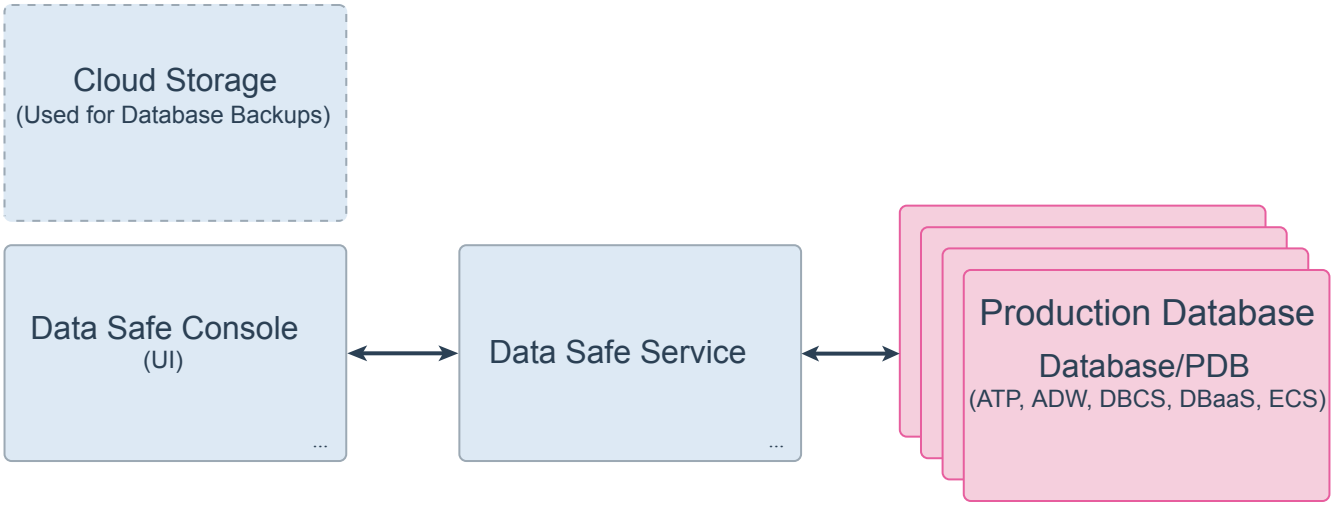
# Oracle Data Safe Technical Architecture

responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

# Oracle Data Safe Introduction




Oracle Data Safe is a fully-integrated Cloud service focused on the security of your data. It provides a complete and integrated set of features for protecting sensitive and regulated data in Oracle Cloud databases.

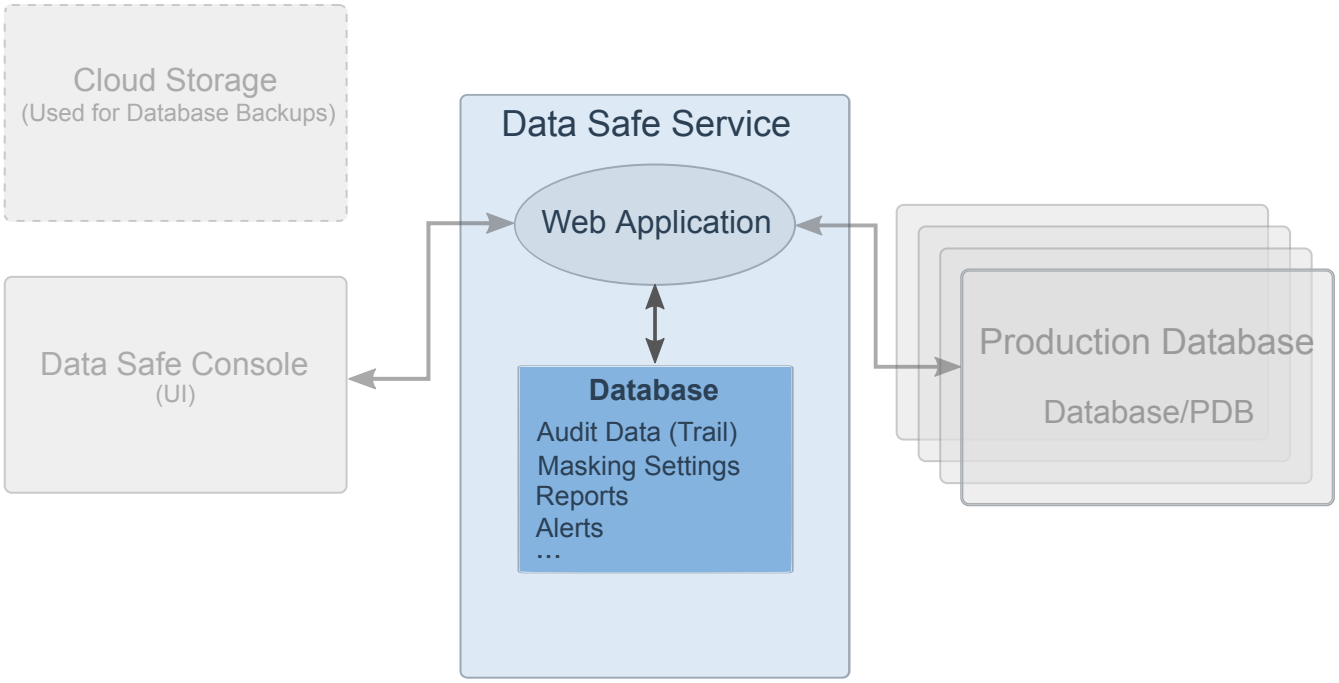
Watch this Introduction to Oracle Data Safe video.

There are four main components to this architecture:

1. As an Oracle Data Safe user, you access the service through a web interface called the Oracle Data Safe Console.
2. After purchasing Oracle Data Safe, the service administrator needs to go into the OCI console and enable Data Safe service in one region of your tenancy. You can watch the Enable Oracle Data Safe video for more information. You can then access the Oracle Data Safe web application and data required to support your service through the Oracle Data Safe Console.
3. Oracle Data Safe is working against what are called targets. These targets are databases you own and want to monitor on the Oracle Public Cloud. Supported targets are currently Autonomous OLT (ATP), Autonomous Data Warehouse (ADW), Database Cloud Service (DBCS), Database systems on OCI (DBaaS), and Exadata Cloud Service (ECS) targets.
   You can use two different protocols to establish connections between your Oracle Data Safe tenancy and your targets:
   a. TCP with network encryption where your target database needs to enable network encryption.
   b. TCPS where the target database has to be configured with TLS 1.1/1.2.
4. The Cloud Storage component is the Oracle Storage Cloud Service or Oracle Cloud Infrastructure Storage Service used to backup your database targets for certain types of

Oracle Data Safe operations like Masking. Depending on how you want to use Oracle Data Safe, this component is optional.

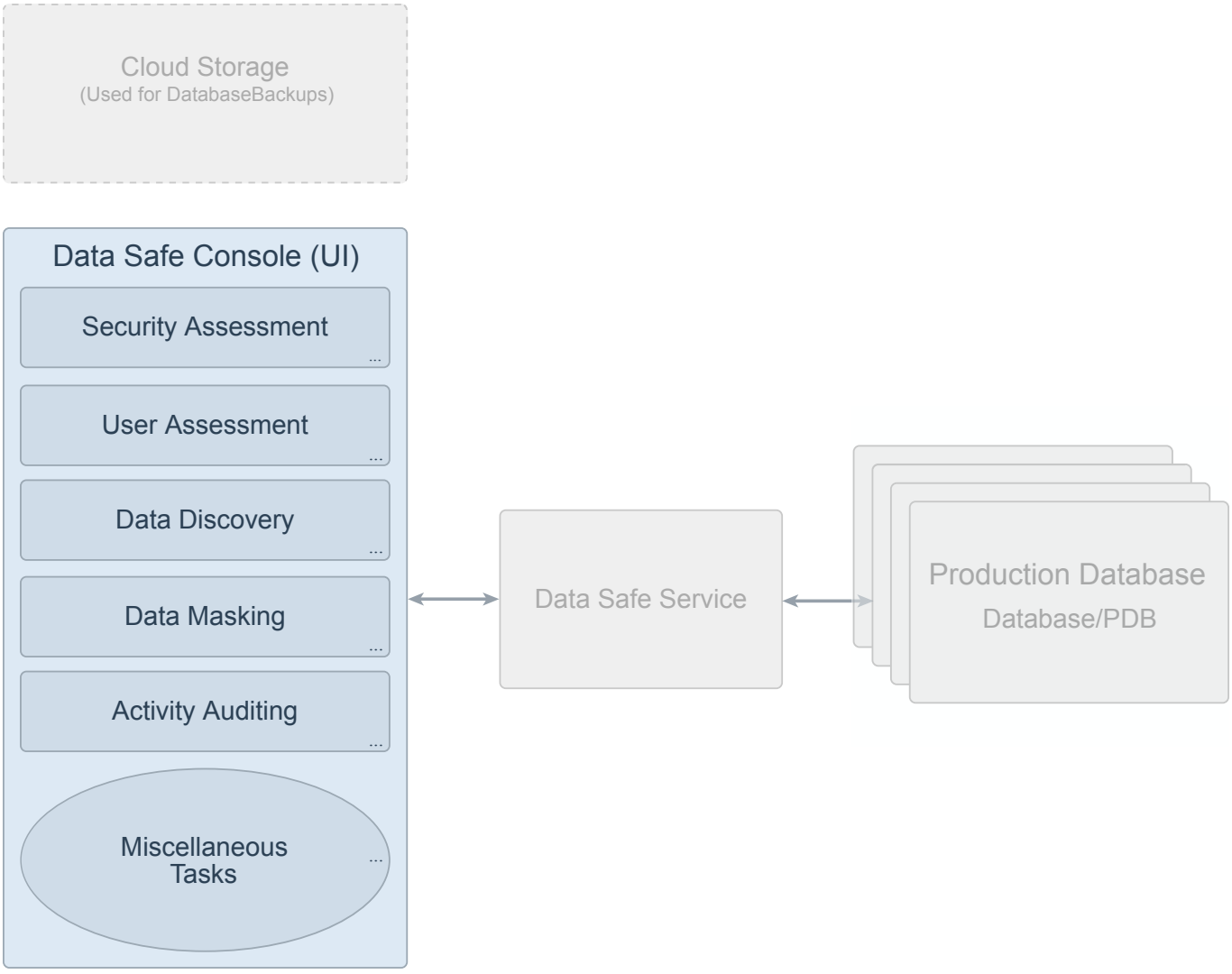
# Oracle Data Safe Service




The Oracle Data Safe service consists of a web application (called Oracle Data Safe Console) and a secure and highly available Oracle Database stored on the Oracle Public Cloud. The database stores your service information, such as audit data, masking settings, reports, alerts, and many other things.

You can access Oracle Data Safe resources through the Oracle Data Safe Console.

# Oracle Data Safe Console



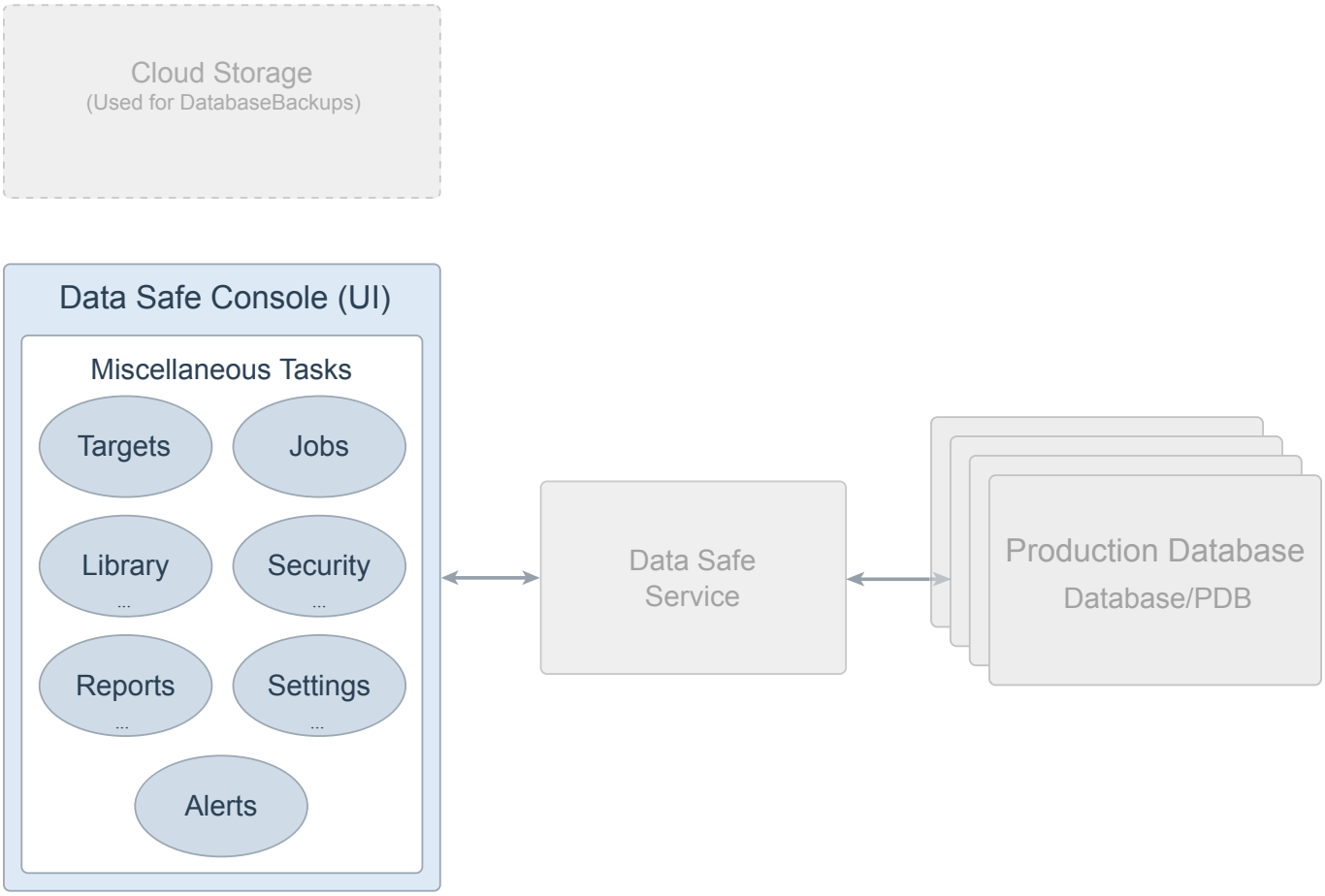

The Oracle Data Safe console, also referred to as the User Interface, or UI, has five main functionalities:

1. Security Assessment analyzes information on your database targets, identifies configuration settings that may unnecessarily introduce risk, and reports recommendations for remediation activities that follow best practices to reduce or mitigate risk.
2. User Assessment provides you information about the risks associated with certain privileged database system users.
3. Data Discovery enables you to discover and classify sensitive data in your database targets.
4. Data Masking enables you to mask sensitive data in your test and development databases.
5. Activity Auditing lets you monitor user activities on selected databases, collect that information, and trigger real-time alerts as needed for unusual or blacklisted behavior.

In addition to the above five main functionalities, you can also perform a number of miscellaneous tasks like managing jobs, viewing reports and alerts, setting parameters, and managing Oracle Data Safe security.

To get a sense of what this UI looks like, watch the Oracle Data Safe Console Walkthrough video.

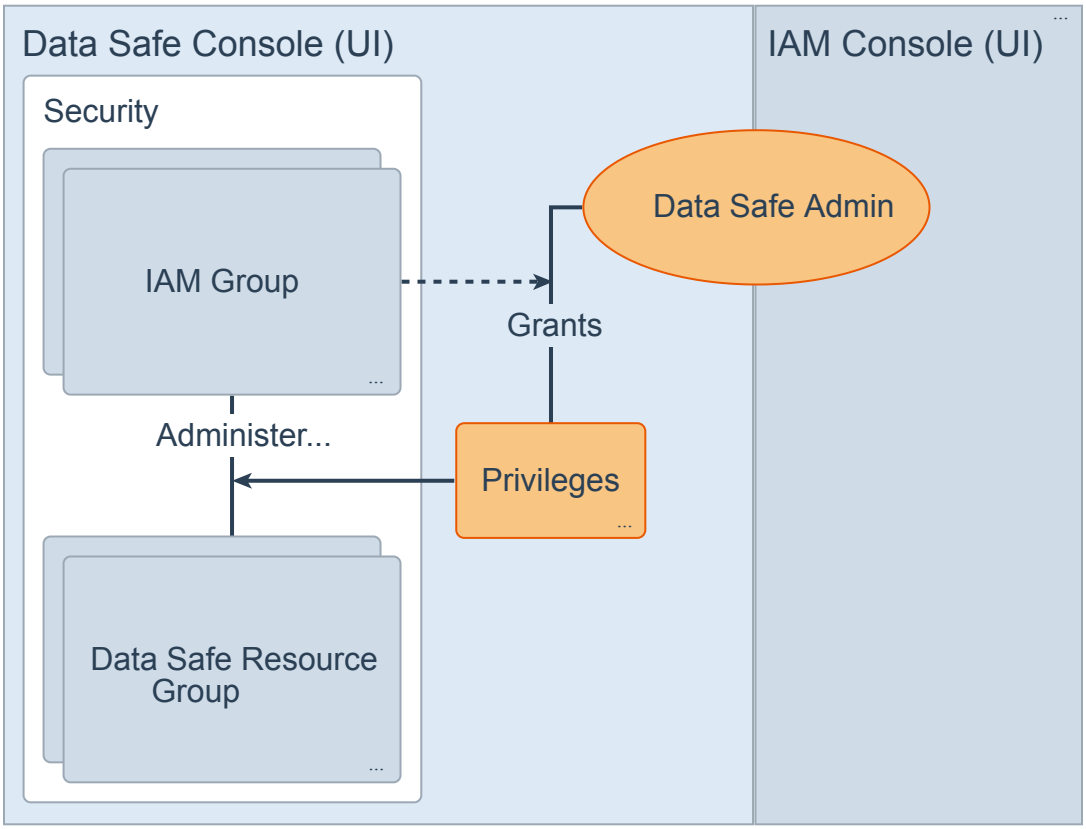
# Miscellaneous Tasks




You can also directly manage some of the following key elements from the Oracle Data Safe Console:

- Targets: You can add new Database targets, configure Oracle Data Safe audit trails for those, and setup your auditing policies.
- Library: From this view, you can look at discovered information for your Database targets and masking data.
- Reports: Here you can look at all the generated reports for audits, masking, discoveries, and assessments, as well as internal (system) information.
- Alerts: The Alerts section give you a summary or details of all triggered alerts and you can close or open these alerts.
- Jobs: The Jobs section shows you all important operations information related to internal processes done by your service.
- Settings: Here you can setup your audit data retention period.
- Security: This is where Oracle Data Safe administrators can add resource groups and grant privileges on those resource groups to user groups.

# Security Overview




There can be multiple users involved in setting up Oracle Data Safe security. At a high level:

- The user who opens an Oracle Cloud Infrastructure (OCI) account (referred to as the Tenancy Administrator)
- Additional users who are added to your Tenancy Administrators group
- Additional users granted the `manage` permission on certain resources through other Identity and Access Management groups

For a very small company, only the user who created your tenancy could be used. The user who administers the Oracle Data Safe service is called the Oracle Data Safe Administrator.

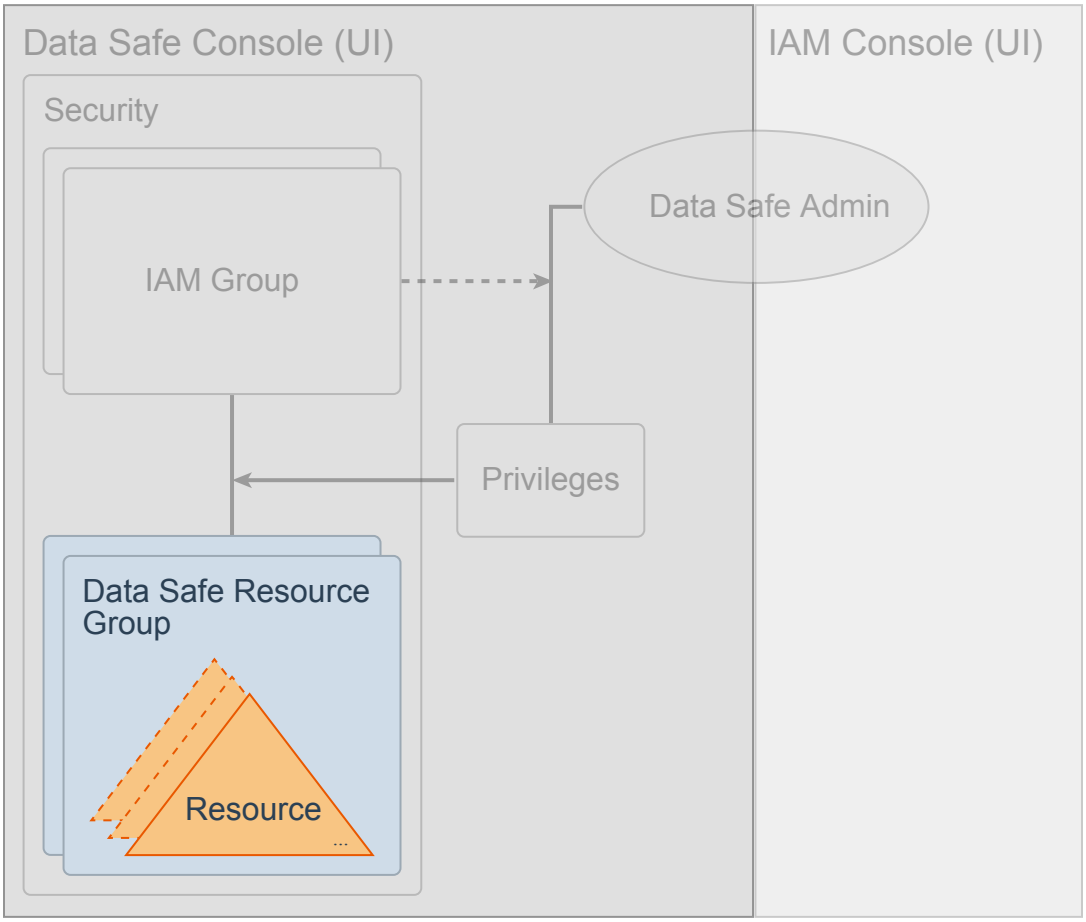
Oracle Data Safe security is established at two levels:

1. From the OCI Identity and Access Management (IAM) Console, the Oracle Data Safe Administrator is responsible for creating additional IAM users and groups that are automatically recognized as valid Oracle Data Safe users and groups in the Oracle Data Safe Console. We refer to these groups as IAM groups.
2. From an Oracle Data Safe tenancy's Console:

- An Oracle Data Safe Administrator can assign Oracle Data Safe privileges to IAM groups for Oracle Data Safe resource groups.
- When an IAM group is granted an administrator-level Oracle Data Safe privilege for a feature (like Assessment) on a particular resource group, any user in that group can then grant corresponding privileges (like `AdministerAssessment` or `ViewAssessment`) to other groups on that same resource group.

For more information about OCI concepts see OCI Key Concepts and Terminology.

# Resource Groups




Oracle Data Safe resource groups are groups of Oracle Data Safe resources that are either automatically created with the tenancy or are created by the administrator.

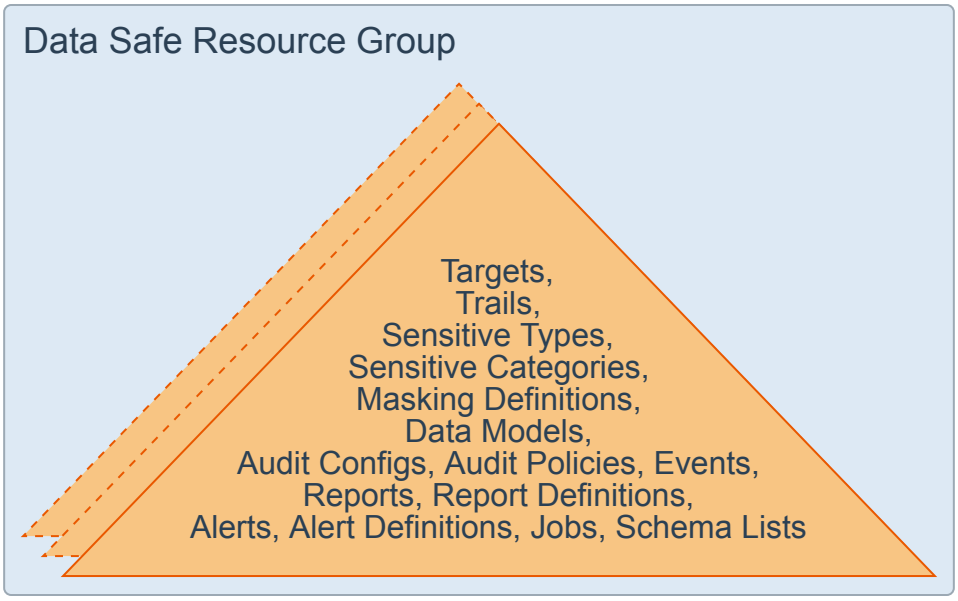
Resource groups streamline the process of assigning resources to users.

By grouping users (through resource groups) and resources (through resource groups) to specific tasks within Oracle Data Safe, you decrease the maintenance complexity of your privileges.

Two internal resource groups are automatically created and cannot be modified: *Oracle Built-in* and *Oracle Privileged*.

A third resource group is automatically created called *Default Resource Group*. By default, all resources are automatically assigned to this resource group. You can create new resource groups and assign resources to your custom resource groups.

# Resources



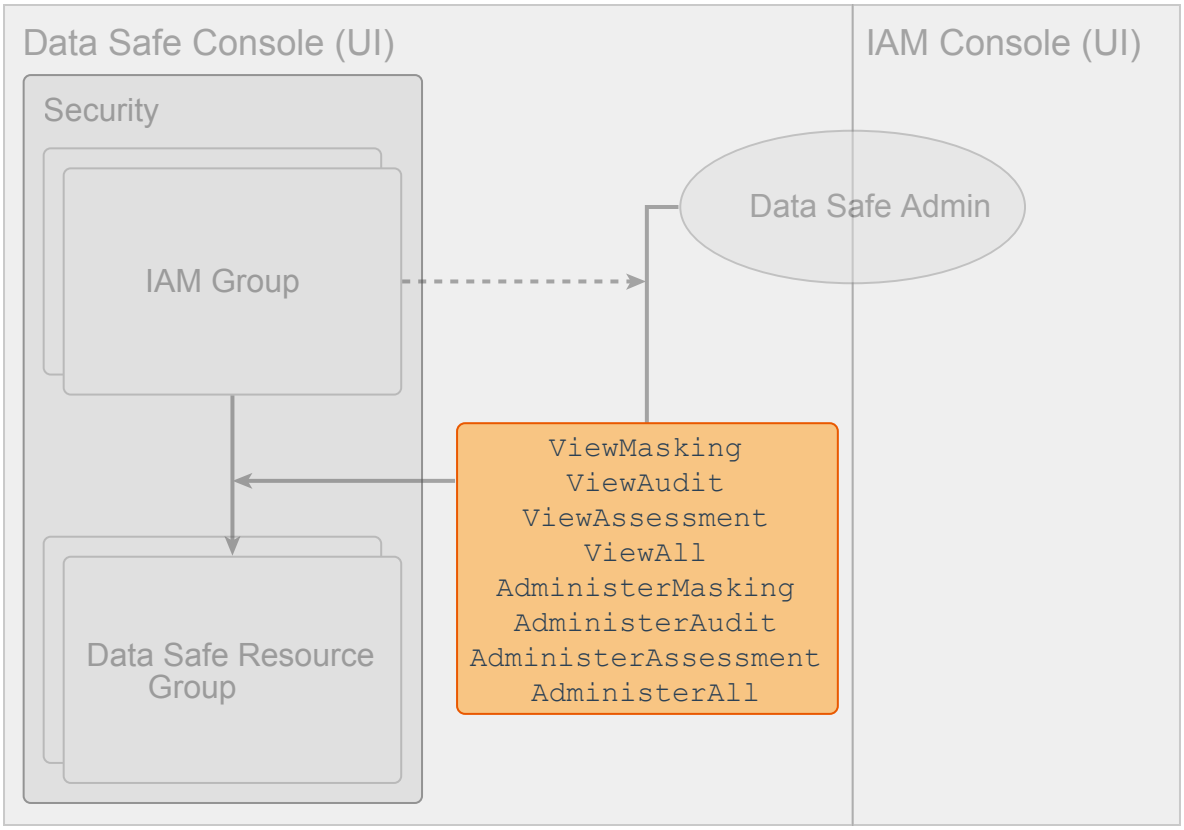

You can add a resource to a resource group when you are creating the resource or modify the resource group assignment later through the resource page. There is no resource groups management page.

Here are some examples of possible Oracle Data Safe resources you can assign to resource groups:

- targets
- sensitive types, sensitive data models
- masking formats, masking policies
- assessment reports, user reports

Others like trail, sensitive categories, masking definitions, report definitions, alerts, alert definitions, events, jobs, and schema lists are internal resources that are automatically managed by Oracle Data Safe.

# Privileges




A group with enough privileges can assign privileges to another group to grant them access to specific features in Oracle Data Safe. Features are divided into four categories: Assessment, Discovery and Masking, and Activity Auditing. There are three different options you can select for a feature: `none`, `view`, or `manage`.

View privileges are as follows:

- `ViewMasking`
- `ViewAuditing`
- `ViewAssessment`
- `ViewAll`

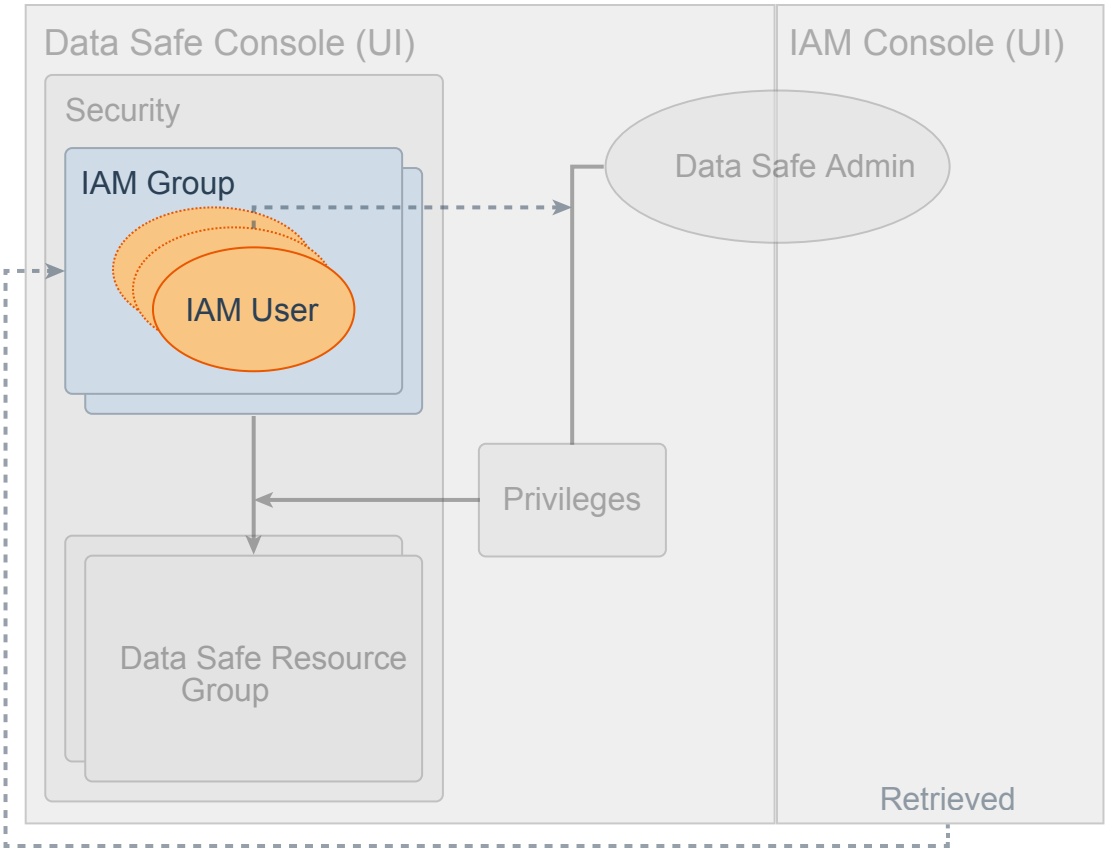
Manage privileges are as follows:

- `AdministerMasking`
- `AdministerAudit`
- `AdministerAssessment`
- `AdministerAll`

The `manage` option on the Authorizations policies tab grants an Administrator level privilege where the group has full control of the feature over all resources in the associated resource group. This option also allows a group to delegate privileges. For example, if you select the `manage` option for Discovery and Masking on Resource Group 1 (RG1), you are essentially granting the group the `AdministerMasking` privilege on RG1, and that group can select the `manage` or `view` option for Discovery and Masking on RG1 for other groups.

With the `view` option selected, a group can only look at the resources in the associated resource group.

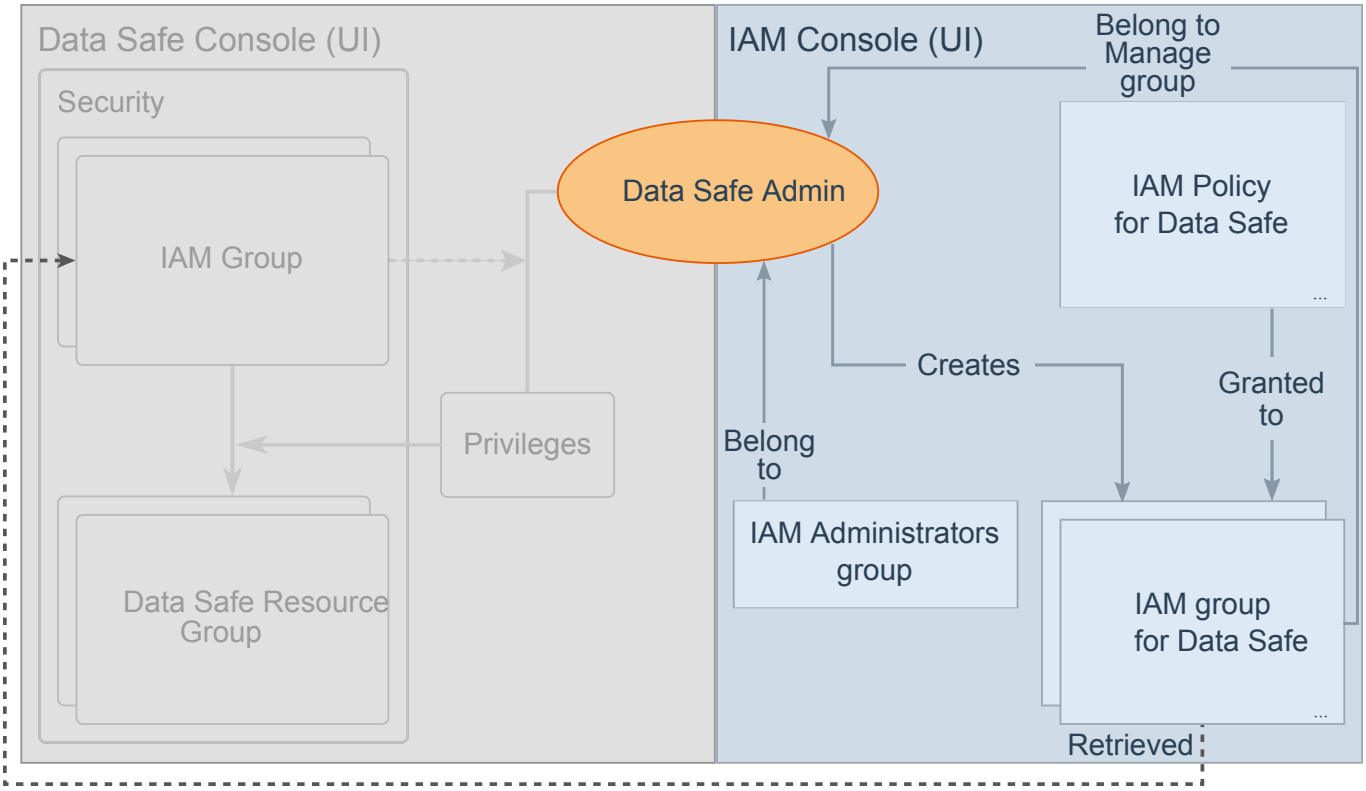
# IAM Groups in Oracle Data Safe




You connect to your Oracle Data Safe Console through the OCI Console. The Oracle Data Safe Administrator is responsible for creating additional users and groups by using the Oracle Cloud Infrastructure Identity and Access Management (IAM) service. This service's interface is referred to as the IAM Console.

The IAM groups in your tenancy are automatically retrieved within your Oracle Data Safe Console so you can use them to connect to your Oracle Data Safe Console and manage Oracle Data Safe resources.

# IAM Console



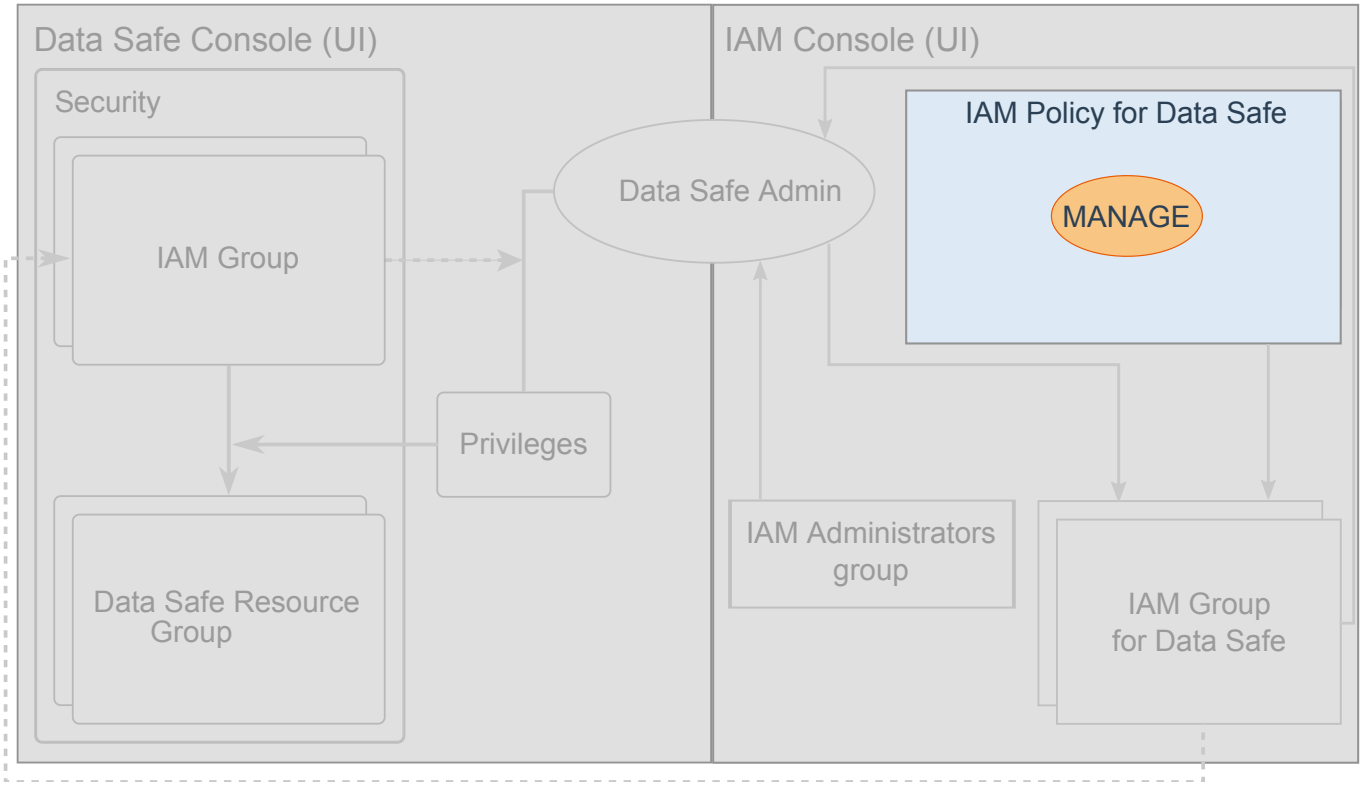

An Oracle Data Safe administrator is defined as an IAM user that either:

1. Belongs to the IAM Administrators group of your tenancy, or
2. Belongs to another IAM group that received the IAM `manage` permission for a particular Oracle Data Safe tenancy through an IAM policy.

An IAM group is automatically retrieved and visible within a particular Oracle Data Safe tenancy's Console if the user connected to that Oracle Data Safe tenancy has IAM `inspect` permission on that group.

For more information about IAM and OCI concepts, see Overview of Oracle Cloud Infrastructure Identity and Access Management.

# IAM Policies



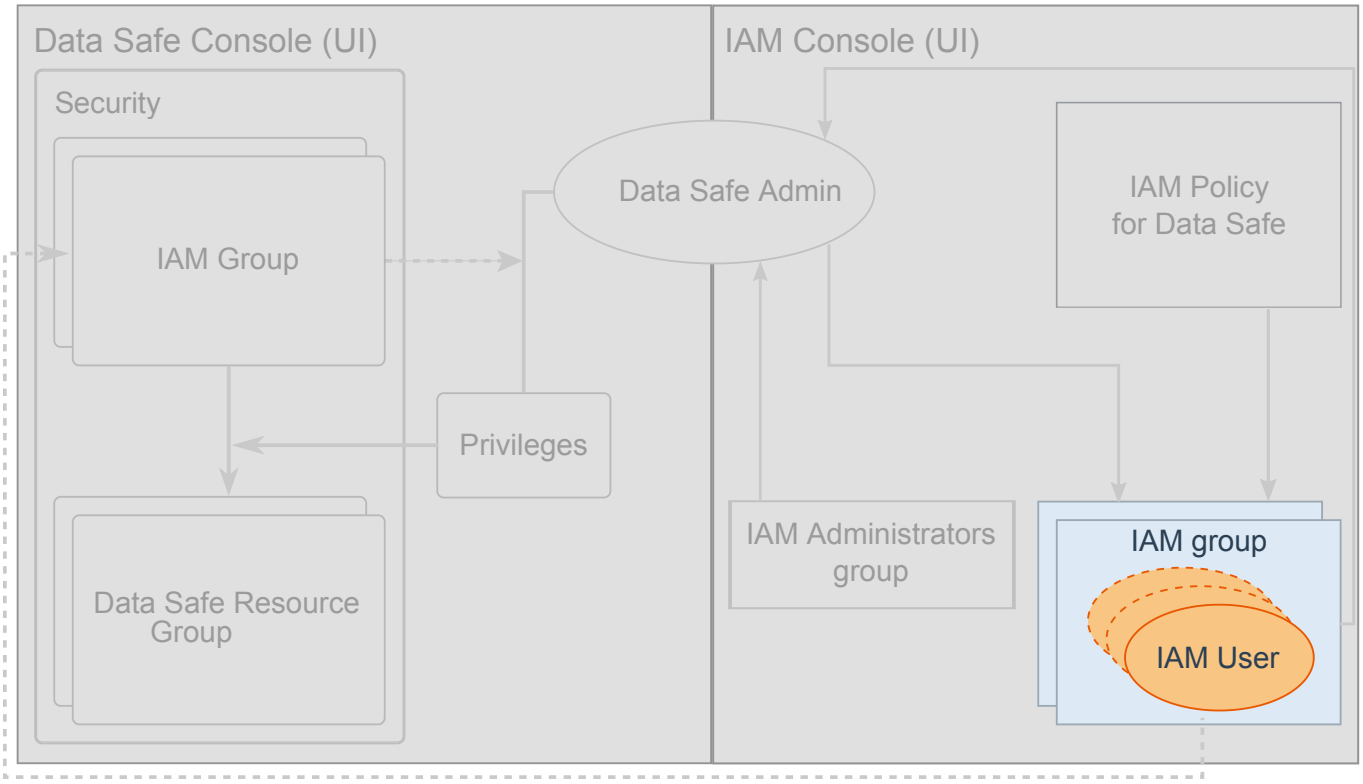

As a Tenancy Administrator in IAM or as another user with enough permissions, you can create OCI policies to grant permissions on your OCI resources in a compartment for a group. The following four permissions can be granted on OCI resources: `inspect`, `read`, `use`, and `manage`.

Here are some examples of policies you could create in the IAM console:

- `Allow group A-Admins to manage all-resources in compartment Project-A`
- `Allow group A-Admins to manage data-safe in tenancy`

For more information, see Getting Started with OCI Policies.

# IAM Groups




In the IAM Console, your Oracle Data Safe Administrator can create users and groups and nest groups as needed. Depending on who is connected to your Oracle Data Safe Console and permissions granted to IAM groups, these groups will automatically be visible in the Oracle Data Safe Console.

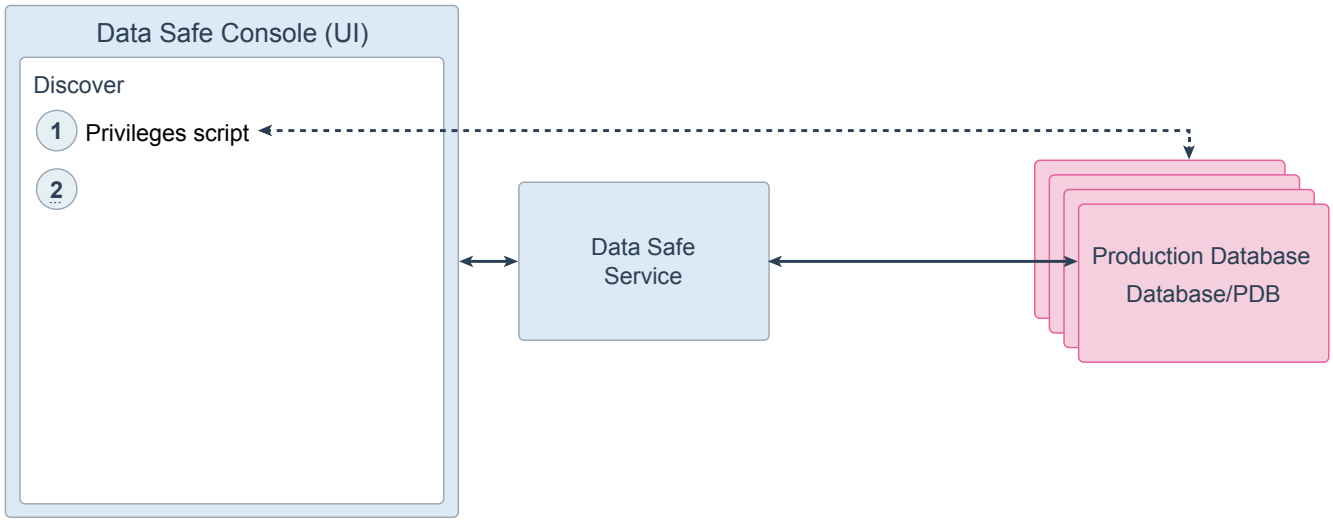
Here is an example of how all of this can be used:

1. Acme Company signs up to use Oracle Data Safe and assigns Adam as the Tenant Administrator. The default seeded policy in Acme Company's tenancy gives Adam the permissions to access and manage all the resources in tenancy, which is the root compartment.
2. In the IAM Console, Adam creates several groups and users.
    - He creates two groups for administrators: A-Admins and B-Admins (for Project A and Project B within the company).
    - He provisions users named Jorge and Cheri and places them in the A-Admins and B-Admins groups, respectively.
    - He grants the A-Admins and B-Admins groups permissions to `inspect` all user groups in the tenancy. This allows users in both of those groups to later grant

privileges to other groups on their Oracle Data Safe resources from the Oracle Data Safe Console.

3. In the Oracle Data Safe Console, Adam creates the following resource groups:
   - Project-A: to organize Project A team's cloud resources and control access to them.
   - Project-B: to organize Project B team's cloud resources and control access to them.
4. In the Oracle Data Safe Console, Adam grants privileges on the resource groups to user groups.
   - He grants the A-Admins group the `manage` privilege on All Features in the Project-A resource group.
   - He grants the B-Admins group the `manage` privilege on All Features in the Project-B resource group.

# Discovery Task - Step 1




The discovery functionality allows you to find sensitive data in your target cloud databases. This information about sensitive data can be leveraged by Oracle Data Safe functionalities like Masking and Auditing.

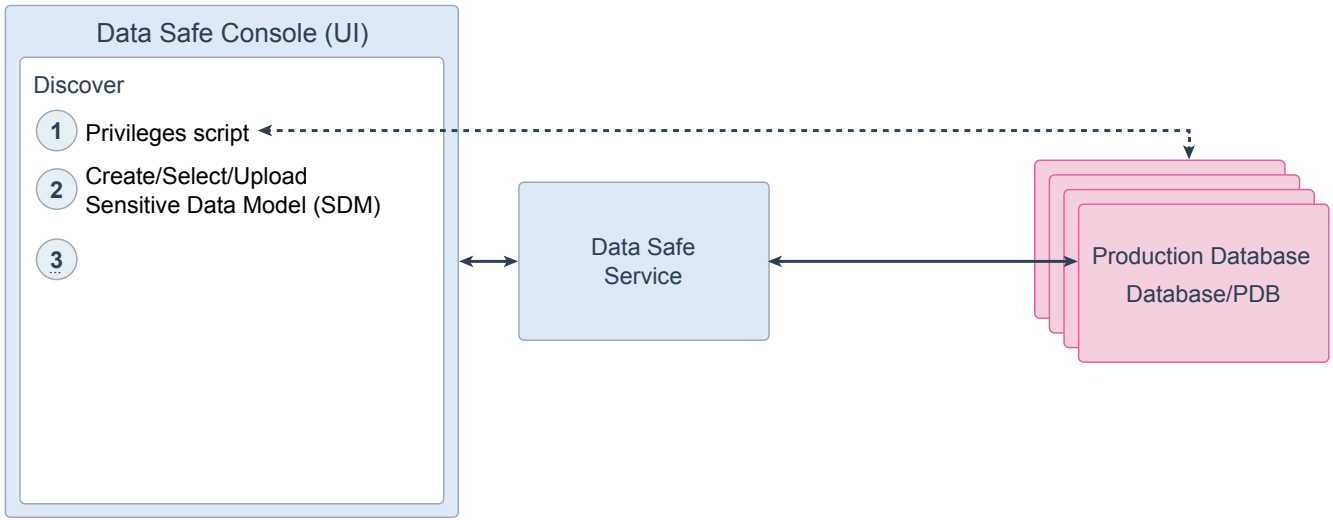
For more information, watch the Discover and Mask Sensitive Data video.

Oracle Data Safe currently supports the following cloud services: Autonomous OLTP Database (ATP), Autonomous Data Warehouse (ADW), Database Cloud Service (DBCS), Oracle Cloud Infrastructure Database System (DBaaS), and Exadata Cloud Service (ECS).

Here are the various tasks you can achieve with Data Discovery:

1. Before you can discover or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. You do not need to discover for an ATP. All you need to do is to go to the ATP console and click register with Oracle Data Safe. It is all automatic.

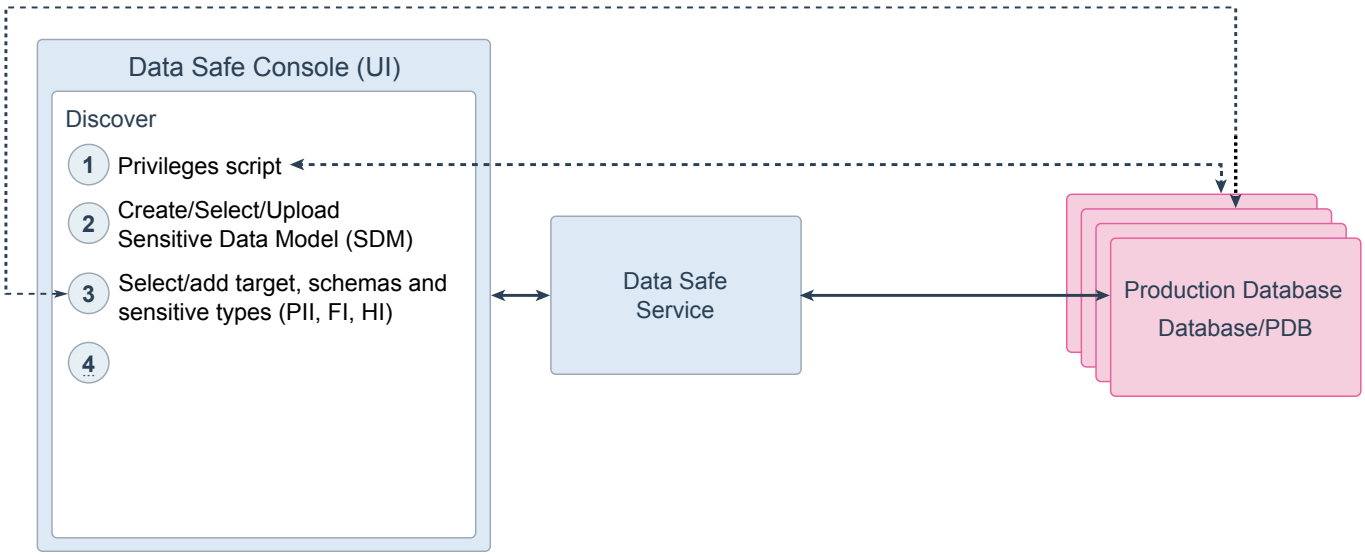
# Discovery Task - Step 2




Here are the various tasks you can achieve with discovery:

1. Before you can discover or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. You do not need to discover for an ATP. All you need to do is to go to the ATP console and click register with Oracle Data Safe. It is all automatic.
2. Before you start a discovery operation, you can create or reuse what is called a Sensitive Data Model (SDM). An SDM is essentially a container for sensitive columns discovered within your database target.

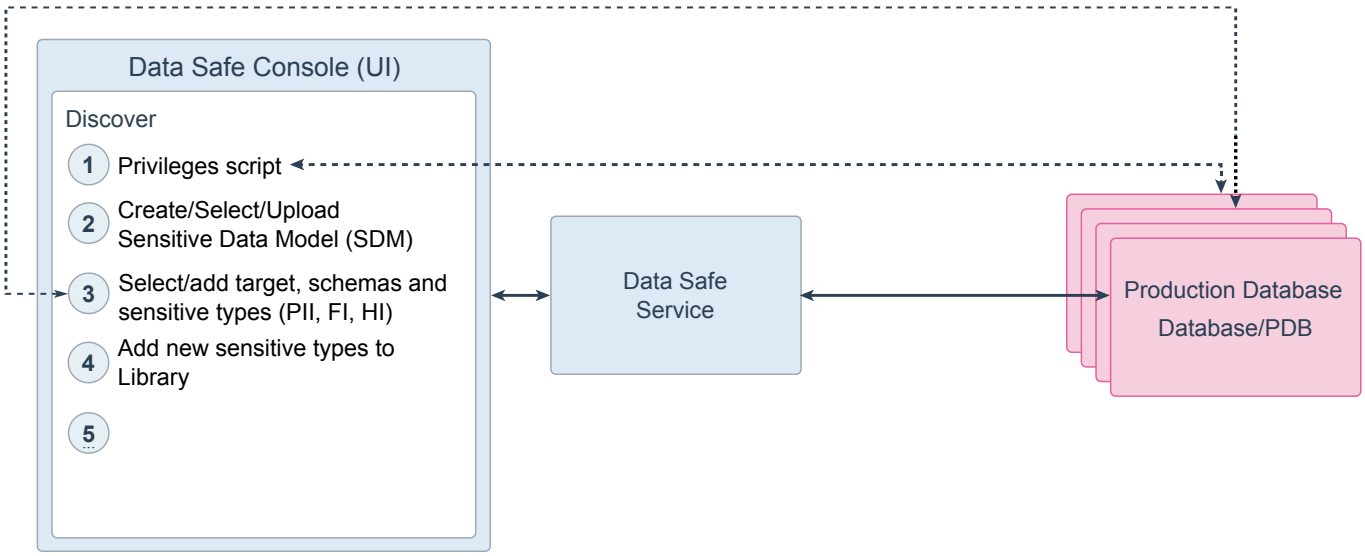
# Discovery Task - Step 3




Here are the various tasks you can achieve with discovery:

1. Before you can discover or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. You do not need to discover for an ATP. All you need to do is to go to the ATP console and click register with Oracle Data Safe. It is all automatic.
2. Before you start a discovery operation, you can create or reuse what is called a Sensitive Data Model (SDM). An SDM is essentially a container for sensitive columns discovered within your database target.
3. You also specify the connection details to your database target as well as the type of sensitive columns you want to identify within your database target: Personally Identifiable Information, Financial Information, or Healthcare Information.

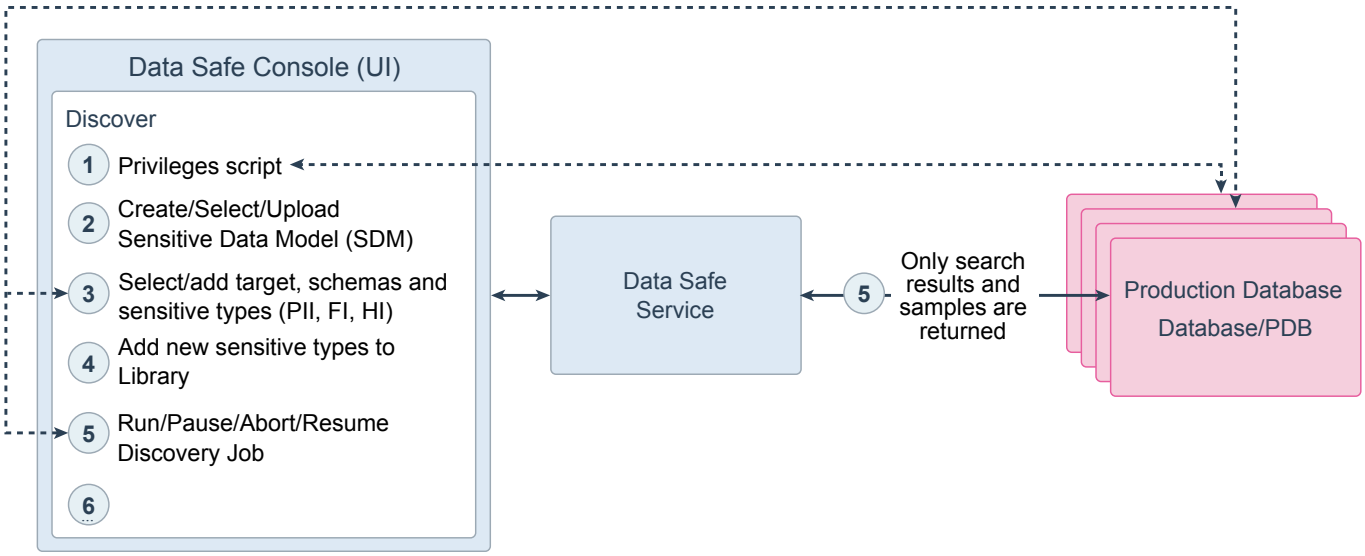
# Discovery Task - Step 4




Here are the various tasks you can achieve with discovery:

1. Before you can discover or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. You do not need to discover for an ATP. All you need to do is to go to the ATP console and click register with Oracle Data Safe. It is all automatic.
2. Before you start a discovery operation, you can create or reuse what is called a Sensitive Data Model (SDM). An SDM is essentially a container for sensitive columns discovered within your database target.
3. You also specify the connection details to your database target as well as the type of sensitive columns you want to identify within your database target: Personally Identifiable Information, Financial Information, or Healthcare Information.
4. You can even add new types of sensitives columns you would like to search for. New sensitive types are added to what is called a Library and are associated to a Resource Group used to control their uses.

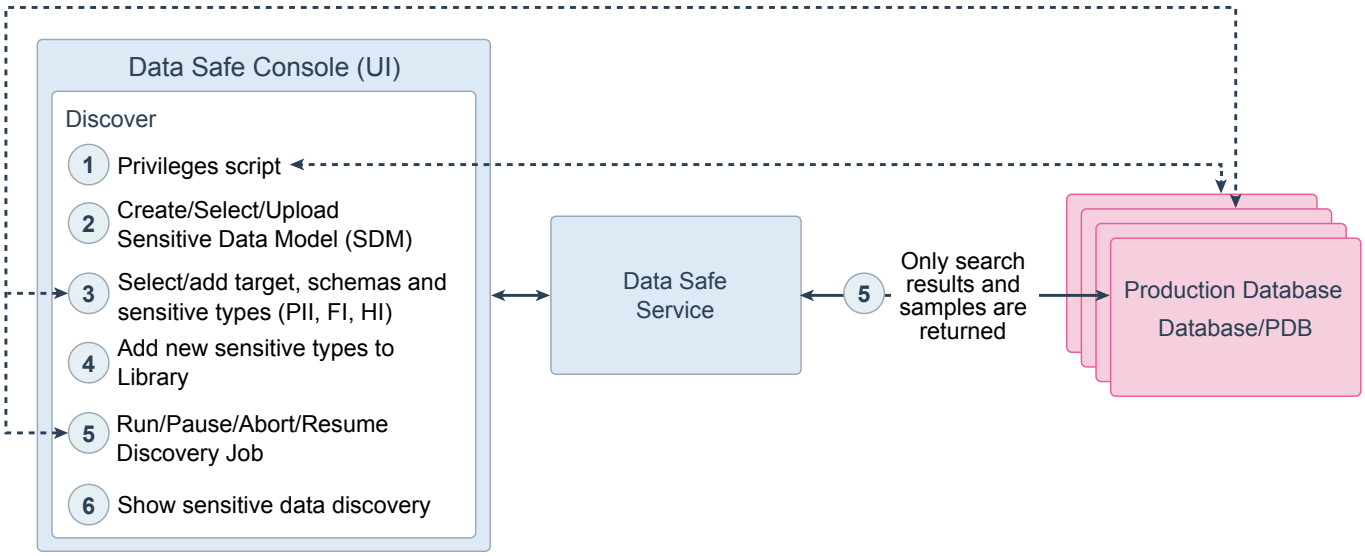
# Discovery Task - Step 5




Here are the various tasks you can achieve with discovery:

1. Before you can discover or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. You do not need to discover for an ATP. All you need to do is to go to the ATP console and click register with Oracle Data Safe. It is all automatic.
2. Before you start a discovery operation, you can create or reuse what is called a Sensitive Data Model (SDM). An SDM is essentially a container for sensitive columns discovered within your database target.
3. You also specify the connection details to your database target as well as the type of sensitive columns you want to identify within your database target: Personally Identifiable Information, Financial Information, or Healthcare Information.
4. You can even add new types of sensitives columns you would like to search for. New sensitive types are added to what is called a Library and are associated to a Resource Group used to control their uses.
5. Once this is all defined, a Discovery Job is started to add the database as a new target for Oracle Data Safe and sensitive columns and optionally sampled data are retrieved for the target. You have the possibility to control this job execution.

# Discovery Task - Step 6




The discovery functionality allows you to find sensitive data in your target cloud databases. This information about sensitive data can be leveraged by Oracle Data Safe functionalities like Masking and Auditing.

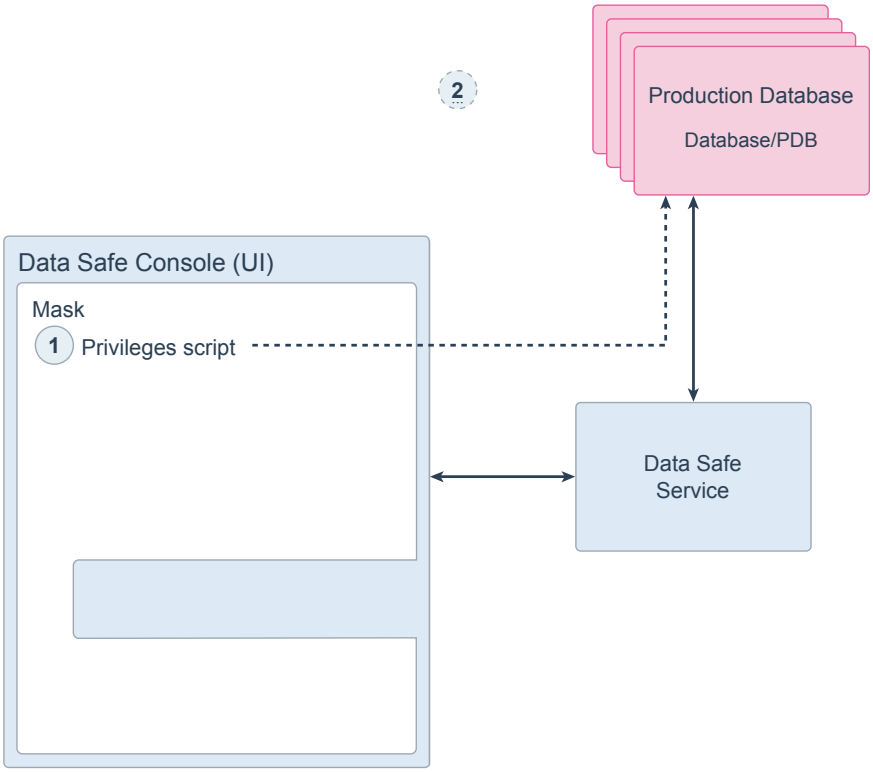
Oracle Data Safe currently supports the following cloud services: Autonomous OLTP Database (ATP), Autonomous Data Warehouse (ADW), Database Cloud Service (DBCS), Oracle Cloud Infrastructure Database System (DBaaS), and Exadata Cloud Service (ECS).

Here are the various tasks you can achieve with discovery:

1. Before you can discover or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. You do not need to discover for an ATP. All you need to do is to go to the ATP console and click register with Oracle Data Safe. It is all automatic.
2. Before you start a discovery operation, you can create or reuse what is called a Sensitive Data Model (SDM). An SDM is essentially a container for sensitive columns discovered within your database target.
3. You also specify the connection details to your database target as well as the type of sensitive columns you want to identify within your database target: Personally Identifiable Information, Financial Information, or Healthcare Information.

4. You can even add new types of sensitives columns you would like to search for. New sensitive types are added to what is called a Library and are associated to a Resource Group used to control their uses.
5. Once this is all defined, a Discovery Job is started to add the database as a new target for Oracle Data Safe and sensitive columns and optionally sampled data are retrieved for the target. You have the possibility to control this job execution.
6. You can then review the findings through various reports.

# Data Masking Task - Step 1




In Oracle Data Safe, you use the Masking Wizard to mask sensitive data. You can choose to use pre-built masking formats and policies or create your own. The system provides a masking report to give you a high level view of your masking activities and results.

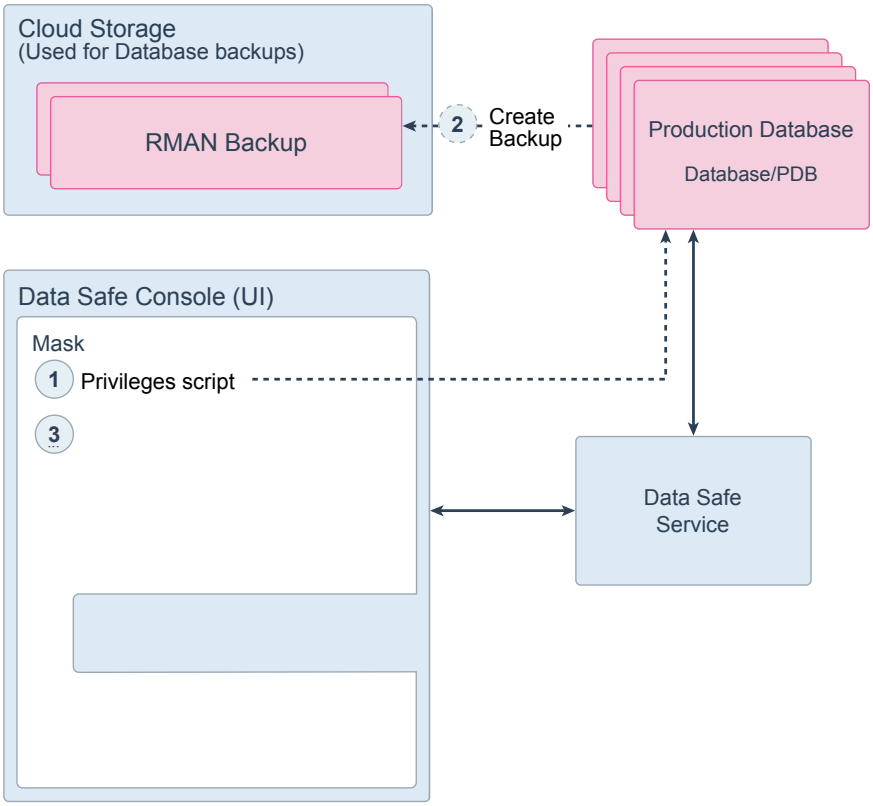
For more information, watch the Discover and Mask Sensitive Data video.

Here we describe the recommended way of using Data Masking. However, another way is to connect to a test database and mask it directly.

1. Before you can mask or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required

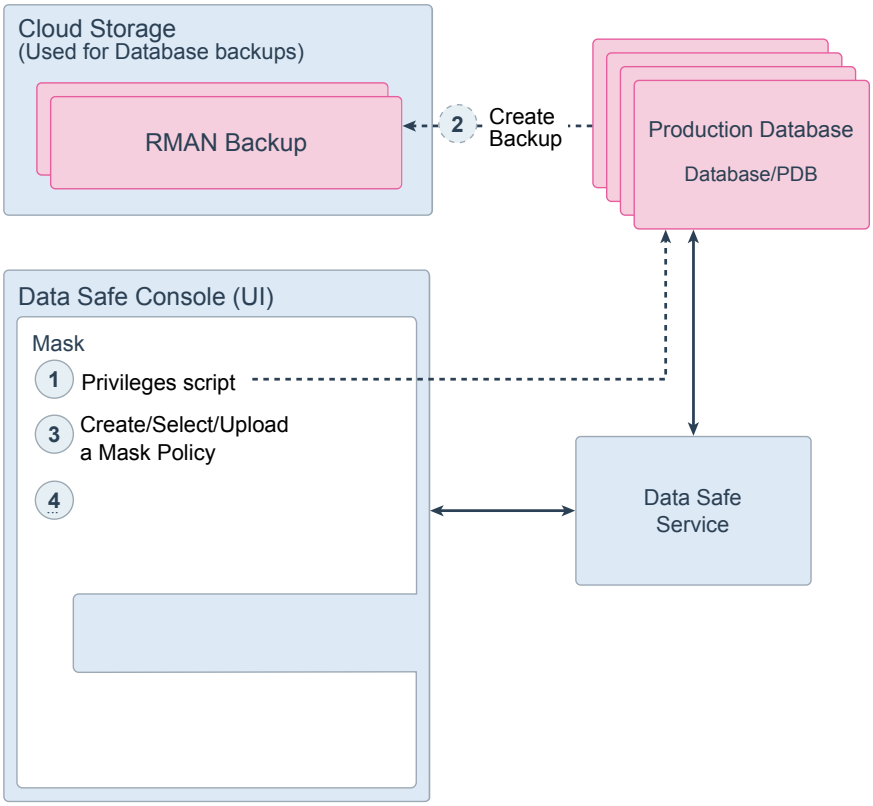
privileges to be granted. If you are using ATP, all you need to do is to go to the ATP console and click register with Oracle Data Safe. It is all automatic.

# Data Masking Task - Step 2




1. Before you can mask or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. If you are using ATP, all you need to do is to go to the ATP console and click register with Oracle Data Safe. It is all automatic.
2. Before masking data from your production databases, you need to create backups of your database targets. This is because you should never mask your production databases. In the process of masking data, you will reuse your database backups to create clones of your databases and use those clones to mask the data. You will then extract the masked data from these clones to create test and development databases on which you will import only the masked data. You could use the Oracle Cloud Storage service or any other backup location to store your production backups using RMAN for example.

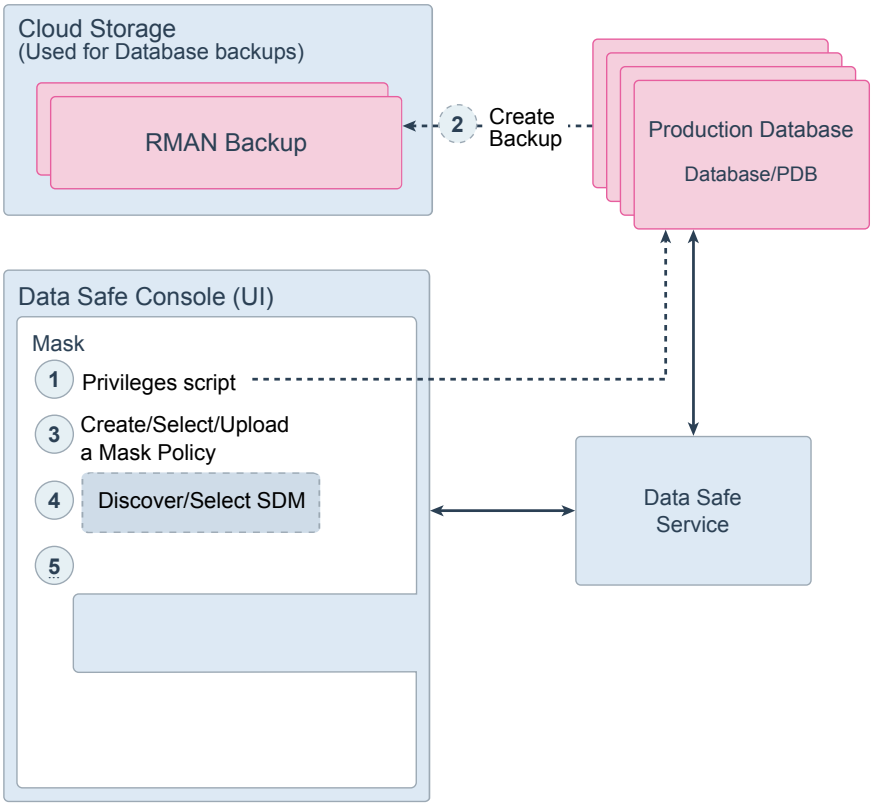
# Data Masking Task - Step 3




1. Before you can mask or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. If you are using ATP, all you need to do is to go to the ATP console and click register with Oracle Data Safe. It is all automatic.
2. Before masking data from your production databases, you need to create backups of your database targets. This is because you should never mask your production databases. In the process of masking data, you will reuse your database backups to create clones of your databases and use those clones to mask the data. You will then extract the masked data from these clones to create test and development databases on which you will import only the masked data. You could use the Oracle Cloud Storage service or any other backup location to store your production backups using RMAN for example.

3. To mask sensitive data, you must first define a masking policy on a Sensitive Data Model (SDM). A masking policy is mainly a container for mask formats you will define in the next steps.

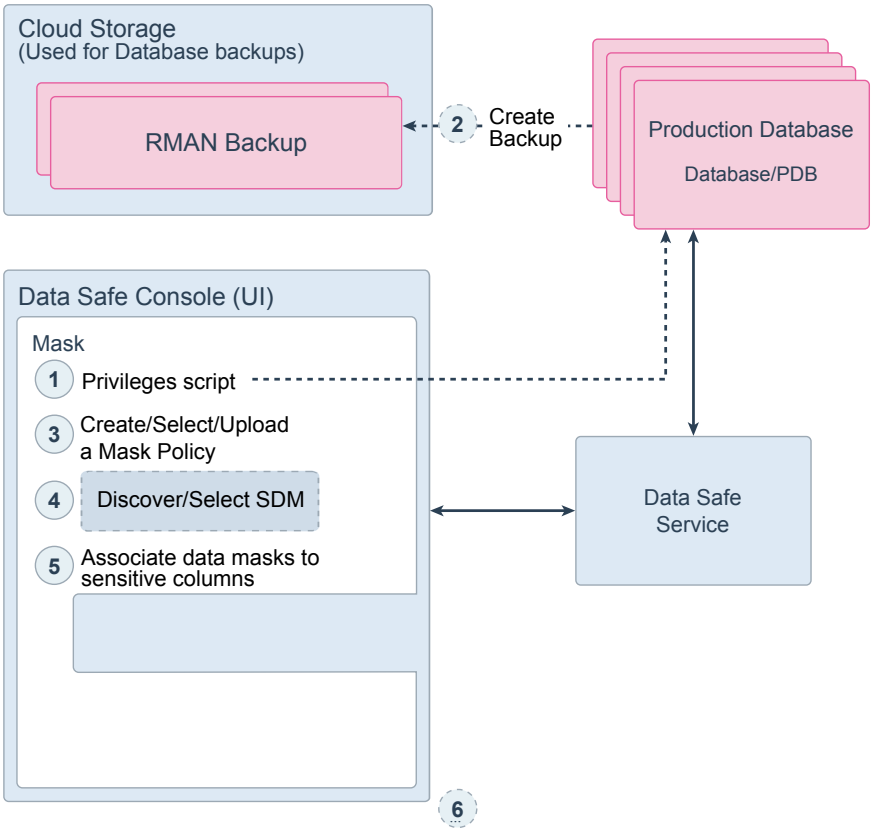
# Data Masking Task - Step 4




1. Before you can mask or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. If you are using ATP, all you need to do is to go to the ATP console and click register with Oracle Data Safe. It is all automatic.
2. Before masking data from your production databases, you need to create backups of your database targets. This is because you should never mask your production databases. In the process of masking data, you will reuse your database backups to create clones of your databases and use those clones to mask the data. You will then extract the masked data from these clones to create test and development databases on which you will import only the masked data. You could use the Oracle Cloud Storage service or any other backup location to store your production backups using RMAN for example.

3. To mask sensitive data, you must first define a masking policy on a Sensitive Data Model (SDM). A masking policy is mainly a container for mask formats you will define in the next steps.
4. If not done already through the Discovery functionality, you can run a discovery job from here too. This will allow you to create an SDM used with your Mask Policy. This step is optional and you could simply reuse an existing SDM done previously.

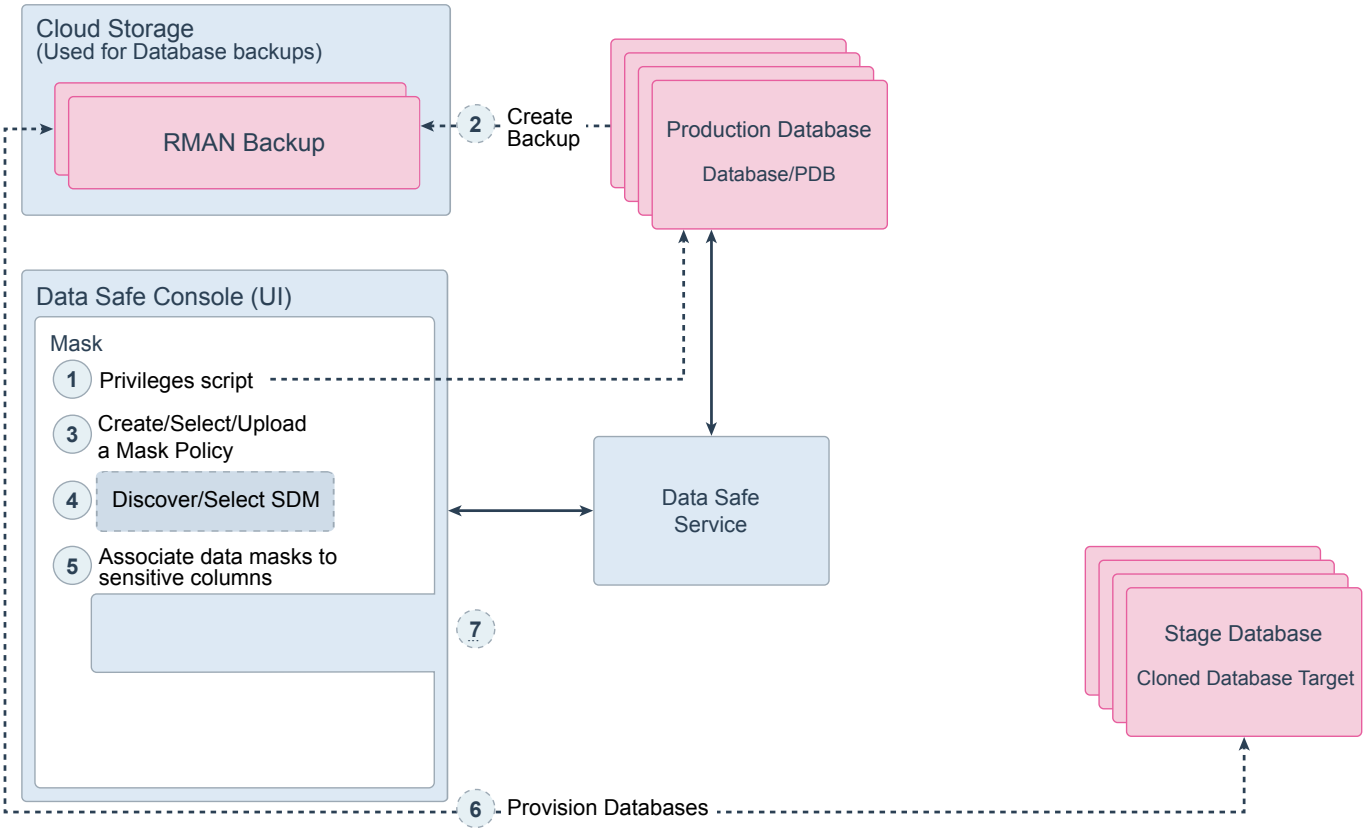
# Data Masking Task - Step 5




1. Before you can mask or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. If you are using ATP, all you need to do is to go to the ATP console and click register with Oracle Data Safe. It is all automatic.
2. Before masking data from your production databases, you need to create backups of your database targets. This is because you should never mask your production databases. In the process of masking data, you will reuse your database backups to create clones of your databases and use those clones to mask the data. You will then extract the masked data from these clones to create test and development databases on which you will import only the masked data. You could use the Oracle Cloud Storage service or any other backup location to store your production backups using RMAN for example.

3. To mask sensitive data, you must first define a masking policy on a Sensitive Data Model (SDM). A masking policy is mainly a container for mask formats you will define in the next steps.
4. If not done already through the Discovery functionality, you can run a discovery job from here too. This will allow you to create an SDM used with your Mask Policy. This step is optional and you could simply reuse an existing SDM done previously.
5. You can then create masking formats that will be used later to mask your sensitive data by replacing your sensitive data with realistic but fictitious data. Masking provides a comprehensive number of predefined mask formats to help you quickly mask data, such as shuffle, random numbers, and unique phone numbers. You can also create custom masks, such as fixed strings.

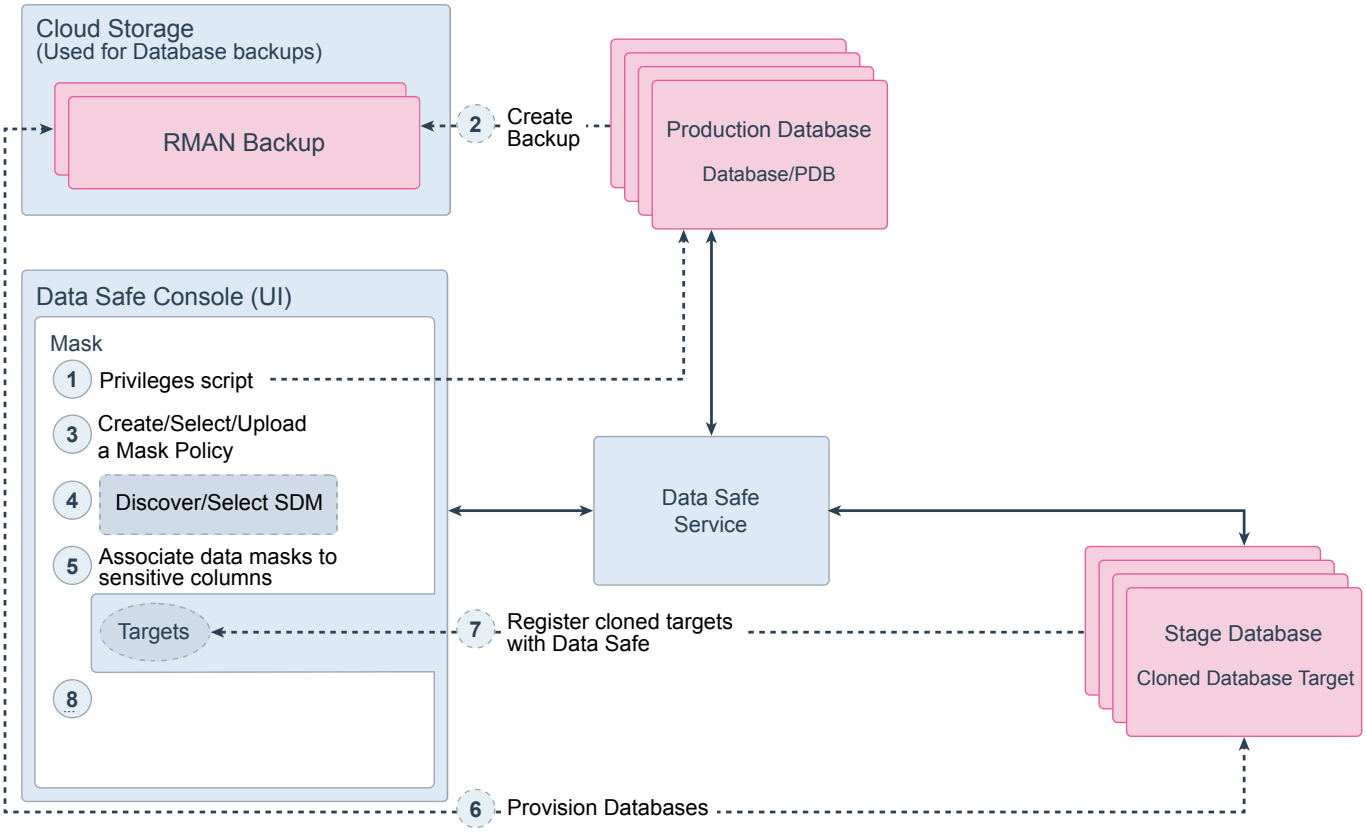
# Data Masking Task - Step 6




1. Before you can mask or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. If you are using ATP, all you need to do is to go to the ATP console and click register with Oracle Data Safe. It is all automatic.
2. Before masking data from your production databases, you need to create backups of your database targets. This is because you should never mask your production databases. In the process of masking data, you will reuse your database backups to create clones of your databases and use those clones to mask the data. You will then extract the masked data from these clones to create test and development databases on which you will import only the masked data. You could use the Oracle Cloud Storage service or any other backup location to store your production backups using RMAN for example.

3. To mask sensitive data, you must first define a masking policy on a Sensitive Data Model (SDM). A masking policy is mainly a container for mask formats you will define in the next steps.
4. If not done already through the Discovery functionality, you can run a discovery job from here too. This will allow you to create an SDM used with your Mask Policy. This step is optional and you could simply reuse an existing SDM done previously.
5. You can then create masking formats that will be used later to mask your sensitive data by replacing your sensitive data with realistic but fictitious data. Masking provides a comprehensive number of predefined mask formats to help you quickly mask data, such as shuffle, random numbers, and unique phone numbers. You can also create custom masks, such as fixed strings.
6. It is now time to create clones of your production databases you want to mask. You do so by using the backups you created. We call these clones, stage databases. They are not meant to be exposed to any user. They will be used to mask your sensitive data only. You must create a stage database on the Oracle Cloud with supported services. This step is optional if you already did it previously.

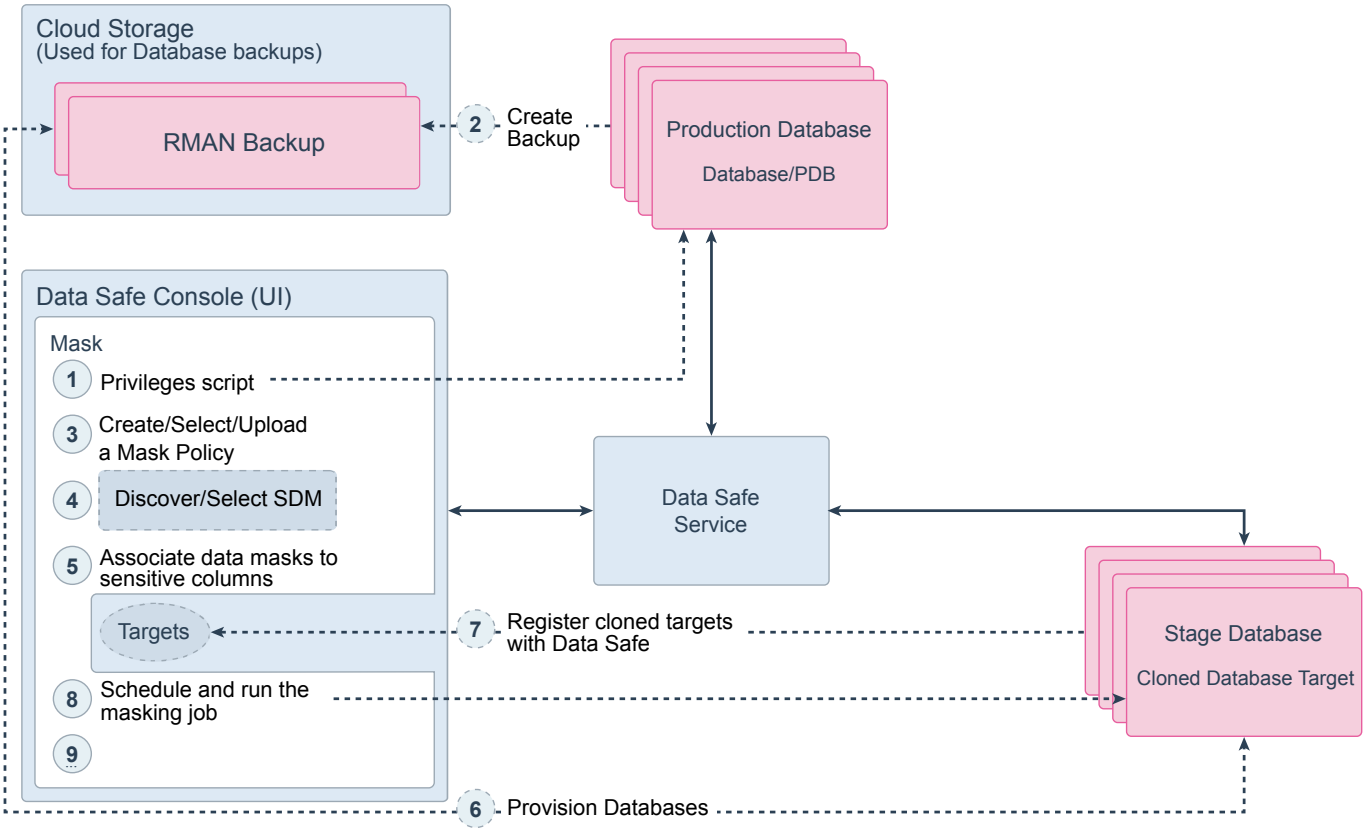
# Data Masking Task - Step 7




1. Before you can mask or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. If you are using ATP, all you need to do is to go to the ATP console and click register with Oracle Data Safe. It is all automatic.
2. Before masking data from your production databases, you need to create backups of your database targets. This is because you should never mask your production databases. In the process of masking data, you will reuse your database backups to create clones of your databases and use those clones to mask the data. You will then extract the masked data from these clones to create test and development databases on which you will import only the masked data. You could use the Oracle Cloud Storage service or any other backup location to store your production backups using RMAN for example.

3. To mask sensitive data, you must first define a masking policy on a Sensitive Data Model (SDM). A masking policy is mainly a container for mask formats you will define in the next steps.
4. If not done already through the Discovery functionality, you can run a discovery job from here too. This will allow you to create an SDM used with your Mask Policy. This step is optional and you could simply reuse an existing SDM done previously.
5. You can then create masking formats that will be used later to mask your sensitive data by replacing your sensitive data with realistic but fictitious data. Masking provides a comprehensive number of predefined mask formats to help you quickly mask data, such as shuffle, random numbers, and unique phone numbers. You can also create custom masks, such as fixed strings.
6. It is now time to create clones of your production databases you want to mask. You do so by using the backups you created. We call these clones, stage databases. They are not meant to be exposed to any user. They will be used to mask your sensitive data only. You must create a stage database on the Oracle Cloud with supported services. This step is optional if you already did it previously.
7. Once you created a stage database, you need to add it to your Oracle Data Safe service. You can do so directly from the Targets menu of your Oracle Data Safe Console.

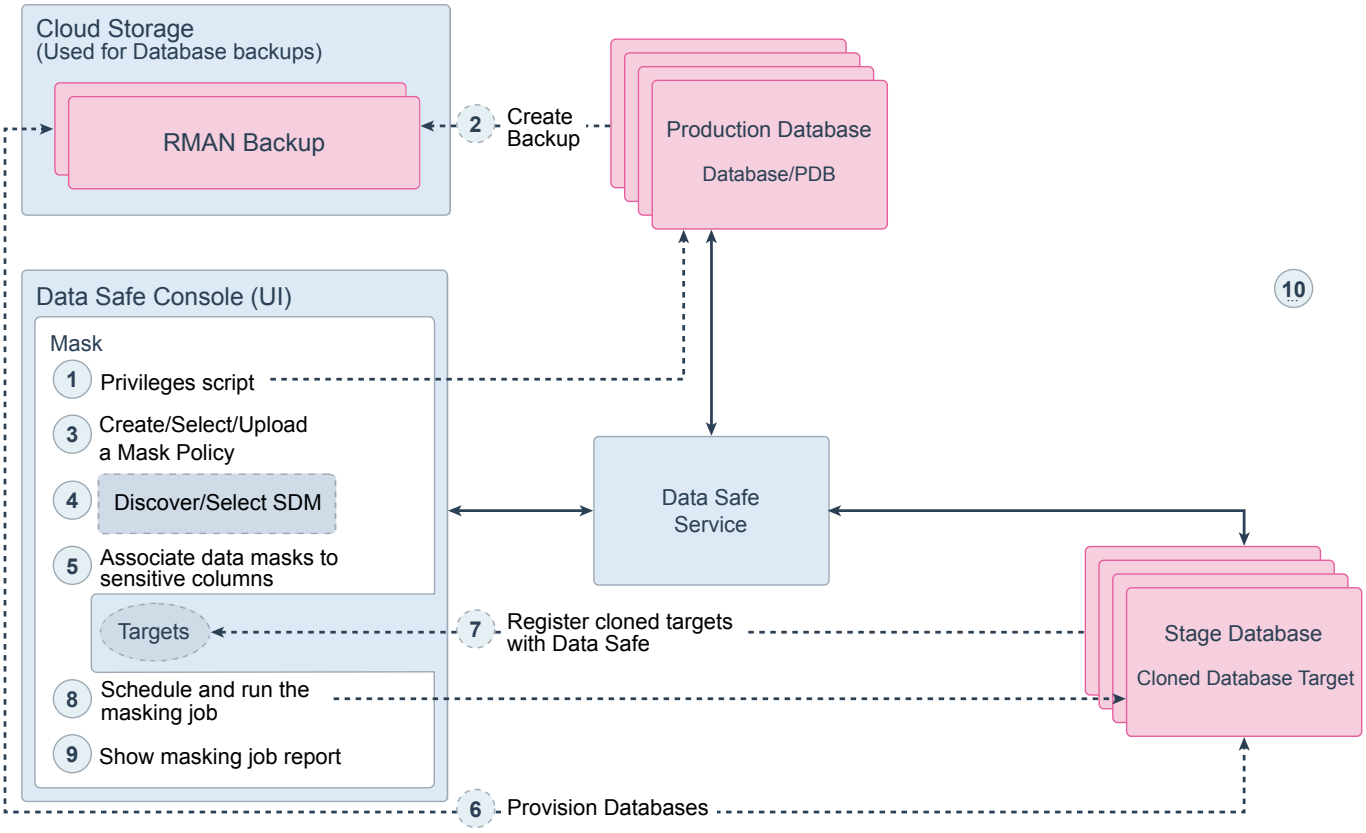
# Data Masking Task - Step 8




1. Before you can mask or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. If you are using ATP, all you need to do is to go to the ATP console and click register with Oracle Data Safe. It is all automatic.
2. Before masking data from your production databases, you need to create backups of your database targets. This is because you should never mask your production databases. In the process of masking data, you will reuse your database backups to create clones of your databases and use those clones to mask the data. You will then extract the masked data from these clones to create test and development databases on which you will import only the masked data. You could use the Oracle Cloud Storage service or any other backup location to store your production backups using RMAN for example.

3. To mask sensitive data, you must first define a masking policy on a Sensitive Data Model (SDM). A masking policy is mainly a container for mask formats you will define in the next steps.
4. If not done already through the Discovery functionality, you can run a discovery job from here too. This will allow you to create an SDM used with your Mask Policy. This step is optional and you could simply reuse an existing SDM done previously.
5. You can then create masking formats that will be used later to mask your sensitive data by replacing your sensitive data with realistic but fictitious data. Masking provides a comprehensive number of predefined mask formats to help you quickly mask data, such as shuffle, random numbers, and unique phone numbers. You can also create custom masks, such as fixed strings.
6. It is now time to create clones of your production databases you want to mask. You do so by using the backups you created. We call these clones, stage databases. They are not meant to be exposed to any user. They will be used to mask your sensitive data only. You must create a stage database on the Oracle Cloud with supported services. This step is optional if you already did it previously.
7. Once you created a stage database, you need to add it to your Oracle Data Safe service. You can do so directly from the Targets menu of your Oracle Data Safe Console.
8. You can now execute a Masking job to actually mask the sensitive data of your stage database.

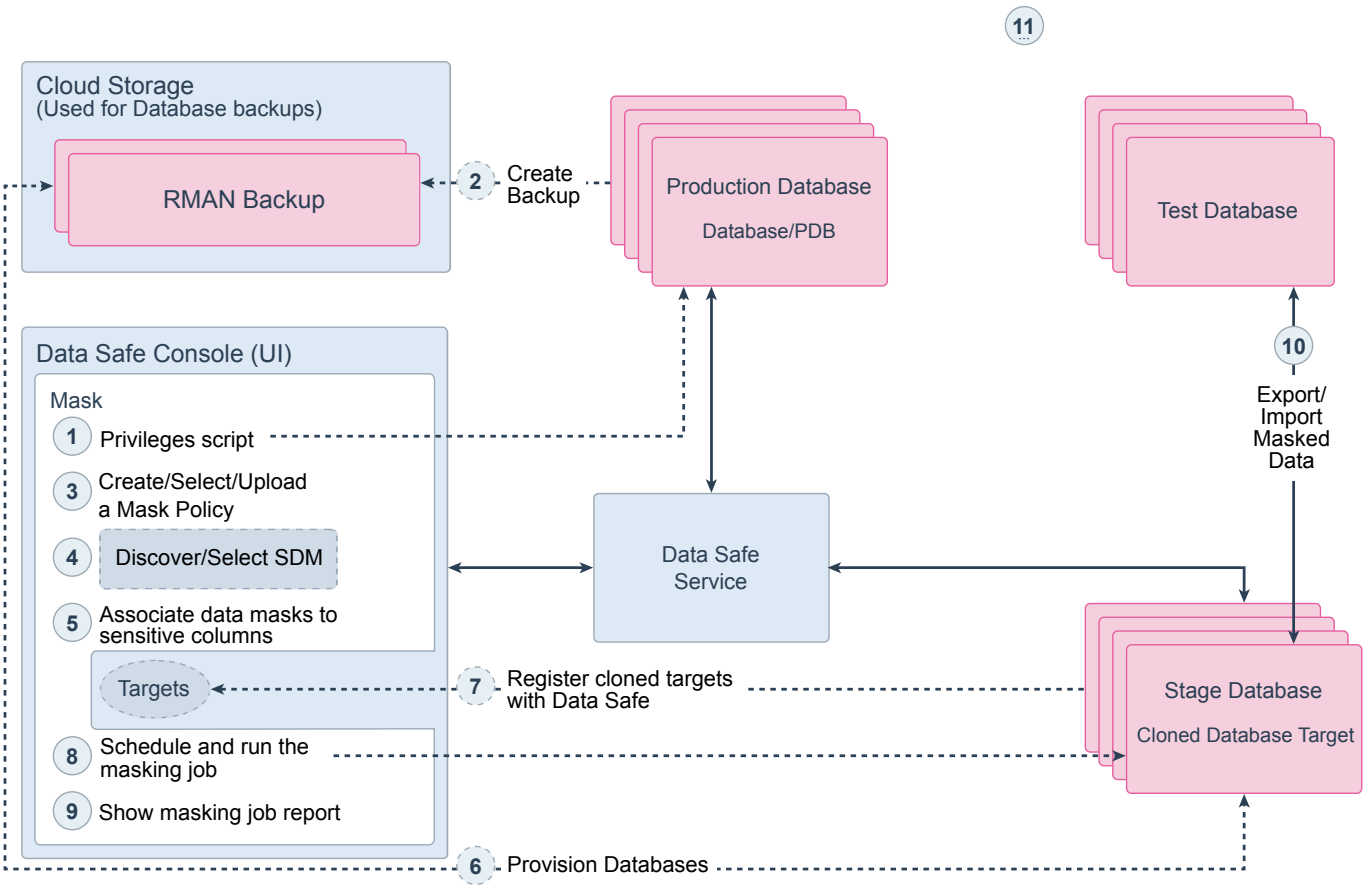
# Data Masking Task - Step 9




1. Before you can mask or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. If you are using ATP, all you need to do is to go to the ATP console and click register with Oracle Data Safe. It is all automatic.
2. Before masking data from your production databases, you need to create backups of your database targets. This is because you should never mask your production databases. In the process of masking data, you will reuse your database backups to create clones of your databases and use those clones to mask the data. You will then extract the masked data from these clones to create test and development databases on which you will import only the masked data. You could use the Oracle Cloud Storage service or any other backup location to store your production backups using RMAN for example.

3. To mask sensitive data, you must first define a masking policy on a Sensitive Data Model (SDM). A masking policy is mainly a container for mask formats you will define in the next steps.
4. If not done already through the Discovery functionality, you can run a discovery job from here too. This will allow you to create an SDM used with your Mask Policy. This step is optional and you could simply reuse an existing SDM done previously.
5. You can then create masking formats that will be used later to mask your sensitive data by replacing your sensitive data with realistic but fictitious data. Masking provides a comprehensive number of predefined mask formats to help you quickly mask data, such as shuffle, random numbers, and unique phone numbers. You can also create custom masks, such as fixed strings.
6. It is now time to create clones of your production databases you want to mask. You do so by using the backups you created. We call these clones, stage databases. They are not meant to be exposed to any user. They will be used to mask your sensitive data only. You must create a stage database on the Oracle Cloud with supported services. This step is optional if you already did it previously.
7. Once you created a stage database, you need to add it to your Oracle Data Safe service. You can do so directly from the Targets menu of your Oracle Data Safe Console.
8. You can now execute a Masking job to actually mask the sensitive data of your stage database.
9. A report is generated and you can view it to look at the results of your masking job.

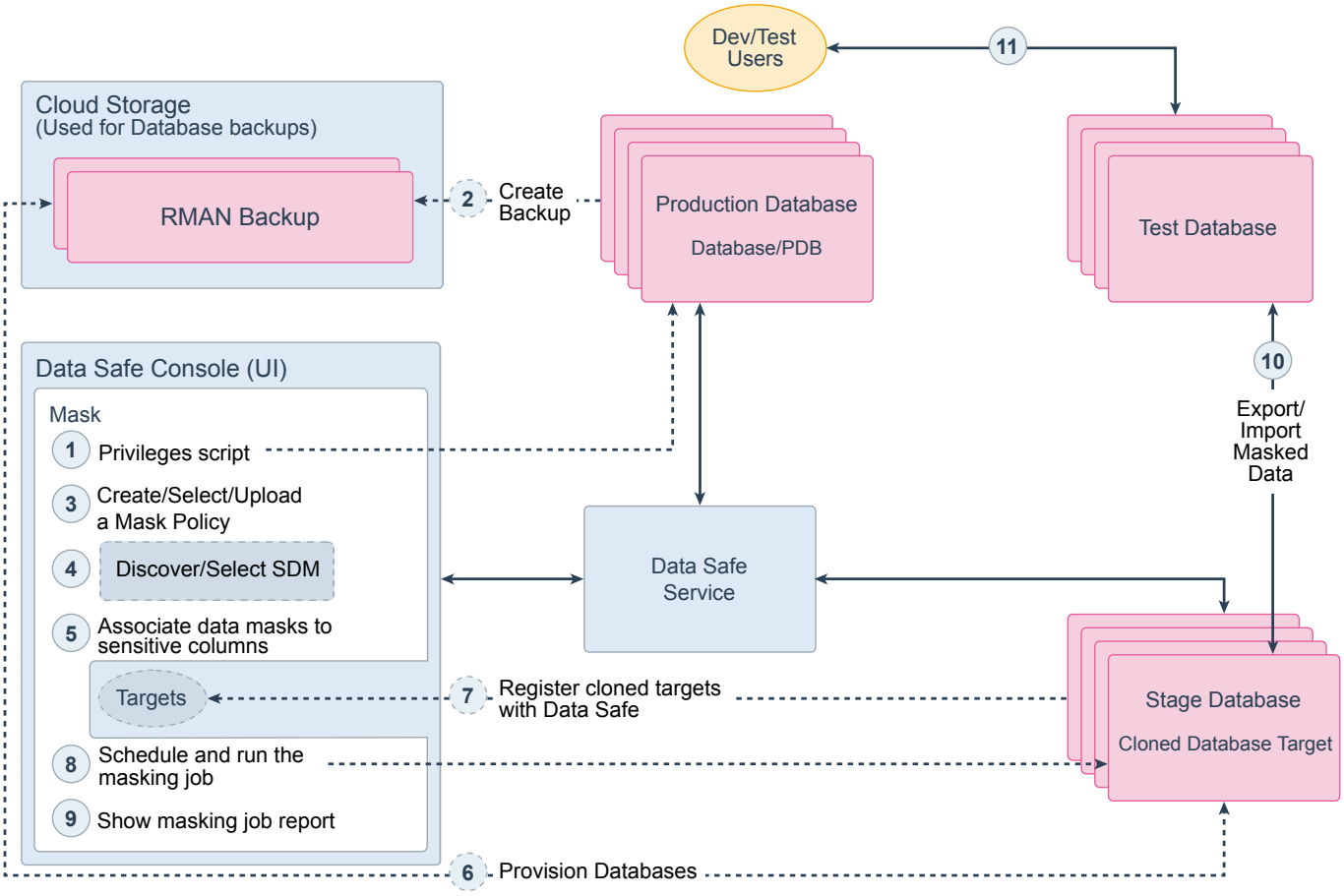
# Data Masking Task - Step 10




1. Before you can mask or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. If you are using ATP, all you need to do is to go to the ATP console and click register with Oracle Data Safe. It is all automatic.
2. Before masking data from your production databases, you need to create backups of your database targets. This is because you should never mask your production databases. In the process of masking data, you will reuse your database backups to create clones of your databases and use those clones to mask the data. You will then extract the masked data from these clones to create test and development databases on which you will import only the masked data. You could use the Oracle Cloud Storage service or any other backup location to store your production backups using RMAN for example.

3. To mask sensitive data, you must first define a masking policy on a Sensitive Data Model (SDM). A masking policy is mainly a container for mask formats you will define in the next steps.
4. If not done already through the Discovery functionality, you can run a discovery job from here too. This will allow you to create an SDM used with your Mask Policy. This step is optional and you could simply reuse an existing SDM done previously.
5. You can then create masking formats that will be used later to mask your sensitive data by replacing your sensitive data with realistic but fictitious data. Masking provides a comprehensive number of predefined mask formats to help you quickly mask data, such as shuffle, random numbers, and unique phone numbers. You can also create custom masks, such as fixed strings.
6. It is now time to create clones of your production databases you want to mask. You do so by using the backups you created. We call these clones, stage databases. They are not meant to be exposed to any user. They will be used to mask your sensitive data only. You must create a stage database on the Oracle Cloud with supported services. This step is optional if you already did it previously.
7. Once you created a stage database, you need to add it to your Oracle Data Safe service. You can do so directly from the Targets menu of your Oracle Data Safe Console.
8. You can now execute a Masking job to actually mask the sensitive data of your stage database.
9. A report is generated and you can view it to look at the results of your masking job.
10. Instead of giving access to your stage databases to test and developer users, we recommend you export only the masked data from the stage databases. Then you can create a new test database in which you import the masked data.

# Data Masking Task - Step 11



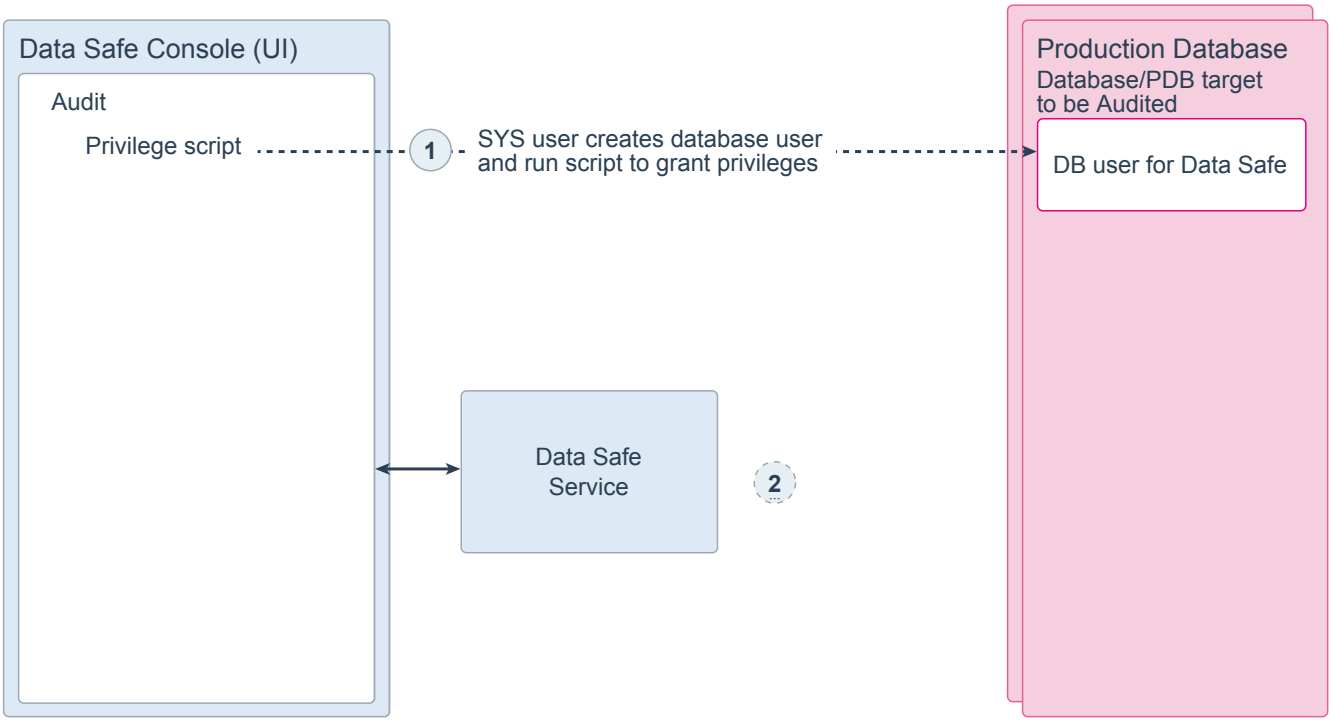

In Oracle Data Safe, you use the Masking Wizard to mask sensitive data. You can choose to use pre-built masking formats and policies or create your own. The system provides a masking report to give you a high level view of your masking activities and results.

Here we describe the recommended way of using the masking. However, another way is to connect to a test database and mask it directly.

1. Before you can mask or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. If you are using ATP, all you need to do is to go to the ATP console and click register with Oracle Data Safe. It is all automatic.

2. Before masking data from your production databases, you need to create backups of your database targets. This is because you should never mask your production databases. In the process of masking data, you will reuse your database backups to create clones of your databases and use those clones to mask the data. You will then extract the masked data from these clones to create test and development databases on which you will import only the masked data. You could use the Oracle Cloud Storage service or any other backup location to store your production backups using RMAN for example.
3. To mask sensitive data, you must first define a masking policy on a Sensitive Data Model (SDM). A masking policy is mainly a container for mask formats you will define in the next steps.
4. If not done already through the Discovery functionality, you can run a discovery job from here too. This will allow you to create an SDM used with your Mask Policy. This step is optional and you could simply reuse an existing SDM done previously.
5. You can then create masking formats that will be used later to mask your sensitive data by replacing your sensitive data with realistic but fictitious data. Masking provides a comprehensive number of predefined mask formats to help you quickly mask data, such as shuffle, random numbers, and unique phone numbers. You can also create custom masks, such as fixed strings.
6. It is now time to create clones of your production databases you want to mask. You do so by using the backups you created. We call these clones, stage databases. They are not meant to be exposed to any user. They will be used to mask your sensitive data only. You must create a stage database on the Oracle Cloud with supported services. This step is optional if you already did it previously.
7. Once you created a stage database, you need to add it to your Oracle Data Safe service. You can do so directly from the Targets menu of your Oracle Data Safe Console.
8. You can now execute a Masking job to actually mask the sensitive data of your stage database.
9. A report is generated and you can view it to look at the results of your masking job.
10. Instead of giving access to your stage databases to test and developer users, we recommend you export only the masked data from the stage databases. Then you can create a new test database in which you import the masked data.
11. At this point, you can grant access to your test databases to your test or developer users.

# Activity Auditing Task - Step 1



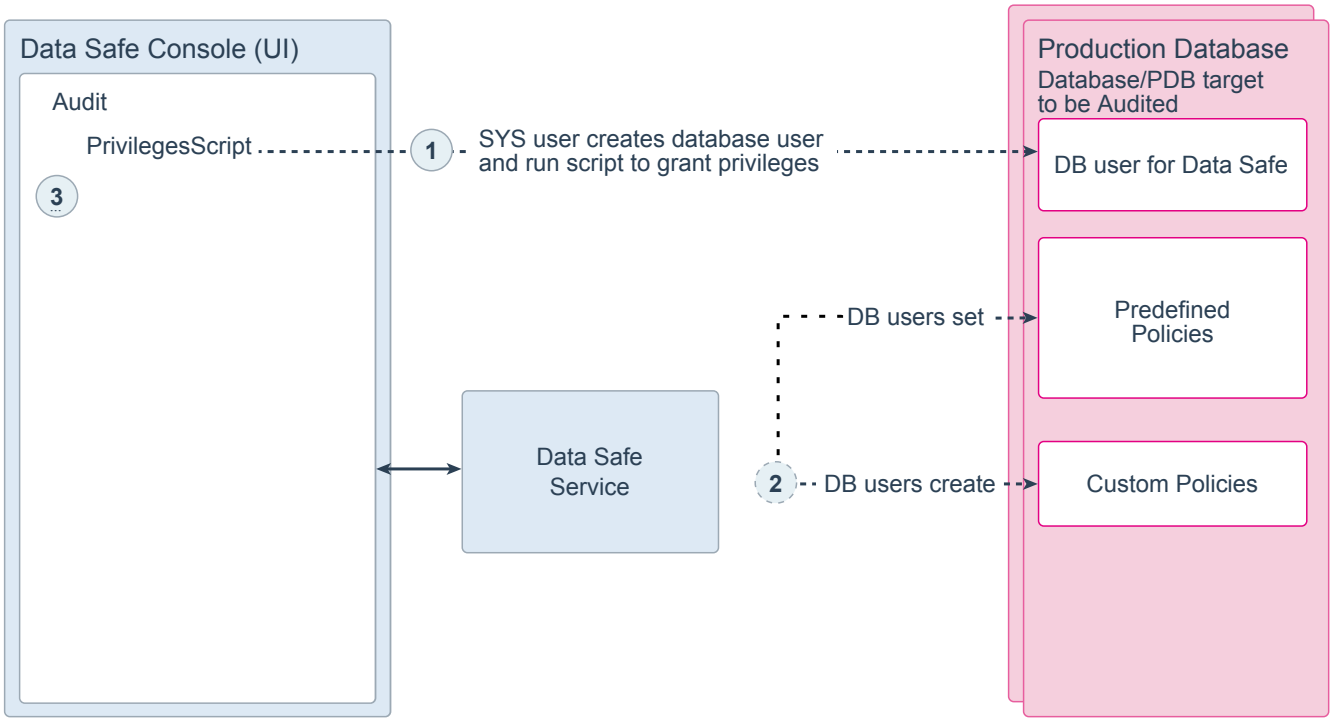

With Oracle Data Safe, you use the Activity Auditing Wizard to audit activities on selected databases, collect information, and trigger real-time alerts.

For more information, watch the Provision Audit and Alert Policies video and Analyze Audit Records and Alerts video.

Here we describe the steps for using Activity Auditing:

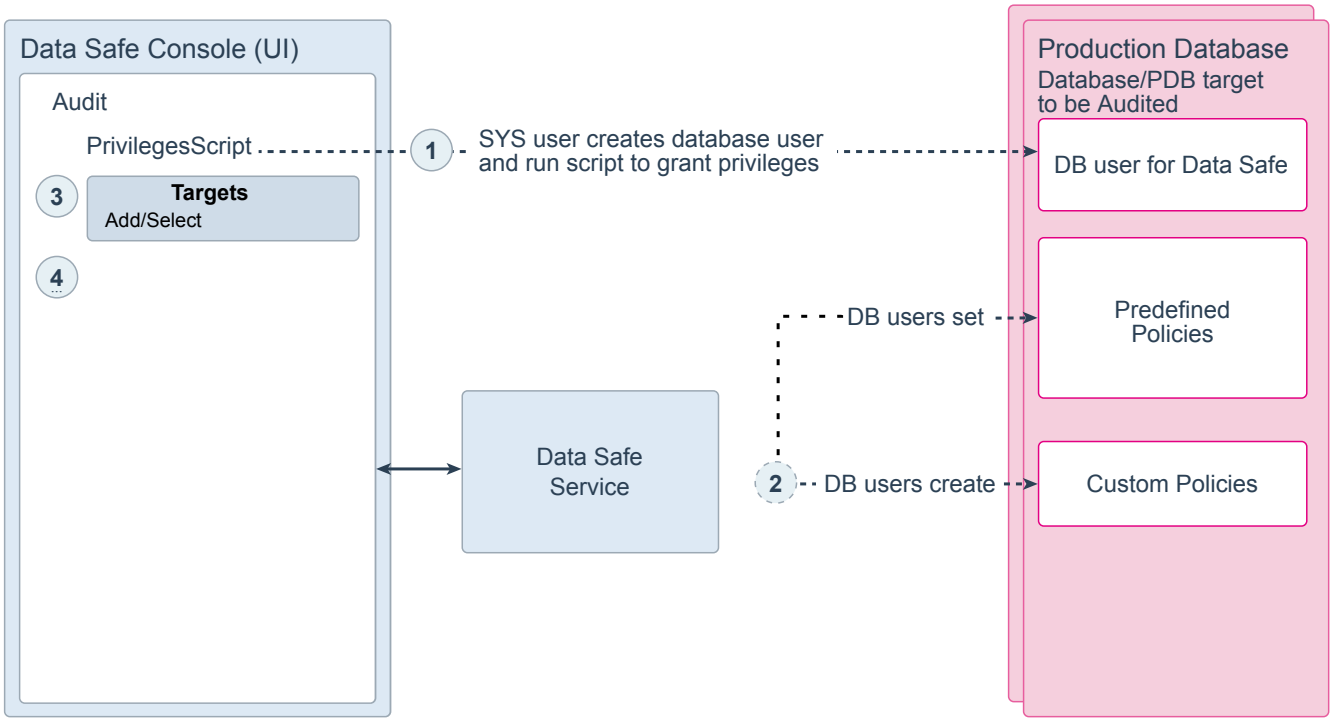
1. Before you can audit or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. If you are using an ATP database, then you go the ATP console where you can register it with Oracle Data Safe automatically once Oracle Data Safe has been enabled in your region.

# Activity Auditing Task - Step 2



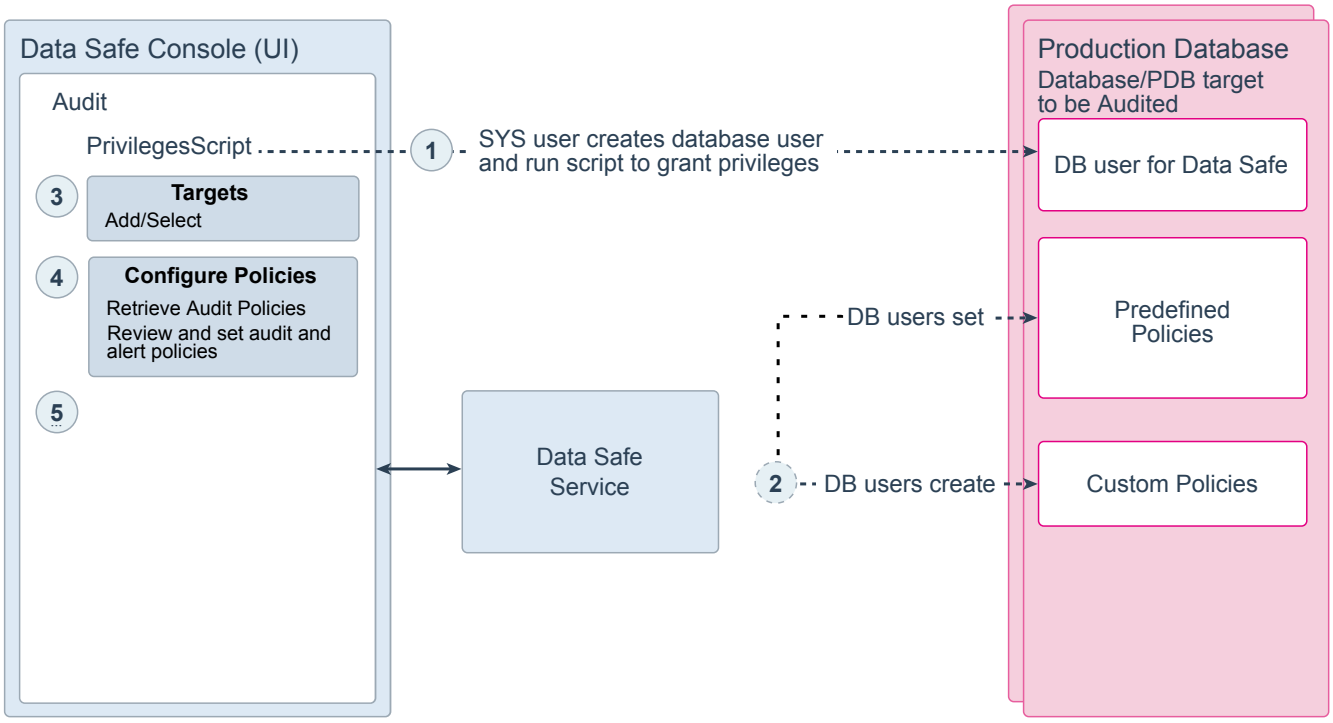

1. Before you can audit or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. If you are using an ATP database, then you go the ATP console where you can register it with Oracle Data Safe automatically once Oracle Data Safe has been enabled in your region.
2. As a Database Administrator you can setup predefined and custom policies directly on your database. Oracle Data Safe will retrieve those. This step is optional.

# Activity Auditing Task - Step 3




1. Before you can audit or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. If you are using an ATP database, then you go the ATP console where you can register it with Oracle Data Safe automatically once Oracle Data Safe has been enabled in your region.
2. As a Database Administrator you can setup predefined and custom policies directly on your database. Oracle Data Safe will retrieve those. This step is optional.
3. You select or add database targets to audit.

# Activity Auditing Task - Step 4



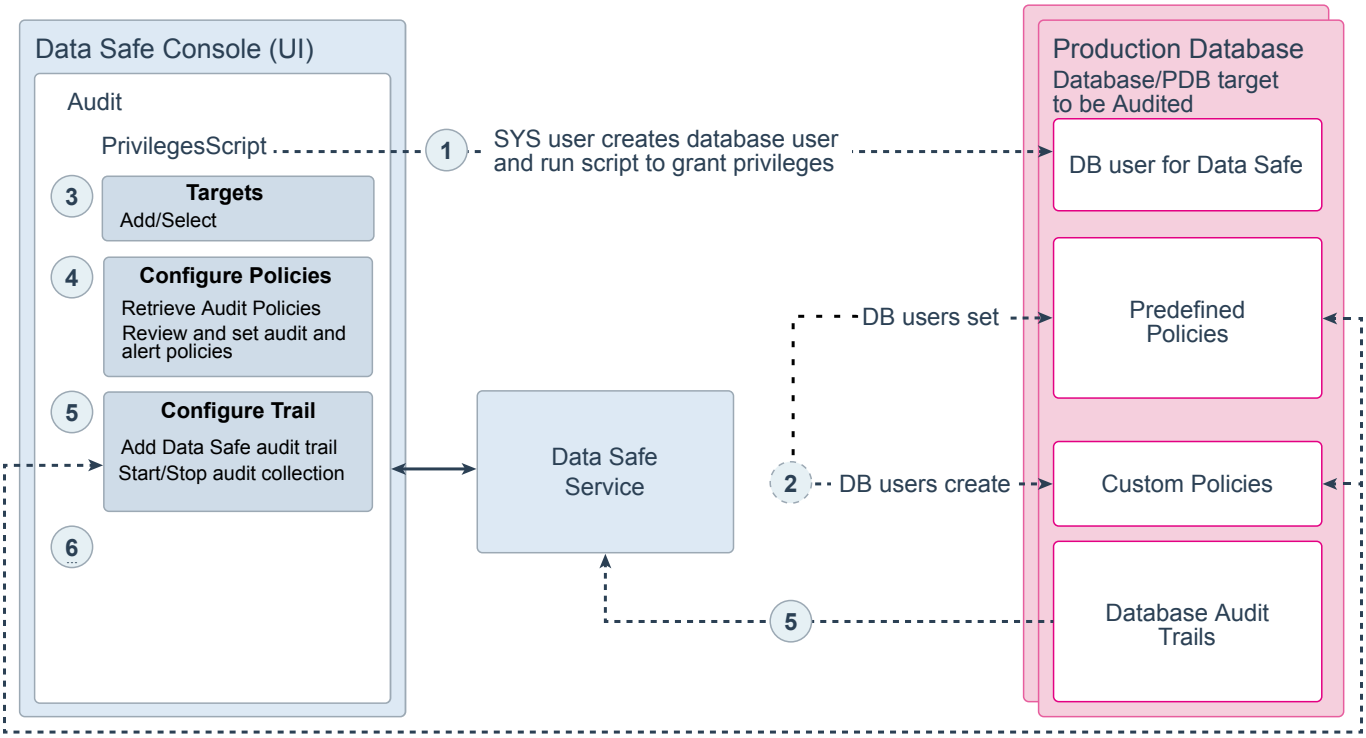

1. Before you can audit or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. If you are using an ATP database, then you go the ATP console where you can register it with Oracle Data Safe automatically once Oracle Data Safe has been enabled in your region.
2. As a Database Administrator you can setup predefined and custom policies directly on your database. Oracle Data Safe will retrieve those. This step is optional.
3. You select or add database targets to audit.
4. The wizard retrieves the predefined and custom policies that are currently set on your database target and also allows you to enable/disable those as well as allowing you to define and enable pre-defined Oracle Data Safe policies on your database target:
    - Basic Auditing: critical database activities, logon events, and database schema changes
    - Admin User Activity Auditing: all administrator-type activities
    - User Activity Auditing: specify particular users and audit all their activities

- Audit Compliance Standard: all users based on the Center for Internet Security (CIS) standards

In addition, you can activate pre-defined alert policies for selected target databases independently from audit policies. For example, an alert is triggered in the Oracle Data Safe Console if a user fails to log in to the target database after three tries. You have a set of alerts you can choose from like failed logins, user creation and deletion, user privileges changes, database parameter changes, and changes in audit settings.

For more information, watch the Provision Auditing and Alerts video

# Activity Auditing Task - Step 5




1. Before you can audit or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. If you are using an ATP database, then you go the ATP console where you can register it with Oracle Data Safe automatically once Oracle Data Safe has been enabled in your region.
2. As a Database Administrator you can setup predefined and custom policies directly on your database. Oracle Data Safe will retrieve those. This step is optional.
3. You select or add database targets to audit.
4. The wizard retrieves the predefined and custom policies that are currently set on your database target and also allows you to enable/disable those as well as allowing you to define and enable pre-defined Oracle Data Safe policies on your database target:
    - Basic Auditing: critical database activities, logon events, and database schema changes
    - Admin User Activity Auditing: all administrator-type activities
    - User Activity Auditing: specify particular users and audit all their activities

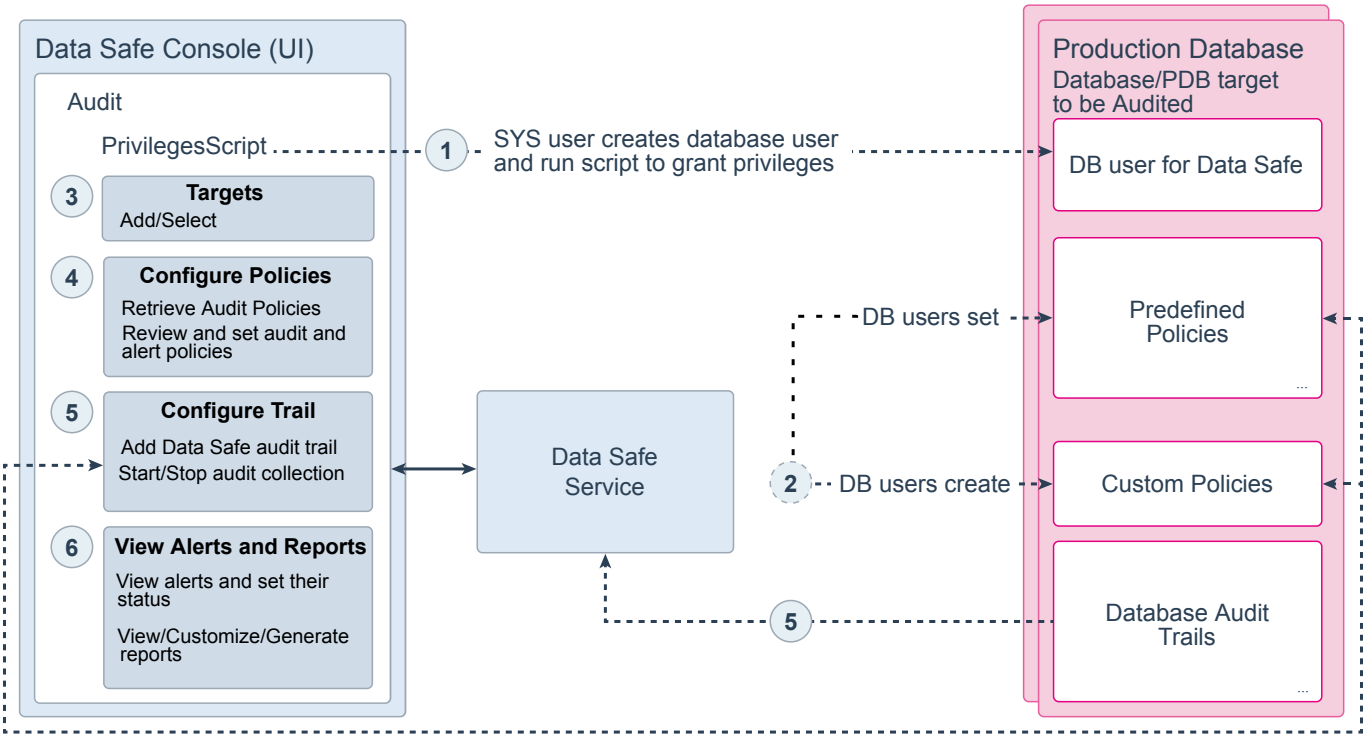
- Audit Compliance Standard: all users based on the Center for Internet Security (CIS) standards

In addition, you can activate pre-defined alert policies for selected target databases independently from audit policies. For example, an alert is triggered in the Oracle Data Safe Console if a user fails to log in to the target database after three tries. You have a set of alerts you can choose from like failed logins, user creation and deletion, user privileges changes, database parameter changes, and changes in audit settings.

For more information, watch the Provision Auditing and Alerts video

5. Once your audit policies and alerts are defined, you have the possibility to configure the Oracle Data Safe trail. Oracle Data Safe trail is a repository stored in your Oracle Data Safe tenancy that contains all the captured audit records from your target databases. When you define a Oracle Data Safe trail, you specify the list of source database audit trails you want to capture from as well as two other parameters: the retention period in the Oracle Data Safe trail which is six months by default, and whether you want to purge the database audit trails each time Oracle Data Safe has collected their data successfully. The purge will be done only on database audit trail records that are one week older than the last successful Oracle Data Safe capture time. When you define a Oracle Data Safe trail, Oracle Data Safe automatically starts capturing the information from your associated database target. However, you also have the possibility to pause the capture process and start it up again whenever you want. This might be useful for example when your target database is shutdown for maintenance purposes. Note that each time you start a Oracle Data Safe trail, it is automatically purged.

# Activity Auditing Task - Step 6




With Oracle Data Safe, you use the Activity Auditing Wizard to audit activities on selected databases, collect information, and trigger real-time alerts.

1. Before you can audit or use any Oracle Data Safe functionality on an Oracle Cloud database, you need to manually create a user and then execute a script to grant certain privileges to that database user. You must do so as user SYS or ADMIN. The privilege script can provision the database user with just the privileges it needs for the supported Oracle Data Safe functionality on that database target. If a different Oracle Data Safe functionality needs to be run against the target database, the privilege script will need to be run again to grant additional required privileges. The privilege script also allows all Oracle Data Safe required privileges to be granted. If you are using an ATP database, then you go the ATP console where you can register it with Oracle Data Safe automatically once Oracle Data Safe has been enabled in your region.
2. As a Database Administrator you can setup predefined and custom policies directly on your database. Oracle Data Safe will retrieve those. This step is optional.
3. You select or add database targets to audit.
4. The wizard retrieves the predefined and custom policies that are currently set on your database target and also allows you to enable/disable those as well as allowing you to define and enable pre-defined Oracle Data Safe policies on your database target:

- Basic Auditing: critical database activities, logon events, and database schema changes
- Admin User Activity Auditing: all administrator-type activities
- User Activity Auditing: specify particular users and audit all their activities
- Audit Compliance Standard: all users based on the Center for Internet Security (CIS) standards

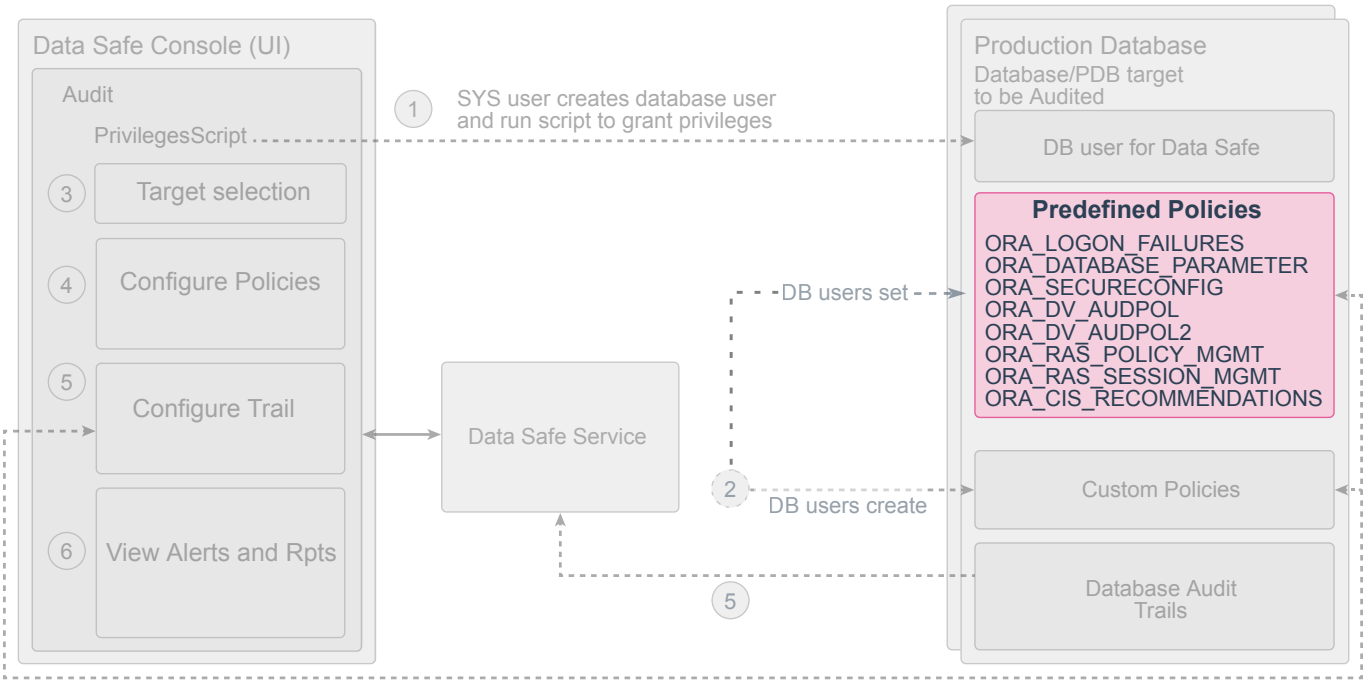
In addition, you can activate pre-defined alert policies for selected target databases independently from audit policies. For example, an alert is triggered in the Oracle Data Safe Console if a user fails to log in to the target database after three tries. You have a set of alerts you can choose from like failed logins, user creation and deletion, user privileges changes, database parameter changes, and changes in audit settings.

For more information, watch the Provision Auditing and Alerts video

5. Once your audit policies and alerts are defined, you have the possibility to configure the Oracle Data Safe trail. Oracle Data Safe trail is a repository stored in your Oracle Data Safe tenancy that contains all the captured audit records from your target databases. When you define a Oracle Data Safe trail, you specify the list of source database audit trails you want to capture from as well as two other parameters: the retention period in the Oracle Data Safe trail which is six months by default, and whether you want to purge the database audit trails each time Oracle Data Safe has collected their data successfully. The purge will be done only on database audit trail records that are one week older than the last successful Oracle Data Safe capture time. When you define an Oracle Data Safe trail, Oracle Data Safe automatically starts capturing the information from your associated database target. However, you also have the possibility to pause the capture process and start it up again whenever you want. This might be useful for example when your target database is shutdown for maintenance purposes. Note that each time you start a Oracle Data Safe trail, it is automatically purged.
6. You then have the possibility to view various customizable reports to look at auditing activity on your targets as well as looking at alert reports.

   For more information, watch the Analyze Audit Records and Alerts video

# Database Auditing Policies

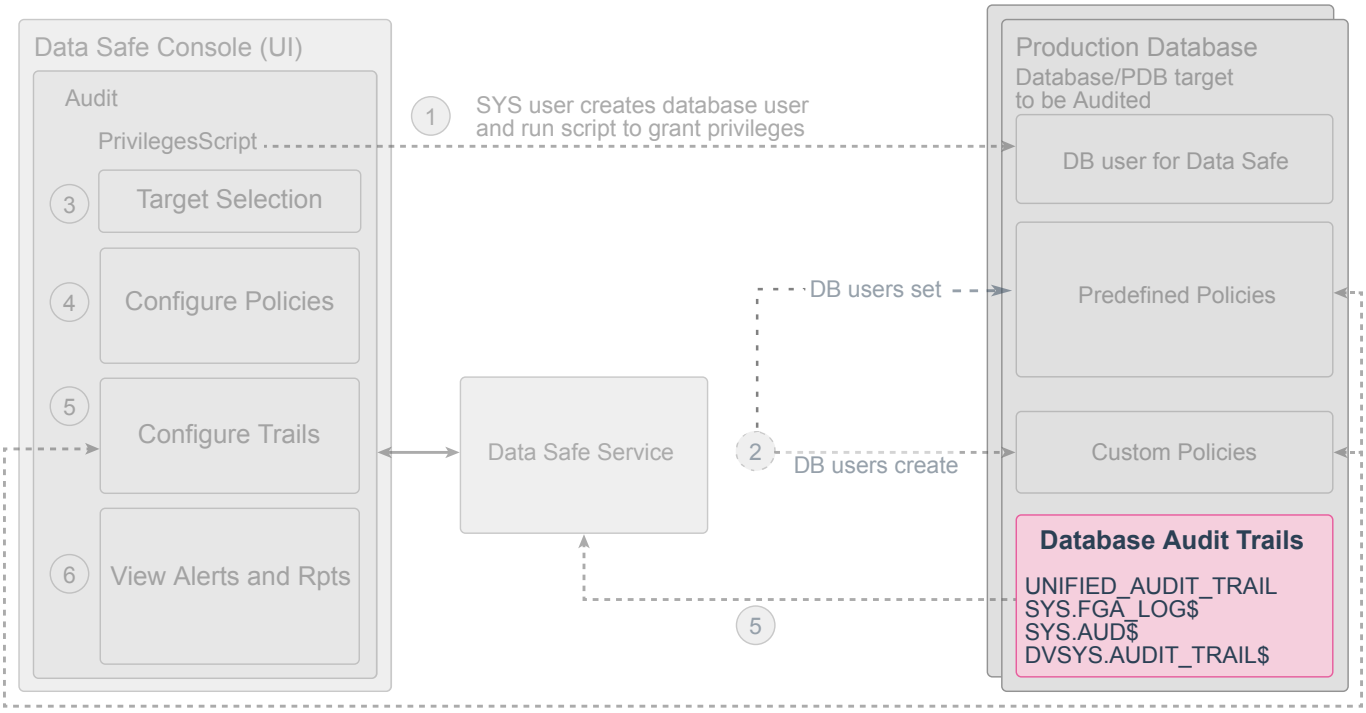



The possible predefined policies you can set as a database administrator on your database targets are:

- `ORA_DATABASE_PARAMETER`
- `ORA_LOGON_FAILURES`
- `ORA_SECURE_CONFIG`
- `ORA_RAS_SESSION_MGMT`
- `ORA_RAS_POLICY_MGMT`
- `ORA_DV_AUDPOL`
- `ORA_DV_AUDPOL2`
- `ORA_CIS_RECOMMENDATIONS`

For more information about predefined unified audit policies see Auditing Activities with the Predefined Unified Audit Policies.

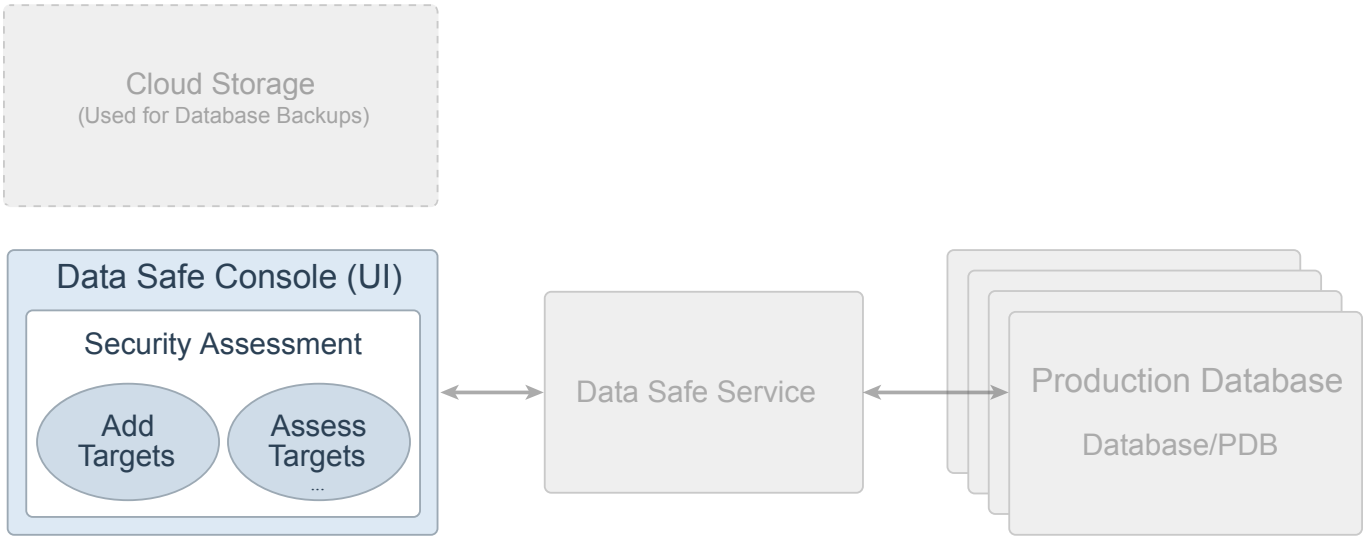
# Database Audit Trails




The source of an Oracle Data Safe trail are the following associated database target audit trails:

- `AUDSYS.UNIFIED_AUDIT_TRAIL`
- `SYS.FGA_LOG$`
- `SYS.AUD$`
- `DVSYS.AUDIT_TRAIL$`

# Security Assessment Task

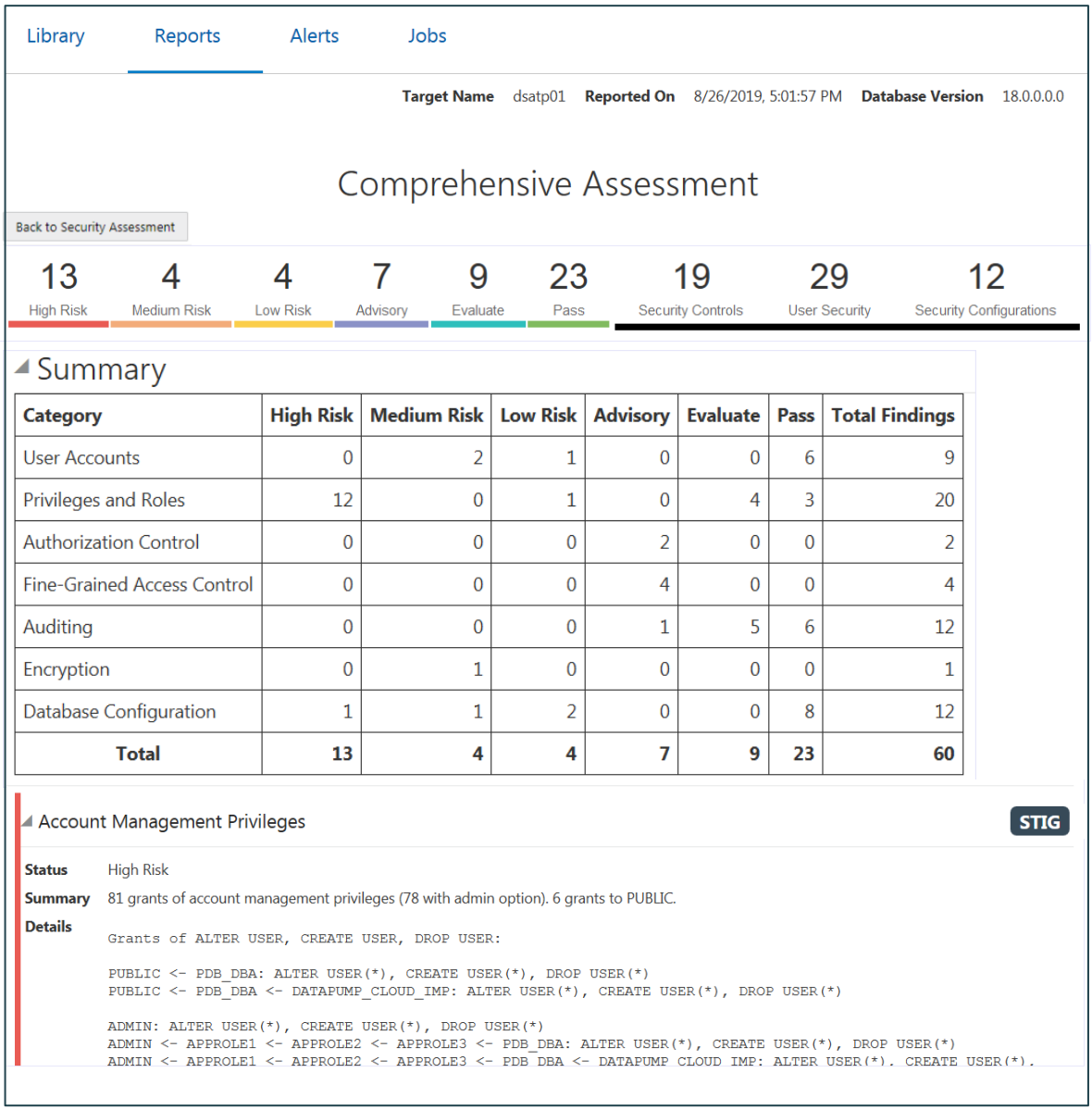



In Oracle Data Safe, you use the Security Assessment and User Assessment interfaces to assess the risks of the current configurations of your target databases and their associated users.

From the Security Assessment page in your Oracle Data Safe Console, you can add database targets and view various reports.

For more information, watch the Assess Database and User Configurations video.

# Security Assessment Reports

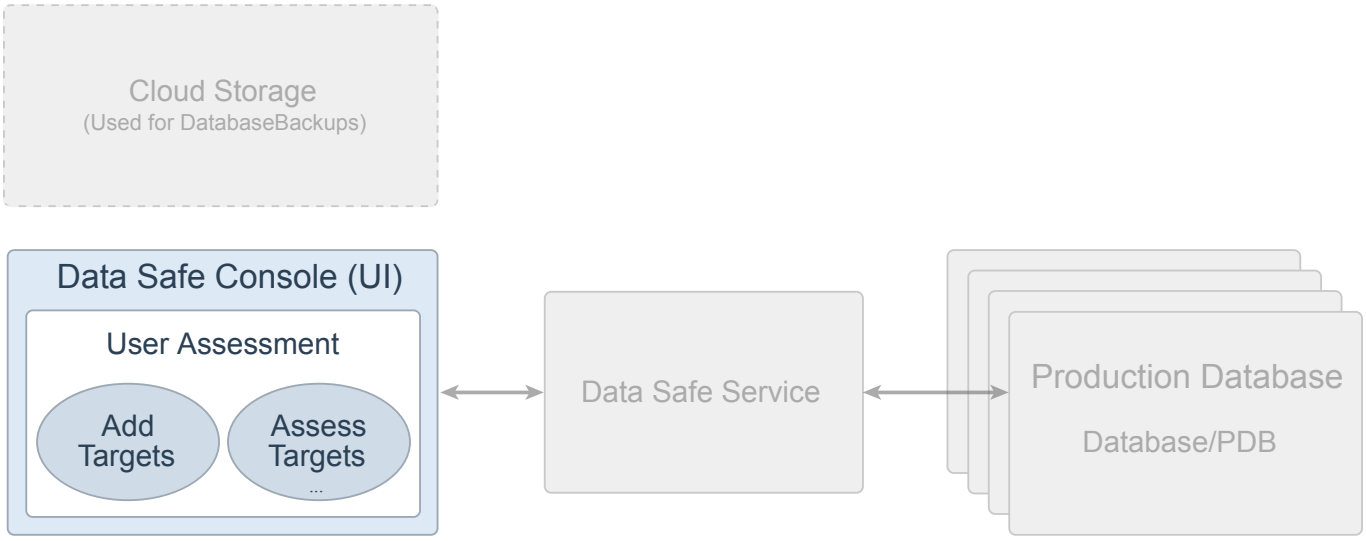



The Security Assessment feature in Oracle Data Safe provides a comprehensive report broken down into several categories, including user accounts, privileges and roles, authorization control, data encryption, fine-grained access control, auditing, and database configuration.

At the top of the report are totals for each risk level, providing you a high-level view of the security status of your target database. Each risk level is color coded. You can also view the total number of findings for each high-level category in the report, including security controls, user security, and security configurations. Each main category in the report is divided into several subcategories, which are also color-coded based on risk level.

You also get recommendations on how to fix issues found on your targets.

# User Assessment Task

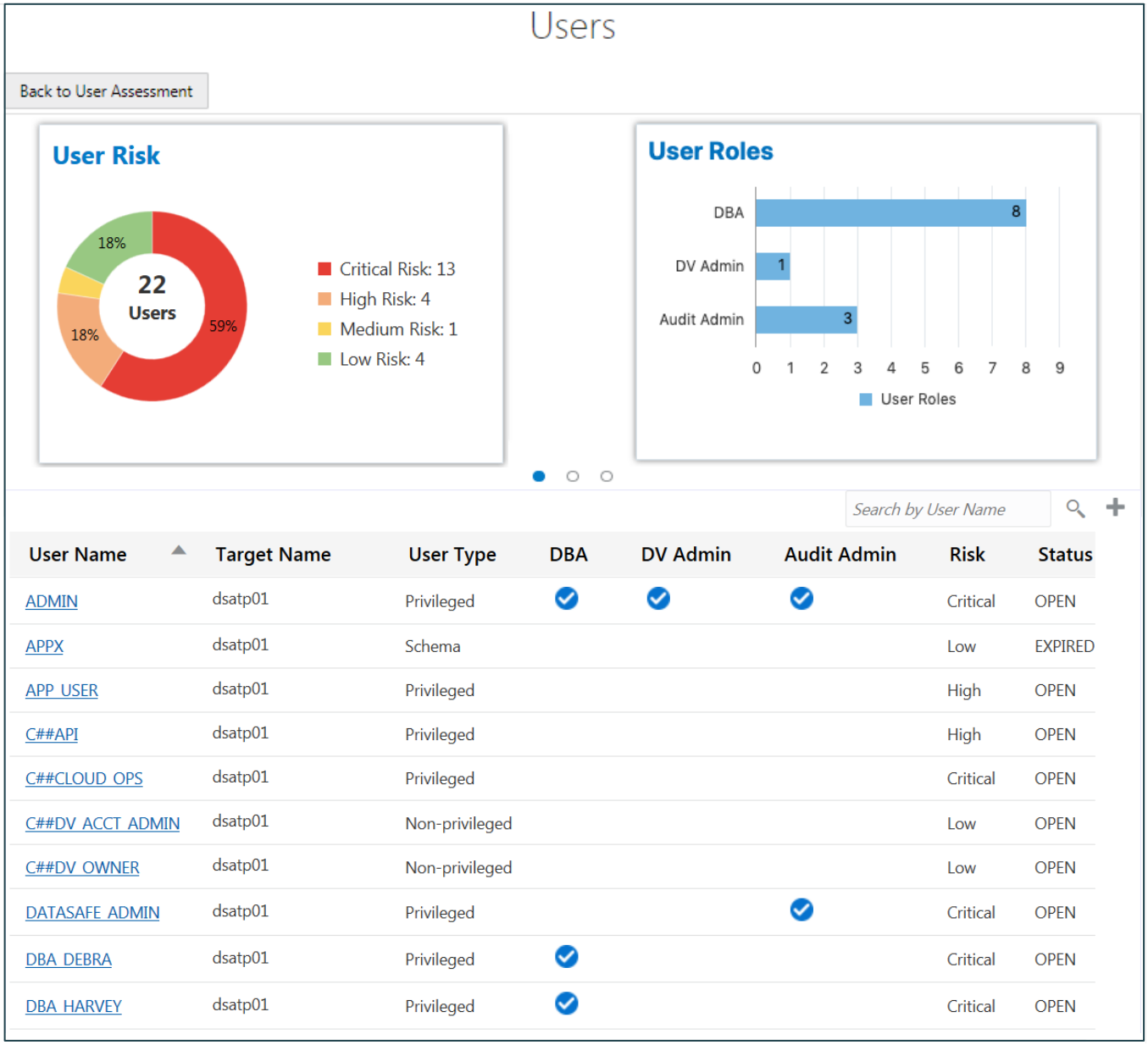



In Oracle Data Safe, you use the Security Assessment and User Assessment interfaces to assess the risks of the current configurations of your target databases and their associated users.

From the User Assessment page in your Oracle Data Safe Console, you can add database targets and view various reports.

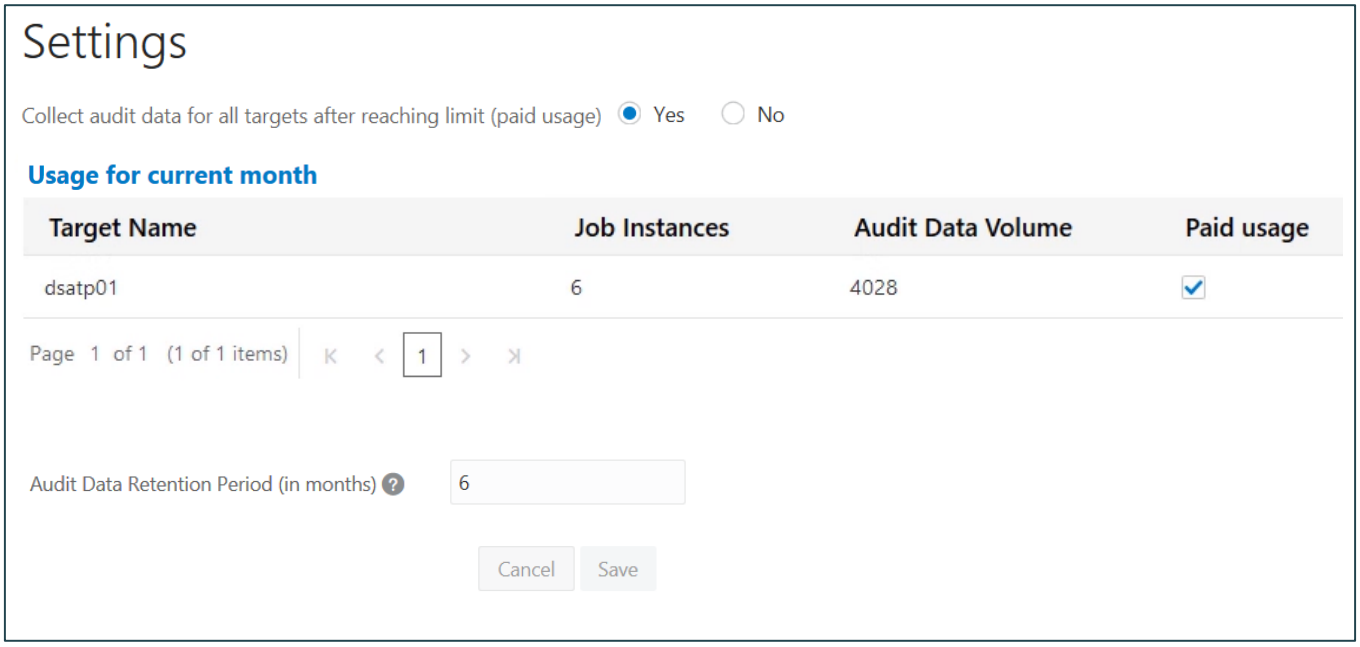
For more information, watch the Assess Database and User Configurations video.

# User Assessment Reports




The User Assessment feature in Oracle Data Safe enables you to identify user settings in your target databases and the risks associated with those users. A user assessment provides important information about each user in a target database: The user type, its risk level, its status (`OPEN`, `LOCKED`, or `EXPIRED & LOCKED`), its last login time, its creation date, and much more.

# Settings

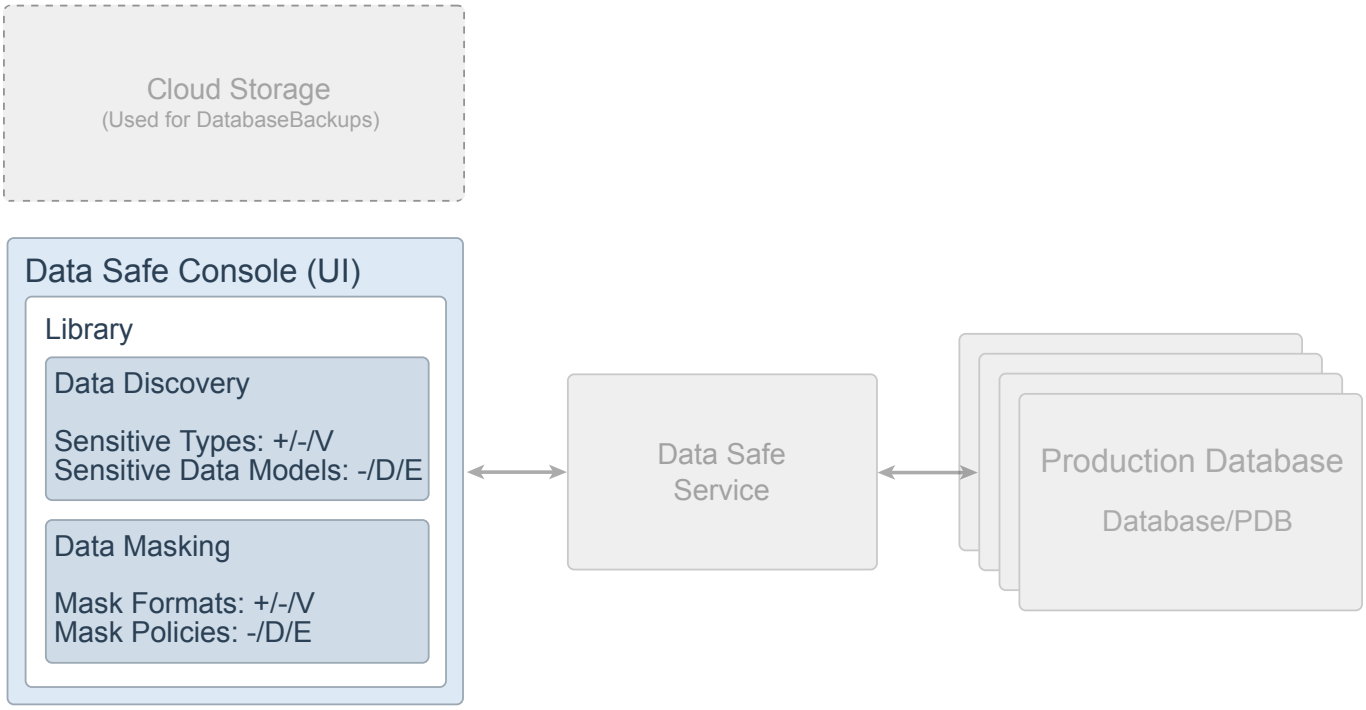



The Settings page allows you to set up the retention time default value for your Oracle Data Safe trail, which is six months by default. On the Settings page, you can also set a global preference for all targets to continue collecting audit data after the allowed number of audit records is reached, or you can select particular target databases. You have to pay to collect audit data beyond the limit.

Am Oracle Data Safe trail is a repository stored in your Oracle Data Safe tenancy that contains all the captured audit records from your target databases. When you define an Oracle Data Safe trail from the Auditing Activity wizard, you specify the list of source database audit trails you want to capture from as well as two other parameters: the retention period in the Oracle Data Safe trail which is six months by default, and whether you want to purge the database audit trails each time Oracle Data Safe has collected their data.

When you define an Oracle Data Safe trail, Oracle Data Safe automatically starts capturing the information from your associated database target. However, you also have the possibility to pause the capture process and start it up again whenever you want. This might be useful for example when your target database is shutdown for maintenance purposes. Note that each time you start an Oracle Data Safe trail, it is automatically purged.

# Viewing Library Resources

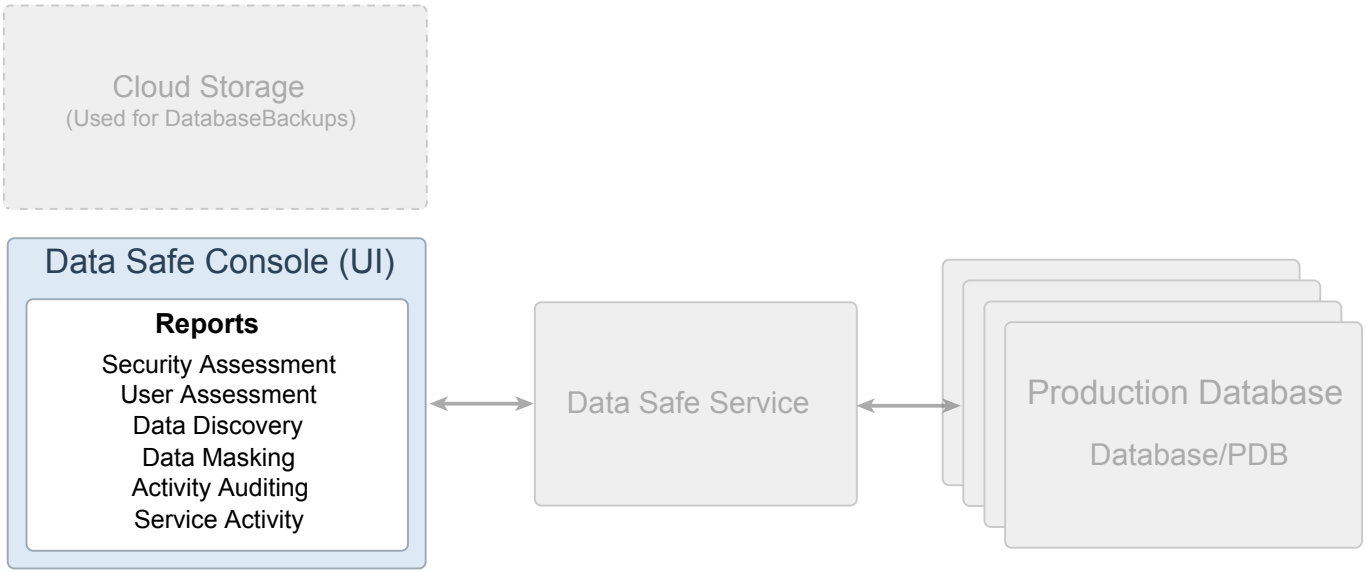



The Library page from the Oracle Data Safe Console shows you all the metadata you can currently use for masking data on your database targets:

- Sensitive types: Properties that define sensitive data using regular expressions.
- Sensitive Data Models: Containers of sensitive data types in target databases.
- Mask Formats: Formats used for masking sensitive data.
- Mask Policies: Mask policies mapping sensitive columns with mask formats.

You can manipulate these entries from this page (- to delete, + to add, E for editing, D for download, and V for view).

# Viewing Reports




Oracle Data Safe generates Security Assessment, User Assessment, Data Discovery, Data Masking, Activity Auditing, and Service Activity reports. You can customize reports as needed.