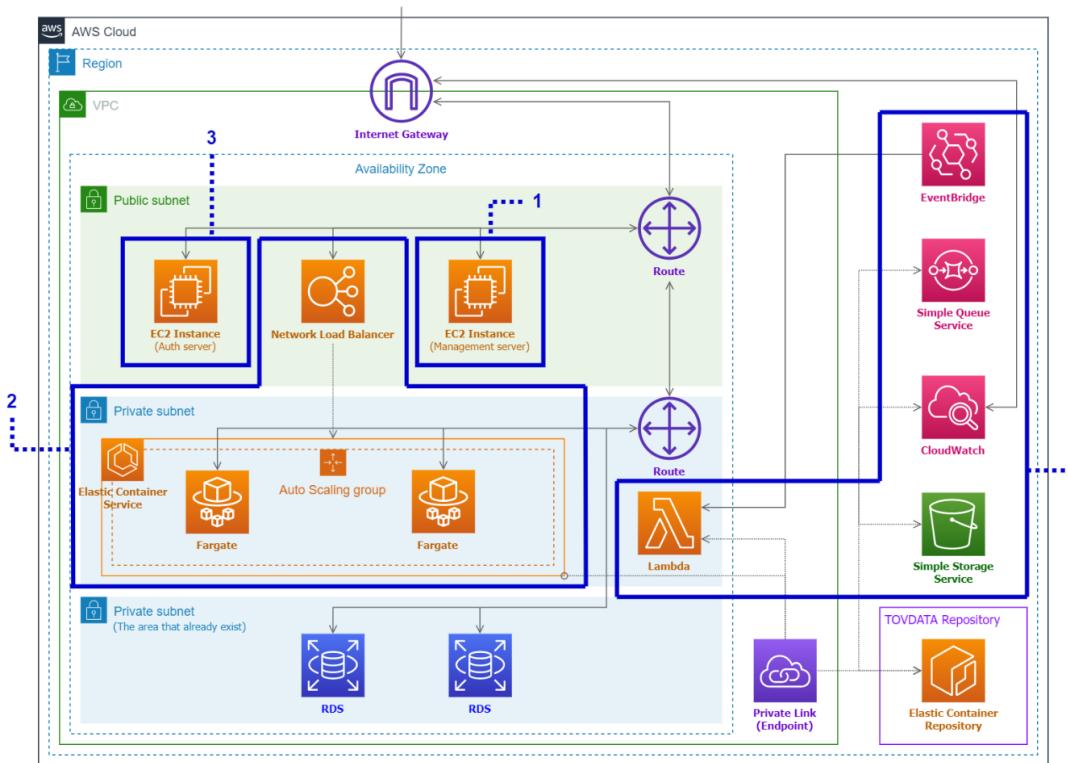
All you need are a publicly accessible subnet and a permission to launch an EC2 instance in that subnet.

- **Region support**

There is no technical restriction to deploy and run the Privacy DAM Manager AMI.

1.3. Architecture Diagrams

The overall solution architecture of the Privacy DAM is shown in the following figure. Though the Privacy DAM Processor modules are not included in this AMI but those are shown in the figure for your information.



1. Privacy DAM Manager

- Located in a public subnet.
- Manages the DB access API information and provides them to the Privacy DAM API Processor.
- Provides a monitoring dashboard for the Privacy DAM API Processor status and API call log reports

2. Privacy DAM API Processor (Worker module)

- Processes the actual DB access and additional data processing according to the registered API information.

3. Privacy DAM API Processor (Auth module)

- Checks whether the API caller has right permission and suitable purpose to call the API.

4. Privacy DAM API Processor (LogProcess module)

- Collecting the API call logs and user authentication logs, performs analysis to provide monitoring information for dashboard and archives log data and reports.

1.4. Security

Inbound traffic to port 22 must be allowed because it is required to access the instance using ssh. Also, inbound traffic to port 80 (HTTP) must be allowed to access the Privacy DAM Manager web pages.

In addition, inbound traffic for port 3306 and 27017 must be allowed for Privacy DAM API Processor to access internal database from processing module and authentication module, and inbound traffic for 9091 must be allowed to measure the performance of the processing module.

- Allow inbound traffic anywhere: 80
- Allow inbound traffic for server manager: 20
- Allow inbound traffic for private subnet: 3306, 9091
- Allow inbound traffic for internal network (VPC): 27017

1.5. Cost

We do not charge for downloading and testing this Privacy DAM Manager.

Only the cost of operating the AWS EC2 instance will be charged from AWS. The cost of operating an instance depends on the type of instance. For more information, visit the AWS site.

1.6. Size

■ Instance type

The minimum instance type for the Privacy DAM Manager is a general purpose EC2 instance type of t2.small or higher performance types. (More than 2 vCPUs and 4GiB memory are recommended for the initial deployment and operations.)

■ Storage

The minimum required EBS storage size for the Privacy DAM Manager is 8GB or larger.

2. Initial Deployment (an Amazon EC2 instance)

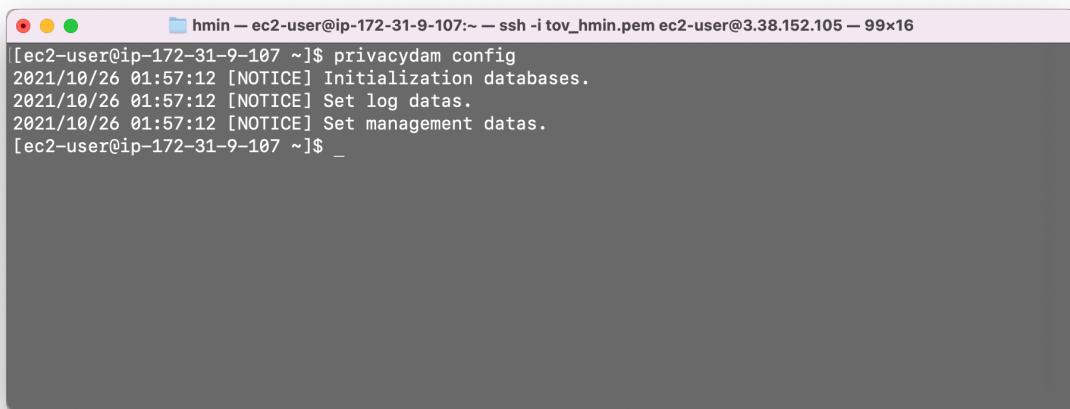
2.1. Create and set an instance for deploy

- Launch an EC2 instance onto the designated public subnet with the shared Privacy DAM AMI.
- Make sure that the public subnet does not have any restriction of connecting from the Internet to the instance via TCP ports 22 and 80. (If you are not sure of this, check the network ACLs of the public subnet.)
- Set a security group that allows the TCP connections to the port number 22 (for SSH) and to the port number 80 (for HTTP) from the Internet (i.e., 0.0.0.0/0) or from your corporate network IP. Make sure a Public IP address is auto-assigned (i.e., Enable ‘Auto-assign Public IP’)
- Create and attach the EBS volume with the instance.
- After a successful deployment of an EC2 instance resource, continue the deployment stage of the Privacy DAM Manager inside the instance.
- Connect to the Privacy DAM Manager instance via SSH.

2.2. Configuration data for demo

Set the Privacy DAM Manager internal database and download test data.

Command) Privacy DAM config

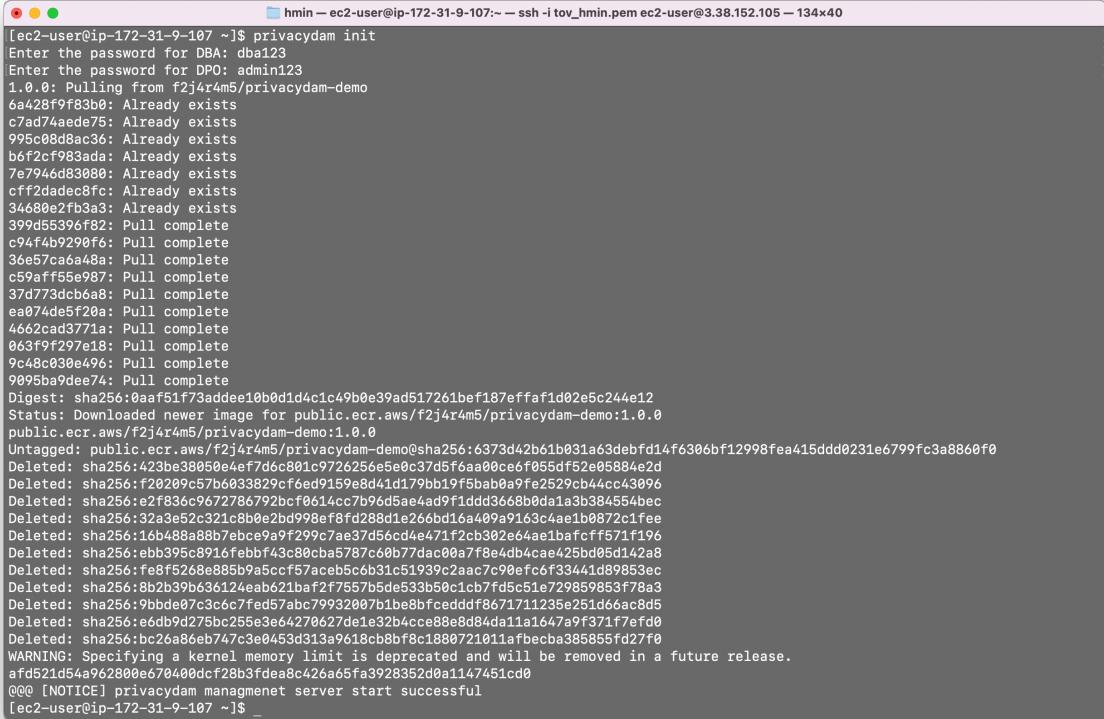


```
[ec2-user@ip-172-31-9-107 ~]$ privacydam config
2021/10/26 01:57:12 [NOTICE] Initialization databases.
2021/10/26 01:57:12 [NOTICE] Set log datas.
2021/10/26 01:57:12 [NOTICE] Set management datas.
[ec2-user@ip-172-31-9-107 ~]$ _
```

2.3. Initialization

Initialize the Privacy DAM Manager passwords and fetch the required container images.

Command) Privacy DAM init



```
[ec2-user@ip-172-31-9-107 ~]$ privacydam init
Enter the password for DBA: dba123
Enter the password for DPO: admin123
1.0.0: Pulling from f2j4r4m5/privacydam-demo
6a428ff9f83b0: Already exists
c7ad74aede75: Already exists
995c08d8ac36: Already exists
b6f2c2f983ada: Already exists
7e7946d83080: Already exists
cff2dadec8fc: Already exists
34680e2fb3a3: Already exists
399d55396fb2: Pull complete
c94f4b9290f6: Pull complete
36e57ca6a48a: Pull complete
c59aff55e987: Pull complete
37d773dc6a8: Pull complete
ea074de5f20a: Pull complete
4662cad3771a: Pull complete
063f9f297e18: Pull complete
9c48c030e496: Pull complete
9095ba9dee74: Pull complete
Digest: sha256:0af51f73addee10b0d1d4c1c49b0e39ad517261bef187effaf1d02e5c244e12
Status: Downloaded newer image for public.ecr.aws/f2j4r4m5/privacydam-demo:1.0.0
public.ecr.aws/f2j4r4m5/privacydam-demo:1.0.0
Untagged: public.ecr.aws/f2j4r4m5/privacydam-demo@sha256:6373d42b61b031a63debfd14f6306bf12998fea415ddd0231e6799fc3a8860f0
Deleted: sha256:e23be38050e4ef7d6c801c9726256e50c37d5f6aa00c6ef055df52e05884e2d
Deleted: sha256:f28299c57b6033829cf6ed9159e8d41d179bb19f5bab0e9fe2529cb44cc43096
Deleted: sha256:e2f836e9672786792bcf0614cc7b96d5ae4ad9f1ddd3668b0d1a3b384554bec
Deleted: sha256:32a3e52c321c8bbe2bd98e8fd288d1e266bd16a409a9163ca4e1b0872c1fee
Deleted: sha256:16ba488a88b87ebce9af299c7ae37d56cd4e471f2cb302e64ae1baafcffff71f196
Deleted: sha256:ebb395c8916febfb43c80cba5787c60b77dac00a7f8e4db4cae425bd085d142a8
Deleted: sha256:fe8f5268e885b9a5ccf57aceb5c6b31c51939c2aac790efc6f33441d89853ec
Deleted: sha256:8b2b396636124eab621ba2f27557b5de533b50c1cb7fd5c51e729859853f7843
Deleted: sha256:9bbde07c3c6c7fed57abc79932007b1be8bfeeeddf8e71711235e251d66ac8d5
Deleted: sha256:6dbd9275bc255e3a64270627de1e32b4cce88e8d4da11a1647a9f371f7efd0
Deleted: sha256:bc26a86eb747c3e0453d313a618cb8bf8c1880721011afbcba385855fd27f0
WARNING: Specifying a kernel memory limit is deprecated and will be removed in a future release.
af5d21d54a962800e670a00dcf2Bb3f3dea8c426a5fa3928352d0a1147451cd0
@@@ [NOTICE] privacydam managemennt server start successful
[ec2-user@ip-172-31-9-107 ~]$ _
```

After you commanded, it asks two passwords; one for DBA(DB access query manager) and the other for DPO(Data Protection Officer who inspects the privacy data access history). Then, it starts to fetch the Privacy DAM Manager container images from the repository.

Now, the initialization is done. You can now connect the Privacy DAM manager web interface using your favorite browser.

2.4. Additional commands for operations

There are some additional commands that might be useful for your operations.

➤ Start application

Command) Privacy DAM start

This command starts the Privacy DAM Manager without checking and fetching the updated container images.

➤ Stop application

Command) Privacy DAM stop

This command stops the running Privacy DAM Manager process.

➤ Restart application

Command) Privacy DAM restart

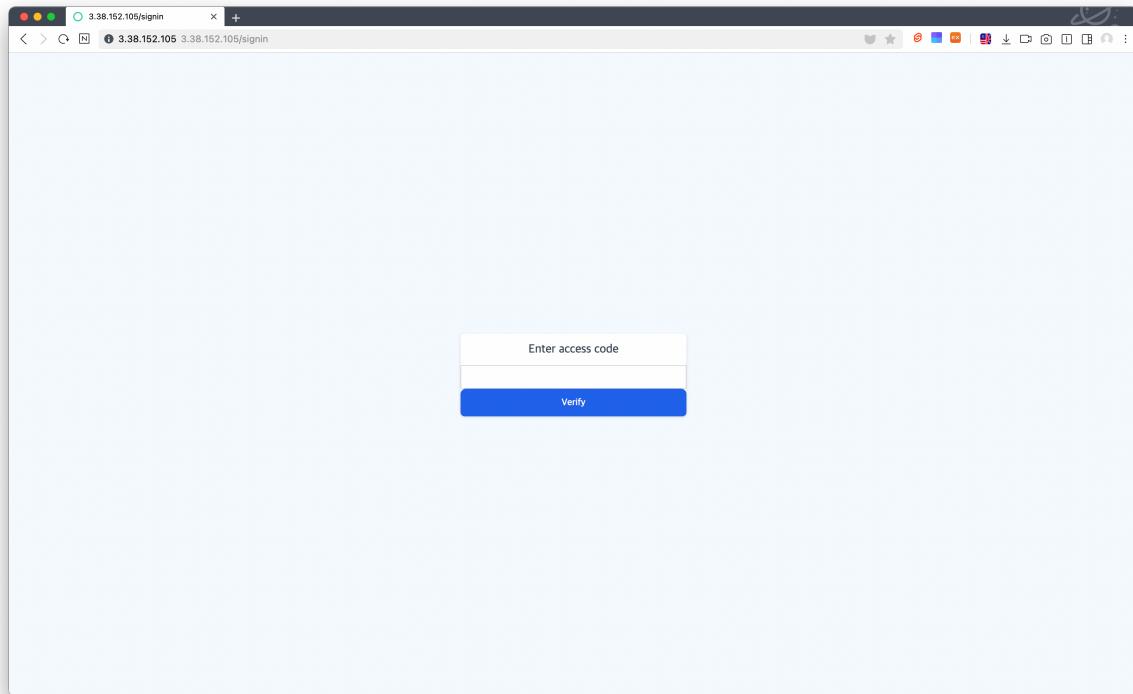
This command stops and restarts the Privacy DAM Manager process.

- Check application status
- Command) Privacy DAM status

This command shows the container status info of the Privacy DAM Manager.

3. Screenshots

- Initial page of Privacy DAM (Enter the access code as you set during the CLI setup sessions)



■ Main page of Privacy DAM (for DBA)

The screenshot shows the Privacy DAM Dashboard for DBA. At the top, there's a header bar with the URL "3.38.152.105/management/api" and a timestamp "2021-10-26 (화) DBA". Below the header is a blue navigation bar with the title "PrivacyDAM Dashboard".

Metric Information

- CPU**: A chart titled "Average CPU Utilization" showing a time series from 10:50 to 11:4. The Y-axis ranges from 0% to 0.0250%. The chart shows several sharp peaks, with one major peak reaching approximately 0.024% around 11:00.
- API Processing Time**: A section titled "API OverAll Processing Time (Average)" which displays the message "No data in response".

API Management

- Source List**: A table showing a single entry: "mainDB (mysql)" with the DSN "username:*****@tcp(dbHost:dbPort)/".
- API List**: A table listing two APIs:

Name	RegDate	ExpDate	Activate
a_marketing_01	2021-10-01 14:55:22	2022-09-30 23:59:59	<input checked="" type="checkbox"/>
a_statistic_01	2021-09-01 09:34:33	2022-03-31 23:59:59	<input checked="" type="checkbox"/>

■ Main page of Privacy DAM (for DPO)

The screenshot shows the Privacy DAM Dashboard for DPO. The layout is similar to the DBA version, with a blue header bar and a "PrivacyDAM Dashboard" title. The timestamp is "2021-10-26 (화) ADMIN".

API Management

API List: A detailed view of the "a_marketing_01" API, showing its configuration:

Name	RegDate	ExpDate	Activate
a_marketing_01	2021-10-01 14:55:22	2022-09-30 23:59:59	<input checked="" type="checkbox"/>

Below the table, there are sections for "Source Type" (mysql), "DSN (Data Source Name)" (username:*****@tcp(dbHost:dbPort)/), "Syntax" (select name, email, country from pdam_dummy_profiles where country in ("france", "germany") and age > ?), "Parameters" (Parameter: age, checkbox checked), and "De-identification option" (Column name: a_statistic_01, Method: encryption, Options: {"algorithm": "hash(md5)"}, Level: 1). The "Activate" status for this row is also checked.

■ Dashboard page of Privacy DAM

Main Page | 3.38.152.105 Main Page | 2021-10-26 (화) | ☰

PrivacyDAM Dashboard

Token

금일 요청량	2
금일 처리량	1
전일 대비 증감률	0 %
이번 주 처리량	2
이번 달 처리량	2

주간 토큰 현황 (10.25 ~ 10.31)

요청 목록	Caller	Created Time
Result: ✓	user001	2021-10-12 18:17:22
Result: ✗	user001	2021-10-12 18:14:56
Result: ✓	user001	2021-10-11 17:57:00

Processed API

금일 요청량	1
금일 처리량	0
전일 대비 증감률	0 %
이번 주 처리량	0
이번 달 처리량	0

주간 처리 현황 (10.25 ~ 10.31)

요청 목록	API Name	Remote IP	Processed Time
Result: ✗	a_marketing_01	10.0.0.57	2021-10-12