Oracle® Cloud

Administering Oracle Data Safe

F42511-55
July 2025

Oracle Cloud Administering Oracle Data Safe,

F42511-55

Copyright © 2021, 2025, Oracle and/or its affiliates.

Primary Authors: Jody Glover, Anna Haikl, Frederick Kush, Rachel Voirin

Contents

Preface

Audience xv
Documentation Accessibility xv
Conventions xv
Related Resources xv

1 Getting Started

Oracle Data Safe Overview 1-1
- Features of Oracle Data Safe 1-1
- Oracle Data Safe Guided Tour 1-2
- Key Concepts and Terminology 1-2

Oracle Data Safe Architecture 1-5
- Oracle Data Safe Service 1-5
- Oracle Data Safe Database Repository 1-6
- Target Databases 1-6

Access Oracle Data Safe 1-7

2 Oracle Data Safe Security

Security Overview 2-1
- Security Levels 2-1
- Administrator Types 2-1
- Regions 2-1
- Compartments 2-3
- Users and Groups 2-5
  - Native Users and Groups 2-5
  - Federated Users and Groups 2-6
- IAM Policies 2-7

Tasks that Require Permissions 2-7
OCI Resources for Oracle Data Safe 2-8
- data-safe-family Resource 2-8
- Target Registration Resources 2-9
  - autonomous-database Resource 2-10

data-safe-private-endpoints Resource 2-10
onprem-connectors Resource 2-11
target-databases Resource 2-12
Virtual Cloud Networking Resources 2-12
Activity Auditing Resources 2-13
data-safe-audit-family Resource 2-13
data-safe-archive-retrievals Resource 2-14
data-safe-audit-events Resource 2-14
data-safe-audit-policies Resource 2-15
data-safe-audit-profiles Resource 2-15
data-safe-audit-trails Resource 2-15
Security and User Assessment Resources 2-16
data-safe-assessment-family Resource 2-16
security-assessments Resource 2-16
user-assessments Resource 2-17
data-safe-security-policy-reports Resource 2-17
Data Discovery Resources 2-18
data-safe-discovery-family Resource 2-18
data-safe-discovery-jobs Resource 2-19
data-safe-sensitive-data-models Resource 2-19
data-safe-sensitive-type-group Resource 2-20
data-safe-sensitive-types Resource 2-20
data-safe-sensitive-types-export Resource 2-21
Data Masking Resources 2-21
data-safe-masking-family Resource 2-22
data-safe-library-masking-formats Resource 2-22
data-safe-masking-policies Resource 2-23
data-safe-masking-reports Resource 2-23
data-safe-masking-policy-healthreport Resource 2-24
Alert Resources 2-24
data-safe-alert-family Resource 2-24
data-safe-alerts Resource 2-25
data-safe-alert-policies Resource 2-25
data-safe-target-alert-policy-associations Resource 2-25
SQL Firewall Resources 2-26
data-safe-sql-firewall-family Resource 2-26
data-safe-database-security-configs Resource 2-27
data-safe-security-policies Resource 2-27
data-safe-security-policy-deployments Resource 2-27
data-safe-sql-collections Resource 2-28
data-safe-sql-firewall-policies Resource 2-28
data-safe-sql-firewall-allowed-sqls Resource 2-28

data-safe-sql-firewall-violations Resource 2-28
Common Resources 2-29
data-safe Resource 2-29
data-safe-report-definitions Resource 2-29
data-safe-reports Resource 2-29
data-safe-work-requests Resource 2-30
What Resources Can Be Deleted While a Target Database is Active 2-31
Create IAM Policies for Oracle Data Safe Users 2-32
General Steps for Creating an IAM Policy for Oracle Data Safe 2-32
Create an Oracle Data Safe Administrators Group 2-33
Permission to Access all Resources of an Oracle Data Safe Feature 2-33
Permission to Access a Specific Resource 2-34
Permissions to Register an Autonomous Database with Oracle Data Safe 2-35
Permissions to Register an Oracle Cloud Database with Oracle Data Safe 2-36
Permissions to Register an On-Premises Oracle Database with Oracle Data Safe 2-36
Permissions to Register an Oracle Database on Compute with Oracle Data Safe 2-37
Permissions to Register an Oracle Cloud@Customer Database with Oracle Data Safe 2-38
Permissions to Register a Target Database with Oracle Data Safe 2-39
Permissions for an Oracle Data Safe Private Endpoint 2-39
Permissions for an Oracle Data Safe On-Premises Connector 2-39
Permission to Run Assessments and View Audit and Alert Data 2-40
Permissions to Discover Sensitive Data 2-40
Permission to Mask Sensitive Data 2-41
Permissions to Use Contextual Event Notifications 2-41
Configure Access to Oracle Data Safe for Federated Users 2-42
Example Security Configuration for Oracle Data Safe 2-43

3 Target Database Registration

Target Database Registration Overview 3-1
Supported Target Databases 3-1
Security Levels for Target Databases 3-5
Where to Register Target Databases 3-5
Connectivity Options for Target Databases 3-5
Public Versus Private Endpoints 3-6
Oracle Data Safe Private Endpoints 3-6
Oracle Data Safe On-Premises Connectors 3-7
TLS and TCP Connection Protocols 3-8
Pre and Post Registration Tasks 3-8
Create an Oracle Data Safe Service Account on Your Target Database 3-9
Exception for Autonomous Databases 3-9
Create an Oracle Data Safe Service Account on a Target Database 3-9

Grant Roles to the Oracle Data Safe Service Account on Your Target Database 3-10
Roles for the Oracle Data Safe Service Account 3-10
Grant Roles to the Oracle Data Safe Service on an Autonomous Database 3-11
Grant Roles to the Oracle Data Safe Service on a Non-Autonomous Database 3-13
Create a Wallet or Certificates for a TLS Connection 3-14
Create a PEM Certificate for a TLS Connection to a Database that has Server Authentication 3-14
Create Wallets for a TLS Connection to a Database that has Mutual Authentication 3-15
Configure a TLS Connection Between the On-Premises Connector on Your Host Machine and Your Oracle Database 3-15
Configure a TLS Connection Between the On-Premises Connector on Your Host Machine and an Autonomous Database on Exadata Cloud@Customer Database 3-16
Add the Security Certificate for the Amazon RDS Region 3-17
Add Security Rules 3-17
Overview 3-17
Add Security Rules for an Oracle Autonomous Database Serverless with Private VCN Access 3-18
Add Security Rules for an Autonomous Database on Dedicated Exadata Infrastructure 3-19
Add Security Rules for an Oracle Cloud Database 3-19
Add Security Rules for an Oracle Database on Compute 3-20
Add Security Rules for an Oracle On-Premises Database 3-20
Add Security Rules for an Exadata Cloud@Customer Database 3-21
Register an Autonomous Database 3-22
Preregistration Tasks for an Autonomous Database 3-23
Run the Autonomous Databases Wizard 3-23
Step 1: Select Database 3-23
Step 2: Connectivity Option 3-24
Step 3: Add Security Rule 3-24
Step 4. Review and Submit 3-25
Step 5. Registration Progress 3-26
Post Registration Tasks for an Autonomous Database 3-26
Register an Oracle Cloud Database 3-27
Preregistration Tasks for an Oracle Cloud Database 3-28
Run the Oracle Cloud Databases Wizard 3-28
Step 1: Select Database 3-28
Step 2: Connectivity Option 3-30
Step 3: Select Peer Database 3-30
Step 4: Add Security Rule 3-31
Step 5: Review and Submit 3-32
Step 6: Registration Progress 3-32
Post Registration Tasks for an Oracle Cloud Database 3-32
Register an Oracle On-Premises Database 3-33

Preregistration Tasks for an Oracle On-Premises Database 3-33
Run the On-Premises Oracle Databases Wizard 3-33
Step 1: Target Information 3-33
Step 2: Connectivity Option 3-34
Step 3: Select Peer Database 3-35
Step 4: Add Security Rule 3-36
Step 5: Review and Submit 3-36
Step 6: Registration Progress 3-37
Post Registration Tasks for an Oracle On-Premises Database 3-37
Register an Oracle Cloud@Customer Database 3-38
Cloud@Customer Preregistration Tasks 3-38
Run the Oracle Cloud@Customer Databases Wizard 3-39
Step 1: Target information 3-39
Step 2: Connectivity Option 3-40
Step 3: Select Peer Database 3-42
Step 4: Add Security Rule 3-43
Step 4: Review and Submit 3-43
Post Registration Tasks for an Oracle Cloud@Customer Database 3-44
Register an Oracle Database on a Compute Instance 3-44
Preregistration Tasks for an Oracle Database on Compute 3-45
Run the Oracle Databases on Compute Wizard 3-45
Step 1: Select Database 3-45
Step 2: Connectivity Option 3-47
Step 3: Add Peer Database 3-48
Step 3: Add Security Rule 3-48
Step 4: Review and Submit 3-49
Step 5: Registration Progress 3-49
Post Registration Tasks for an Oracle Database on Compute 3-50
Register an Amazon RDS for Oracle database 3-51
Register Amazon RDS for Oracle with an On-Premises Connector 3-51
Preregistration Tasks for Registering Amazon RDS for Oracle with an On-Premises Connector 3-51
Run the Amazon RDS for Oracle Wizard 3-52
Post Registration Tasks 3-54
Register Amazon RDS for Oracle with an Oracle Data Safe Private Endpoint 3-55
Preregistration Tasks for Registering Amazon RDS for Oracle with an Oracle Data Safe Private Endpoint 3-55
Run the Amazon RDS for Oracle Wizard 3-55
Manually Register a Target Database 3-59
Overview 3-59
Preregistration Tasks for Manual Target Database Registration 3-59
Manually Register an Autonomous Database 3-60

Manually Register an Oracle Cloud Database 3-61
Manually Register an Oracle On-Premises Database 3-63
Manually Register an Oracle Database on Compute 3-64
Manually Register a Cloud@Customer Database 3-66
Manually Register an Amazon RDS for Oracle database 3-69
Preregistration Tasks for Registering Amazon RDS for Oracle with Private IP 3-69
Manually Register Amazon RDS for Oracle 3-70
Post Registration Tasks for Manual Target Database Registration 3-72
Manage Target Databases 3-72
View Registration Details for a Target Database 3-73
Update Connection Details for a Target Database 3-73
Update a Target Database Name and Description 3-73
Update the Database User 3-74
Manage Peer Databases Associated with a Registered Active Data Guard Primary Database 3-74
What to Do in Data Safe After Performing a Manual Switch Over of Active Data Guard Associated Target Databases? 3-76
Move a Target Database to a Different Compartment 3-76
Activate or Deactivate a Target Database 3-77
Deregister a Target Database 3-77
Resources That Are Automatically Deleted When a Target Database is De-registered 3-78
Resources That Are Automatically Deleted When a Target Database is De-registered 3-79
Manage Network Access Changes for an Oracle Autonomous Database Serverless 3-81
Overview 3-81
Workflow 3-82
Update the Security Rules to Allow Communication Between Oracle Data Safe and Your Database 3-83
What to Do if an Autonomous Database Name Changes 3-84
Create an Oracle Data Safe Private Endpoint 3-85
Prerequisites Tasks for Creating an Oracle Data Safe Private Endpoint 3-85
Create an Oracle Data Safe Private Endpoint 3-85
Create an Oracle Data Safe On-Premises Connector 3-87
Prerequisites for Creating an Oracle Data Safe On-Premises Connector 3-87
Hardware Requirements 3-88
Software Requirements 3-88
Create an Oracle Data Safe On-Premises Connector 3-89
Download the Install Bundle for the Oracle Data Safe On-Premises Connector 3-89
Install an Oracle Data Safe On-Premises Connector 3-90
High Availability of an On-Premises Connector 3-92
Check the Status of an On-Premises Connector 3-92
Restart an On-Premises Connector 3-92
Creating OS User Service for Existing On-Premises Connectors 3-92

Update an Oracle Data Safe On-Premises Connector 3-92
Uninstall an Oracle Data Safe On-Premises Connector 3-93
Find the Log Files for an On-Premises Connector 3-94
Troubleshooting Install or Update Issues 3-94
Troubleshoot Target Registration 3-94
Error Message: ORA-17292: No valid logon method found 3-94
Error Message: ORA-12650: No common encryption or data integrity algorithm 3-95
Target Database Turns INACTIVE If In NEEDS_ATTENTION Status for 15 Days 3-95
Please Choose the Right Database Category Error Message 3-95

4 Events

Overview of Oracle Data Safe Events 4-1
Rule Conditions 4-1
Notification Text 4-1
About Oracle Data Safe Events 4-2
Event Types for Oracle Data Safe 4-3
Target Database Event Types 4-3
Oracle Data Safe On-Premises Connector Event Types 4-4
Oracle Data Safe Private Endpoint Event Types 4-5
Security Assessment Event Types 4-6
User Assessment Event Types 4-8
Activity Auditing Event Types 4-11
Alert Event Types 4-13
Data Discovery Event Types 4-15
Data Masking Event Types 4-17
SQL Firewall Event Types 4-20
Event Notifications in Data Safe 4-22
Create and Modify Event Notifications for Targets and Connectivity Options 4-23
Creating Event Notifications for Target Registration 4-23
Modifying Event Notifications For Target Registration 4-24
Creating Event Notifications for Private Endpoints 4-25
Modifying Event Notifications For Private Endpoints 4-26
Creating Event Notifications for On-Premises Connectors 4-27
Modifying Event Notifications For On-Premises Connectors 4-28

5 Reference

Target Database Information Stored in Oracle Data Safe 5-1
Service Limits 5-2

License Restrictions Warranty/Consequential Damages Disclaimer

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

Restricted Rights Notice

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Hazardous Applications Notice

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Trademark Notice

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

Third-Party Content, Products, and Services Disclaimer

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not 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.

Preface

The *Administering Oracle Data Safe* guide focuses on security administration and target database registration in Oracle Data Safe.

The following sections are included:

Audience

The *Administering Oracle Data Safe* guide is intended for Oracle Data Safe administrators who need to register target databases with Oracle Data Safe and manage user access to Oracle Data Safe features and resources.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Related Resources

You may find the following resources useful:

- Using Oracle Data Safe
- What's New for Oracle Data Safe

- Oracle Cloud Infrastructure

1

Getting Started

This section describes the main features of Oracle Data Safe and its architecture. You also learn how to access Oracle Data Safe in the Oracle Cloud Infrastructure Console.

Oracle Data Safe Overview

Oracle Data Safe is a unified control center for your Oracle databases which helps you understand the sensitivity of your data, evaluate risks to data, mask sensitive data, implement and monitor security controls, assess user security, monitor user activity, address data security compliance requirements, collect centralized audit records, and manage audit policies.

Features of Oracle Data Safe

Oracle Data Safe provides the following set of features for protecting sensitive and regulated data in Oracle databases, all in a single, easy-to-use database security control center:

- **Security Assessment** helps in evaluating the security of your database configurations. It examines database configurations, user accounts, and security controls, and subsequently provides findings along with recommendations for remedial actions following best practices to reduce or mitigate risks. Recommendations are based on the Security Technical Implementation Guides (STIG), Center for Internet Security (CIS) Configurations, recommendations from the General Data Protection Regulation (EU GDPR) and Oracle best practices.
- **User Assessment** assists in identifying highly privileged accounts that may pose a threat if misused or compromised. It scrutinizes information about users in the data dictionary of target databases and calculates a potential risk score for each user. This evaluation includes user types, authentication methods, password policies, password change frequency, and provides direct links to related audit records. With this information, appropriate security controls and policies can be deployed.
- **Data Discovery** facilitates the detection of sensitive data within your databases. By specifying the type of sensitive data to search for, Data Discovery examines the actual data and data dictionary, presenting a list of sensitive columns. It comes with default search capabilities covering various sensitive data categories, such as identification, biographic, IT, financial, healthcare, employment, and academic information.
- **Data Masking** offers a means to mask sensitive data, ensuring its safety for non-production purposes. For instance, when organizations need to create copies of production data for development and testing, Data Masking replaces sensitive data with realistic but fictitious information, mitigating the risk associated with exposing sensitive data to new users.
- **Activity Auditing** lets you audit user activity on your databases so you can monitor database usage.
- **Alerts** keep you informed of unusual database activities as they happen.
- **SQL Firewall** protects against risks such as SQL injection attacks or compromised accounts. SQL Firewall is a new security capability built into the Oracle Database 23ai

kernel and offers protection against these risks. The SQL Firewall feature in Oracle Data Safe lets you centrally manage and monitor the SQL Firewall policies for your target databases. Oracle Data Safe lets you collect authorized SQL activities of a database user, generate and enable the policy with allowlists of approved SQL statements and database connection paths, and provides a comprehensive view of any SQL Firewall violations across the fleet of your target databases.

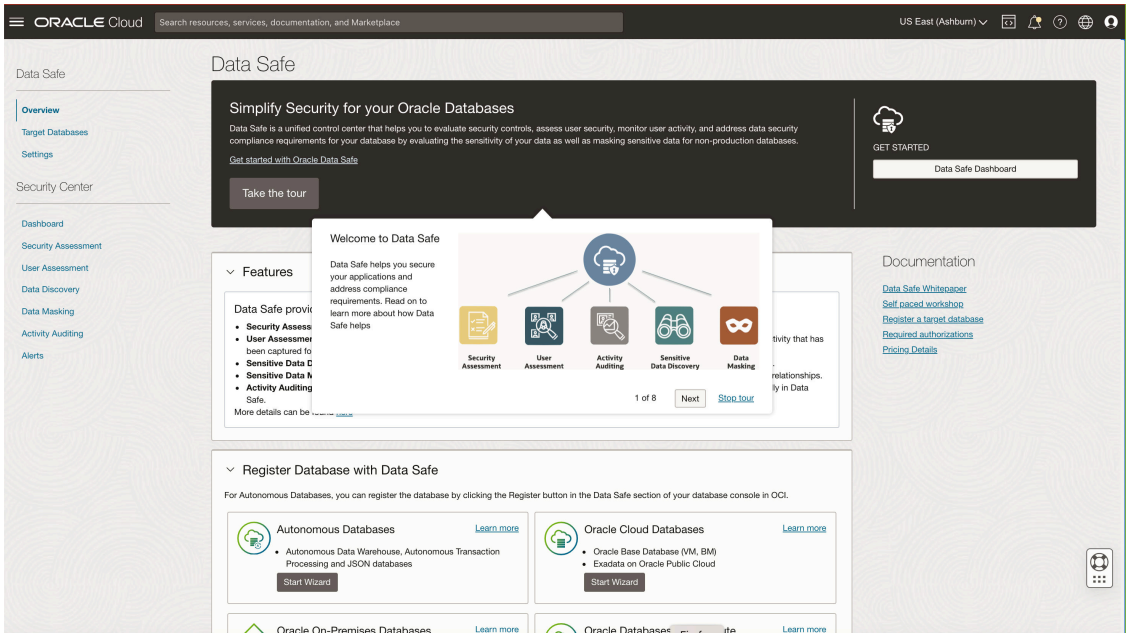
Oracle Data Safe Guided Tour

The Oracle Data Safe guided tour gives you a high-level overview of the features of Oracle Data Safe and how to start using them to improve the security of your databases.

If you do not have any target databases registered with Oracle Data Safe the tour will begin automatically. If you navigate to the Overview page again during the same session the tour will no longer start automatically.

Anyone can initiate the tour at any time by navigating to the Overview page and clicking **Take the tour**.

You can click through the walk through by clicking **Next** or stop the tour at any time by clicking **Stop tour**.



Key Concepts and Terminology

Understand the following concepts and terminology to help you get started with Oracle Data Safe.

Oracle Cloud Infrastructure

Oracle Cloud Infrastructure is a set of complementary cloud services that enables you to build and run a wide range of applications and services in a highly available hosted environment. Oracle Cloud Infrastructure offers high-performance compute capabilities (as physical hardware instances) and storage capacity in a flexible overlay virtual network that is securely

accessible from your on-premises network. Oracle Data Safe is integrated as a service into Oracle Cloud Infrastructure.

Oracle Cloud Infrastructure Console

The Oracle Cloud Infrastructure Console is a simple and intuitive web-based user interface that you can use to access and manage Oracle Cloud Infrastructure. You can access Oracle Data Safe in the Oracle Cloud Infrastructure Console.

Tenancy

A tenancy is a secure and isolated partition within Oracle Cloud Infrastructure where you can create, organize, and administer your cloud resources.

Region and Availability Domain

Oracle Cloud Infrastructure is *physically* hosted in regions and availability domains. A region is a localized geographic area, and an availability domain is one or more data centers located within a region. A region is composed of one or more availability domains. Oracle Cloud Infrastructure resources are either region-specific, such as a virtual cloud network, or availability domain-specific, such as a compute instance.

Oracle Data Safe

Oracle Data Safe is a fully-integrated Cloud service in Oracle Cloud Infrastructure focused on the security of your data. It provides a complete and integrated set of features for protecting sensitive and regulated data in Oracle databases. The Security Center in Oracle Data Safe is the main area where you can access all the features.

Oracle Cloud Infrastructure Identity and Access Management (IAM)

The IAM service is the default, fully integrated, identity management service for Oracle Cloud Infrastructure. It lets you control who has access to your cloud resources, what type of access user groups have, and to which specific resources user groups have access. Oracle Data Safe uses all the shared services in Oracle Cloud Infrastructure, including IAM.

IAM Compartment

In IAM, compartments allow you to organize and control access to your cloud resources. A compartment is a collection of related resources, such as database instances, virtual cloud networks, and block volumes. A compartment should be thought of as a logical group and not a physical container. When you begin working with resources in the Oracle Cloud Infrastructure Console, the compartment acts as a filter for what you are viewing. A group requires permission by an administrator to access a compartment.

IAM User Group

A user group in IAM is a collection of users who all need the same type of access to a particular set of resources or compartment. Tenancy administrators can create users and groups in the root compartment of a tenancy with the IAM service in Oracle Cloud Infrastructure. Oracle Data Safe retrieves user groups from IAM, and in some cases, individual users.

Oracle automatically creates a tenancy administrator for you and adds it to the tenancy's `Administrators` group. This group has all permissions on all resources in the tenancy, and is responsible for creating the users, groups, and compartments for the tenancy.

IAM Policy

An IAM policy is a document that specifies who can access which resources in Oracle Cloud Infrastructure, and how. Access is granted at the group and compartment level, which means you can write a policy that gives a group a specific type of access within a specific compartment, or to the tenancy itself. If you give a group access to your tenancy, the group automatically gets the same type of access to all the compartments inside your tenancy. Only tenancy administrators can create policies. An administrator can create IAM policies to define user privileges for all Oracle Data Safe resources.

Oracle Data Safe Console

The Oracle Data Safe Console is the former user interface for Oracle Data Safe. Administrators need to migrate content from this Console to the new Security Center in Oracle Cloud Infrastructure.

Oracle Data Safe Repository

The Oracle Data Safe repository is an Oracle database that stores audit data and metadata for Oracle Data Safe.

Target Database

A target database is an Oracle Database on which Oracle Data Safe can perform user and security assessment, data discovery, data masking, activity auditing, and alerts.

Sensitive Type

A sensitive type is a classification of sensitive data and defines the kind of sensitive columns to search for. For example, the US Social Security Number (SSN) sensitive type helps you discover columns containing Social Security numbers. Data Discovery searches for sensitive data in your databases based on the sensitive types that you choose. You can choose from a wide variety of predefined sensitive types and can also create your own sensitive types.

Sensitive types are divided into categories. The top-level categories are Identification Information, Biographic Information, IT Information, Financial Information, Healthcare Information, Employment Information, and Academic Information. You can choose individual sensitive types or sensitive categories to search sensitive data.

Sensitive Data Model

A sensitive data model is a collection of sensitive columns and referential relationships. Data Discovery identifies sensitive columns and referential relationships and creates a sensitive data model. Data Discovery automatically searches the Oracle data dictionary to find relationships between primary key columns and foreign key columns and flags them as sensitive. It can also discover non-dictionary referential relationships, which are relationships defined in applications and not in the Oracle data dictionary.

Masking Format

A masking format defines the logic to mask sensitive data in a database column. For example, the Shuffle masking format randomly shuffles values in a column. The Email Address masking format replaces values in a column with random email addresses. Oracle Data Safe provides many predefined masking formats. If needed, you can create your own.

Masking Policy

A masking policy maps sensitive columns to masking formats that should be used to mask the data. You can use a masking policy to perform data masking on a target database. You can create a masking policy using a sensitive data model.

Audit Data Retrieval

An audit data retrieval represents an archive retrieve request for audit data. You can retrieve audit data for a target database from the archive and store it online.

Audit Policy

An audit policy represents the audit policies for the target database and their provisioning status on the target database.

Audit Profile

An audit profile represents audit profile settings and audit configurations for the database target, and helps determine the audit data volume available on the target and the volume collected by Oracle Data Safe.

Alert Policy

In Oracle Data Safe, you can provision alert policies on your target databases. An alert policy defines an event in a database to monitor. Alert policies are rule-based and are triggered based on the audit data collected.

Audit Trail

An audit trail represents the source of audit records that provides documentary evidence of the sequence of activities in the target database.

Alert

An alert is a message that notifies you when a particular audit event happens on a target database.

Oracle Data Safe Architecture

The main components of Oracle Data Safe are the Oracle Data Safe service in Oracle Cloud Infrastructure, a back-end Oracle database repository, and target databases.

Oracle Data Safe Service

You can access the Oracle Data Safe service in Oracle Cloud Infrastructure. The service has the following pages:

- **Overview** page - On this page you can review what's new in Oracle Data Safe, access the Oracle Data Safe dashboard, register target databases with Oracle Data Safe, and access documentation and related resources.
- **Target Databases** page - On this page, you can view details for target databases to which you have access and register new target databases, either manually or by using a wizard.
- **Settings** page - On this page, you can set global paid usage and global audit record retention policy settings for the regional Oracle Data Safe service.

- **Security Center** pages - The Security Center page provides access to the Dashboard, Security Assessment, User Assessment, Data Discovery, Data Masking, Activity Auditing, and Alerts pages.

  > **Note:**
  >
  > To migrate content from the former Oracle Data Safe Console to Security Center, you need access to the Oracle Data Safe Console. Links to this Console are provided in the Security Center user interface.

- **Private Endpoints** page - On this page, you can manually create and manage Oracle Data Safe private endpoints. Private endpoints are needed to connect to Oracle Cloud databases running in a private VCN (including Oracle Database on OCI Compute) as well as to connect to Oracle on-premises databases and Cloud at Customer databases that have a FastConnect or IPSec VPN connection to OCI.
- **On-Premises Connectors** page - On this page, you can manually create and manage Oracle Data Safe on-premises connectors. On-premises connectors are needed to access Oracle on-premises databases via a locally installed on-premises connector.

Oracle Data Safe Database Repository

Oracle Data Safe uses its own Oracle Autonomous Database to store your service information, such as audit data (trails), masking settings, reports, alerts, and many other things. However, only your Oracle Data Safe information is stored in this database and your information is not stored alongside other Oracle Data Safe information .

There is a dedicated database for each tenancy's Oracle Data Safe instance per region and the databases are automatically provisioned and included with the Oracle Data Safe service. The databases are secure and highly available in the Oracle Cloud.

Target Databases

Oracle Data Safe can connect to your Oracle databases, including Autonomous Databases, DB systems (Bare Metal, Virtual Machine, and Exadata), on-premises Oracle Databases, Oracle Cloud@Customer databases (Exadata Cloud@Customer and Autonomous Database on Exadata Cloud@Customer), and Oracle Databases on compute instances in both Oracle Cloud Infrastructure and non-Oracle cloud environments.

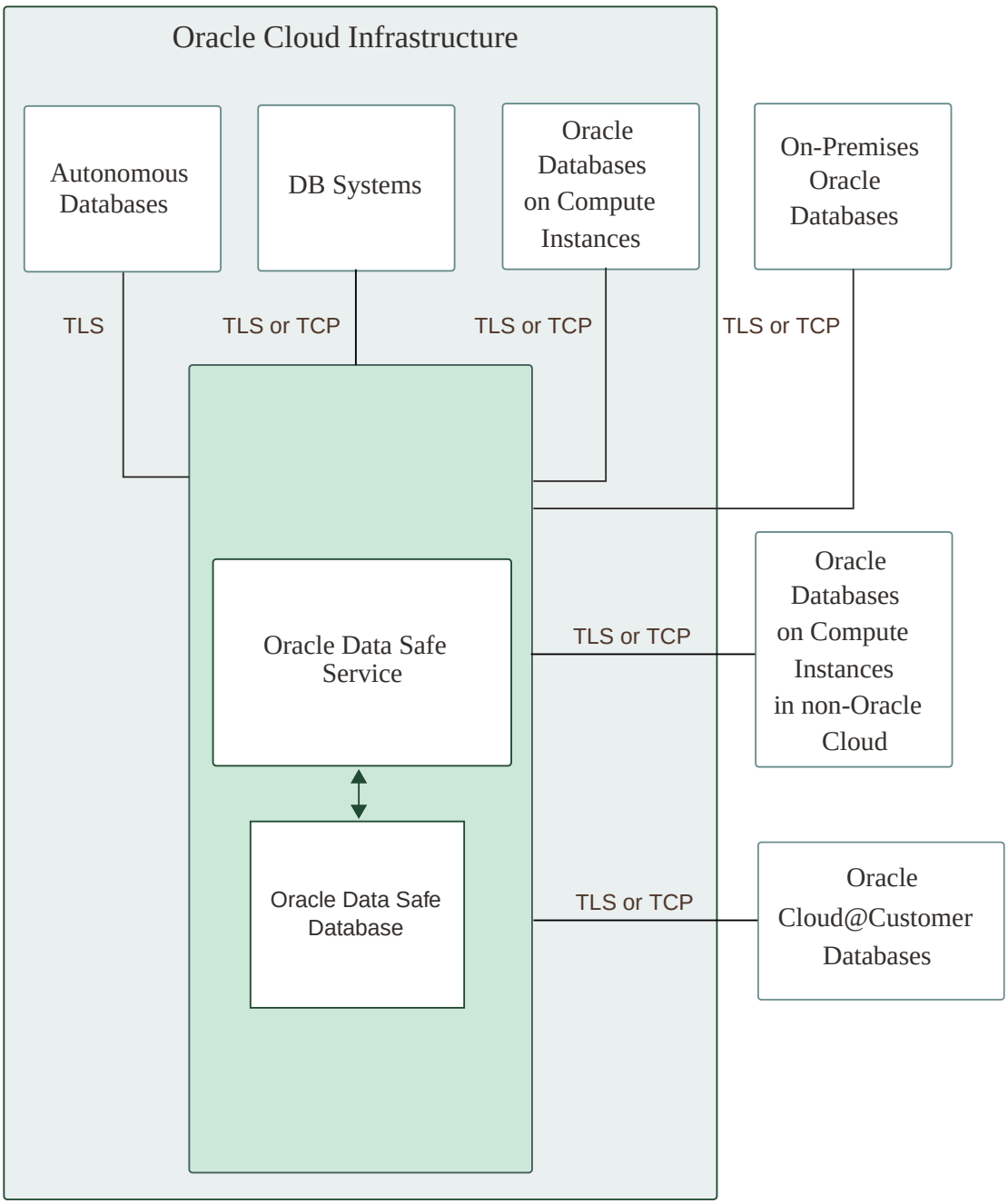
You can choose to use all Oracle Data Safe features with a target database or just certain ones. For example, you may want to use Activity Auditing with one target database and use Data Discovery and Data Masking with another.

Two different protocols are supported for connecting Oracle Data Safe to your target databases:

- TCP with network encryption, where your target database has to have network encryption enabled.
- TCPS, where your target database has to be configured with TLS version 1.2.

Oracle recommends that you back up your target databases when using features like Data Masking. You can use services in Oracle Cloud Infrastructure, such as Oracle Storage Cloud Service or Oracle Cloud Infrastructure Storage Service to back up your target databases.

The following diagram illustrates the Oracle Data Safe components, including the Oracle Data Safe service, Oracle Data Safe's back-end database, and target databases.



Access Oracle Data Safe

You can access Oracle Data Safe through the navigation menu in the Oracle Cloud Infrastructure Console.

1. To sign in to an OC1 realm (for most commercial and user accounts), open a supported browser and enter the following URL:

   ```
   https://cloud.oracle.com
   ```

To sign in to a different realm, include the realm in the URL; for example `https://oc2.cloud.oracle.com`, where `oc2` is the realm name.

If you directly access and sign in to the Oracle Data Safe Console via a previously saved bookmark, then when you navigate to an Oracle Cloud Infrastructure native feature (for example, Security Assessment), you are presented with an Oracle Cloud Infrastructure login page. Click **Next** to continue to the feature. You do not need to reenter your user credentials.

2. In the **Cloud Account Name** field, enter your tenancy name, and then click **Next**.

   The **SIGN IN** page is displayed.

3. If the **Single Sign-On** option is presented on your sign-in page, it means that your tenancy is federated with an identity service other than the default one. You can sign in the following way:

   a. Select your identity provider and click **Continue**.

      You are redirected to your identity provider to sign in.

   b. Enter your user name and password.

   You are signed in to your home region in the Oracle Cloud Infrastructure Console.

4. If the **Single Sign-On** option is not presented on your sign-in page, then your tenancy uses the default identity service, which is Oracle Cloud Infrastructure Identity and Access Management (IAM). You can sign in the following way:

   a. Enter your Oracle Cloud Infrastructure user name and password, and then click **Sign In**.

   b. If you are signing in for the first time, you are prompted to change your temporary password. Enter a new password, making sure to follow the password criteria, and click **Submit**.

   You are signed in to your home region in the Oracle Cloud Infrastructure Console.

5. (Optional) In the upper-right corner of the window, select the appropriate region in your tenancy; for example, **US East (Ashburn)**.

   Oracle Data Safe resources, such as sensitive data models, masking policies, and registered target databases are region-specific. Therefore, you want to make sure that you select Oracle Data Safe in the region that contains the resources that you need.

6. From the navigation menu, select **Oracle Database**, and then **Data Safe - Database Security**.

   The **Overview** page for the Oracle Data Safe service is displayed.

2

Oracle Data Safe Security

This section is intended for tenancy administrators, database administrators, and Oracle Data Safe administrators. It describes the key security concepts in Oracle Data Safe, including Oracle Data Safe's integration with Oracle Cloud Infrastructure security. It also identifies tasks that administrators perform to implement security in Oracle Data Safe.

Security Overview

Oracle Data Safe makes use of Oracle Cloud Infrastructure Identity and Access Management (IAM) components, such as regions, compartments, users and groups, and IAM policies. As an Oracle Data Safe administrator, it's important to become familiar with these components and database security.

Security Levels

Security for Oracle Data Safe is managed in two places:

- **In Oracle Cloud Infrastructure Identity and Access Management (IAM)** - To control user access to Oracle Data Safe resources and other Oracle Cloud Infrastructure resources, a tenancy administrator is required to create policies.
- **On the target database** - To control user access to target database data, database administrators need to grant users access to the schemas that they use. Database administrators also need to enable the appropriate Oracle Data Safe features on each target database by granting Oracle Data Safe roles to the Oracle Data Safe service account.

Administrator Types

The following table describes the types of administrators needed to manage Oracle Data Safe.

Administrator Type	Description
Tenancy administrator	This person is needed to create compartments, users, groups, and policies in the tenancy using IAM.
Oracle Data Safe administrator	This person can use all the features in Oracle Data Safe and manage content in Security Center.
Database administrator	This person is needed to grant users access to data on target databases and enable Oracle Data Safe features on target databases.

Regions

When you sign up for Oracle Cloud Infrastructure, Oracle creates a tenancy for you in one region. This is your *home region*. Your home region is where your Oracle Cloud Infrastructure Identity and Access Management (IAM) resources are defined. When you subscribe to another

region, your IAM resources are available in the new region, however, the master definitions reside in your home region and can only be changed there.

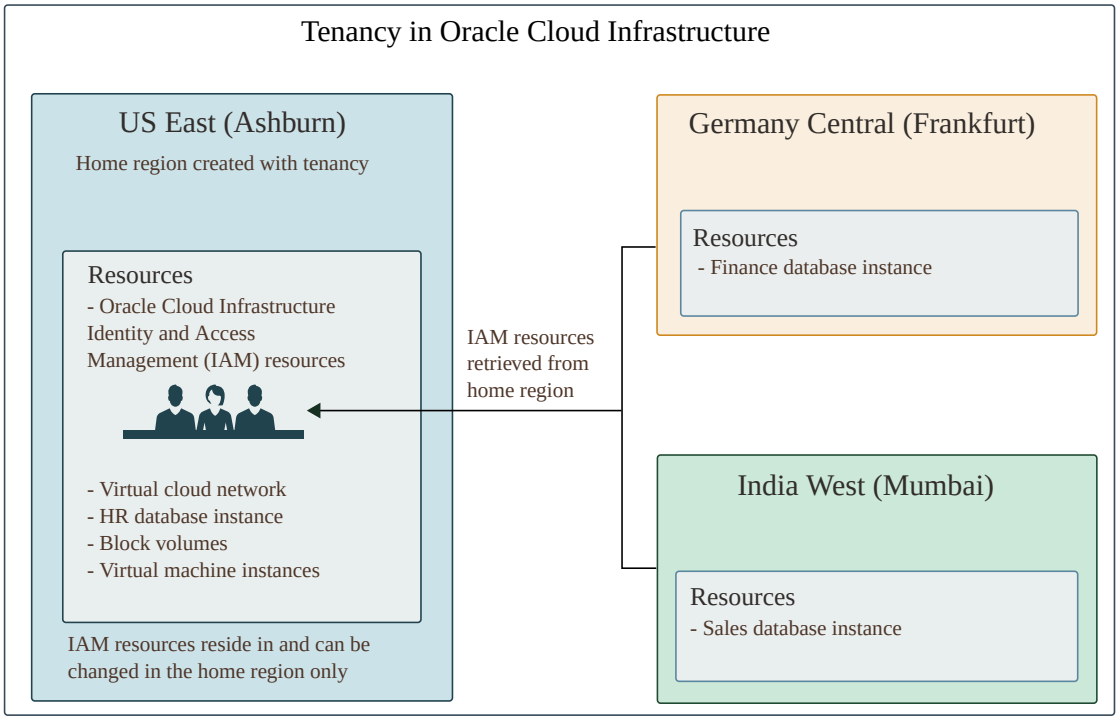
Resources that you can create and update only in the home region are as follows:

- Users
- Groups
- Policies
- Compartments
- Dynamic groups
- Federation resources

When you subscribe your tenancy to a new region, all the policies from your home region are enforced in the new region. If you want to limit access for groups of users to specific regions, you can write policies to grant access to specific regions only. A user wanting access to Oracle Data Safe features and resources requires permissions through an IAM policy.

Oracle Data Safe resources are specific to each regional Oracle Data Safe service. For example, suppose a user creates a data masking policy in the Oracle Data Safe service in the Phoenix region. If the user then signs in to the Oracle Data Safe service in the Frankfurt region, the user will not be able to find and use the same data masking policy. The policy would need to be recreated in the Frankfurt region. Registered target databases in Oracle Data Safe are region-specific too. Cross-regional target registration is not supported.

In the diagram below, there are three regions: US East (Ashburn), Germany Central (Frankfurt), and India West (Mumbai). US East is the home region for the tenancy. Frankfurt and Mumbai retrieve Oracle Cloud Infrastructure Identity and Access Management (IAM) resources, such as users, groups, and compartments, from the home region. Each region has its own resources. Frankfurt has a Finance database instance and Mumbai has a Sales database instance. The home region has IAM resources, a virtual cloud network (VCN), Human Resources database, block volumes, and virtual machine instances. A user who has the appropriate permissions can register the Sales database with the Oracle Data Safe service in Mumbai, but those same Mumbai-specific permissions do not allow the user to register a database in other regions.



Compartments

Compartments in Oracle Cloud Infrastructure are logical structures that help you to organize and control access to your cloud resources, including Oracle Data Safe resources. Users can create compartments by using the Oracle Cloud Infrastructure Identity and Access Management (IAM) service.

Compartments in Oracle Cloud Infrastructure contain resources, such as database instances, virtual cloud networks, and block volumes. Think of a compartment as a logical group and not a physical container. It acts as a filter for what you are viewing. Whenever you add a resource in Oracle Cloud Infrastructure, you create it in a particular compartment. If needed, you can move resources from one compartment to another. Users require permissions to access compartments and the resources in them.

When you sign up for Oracle Cloud Infrastructure, Oracle creates a tenancy for you, which is considered the *root* compartment. The root compartment holds all of your cloud resources. Inside the tenancy, you can create compartments that are direct children or further descendants of the root compartment, based on your organization's needs. For example, you might create a compartment to store all of the resources for a financial application. To control access to resources in each compartment (and optionally its children), a member of your tenancy's Administrators group creates policies. Ultimately, the goal is to ensure that each person has access to only the resources they need.

When you create an Oracle Data Safe resource, you specify the compartment to which you want the resource to belong. The following Oracle Data Safe resources are stored in compartments:

- Target databases
- Private endpoints
- On-premises connectors
- Sensitive data models (SDMs)

- User-defined sensitive types
- User-defined masking formats
- Masking policies
- Audit policies
- Audit trails
- Custom reports

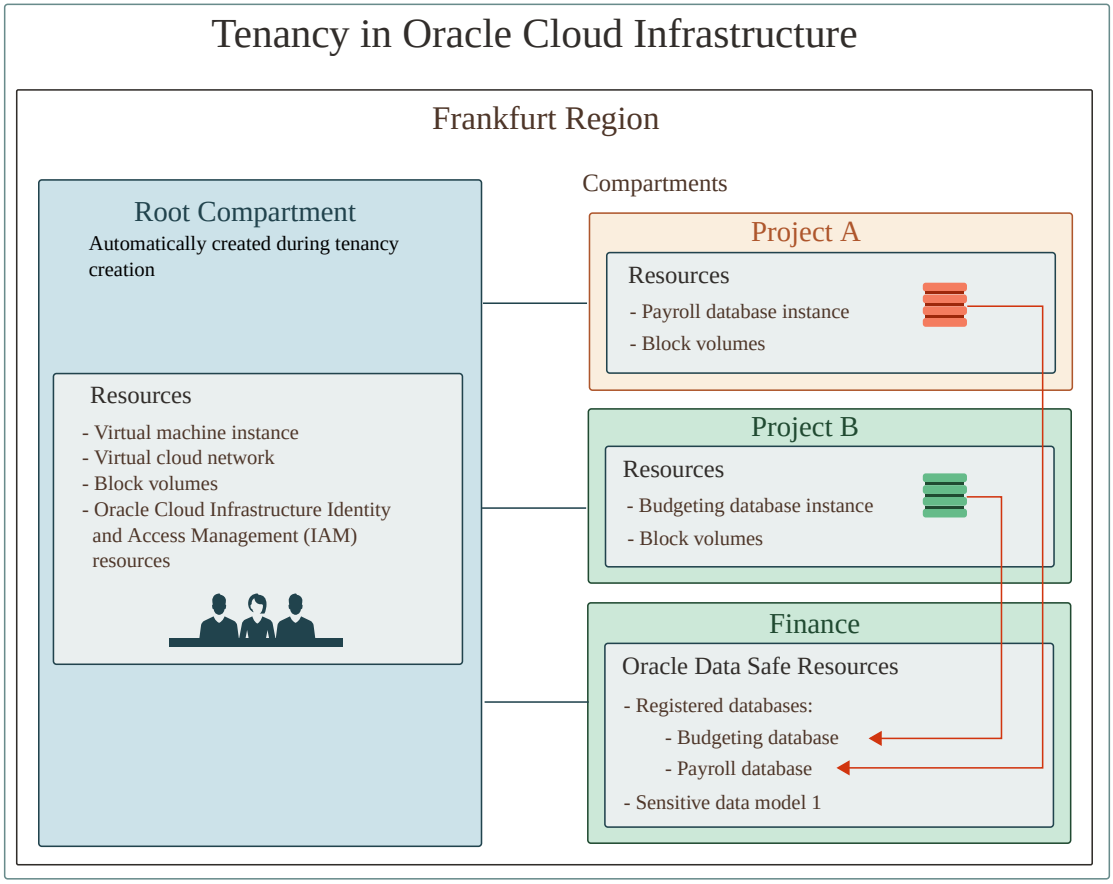
In order for a user to view and select compartments when creating Oracle Data Safe resources, the user needs to be granted permissions on those compartments through Oracle Cloud Infrastructure Identity and Access Management (IAM) policies. A user can add multiple resources to a compartment. Only tenancy administrators can delete compartments through IAM.

Oracle Data Safe resources are specific to a region in a tenancy. A user can register a target database with Oracle Data Safe to only one compartment.

The diagram below illustrates the concept of compartments. In the tenancy in Oracle Cloud Infrastructure, the root compartment contains a virtual machine instance, a virtual cloud network, block volumes, and Oracle Cloud Infrastructure Identity and Access Management (IAM) resources (for example, users, groups, and policies). The root compartment is automatically created when the tenancy is created.

In the Frankfurt region, three compartments are used: Project A, Project B, and Finance.

- The **Project A** compartment contains resources for Project A, including a Payroll database instance and block volumes.
- The **Project B** compartment contains resources for Project B, including a Budgeting database instance and block volumes.
- Because the same users work on Projects A and B, the two databases are registered in Oracle Data Safeto the same compartment - **Finance**. An Oracle Data Safe sensitive data model named Sensitive Data Model 1, is also saved to the Finance compartment. Notice that you don't have to register target databases to the same compartment in which they reside.



Users and Groups

Oracle Data Safe supports both native and federated users and groups in Oracle Cloud Infrastructure.

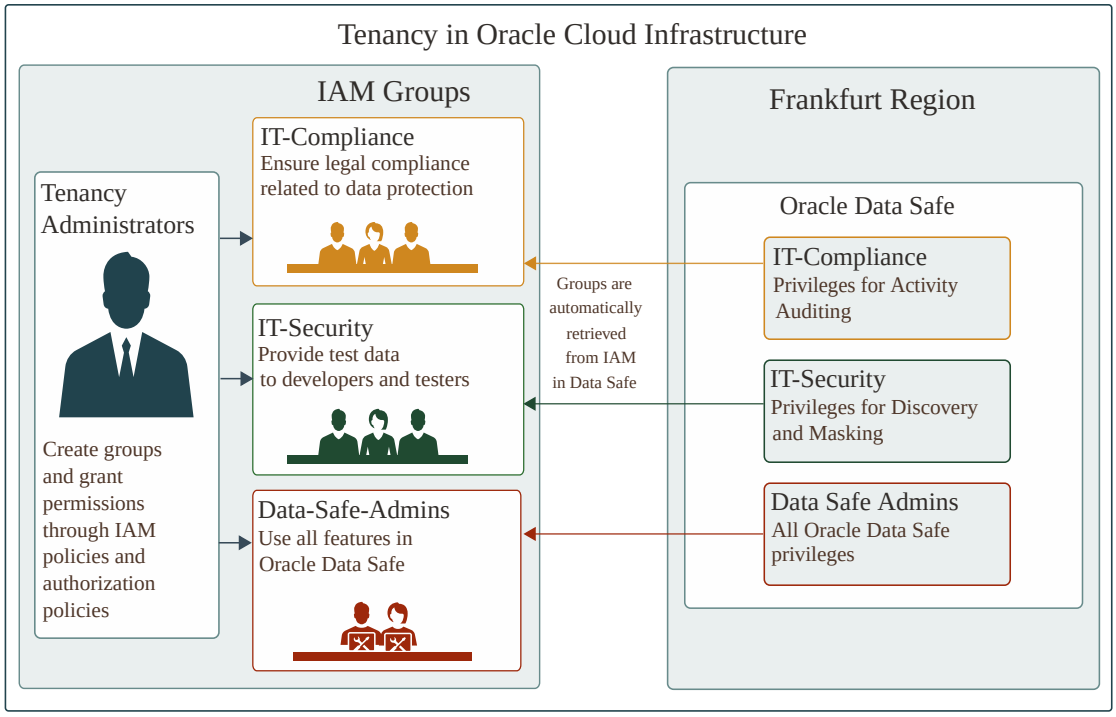
Native Users and Groups

A *native* user or group is one that is created in Oracle Cloud Infrastructure Identity and Access Management (IAM). IAM is the default service in Oracle Cloud Infrastructure that administrators can use to control user access to cloud resources. Users and groups can be created by tenancy administrators in the `root` compartment only.

When your organization gets an Oracle Cloud account, Oracle automatically sets up a default administrator for the account and an `Administrators` group. Members of this group are responsible for creating users and groups in IAM and granting the groups permission to access what they need through policies. To determine how to group users, they examine the users who require the same type of access to particular resources and compartments. Only tenancy administrators can create groups and add users to groups. However, a tenancy administrator can create a policy that gives a regular user the power to create other users and credentials.

Let's examine the diagram below. Suppose you have an IT Compliance and IT Security group created in IAM. The IT Compliance group is responsible for ensuring legal compliance related to data protection and only needs to use Activity Auditing. The IT Security group is responsible for protecting sensitive data and needs to provide data sets to testers and developers. They require access to the Data Discovery and Data Masking features. With this information, a

tenancy administrator creates two groups in IAM called `IT-Compliance` and `IT-Security` and assigns the users to their appropriate groups. The administrator creates an IAM policy that grants the IT-Compliance group `manage` access to Activity Auditing resources. The administrator creates another policy in IAM for the `IT-Security` group that grants the group `manage` access to the Data Discovery and Data Masking resources. The administrator creates a group in IAM called `Data-Safe-Admins` for the power users who need to use all Oracle Data Safe features. The administrator creates a third IAM policy that grants the `Data-Safe-Admins` group `manage` access on all Oracle Data Safe resources.



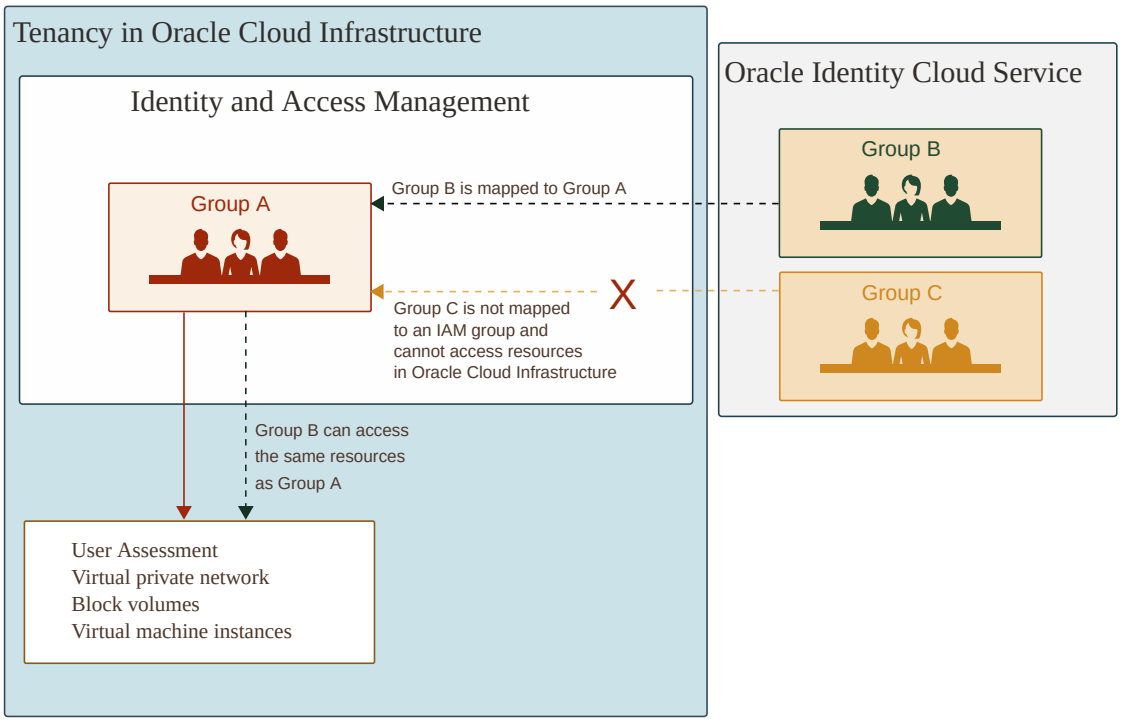
Federated Users and Groups

When someone in your company wants to use Oracle Cloud Infrastructure resources in the Console, they must sign in with a user login and password. Enterprise companies commonly use an identity provider (IdP), such as Oracle Identity Cloud Service or Microsoft Active Directory, to authenticate users for access to websites, services, and resources. In the Oracle Cloud Infrastructure Console, an administrator can federate with a supported IdP so that each employee can use an existing login and password and not have to create a new set to use Oracle Cloud Infrastructure resources.

An IdP administrator creates users and groups in the IdP and assigns each user to one or more groups according to the type of access needed. The administrator can map an IdP group to an Oracle Cloud Infrastructure Identity and Access Management (IAM) group so that the IdP group can access the same Oracle Cloud Infrastructure resources as the IAM group. Groups created in the IdP have no privileges in Oracle Cloud Infrastructure until a tenancy administrator maps them to a group in Oracle Cloud Infrastructure. The tenancy administrator can define IAM policies for the group to permit access to Oracle Cloud Infrastructure resources.

The diagram below illustrates the concept of federated users. Group A is an IAM group that has access to several resources, including User Assessment resources, a virtual private network, block volumes, and virtual machine instances. Group B is an Oracle Identity Cloud Service group. In the Oracle Cloud Infrastructure Console, an administrator maps Group B to

Group A. This mapping allows Group B to access the same resources as Group A. Group C is another group in Oracle Identity Cloud Service and is not mapped to any group in IAM. Therefore, Group C cannot access any resources in Oracle Cloud Infrastructure.



IAM Policies

Oracle Data Safe uses Oracle Cloud Infrastructure Identity and Access Management (IAM) policies to control user access to Oracle Data Safe resources. A policy is a document, written by a tenancy administrator in IAM, that specifies who can access which resource that your company has, and how. It simply allows a group to work in certain ways with specific types of resources in a particular compartment. Each policy consists of one or more policy statements.

Tasks that Require Permissions

Many tasks that you perform in Oracle Data Safe require permissions.

The following table links you to the information on how to obtain the appropriate permissions for certain tasks. You can use this table as a quick reference.

Task	Required Permissions
Create an Oracle Data Safe administrator	Create an Oracle Data Safe Administrators Group
Register an Autonomous Database	Permissions to Register an Autonomous Database with Oracle Data Safe
Register an Oracle Cloud Database	Permissions to Register an Oracle Cloud Database with Oracle Data Safe
Register an Oracle On-Premises Database	Permissions to Register an On-Premises Oracle Database with Oracle Data Safe
Register an Oracle Database on Compute	Permissions to Register an Oracle Database on Compute with Oracle Data Safe

Task	Required Permissions
Register a Cloud@Customer Database	Permissions to Register an Oracle Cloud@Customer Database with Oracle Data Safe
Create a private endpoint	See the section called **Target Registration Resources** in OCI Resources for Oracle Data Safe
Create an on-premises connector	See the section called **Target Registration Resources** in OCI Resources for Oracle Data Safe
Grant roles to the Oracle Data Safe service account on a target database	Grant Roles to the Oracle Data Safe Service Account on Your Target Database
Create security assessments	Prerequisites for Using Security Assessment
Create user assessments	Prerequisites for User Assessment
Discover sensitive data on a target database	Prerequisites for Using Data Discovery
Mask sensitive data on a target database	Prerequisites for Using Data Masking
Audit user activity	Prerequisites for Using Activity Auditing
Generate alerts	Prerequisites for Using Alerts

OCI Resources for Oracle Data Safe

Administrators specify Oracle Data Safe resources and other Oracle Cloud Infrastructure resources when creating policies for Oracle Data Safe in Oracle Cloud Infrastructure Identity and Access Management (IAM).

In Oracle Cloud Infrastructure, there are individual resource types and family resource types. Each individual type represents a specific type of resource. For example, the `masking-reports` resource type is specifically for Data Masking reports in Oracle Data Safe. To make policy writing easier, there are family types that include multiple individual resource types that are often managed together. There is a family resource for each feature of Oracle Data Safe as well as a `data-safe-family` reource. The `data-safe-family` reource grants access to all of the resources within Oracle Data Safe, whereas the family resource for a specific feature limits access to the given feature. For example, the `data-safe-assessment-family` resource only includes all the User Assessment and Security Assessment resources in Oracle Data Safe.

data-safe-family Resource

The `data-safe-family` resource represents all the Oracle Data Safe resources in Oracle Cloud Infrastructure, which includes the following:

- `data-safe`
- `data-safe-private-endpoints`
- `onprem-connectors`
- `data-safe-work-requests`
- `user-assessments`
- `data-safe-security-policy-reports`
- `target-databases`
- `security-assessments`
- `data-safe-sensitive-data-models`

- `data-safe-sensitive-types`
- `data-safe-sensitive-types-export`
- `data-safe-discovery-jobs`
- `data-safe-masking-policies`
- `data-safe-library-masking-formats`
- `data-safe-masking-reports`
- `data-safe-audit-profiles`
- `data-safe-audit-trails`
- `data-safe-archive-retrievals`
- `data-safe-report-definitions`
- `data-safe-reports`
- `data-safe-audit-policies`
- `data-safe-audit-events`
- `data-safe-alerts`
- `data-safe-alert-policies`
- `data-safe-target-alert-policy-associations`
- `data-safe-database-security-configs`
- `data-safe-security-policies`
- `data-safe-security-policy-deployments`
- `data-safe-sql-collections`
- `data-safe-sql-firewall-policies`
- `data-safe-sql-firewall-allowed-sqls`
- `data-safe-sql-firewall-violations`

The following table describes the permissions that you can assign to a group for the `data-safe-family` resource.

Permission	Description
`inspect`	The user group can list all Oracle Data Safe resources in a specified compartment.
`read` or `use`	The user group can list and view properties for all Oracle Data Safe resources in a specified compartment.
`manage`	The user group can list, view properties for, create, update, delete, and move (to another compartment) *any* Oracle Data Safe resource in a specified compartment.

Target Registration Resources

The target registration resources that you require to register a target database depend on the database type and how you plan to connect to your database.

An administrator in Oracle Cloud Infrastructure Identity and Access Management (IAM) can grant permissions as needed on the following target registration resources:

autonomous-database Resource

The `autonomous-database` resource represents an Autonomous Database in Oracle Cloud Infrastructure. To register an Autonomous Database with Oracle Data Safe or use an Autonomous Database with Oracle Data Safe, a user group requires, at a minimum, the `use` permission on the `autonomous-database` resource. For more information and other examples, see Policy Details for Autonomous Database.

Example 2-1 Specific permission - Grant a user group the `use` permission on the `Autonomous Database` resource in a compartment

The following policy statement grants the `Data-Safe-Admins` group the `use` permission on all Autonomous Databases in the `Finance` compartment.

```
allow group Data-Safe-Admins to use autonomous-database in compartment Finance
```

data-safe-private-endpoints Resource

The `data-safe-private-endpoints` resource represents the Oracle Data Safe private endpoint resource in Oracle Cloud Infrastructure.

The following table describes the permissions available for the `data-safe-private-endpoints` resource.

Permission	Description
`inspect`	The user group can list Oracle Data Safe private endpoints in the Oracle Cloud Infrastructure Console.
`read` or `use`	The user group can list and view properties for Oracle Data Safe private endpoints in the Oracle Cloud Infrastructure Console. The user group can also select private endpoints during target registration.
`manage`	The user group can list, view properties for, create, update, delete, and move (to another compartment) Oracle Data Safe private endpoints in the Oracle Cloud Infrastructure Console.

Example 2-2 Specific Permission - Allow a user group to use Oracle Data Safe private endpoints from a specific compartment during target registration

The following policy statement allows a user group named `IT-Security` to view and select Oracle Data Safe private endpoints from the compartment named `Info-Tech` during target registration.

```
allow group IT-Security to manage data-safe-private-endpoints in compartment
Info-Tech
```

Example 2-3 Broad Permission - Allow a user group to use Oracle Data Safe private endpoints from any compartment during target registration

The following policy statement allows a user group named `IT-Security` to view and select Oracle Data Safe private endpoints from any compartment in the tenancy during target registration.

```
allow group IT-Security to manage data-safe-private-endpoints in tenancy
```

onprem-connectors Resource

The `onprem-connectors` resource represents the Oracle Data Safe on-premises resource in Oracle Cloud Infrastructure.

The following table describes the permissions available for the `onprem-connectors` resource.

Permission	Description
`inspect`	The user group can list Oracle Data Safe on-premises connectors in the Oracle Cloud Infrastructure Console.
`read` or `use`	The user group can list and view properties for Oracle Data Safe on-premises connectors in the Oracle Cloud Infrastructure Console. The user group can also select on-premises connectors during target registration.
`manage`	The user group can list, view properties for, create, update, delete, and move (to another compartment) Oracle Data Safe on-premises connectors in the Oracle Cloud Infrastructure Console.

Example 2-4 Specific Permission - Allow a user group to use Oracle Data Safe on-premises connectors from a specific compartment during target registration

The following policy statement allows a user group named `IT-Security` to view and select Oracle Data Safe on-premises connectors from the compartment named `Info-Tech` during target registration.

```
allow group IT-Security to manage onprem-connectors in compartment Info-Tech
```

Example 2-5 Broad Permission - Allow a user group to use Oracle Data Safe on-premises connectors from any compartment during target registration

The following policy statement allows a user group named `IT-Security` to view and select Oracle Data Safe on-premises connectors from any compartment in the tenancy during target registration.

```
allow group IT-Security to manage onprem-connectors in tenancy
```

target-databases Resource

The `target-databases` resource represents an Oracle Data Safe target database resource in Oracle Cloud Infrastructure.

The following table describes the permissions available for the `target-databases` resource.

Permission	Description
`inspect`	The user group can list Oracle Data Safe target databases in the Oracle Cloud Infrastructure Console.
`read` or `use`	The user group can list and view properties for Oracle Data Safe target databases in the Oracle Cloud Infrastructure Console.
`manage`	The user group can list, view properties for, create (register), update, delete, activate, deactivate, and move (to another compartment) Oracle Data Safe target databases in the Oracle Cloud Infrastructure Console.

Virtual Cloud Networking Resources

To use an Oracle Data Safe private endpoint to connect to a target database, prior to creating or using an existing private endpoint, you need to obtain permissions in Oracle Cloud Infrastructure Identity and Access Management (IAM) on the underlying virtual networking resources of a private endpoint for the relevant compartments in your tenancy. The underlying resources of a private endpoint include a virtual network interface card (vnic), network security group, subnet, and so on.

The following table lists the Oracle Data Safe operations and the corresponding activities that you need to be able to perform for each type of virtual networking resource.

Oracle Data Safe private endpoint Operation	Required Activities on Virtual Networking Resources
Create an Oracle Data Safe private endpoint	For the Oracle Data Safe private endpoint compartment: • Create VNIC • Delete VNIC • (Optional) Update members in a network security group • (Optional) Associate a network security group For the subnet compartment: • Attach subnet • Detach subnet
Update an Oracle Data Safe private endpoint	For the Oracle Data Safe private endpoint compartment: • Update VNIC • (Optional) Update members in a network security group • (Optional) Associate a network security group

Oracle Data Safe private endpoint Operation	Required Activities on Virtual Networking Resources
Delete an Oracle Data Safe private endpoint	For the Oracle Data Safe private endpoint compartment: • Delete VNIC • (Optional) Update members in a network security group For the subnet compartment • Detach subnet

Example 2-6 Broad permission

In this example, the `dbadmin` group has broad permission to use all virtual networking resources in the compartment `ADWcmp1`.

```
allow group dbadmin to manage virtual-network-family in compartment ADWcmp1
```

Example 2-7 Specific permissions

In this example, the `dbadmin` group has specific permissions on network resources. The third statement is required only if you want to use network security groups to control traffic to and from the private endpoint.

```
allow group dbadmin to manage vnics in compartment ADWcmp1
allow group dbadmin to use subnets in compartment ADWcmp1
allow group dbadmin to use network-security-groups in compartment ADWcmp1
```

Activity Auditing Resources

An administrator in Oracle Cloud Infrastructure Identity and Access Management (IAM) can grant permissions as needed on the following Activity Auditing resources. As an alternative to selectively granting permissions, you can grant permissions on `data-safe-audit-family` in the relevant compartments, which would include permissions on all of the resources below and target registration permissions.

- `data-safe-reports` Resource (see Common Resources)
- `data-safe-report-definitions` Resource (see Common Resources)
- `data-safe-work-requests` Resource (see Common Resources)

data-safe-audit-family Resource

The `data-safe-audit-family` resource represents all Oracle Data Safe resources that pertain to Activity Auditing. The resources are as follows:

- `data-safe`
- `data-safe-private-endpoints`
- `onprem-connectors`
- `data-safe-work-requests`
- `target-databases`

- data-safe-audit-profiles
- data-safe-audit-trails
- data-safe-audit-events
- data-safe-archive-retrievals
- data-safe-report-definitions
- data-safe-reports
- data-safe-audit-policies

The following table describes the permissions that you can assign to a group for the data-safe-audit-family resource.

Permission	Description
inspect	The user group can list all Activity Auditing resources in a specified compartment.
read or use	The user group can list and view properties for all Activity Auditing resources in a specified compartment.
manage	The user group can do the following: • List, view properties for, create, update, delete, and move (to another compartment) all Activity Auditing resources in a specified compartment. • Inspect, read, create, update, delete, and move Oracle Data Safe private endpoints, Oracle Data Safe on-premises connectors, and Oracle Data Safe target databases • Read work requests in Oracle Data Safe.

data-safe-archive-retrievals Resource

The data-safe-archive-retrievals resource represents archive data retrieval objects in Activity Auditing.

The following table describes the permissions available for the data-safe-archive-retrieval resource.

Permission	Description
inspect	The user group can list archive data retrievals.
read or use	The user group can list and view details for archive data retrievals.
manage	The user group can list, view details for, create, update, delete, and move (to another compartment) archive data retrievals. The group can also retrieve archive audit data and return it back to the archive.

data-safe-audit-events Resource

The data-safe-audit-events resource represents audit events for target databases in Activity Auditing.

The following table describes the permissions available for the data-safe-audit-events resource.

Permission	Description
inspect	The user group can list audit events.

Permission	Description
`read`	The user group can list and view details for audit events.

data-safe-audit-policies Resource

The `data-safe-audit-policies` resource represents audit policies for target databases in Activity Auditing.

The following table describes the permissions available for the `data-safe-audit-policies` resource.

Permission	Description
`inspect`	The user group can list audit policies.
`read` or `use`	The user group can list and view details for audit policies.
`manage`	The user group can list, view details for, create, update, delete, and move (to another compartment) audit policies.

data-safe-audit-profiles Resource

The `data-safe-audit-profiles` resource represents audit profiles for target databases in Activity Auditing.

The following table describes the permissions available for the `data-safe-audit-profiles` resource.

Permission	Description
`inspect`	The user group can list audit profiles.
`read` or `use`	The user group can list and view details for audit profiles.
`manage`	The user group can list, view details for, create, update, delete, and move (to another compartment) audit profiles. A user can update the online and offline retention periods and paid usage setting.

data-safe-audit-trails Resource

The `data-safe-audit-trails` resource represents audit trails for target databases in Activity Auditing.

The following table describes the permissions available for the `data-safe-audit-trails` resource.

Permission	Description
`inspect`	The user group can list audit trails.
`read` or `use`	The user group can list and view details for audit trails.
`manage`	The user group can list, view details for, create, update, delete, and move (to another compartment) audit trails.

Security and User Assessment Resources

An administrator in Oracle Cloud Infrastructure Identity and Access Management (IAM) can grant permissions as needed on the following Activity Auditing resources. The `data-safe-work-requests` resources is required if a user group needs to set baselines or compare assessments. As an alternative to selectively granting permissions, you can grant permissions on `data-safe-assessment-family` in the relevant compartments, which would include permissions on all of the resources below and target registration permissions.

- `data-safe-work-requests` Resource (see Common Resources)

data-safe-assessment-family Resource

The `data-safe-assessment-family` resource represents all the Oracle Data Safe resources that pertain to User Assessment and Security Assessment. The resources are as follows:

- `data-safe`
- `data-safe-private-endpoints`
- `onprem-connectors`
- `target-databases`
- `user-assessments`
- `security-assessments`
- `data-safe-work-requests`
- `data-safe-security-policy-reports`

The following table describes the permissions that you can assign to a group for the `data-safe-assessment-family` resource.

Permission	Description
`inspect`	The user group can list all Security Assessment and User Assessment resources in a specified compartment.
`read` or `use`	The user group can list and view properties for all Security Assessment and User Assessment resources in a specified compartment.
`manage`	The user group can do the following: • List, view properties for, create, update, delete, and move (to another compartment) Security Assessment and User Assessment resources in a specified compartment. • Inspect, read, create, update, delete, and move Oracle Data Safe private endpoints, Oracle Data Safe on-premises connectors, and Oracle Data Safe target databases. • Read work requests in Oracle Data Safe.

security-assessments Resource

The `security-assessments` resource represents all Security Assessment resources in Oracle Data Safe.

The following table describes the permissions available for the `security-assessments` resource.

Permission	Description
`inspect`	The user group can list Security Assessment resources.
`read` or `use`	The user group can list and view properties for Security Assessment resources.
`manage`	The user group can perform all tasks in Security Assessment, including the following: • List and view properties for Security Assessment resources • Create, update, delete, and move (to another compartment) security assessments • Refresh assessments, set and unset baseline assessments, generate and download assessment reports, and compare assessment reports

user-assessments Resource

The `user-assessments` resource represents all User Assessment resources in Oracle Data Safe.

The following table describes the permissions available for the `user-assessments` resource.

Permission	Description
`inspect`	The user group can list User Assessment resources.
`read` or `use`	The user group can list and view properties for User Assessment resources.
`manage`	The user group can perform all tasks in User Assessment, including the following: • List and view properties for User Assessment resources • Create, update, delete, and move (to another compartment) user assessments • Refresh assessments, set and unset baseline assessments, generate and download assessment reports, and compare assessment reports

`data-safe-security-policy-reports` Resource

The `data-safe-security-policy-reports` resource represents the security policy reports that provide you with the details about the schemas and tables that a user has access to as well as what privileges the user was granted on these schemas and tables. This information is available in User Assessment in Oracle Data Safe.

The following table describes the permissions available for the `data-safe-security-policy-reports` resource.

Permission	Description
`inspect`	The user group can list the security policy reports available in User Assessment.
`read` or `use`	The user group can list and view properties for the security policy reports available in User Assessment.

Data Discovery Resources

An administrator in Oracle Cloud Infrastructure Identity and Access Management (IAM) can grant permissions as needed on the following Data Discovery resources. As an alternative to selectively granting permissions, you can grant permissions on `data-safe-discovery-family` in the relevant compartments, which would include permissions on all of the resources below and target registration permissions.

- `data-safe-work-requests` Resource (see Common Resources)

data-safe-discovery-family Resource

The `data-safe-discovery-family` resource represents all Oracle Data Safe resources that pertain to Data Discovery. The resources are as follows:

- `data-safe`
- `data-safe-private-endpoints`
- `onprem-connectors`
- `target-databases`
- `data-safe-sensitive-data-models`
- `data-safe-sensitive-type-group`
- `data-safe-sensitive-types`
- `data-safe-sensitive-types-export`
- `data-safe-discovery-jobs`
- `data-safe-work-requests`

The following table describes the permissions that you can assign to a group for the `data-safe-discovery-family` resource.

Permission	Description
`inspect`	The user group can list all Data Discovery resources in a specified compartment.
`read` or `use`	The user group can list and view properties for all Data Discovery resources in a specified compartment.

Permission	Description
`manage`	The user group can do the following: • List, view properties for, create, update, delete, and move (to another compartment) all Data Discovery resources in a specified compartment. • Inspect, read, create, update, delete, and move Oracle Data Safe private endpoints, Oracle Data Safe on-premises connectors, and Oracle Data Safe target databases. • Read work requests in Oracle Data Safe.

data-safe-discovery-jobs Resource

The `data-safe-discovery-jobs` resource represents incremental data discovery jobs in Oracle Data Safe.

The following table describes the permissions available for the `data-safe-discovery-jobs` resource.

Permission	Description
`inspect`	The user group can list incremental data discovery jobs.
`read` or `use`	The user group can list and view properties of incremental data discovery jobs.
`manage`	The user group can perform all tasks with incremental data discovery jobs, including the following: • List and view properties of incremental data discovery jobs • Create, update, delete, and move (to another compartment) incremental data discovery jobs

data-safe-sensitive-data-models Resource

The `data-safe-sensitive-data-models` resource represents sensitive data models in Data Discovery.

The following table describes the permissions available for the `data-safe-sensitive-data-models` resource.

Permission	Description
`inspect`	The user group can list sensitive data models.
`read` or `use`	The user group can list and view properties of sensitive data models.
`manage`	The user group can perform all tasks with sensitive data models, including the following: • List and view properties of sensitive data models • Run a data discovery job • Create, update, delete, and move (to another compartment) sensitive data models

data-safe-sensitive-type-group Resource

The `data-safe-sensitive-type-group` resource represents sensitive type groups in Data Discovery.

The following table describes the permissions available for the `data-safe-sensitive-type-group` resource.

Permission	Description
`inspect`	The user group can list all sensitive type group resources.
`read` or `use`	The user group can list and view properties for all sensitive type group resources.
`manage`	The user group can perform all tasks with sensitive type groups, including the following: • List and view properties of sensitive type groups • Create, update, delete, and move (to another compartment) sensitive type groups **Note:** The user group cannot update, delete, or move the Oracle-defined common sensitive type group.

data-safe-sensitive-types Resource

The `data-safe-sensitive-types` resource represents sensitive types in Data Discovery.

The following table describes the permissions available for the `data-safe-sensitive-types` resource.

Permission	Description
`inspect`	The user group can list Oracle-defined and user-defined sensitive types.
`read` or `use`	The user group can list and view properties of Oracle-defined and user-defined sensitive types.

Permission	Description
`manage`	The user group can perform all tasks with sensitive types, including the following: • List and view properties of Oracle-defined and user-defined sensitive types • Create, update, delete, and move (to another compartment) user-defined sensitive types **Note:** The user group cannot update, delete, or move an Oracle-defined sensitive type.

data-safe-sensitive-types-export Resource

The `data-safe-sensitive-types-export` resource contains an XML file with exported sensitive types and categories, along with metadata about the export, including the creation timestamp, name, description, and other relevant details.

The following table describes the permissions available for the `data-safe-sensitive-types-export` resource.

Permission	Description
`inspect`	The user group can list all sensitive types export resources in a specified compartment.
`read` or `use`	The user group can list and view properties for all sensitive types export resources and download the corresponding XML files in a specified compartment.
`manage`	The user group can list, view properties for, create, update, delete, and move (to another compartment) sensitive types export resources in a specified compartment.

Related Topics

- Export and Upload User-Defined Sensitive Types

Data Masking Resources

An administrator in Oracle Cloud Infrastructure Identity and Access Management (IAM) can grant permissions as needed on the following Data Masking resources. As an alternative to selectively granting permissions, you can grant permissions on `data-safe-masking-family` in the relevant compartments, which would include permissions on all of the resources below and target registration permissions.

- `data-safe-work-requests` Resource (see Common Resources)

data-safe-masking-family Resource

The `data-safe-masking-family` resource represents all Oracle Data Safe resources that pertain to Data Masking. The resources are as follows:

- `data-safe`
- `data-safe-private-endpoints`
- `onprem-connectors`
- `target-databases`
- `data-safe-masking-policies`
- `data-safe-library-masking-formats`
- `data-safe-masking-reports`
- `data-safe-masking-policy-healthreport`
- `data-safe-work-requests`

The following table describes the permissions that you can assign to a group for the `data-safe-masking-family` resource.

Permissions	Description
`inspect`	The user group can list all Data Masking resources in a specified compartment.
`read` or `use`	The user group can list and view properties for all Data Masking resources in a specified compartment.
`manage`	The user group can do the following: • List, view properties for, create, update, delete, and move (to another compartment) all Data Masking resources in a specified compartment. • Inspect, read, create, update, delete, and move Oracle Data Safe private endpoints, Oracle Data Safe on-premises connectors, and Oracle Data Safe target databases • Read work requests in Oracle Data Safe.

data-safe-library-masking-formats Resource

The `data-safe-library-masking-formats` resource represents Oracle-defined and user-defined masking formats in Data Masking.

The following table describes the permissions available for the `data-safe-library-masking-formats` resource.

Permission	Description
`inspect`	The user group can list Oracle-defined and user-defined masking formats in Data Masking.
`read` or `use`	The user group can list and view properties of Oracle-defined and user-defined masking formats in Data Masking.

Permission	Description
`manage`	The user group can perform all tasks with masking formats, including the following: • List and view properties of Oracle-defined and user-defined masking formats in Data Masking • Create, update, delete, and move (to another compartment) user-defined masking formats **Note:** The user group cannot update, delete, or move Oracle-predefined masking formats.

data-safe-masking-policies Resource

The `data-safe-masking-policies` resource represents masking policies in Data Masking.

The following table describes the permissions available for the `data-safe-masking-policies` resource.

Permission	Description
`inspect`	The user group can list masking policies.
`read` or `use`	The user group can list and view properties of masking policies.
`manage`	The user group can perform all tasks with masking policies, including the following: • List and view properties of masking policies • Create, update, delete, and move (to another compartment) masking policies

data-safe-masking-reports Resource

The `data-safe-masking-reports` resource represents reports in Data Masking.

The following table describes the permissions available for the `data-safe-masking-reports` resource.

Permission	Description
`inspect`	The user group can list masking reports.
`read` or `use`	The user group can list and view properties of masking reports.
`manage`	The user group can perform all tasks with masking reports, including the following: • List and view properties of masking reports • Run a data masking job • Update masking reports

data-safe-masking-policy-healthreport Resource

The `data-safe-masking-policy-healthreport` resource represents pre-masking reports in Data Masking.

The following table describes the permissions available for the `data-safe-masking-policy-healthreport` resource.

Permission	Description
`inspect`	The user group can list pre-masking reports.
`read` or `use`	The user group can list and view properties of pre-masking reports.
`manage`	The user group can perform all tasks with pre-masking reports, including the following: • List and view properties of pre-masking reports • Run a pre-masking check • Move pre-masking reports to a different compartment • Delete the pre-masking report

Alert Resources

An administrator in Oracle Cloud Infrastructure Identity and Access Management (IAM) can grant permissions as needed on the following Alert resources. As an alternative to selectively granting permissions, you can grant permissions on `data-safe-alert-family` in the relevant compartments, which would include permissions on all of the resources below and target registration permissions.

- `data-safe-reports` Resource (see Common Resources)
- `data-safe-report-definitions` Resource (see Common Resources)
- `data-safe-work-requests` Resource (see Common Resources)

data-safe-alert-family Resource

The `data-safe-alert-family` resource represents all Oracle Data Safe resources that pertain to alerts. The resources are as follows:

- `data-safe`
- `data-safe-private-endpoints`
- `onprem-connectors`
- `data-safe-work-requests`
- `target-databases`
- `data-safe-alerts`
- `data-safe-alert-policies`
- `data-safe-target-alert-policy-associations`

The following table describes the permissions that you can assign to a group for the `data-safe-alert-family` resource.

Permission	Description
`inspect`	The user group can list all alert resources in a specified compartment.
`read` or `use`	The user group can list and view properties for all alert resources in a specified compartment.
`manage`	The user group can do the following: • List, view properties for, create, update, delete, and move (to another compartment) all alert resources in a specified compartment. • Inspect, read, create, update, delete, and move Oracle Data Safe private endpoints, Oracle Data Safe on-premises connectors, and Oracle Data Safe target databases. • Read work requests in Oracle Data Safe.

data-safe-alerts Resource

The `data-safe-alerts` resource represents alerts in Oracle Data Safe.

The following table describes the permissions available for the `data-safe-alerts` resource.

Permission	Description
`inspect`	The user group can list alerts.
`read` or `use`	The user group can list and view details for alerts.
`manage`	The user group can perform the following tasks with alerts: • List and view details for alerts • Update, delete, and move (to another compartment) alerts.

data-safe-alert-policies Resource

The `data-safe-alert-policies` resource represents alert policies for target databases.

The following table describes the permissions available for the `data-safe-alert-policies` resource.

Permission	Description
`inspect`	The user group can list alert policies.
`read` or `use`	The user group can list and view details for alert policies.
`manage`	The user group can perform all tasks with alert policies, including the following: • Create custom alert policies • List and view details for alert policies • Create, update, delete, and move (to another compartment) alert policies.

data-safe-target-alert-policy-associations Resource

The `data-safe-target-alert-policy-associations` resource represents target database associations with alert policies (referred to as just target-policy associations).

The following table describes the permissions available for the `data-safe-target-alert-policy-associations` resource.

Permission	Description
`inspect`	The user group can list target-policy associations.
`read` or `use`	The user group can list and view details for target-policy associations.
`manage`	The user group can perform all tasks with target-policy associations, including the following: • List and view details for target-policy associations • Create, update, delete, and move (to another compartment) target-policy associations.

SQL Firewall Resources

An administrator in Oracle Cloud Infrastructure Identity and Access Management (IAM) can grant permissions as needed on the following SQL Firewall resources.

`data-safe-sql-firewall-family` Resource

The `data-safe-sql-firewall-family` resource represents all Oracle Data Safe resources that pertain to SQL Firewall. The resources are as follows:

Common resources for which information can be found in the *Administering Oracle Data Safe* guide:

- data-safe
- data-safe-private-endpoints
- onprem-connectors
- data-safe-work-requests
- target-databases
- data-safe-audit-policies
- data-safe-reports
- data-safe-report-definitions

SQL Firewall resources:

- data-safe-database-security-configs
- data-safe-security-policies
- data-safe-security-policy-deployments
- data-safe-sql-collections
- data-safe-sql-firewall-policies
- data-safe-sql-firewall-allowed-sqls
- data-safe-sql-firewall-violations

The following table describes the permissions that you can assign to a group for the `data-safe-sql-firewall-family` resource.

Permission	Description
`inspect`	The user group can list all SQL Firewall resources in a specified compartment.

Permission	Description
`read` or `use`	The user group can list and view properties for all SQL Firewall resources in a specified compartment
`manage`	The user group can do the following: • List, view properties for, create, update, delete, and move (to another compartment) all SQL Firewall resources in a specified compartment. • Inspect, read, create, update, delete, and move Oracle Data Safe private endpoints, Oracle Data Safe on-premises connectors, and Oracle Data Safe target databases • Read work requests in Oracle Data Safe.

`data-safe-database-security-configs` Resource

The `data-safe-database-security-configs` resource represents security configurations for target databases in SQL Firewall.

The following table describes the permissions available for the `data-safe-database-security-configs` resource.

Permission	Description
`inspect`	The user group can list database security configurations.
`read` or `use`	The user group can list and view details for database security configurations.
`manage`	The user group can list, view details for, update, and move (to another compartment) database security configurations.

`data-safe-security-policies` Resource

The `data-safe-security-policies` resource represents the security policies for target databases in SQL Firewall.

The following table describes the permissions available for the `data-safe-security-policies` resource.

Permission	Description
`read` or `use`	The user group can list and view details for database security policies.
`inspect`	The user group can list database security policies.
`manage`	The user group can list, view details for, create, update, and move (to another compartment) database security policies.

`data-safe-security-policy-deployments` Resource

The `data-safe-security-policy-deployments` resource represents the state of the deployment of a security policy on a target. This resource provides mapping for all target databases to all security policies, such as a SQL Firewall policy.

The following table describes the permissions available for the `data-safe-security-policy-deployments` resource.

Permission	Description
`inspect`	The user group can list database security policy deployments.

Permission	Description
`read` or `use`	The user group can list and view details for database security policy deployments.
`manage`	The user group can list, view details for, create, update, and move (to another compartment) database security policy deployments.

`data-safe-sql-collections` Resource

The `data-safe-sql-collections` resource represents the SQL collections for target databases in SQL Firewall.

The following table describes the permissions available for the `data-safe-sql-collections` resource.

Permission	Description
`inspect`	The user group can list the SQL collections.
`read` or `use`	The user group can list and view details for the SQL collections.
`manage`	The user group can list, view details for, create, update, delete, and move (to another compartment) the SQL collections.

`data-safe-sql-firewall-policies` Resource

The `data-safe-sql-firewall-policies` resource represents the SQL Firewall policies for target databases in SQL Firewall.

The following table describes the permissions available for the `data-safe-sql-firewall-policies` resource.

Permission	Description
`inspect`	The user group can list the SQL Firewall policies.
`read` or `use`	The user group can list and view details for the SQL Firewall policies.
`manage`	The user group can list, view details for, create, update, delete, and move (to another compartment) the SQL Firewall policies.

`data-safe-sql-firewall-allowed-sqls` Resource

The `data-safe-sql-firewall-allowed-sqls` resource represents the list of allowed SQL statements for target databases in SQL Firewall.

The following table describes the permissions available for the `data-safe-sql-firewall-allowed-sqls` resource.

Permission	Description
`inspect`	The user group can list the allowed SQL statements.
`read`	The user group can list and view details for the allowed SQL statements.

`data-safe-sql-firewall-violations` Resource

The `data-safe-sql-firewall-violations` resource represents the SQL and context violations for target databases in SQL Firewall.

The following table describes the permissions available for the `data-safe-sql-firewall-violations` resource.

Permission	Description
`inspect`	The user group can list the SQL and context violations.
`read`	The user group can list and view details for the SQL and context violations.

Common Resources

The following resources are optional for multiple Oracle Data Safe features.

data-safe Resource

The `data-safe` resource represents the global settings for paid usage and audit data retention for Oracle Data Safe.

The following table describes the permissions available for the `data-safe` resource.

Permission	Description
`read` or `use`	The user group can view global settings for paid usage and details for audit data retention.
`manage`	The user group can set global settings for paid usage and audit data retention.

data-safe-report-definitions Resource

The `data-safe-report-definitions` resource represents Oracle predefined and custom Activity Auditing and Alert reports.

The following table describes the permissions available for the `data-safe-report-definitions` resource.

Permission	Description
`inspect`	The user group can list Oracle predefined and custom Activity Auditing and Alert reports.
`read` or `use`	The user group can list and view details for Oracle predefined and custom Activity Auditing and Alert reports.
`manage`	The user group can perform all tasks with Oracle predefined and custom Activity Auditing and Alert reports, including the following: • List and view details for custom reports • Create, update, delete, and move (to another compartment) custom reports. • Create, update, and delete schedules for generating audit reports in PDF/XLS format.

data-safe-reports Resource

The `data-safe-reports` resource represents generated PDF and XLS reports. This resource applies only to Oracle predefined and custom Activity Auditing and Alert reports.

The following table describes the permissions available for the `data-safe-reports` resource.

Permission	Description
`inspect`	The user group can list generated PDF and XLS reports.
`read` or `use`	The user group can list and view details for generated PDF and XLS reports.
`manage`	The user group can perform the following tasks with generated PDF and XLS reports: • List and view details for generated PDF and XLS reports • Update, move (to another compartment), and generate PDF and XLS reports

data-safe-work-requests Resource

The `data-safe-work-requests` resource represents all the work requests that correspond to Oracle Data Safe in Oracle Cloud Infrastructure. For example, when a user creates an Oracle Data Safe private endpoint or generates a comparison report in Security Assessment, Oracle Data Safe issues a work request.

> **Note:**
>
> `read` permission on the `data-safe-work-requests` resource is required for a user to be able to set baselines and compare assessments in User Assessment and Security Assessment.

The information about the work request is available through Oracle Data Safe 's API. For more information about the API, see WorkRequest Reference.

The following table describes the permissions available for the `data-safe-work-requests` resource.

Permission	Description
`inspect`	The user group can list Oracle Data Safe work requests without access to any confidential information or user-specific metadata that may be part of the work request.
`read` or `use`	The user group has `inspect` permission plus can do the following: • Get user-specified metadata and the actual resource itself • Set baselines and compare assessments in User Assessment and Security Assessment.
`manage`	The user group has all permissions on Oracle Data Safe work requests (create, update, move, and so on).

Example 2-8 Allow a user group to compare assessments in Security Assessment

The following policy statements allow a user group named `IT-Security` to compare security assessments in the compartment named `Info-Tech`.

```
allow group IT-Security to manage security-assessments in compartment Info-
Tech
allow group IT-Security to read data-safe-work-requests in compartment Info-
Tech
```

What Resources Can Be Deleted While a Target Database is Active

While a target database is active in Oracle Data Safe, only some of the associated resources can be manually deleted. See the table below to identify which resources can and can't be manually deleted while a target database is active.

Functional Area	Data Safe Resource	Data Safe Resource Name in OCI IAM	Can this resource be manually deleted while the associated target database is active?
Connectivity	Private Endpoint	data-safe-private-endpoints	No
Connectivity	On-premises Connector	onprem-connectors	No
Activity Auditing	Audit Profile	data-safe-audit-profiles	No
Activity Auditing	Audit Trail	data-safe-audit-trails	Yes
Activity Auditing	Audit Event	data-safe-audit-events	No
Activity Auditing	Audit Policy	data-safe-audit-policies	No
Activity Auditing/Alerts	Target Alert Policy Associations	data-safe-target-alert-policy-associations	Yes
Activity Auditing/Alerts	Alert	data-safe-alerts	No
Activity Auditing/Alerts	Custom Report Definition	data-safe-report-definitions	Yes
Activity Auditing/Alerts	Report	data-safe-reports	No
Activity Auditing	Archive Retrievals	data-safe-archive-retrievals	Yes
User Assessment	Latest User Assessment	user-assessments	No
User Assessment	User Assessment	user-assessments	Yes
Security Assessment	Latest Security Assessment	security-assessments	No
Security Assessment	Security Assessment	security-assessments	Yes
Data Discovery	Sensitive Data Model	data-safe-sensitive-data-models	Yes
Data Discovery	Data Safe Pre-defined Sensitive Types	data-safe-sensitive-types	No
Data Discovery	Custom Sensitive Types	data-safe-sensitive-types	Yes
Data Discovery	Discovery Job	data-safe-discovery-jobs	Yes
Data Masking	Masking Policy	data-safe-masking-policies	Yes
Data Masking	Data Safe Pre-defined Masking Formats	data-safe-library-masking-formats	No
Data Masking	Custom Masking Formats	data-safe-library-masking-formats	Yes
Data Masking	Masking Report	data-safe-masking-reports	Yes
SQL Firewall	Database Security Config	data-safe-database-security-configs	No
SQL Firewall	Security Policy	data-safe-security-policies	No

Functional Area	Data Safe Resource	Data Safe Resource Name in OCI IAM	Can this resource be manually deleted while the associated target database is active?
SQL Firewall	Security Policy Deployment	data-safe-security-policy-deployments	No
SQL Firewall	Firewall Policy	data-safe-sql-firewall-policies	Yes
SQL Firewall	SQL Collection	data-safe-sql-collections	Yes
SQL Firewall	Violation Logs	data-safe-sql-firewall-violations	No
SQL Firewall	SQL Firewall Allowed SQL	data-safe-sql-firewall-allowed-sqls	No

Create IAM Policies for Oracle Data Safe Users

A tenancy administrator can create policies in Oracle Cloud Infrastructure Identity and Access Management (IAM) that grant users access to resources for Oracle Data Safe.

General Steps for Creating an IAM Policy for Oracle Data Safe

Follow these general steps to create an IAM policy that grants a user group permissions on Oracle Data Safe resources.

1. As a tenancy administrator, from the navigation menu in Oracle Cloud Infrastructure, select **Identity and Security**, and then click **Policies** on the right.

   The **Policies** page is displayed in Oracle Cloud Infrastructure Identity and Access Management (IAM).
2. Under **List Scope**, select the compartment in which you want to store the policy. You can select the `root` compartment, if needed.
3. Click **Create Policy**.

   The **Create Policy** page is displayed.
4. Enter a name for your policy. No spaces are allowed. Only letters, numerals, hyphens, periods, and underscores are allowed.
5. Enter a brief description for your policy.
6. Select a different compartment if needed.
7. In the **Policy Builder** section, move the **Show manual editor** slider to the right.

   A box is displayed where you can enter policy statements.
8. Enter one or more policy statements using the following syntax.

   ```
   Allow group <group-name> to <verb> <resource-type> in compartment
   <compartment-name>
   ```

   For `<group-name>`, enter the name of the IAM group to which the policy applies.

   For `<verb>`, you can use `inspect`, `read`, `use`, or `manage`.

For `<resource-type>`, enter a resource that is used by Oracle Data Safe. For a list of resources, see OCI Resources for Oracle Data Safe.

For `<compartment>`, enter the name of the compartment that contains the resources to which you want to grant permissions.

To specify subcompartments in a policy statement, use the following syntax, where `<parent-compartment>` is the compartment under the `root` compartment and `<child-compartment>` is the compartment under the `<parent-compartment>`. You can add as many child compartments as needed separated by a colon.

```
allow group <group-name> to <verb> <resource-type> in compartment <parent-compartment>:<child-compartment>
```

9. To add tags, click **Show Advanced Options** and configure tags.
10. Click **Create**.

Create an Oracle Data Safe Administrators Group

A tenancy administrator can create an Oracle Data Safe administrators group in Oracle Cloud Infrastructure Identity and Access Management (IAM). The purpose of this group is to oversee and manage the Oracle Data Safe resources in a region.

1. As a tenancy administrator, access IAM in Oracle Cloud Infrastructure.
2. Create a group for Oracle Data Safe administrators and appropriate users to the group.
3. Create a policy for the Oracle Data Safe administrators group that allows the group to `manage` the `data-safe-family` resource. The following examples show you different ways to do this.
   - **Option 1:** Allow the `Data-Safe-Admins` group to manage Oracle Data Safe resources across the entire tenancy.

     ```
     Allow group Data-Safe-Admins to manage data-safe-family in tenancy
     ```

   - **Option 2:** Allow the `Data-Safe-Admins` group to manage all types of Oracle Cloud Infrastructure resources in the tenancy (including Oracle Data Safe resources).

     ```
     Allow group Data-Safe-Admins to manage all-resources in tenancy
     ```

   - **Option 3:** Allow a `Data-Safe-Admins` group to manage all types of Oracle Data Safe resources in the `us-phoenix-1` region of a tenancy.

     ```
     Allow group Data-Safe-Admins to manage data-safe-family in tenancy
     where request.region='phx'
     ```

Permission to Access all Resources of an Oracle Data Safe Feature

You can use an Oracle Data Safe family resource to quickly grant a user group permission on all resources for a particular Oracle Data Safe feature. For example, to grant a user group permission to perform all tasks in Data Masking, grant the user group the `manage` permission on the `data-safe-masking-family` resource. Family resources that pertain to specific features include `data-safe-assessment-family` (for Security Assessment and User Assessment),

`data-safe-discovery-family` (for Data Discovery), `data-safe-masking-family` (for Data Masking), `data-safe-alert-family` (for Alerts), `data-safe-audit-family` (for Activity Auditing), and `data-safe-family` (for all features).

To grant a user group permission to access an Oracle Data Safe feature, create a policy in Oracle Cloud Infrastructure Identity and Access Management (IAM) that allows the group to either `list`, `read`, `use`, or `manage` resources for the feature.

Here are two examples:

- **Example 1:** To allow a group to list and view details for all resources for a particular Oracle Data Safe family in a specific compartment, write the policy statement the following way:

  ```
  allow group <group-name> to read <data-safe-family-name> in compartment
  <compartment-name>
  ```

- **Example 2:** To allow a group to perform any and all tasks related to a Oracle Data Safe feature in a specific compartment, write the policy statement the following way:

  ```
  allow group <group-name> to manage <data-safe-family-name> in compartment
  <compartment-name>
  ```

Permission to Access a Specific Resource

Each Oracle Data Safe family resource consists of several resources that pertain to that feature. In most cases, you can grant a user group the `inspect`, `read`, `use`, or `manage` permission on any one of those specific resources, rather than grant the group access to all the resources in the family.

- The `inspect` permission allows a user group to view the list of resource objects. For example, if a group has `inspect` permission on the `data-safe-audit-policies` resource, then that group can view the list of audit policies in Security Center. They cannot, however, click on an audit policy and view its details.
- The `read` permission allows a user group to view the list of resource objects and view their properties. Using our previous example, the user group can click on an audit policy and view its details.
- The `use` permission includes the `read` permission plus the ability to work with existing resources (the actions vary by resource type). It includes the ability to update the resource, except for resource-types where the update operation has the same effective impact as the create operation, in which case the update ability is available only with the `manage` verb. In general, this verb does not include the ability to create or delete that type of resource.
- The `manage` permission generally grants the user group full permission on the resource (list, view, update, create, delete, and move). Using our previous example, if the group has the `manage` permission, it can list and view details for audit policies, as well as update, create, delete, and move them.

Keep in mind that all four permissions (inspect, read, use, and manage) may not be available for all resources. And, sometimes the `manage` permission grants only a subset of operations (for example: list, read, update, create, delete, and/or move). Therefore, it's best to refer to the resource itself to understand what is possible.

Here are three examples:

- **Example 1:** Create a policy for a user group that allows the group to list resource objects in Security Center. For example, the following policy statement allows a user group named `IT-Security` to view the list of audit profiles in the compartment named `Info-Tech`.

  ```
  allow group IT-Security to inspect data-safe-audit-profiles in compartment
  Info-Tech
  ```

- **Example 2:** Create a policy for a user group that allows the group to list and view properties for a resource. For example, the following policy statement allows a user group named `IT-Security` to list and view properties for audit profiles in the compartment named `Info-Tech`.

  ```
  allow group IT-Security to read data-safe-audit-profiles in compartment
  Info-Tech
  ```

- **Example 3:** Create a policy for a user group that allows the group to manage a resource. For example, the following policy statement allows a user group named `IT-Security` to manage audit profiles in the compartment named `Info-Tech`.

  ```
  allow group IT-Security to manage data-safe-audit-profiles in compartment
  Info-Tech
  ```

Permissions to Register an Autonomous Database with Oracle Data Safe

To register an Autonomous Database with Oracle Data Safe, a user group requires permissions in Oracle Cloud Infrastructure Identity and Access Management (IAM) to do the following:

- **Access the Autonomous Database:** The user group requires at least the `use` permission on the `autonomous-database` resource in Oracle Cloud Infrastructure, for example:

  ```
  allow group <group-name> to use autonomous-database in compartment
  <compartment-name>
  ```

- **Register a target database with Oracle Data Safe:** The user group requires the `manage` permission on the `target-databases` resource, for example:

  ```
  allow group <group-name> to manage target-databases in compartment
  <compartment-name>
  ```

- **For an Autonomous Databases that has a private IP address:** The user group requires at least the `use` permission on an Oracle Data Safe private endpoint and on the underlying virtual networking resources of the private endpoint for the relevant compartments. For example, the following statements allow a group to create a private endpoint:

  ```
  allow group <group-name> to manage data-safe-private-endpoints in
  compartment <compartment-name>
  allow group <group-name> to manage virtual-network-family in compartment
  <compartment-name>
  ```

  If the group already has an Oracle Data Safe private endpoint and wants to reuse it, then replace `manage` with `use` in the statements above.

For more information about the resources and their permissions, see OCI Resources for Oracle Data Safe.

Permissions to Register an Oracle Cloud Database with Oracle Data Safe

To register an Oracle Cloud Database with Oracle Data Safe, a user group requires permissions in Oracle Cloud Infrastructure Identity and Access Management (IAM) to do the following:

- **Access the Oracle Cloud Database:**

  ```
  allow group <group-name> to manage database-family in compartment
  <compartment-name>
  allow group <group-name> to inspect vnics in tenancy
  ```

- **(Exadata Cloud Service only) Inspect cloud virtual machine clusters in the tenancy:**

  ```
  allow group <group-name> to inspect cloud-vmclusters in tenancy
  ```

- **Register a target database with Oracle Data Safe:**

  ```
  allow group <group-name> to manage target-databases in compartment
  <compartment-name>
  ```

- **Use or create an Oracle Data Safe private endpoint:** The user group requires at least the `use` permission on an Oracle Data Safe private endpoint and on the underlying virtual networking resources of the private endpoint for the relevant compartments. For example, the following statements allow a group to create a private endpoint:

  ```
  allow group <group-name> to manage data-safe-private-endpoints in
  compartment <compartment-name>
  allow group <group-name> to manage virtual-network-family in compartment
  <compartment-name>
  ```

  If the group already has an Oracle Data Safe private endpoint and wants to reuse it, then replace `manage` with `use` in the statements above.

For more information about the resources and their permissions, see OCI Resources for Oracle Data Safe.

Permissions to Register an On-Premises Oracle Database with Oracle Data Safe

To register an on-premises Oracle database with Oracle Data Safe, a user group requires permissions in Oracle Cloud Infrastructure Identity and Access Management (IAM) to do the following:

- **Register a target database with Oracle Data Safe:**

  ```
  allow group <group-name> to manage target-databases in compartment
  <compartment-name>
  ```

- **(Option 1) Use or create an Oracle Data Safe private endpoint:** If your target database has a private IP address, you can connect to it using an Oracle Data Safe private endpoint. The user group requires at least the `use` permission on an Oracle Data Safe private endpoint and on the underlying virtual networking resources of the private endpoint for the relevant compartments. For example, the following statements allow a group to create a private endpoint:

  ```
  allow group <group-name> to manage data-safe-private-endpoints in
  compartment <compartment-name>
  allow group <group-name> to manage virtual-network-family in compartment
  <compartment-name>
  ```

  If the group already has an Oracle Data Safe private endpoint and wants to reuse it, then replace `manage` with `use` in the statements above.

- **(Option 2) Use or create an Oracle Data Safe on-premises connector:** If your target database has a private IP address, you can connect to it using an Oracle Data Safe on-premises connector. Include permission to access or create an on-premises connector, for example:

  ```
  allow group <group-name> to manage onprem-connectors in compartment
  <compartment-name>
  ```

For more information about the resources and their permissions, see OCI Resources for Oracle Data Safe.

Permissions to Register an Oracle Database on Compute with Oracle Data Safe

To register an Oracle Database on Compute with Oracle Data Safe, a user group requires permissions in Oracle Cloud Infrastructure Identity and Access Management (IAM) to do the following:

- **Register a target database with Oracle Data Safe:**

  ```
  allow group <group-name> to manage target-databases in compartment
  <compartment-name>
  ```

- **(Option 1) Use or create an Oracle Data Safe private endpoint:** The user group requires at least the `use` permission on an Oracle Data Safe private endpoint and on the underlying virtual networking resources of the private endpoint for the relevant compartments. For example, the following statements allow a group to create a private endpoint:

  ```
  allow group <group-name> to manage data-safe-private-endpoints in
  compartment <compartment-name>
  allow group <group-name> to manage virtual-network-family in compartment
  <compartment-name>
  ```

  If the group already has an Oracle Data Safe private endpoint and wants to reuse it, then replace `manage` with `use` in the statements above.

- **(Option 2) Use or create an Oracle Data Safe on-premises connector:** Include permission to use or create an Oracle Data Safe on-premises connector, for example:

```
allow group <group-name> to manage onprem-connectors in compartment
<compartment-name>
```

For more information about the resources and their permissions, see OCI Resources for Oracle Data Safe.

Permissions to Register an Oracle Cloud@Customer Database with Oracle Data Safe

To register an Oracle Cloud@Customer database (Exadata Database on Cloud@Customer or Autonomous Database on Exadata Cloud@Customer database) with Oracle Data Safe, a user group requires permissions in Oracle Cloud Infrastructure Identity and Access Management (IAM) to do the following:

- **Register a target database with Oracle Data Safe:**

```
allow group <group-name> to manage target-databases in compartment
<compartment-name>
```

- **(Exadata Database on Cloud@Customer) Register or update the target database:**

```
allow group <group-name> to inspect exadata-infrastructures in compartment
<compartment-name>
allow group <group-name> to inspect vmcluster-network in compartment
<compartment-name>
```

- **(Autonomous Database on Exadata Cloud@Customer) Register or update the target database:**

```
allow group <group-name> to read autonomous-databases in compartment
<compartment-name>
allow group <group-name> to inspect autonomous-container-databases in
compartment <compartment-name>
allow group <group-name> to inspect autonomous-vmclusters in compartment
<compartment-name>
allow group <group-name> to inspect exadata-infrastructures in compartment
<compartment-name>
allow group <group-name> to inspect vmcluster-network in compartment
<compartment-name>
```

- **(Option 1) Use or create an Oracle Data Safe private endpoint:** The user group requires at least the `use` permission on an Oracle Data Safe private endpoint and on the underlying virtual networking resources of the private endpoint for the relevant compartments. For example, the following statements allow a group to create a private endpoint:

```
allow group <group-name> to manage data-safe-private-endpoints in
compartment <compartment-name>
allow group <group-name> to manage virtual-network-family in compartment
<compartment-name>
```

If the group already has an Oracle Data Safe private endpoint and wants to reuse it, then replace `manage` with `use` in the statements above.

- **(Option 2) Use or create an Oracle Data Safe on-premises connector:** Include permission to use or create an Oracle Data Safe on-premises connector, for example:

```
allow group <group-name> to manage onprem-connectors in compartment
<compartment-name>
```

For more information about the resources and their permissions, see OCI Resources for Oracle Data Safe.

Permissions to Register a Target Database with Oracle Data Safe

To register a target database with Oracle Data Safe, a user group requires permissions in Oracle Cloud Infrastructure Identity and Access Management (IAM) to do the following:

Register a target database with Oracle Data Safe:

```
allow group <group-name> to manage target-databases in compartment
<compartment-name>
```

For more information about the resources and their permissions, see OCI Resources for Oracle Data Safe.

Permissions for an Oracle Data Safe Private Endpoint

Use or create an Oracle Data Safe private endpoint, a user group requires permissions in Oracle Cloud Infrastructure Identity and Access Management (IAM) to do the following:

If your target database has a private IP address, you can connect to it using an Oracle Data Safe private endpoint. The user group requires at least the `use` permission on an Oracle Data Safe private endpoint and on the underlying virtual networking resources of the private endpoint for the relevant compartments. For example, the following statements allow a group to create a private endpoint:

```
allow group <group-name> to manage data-safe-private-endpoints in compartment
<compartment-name>
allow group <group-name> to manage virtual-network-family in compartment
<compartment-name>
```

If the group already has an Oracle Data Safe private endpoint and wants to reuse it, then replace `manage` with `use` in the statements above.

For more information about the resources and their permissions, see OCI Resources for Oracle Data Safe.

Permissions for an Oracle Data Safe On-Premises Connector

Use or create an Oracle Data Safe on-premises connector, a user group requires permissions in Oracle Cloud Infrastructure Identity and Access Management (IAM) to do the following:

If your target database has a private IP address, you can connect to it using an Oracle Data Safe on-premises connector. Include permission to access or create an on-premises connector, for example:

```
allow group <group-name> to manage onprem-connectors in compartment
<compartment-name>
```

For more information about the resources and their permissions, see OCI Resources for Oracle Data Safe.

Permission to Run Assessments and View Audit and Alert Data

If a user group only needs to be able to run assessments and view audit and alert data, you can create a policy with the following statements. With this policy, the user group cannot change masking policies, mask sensitive data, discover sensitive data, or register target databases.

```
allow group <user-group> to manage data-safe-assessment-family in compartment
<compartment name>
Allow group <user-group> to read data-safe-report-definitions in compartment
<compartment-name>
Allow group <user-group> to read data-safe-reports in compartment
<compartment-name>
Allow group <user-group> to read data-safe-alerts in compartment <compartment-
name>
```

Permissions to Discover Sensitive Data

A tenancy administrator can grant permissions on specific Data Discovery resources in specified compartments in Oracle Cloud Infrastructure Identity and Access Management to allow a user group to perform certain tasks.

Here are some examples.

Example 2-9 Run data discovery jobs (create sensitive data models)

```
allow group <user-group> to manage data-safe-sensitive-data-models in
compartment <compartment-name>
allow group <group-name> to read target-databases in compartment <compartment-
name>
```

Example 2-10 Run incremental data discovery jobs on target databases

```
allow group <user-group> to manage data-safe-discovery-jobs in compartment
<compartment-name>
allow group <user-group> to read data-safe-sensitive-data-models in
compartment <compartment-name>
allow group <user-group> to read data-safe-work-requests in compartment
<compartment-name>
```

Example 2-11 Create sensitive types

```
allow group <user-group> to manage data-safe-sensitive-types in compartment
<compartment-name>
```

Example 2-12 Perform all tasks in Data Discovery

```
allow group <user-group> to manage data-safe-discovery-family in compartment
<compartment-name>
```

Permission to Mask Sensitive Data

A tenancy administrator can grant permissions on specific Data Masking resources in specified compartments in Oracle Cloud Infrastructure Identity and Access Management to allow a user group to perform certain tasks.

Here are some examples.

Example 2-13 Mask sensitive data on target databases in a specified compartment using a precreated masking policy

```
allow group <user-group> to manage data-safe-masking-policies in compartment
<compartment-name>
allow group <user-group> to manage data-safe-masking-reports in compartment
<compartment-name>
allow group <user-group> to read data-safe-work-requests in compartment
<compartment-name>
allow group <user-group> to read target-databases in compartment <compartment-
name>
```

Example 2-14 Create and manage masking policies in a specified compartment

```
allow group <user-group> to manage data-safe-masking-policies in compartment
<compartment-name>
```

Example 2-15 Create and manage library masking formats in a specified compartment

```
allow group <user-group> to manage data-safe-library-masking-formats in
compartment <compartment-name>
```

Permissions to Use Contextual Event Notifications

In Data Safe you can create event notifications and alarms through a workflow available in Data Safe's features. This allows you to create event notifications and alarms in context. For example, while viewing Security Assessment, you can view the **Notifications** tab and easily create event notifications for security assessments through a simplified workflow.

Though creating contextual event notifications and alarms occurs in Data Safe, the IAM permissions required to use this feature are for the Events Service. To use contextual event notifications and alarm ensure that you have been granted the following permissions:

Give a user group access to notifications topics:

```
allow group <user-group> to manage ons-topic in compartment <compartment-name>
```

Give a user group access to event rules:

```
allow group <user-group> to manage cloudevents-rules in compartment
<compartment-name>
```

Give a user group access to alarms:

```
allow group <user-group> to manage alarms in compartment <compartment-name>
```

Give a user group access to alarm history:

```
allow group <user-group> to read metrics in compartment <compartment-name>
```

See the below related links for more detailed information.

Related Topics

- Events and IAM Policies
- Security Monitoring
- Securing Notifications

Configure Access to Oracle Data Safe for Federated Users

For federated users to access Oracle Data Safe and Oracle Cloud Infrastructure resources, an Oracle Cloud Infrastructure Identity and Access Management (IAM) administrator needs to map each identity provider (IdP) group that needs access to Oracle Cloud Infrastructure (OCI) resources to an IAM group that has the required access.

1. As an IdP administrator, create federated users and groups in your IdP.
2. From the navigation menu in the Oracle Cloud Infrastructure Console, select **Identity & Security**, and then **Federation**.
3. On the **Federation** page, click the name of your IdP.
4. Under **Resources**, click **Group Mappings**.
5. Click **Add Mappings**.

   The **Add Mappings** dialog box is displayed.
6. From the **Identity Provider Group** drop-down list, select your IdP group that needs access to OCI resources.
7. From the **OCI Group** drop-down list, select the native OCI group that has the required permissions to access the needed OCI resources.
8. Click **Add Mappings**.
9. To test the mapping, sign in to the Oracle Data Safe Console with a federated user's credentials.
   a. From any browser, enter the url to the Oracle Data Safe Console for your region.

b. In the **Single Sign-On (SSO)** section, select your IdP, and then click **Continue**.

c. Sign in with a federated user's IdP credentials.

Example Security Configuration for Oracle Data Safe

In this example you can follow Susan, who is a tenancy administrator, while she creates an Oracle Data Safe environment to support two internal projects in her organization.

A company has a tenancy in Oracle Cloud Infrastructure. The tenancy's home region is Germany Central (Frankfurt). A department in the United States has two projects, Project A and Project B, that require Oracle Data Safe to help with auditing and data masking activities respectively. Susan, who is a tenancy administrator, is asked to create an Oracle Data Safe environment to support these projects.

Step 1: Subscribe to the Phoenix region

`Susan` signs in to Oracle Cloud Infrastructure and subscribes to the US West (Phoenix) region so that the projects can use a data center based in the United States. Now the tenancy is subscribed to two regions: Frankfurt and Phoenix.

Step 2: Create groups in Oracle Cloud Infrastructure Identity and Access Management (IAM)

In IAM, `Susan` creates the following groups:

- `Data-Safe-Admins`: Members of this group are power users and can access all features and resources in Oracle Data Safe. `Susan` adds the user named `Adam` to this group.
- `A-Admins`: Members of this group are responsible for managing Activity Auditing resources for Project A in Oracle Data Safe. `Susan` adds the user named `Jorge` to this group.
- `B-Admins`: Members of this group are responsible for managing Data Masking resources for Project B in Oracle Data Safe. `Susan` adds the user named `Cheri` to this group.

Step 3: Designate two compartments for Oracle Data Safe resources

In IAM, `Susan` creates two compartments specifically for Oracle Data Safe resources:

- Project-A
- Project-B

Step 4: Create IAM policies

In IAM, `Susan` creates the following policies in the `root` compartment of the tenancy:

- **Data-Safe-Admins**: This policy is needed so that members of the `Data-Safe-Admins` group can oversee and manage all Oracle Data Safe resources. The policy includes the following statement:

  ```
  Allow group Data-Safe-Admins to manage data-safe-family in tenancy
  ```

- **Project-A**: This policy is needed so that the `A-Admins` group can oversee and manage the Activity Auditing resources for Project A. The policy includes the following statement:

  ```
  Allow group A-Admins to manage data-safe-audit-family in compartment
  Project-A
  ```

- **Project-B**: This policy is needed so that the `B-Admins` group can oversee and manage the Data Masking resources for Project B. The policy includes the following statement:

  ```
  Allow group B-Admins to manage data-safe-masking-family in compartment
  Project-B
  ```

Step 5: Perform user tasks

`Jorge`, who is a member of the `A-Admins` group, accesses Activity Auditing in Security Center. He updates an audit policy for a target database.

`Cheri`, who is a member of the `B-Admins` group, accesses Data Masking in Security Center. She creates a masking policy using an existing sensitive data model and masks sensitive data on a target database.

3

Target Database Registration

This section discusses how to register target databases with Oracle Data Safe. You need to register your target databases before you can use them with Oracle Data Safe features.

Target Database Registration Overview

To use an Oracle database with Oracle Data Safe, you first need to register it with Oracle Data Safe.

Supported Target Databases

The following tables lists the Oracle databases that you can register with Oracle Data Safe; their supported workload types, software editions, and versions; connection protocol options; and connection requirements. The first table lists the supported Oracle databases running on Oracle Cloud Infrastructure or on-premises, while the second lists the supported Oracle databases running in other cloud environments.

> **Note:**
>
> - SQL Firewall management in Oracle Data Safe is only available for Oracle Database 23ai target databases.
> - Oracle Data Safe supports the registration of Active Data Guard deployments for Oracle Database 12.2 and above. The minimum version supported for using Activity Auditing with Active Data Guard is Oracle Database 19.21.
> - Oracle Data Safe supports the registration of container databases (CDBs) in Oracle Database 19c and above.
> - Provisioning and retrieval of audit policies is not supported in Oracle Database 12.1 and below.

Table 3-1 Oracle databases running in Oracle Cloud Infrastructure or on-premises

Oracle Database	Supported Workload Types/Oracle Database Software Editions/ Versions	TCP/TLS Connection Protocol Options	Connectivity Options	Active Data Guard Support
On-Premises Oracle Database	Oracle Database software editions: • Standard Edition • Enterprise Edition Versions: 11.2.0.4, 12.1, 12.2.0.1 or later	TCP or TLS	• Private endpoint • On-premises connector	Supported

Table 3-1 (Cont.) Oracle databases running in Oracle Cloud Infrastructure or on-premises

Oracle Database	Supported Workload Types/Oracle Database Software Editions/ Versions	TCP/TLS Connection Protocol Options	Connectivity Options	Active Data Guard Support
Oracle Autonomous Database on Dedicated Exadata Infrastructure (Private IPs)	Workload types: • Autonomous Data Warehouse • Autonomous Transaction Processing Versions: Latest version	TLS	Private endpoint	Not supported
Oracle Autonomous Database on Exadata Cloud@Customer	Workload types: • Autonomous Data Warehouse • Autonomous Transaction Processing • Autonomous JSON Database* Versions: Latest version	TLS	• Private endpoint • On-premises connector	Not supported
Oracle Autonomous Database Serverless	Workload types: • Autonomous Data Warehouse • Autonomous Transaction Processing • Autonomous JSON Database* Versions: Latest version	TLS	Public IP: No requirements Private IP: Private endpoint	Not supported
Oracle Base Database Service DB system - Virtual Machine	Oracle Database software editions: • Standard Edition • Enterprise Edition • Enterprise Edition High Performance • Enterprise Edition Extreme Performance Versions: 11.2.0.4, 12.1, 12.2.0.1 or later	TCP or TLS	Private IP: Private endpoint	Supported
Oracle Database on a compute instance in Oracle Cloud Infrastructure	Oracle Database software editions: • Standard Edition • Enterprise Edition Versions: 11.2.0.4, 12.1, 12.2.0.1 or later	TCP or TLS	• Private endpoint (recommended) • On-premises connector	Supported

Table 3-1 (Cont.) Oracle databases running in Oracle Cloud Infrastructure or on-premises

Oracle Database	Supported Workload Types/Oracle Database Software Editions/ Versions	TCP/TLS Connection Protocol Options	Connectivity Options	Active Data Guard Support
Oracle Exadata Database Service on Cloud@Customer	Oracle Database software editions: • Standard Edition • Enterprise Edition Versions: 11.2.0.4, 12.1, 12.2.0.1 or later	TCP or TLS	• Private endpoint • On-premises connector	Supported
Oracle Exadata Database Service on Dedicated Infrastructure	Oracle Database software editions: • Standard Edition • Enterprise Edition • Enterprise Edition High Performance • Enterprise Edition Extreme Performance Versions: 11.2.0.4, 12.1, 12.2.0.1 or later	TCP or TLS	Private IP: Private endpoint	Supported
Oracle Exadata Database Service on Exascale Infrastructure	Oracle Database software editions: • Standard Edition • Enterprise Edition • Enterprise Edition High Performance • Enterprise Edition Extreme Performance Versions: 11.2.0.4, 12.1, 12.2.0.1 or later	TCP or TLS	Private IP: Private endpoint	Supported

Table 3-2 Oracle database running in other cloud environments

Oracle Database	Supported Workload Types/Oracle Database Software Editions/ Versions	TCP/TLS Connection Protocol Options	Connectivity Options	Active Data Guard Support
Amazon RDS for Oracle	Oracle Database software editions: • Standard Edition 2 • Enterprise Edition Versions: 19c or 21c	TCP or TLS	• Private endpoint • On-premises connector	Supported

Table 3-2 (Cont.) Oracle database running in other cloud environments

Oracle Database	Supported Workload Types/Oracle Database Software Editions/ Versions	TCP/TLS Connection Protocol Options	Connectivity Options	Active Data Guard Support
Oracle Database@AWS Oracle Exadata Database Service *Registration through the Oracle Cloud Database Wizard*	Oracle Database software editions: • Enterprise Edition • Enterprise Edition High Performance • Enterprise Edition Extreme Performance Versions: 19c	TCP or TLS	Private endpoint	Supported
Oracle Database@Azure Oracle Autonomous Database *Registration through the Autonomous Database Wizard*	Workload types: • Autonomous Data Warehouse • Autonomous Transaction Processing • Autonomous JSON Database* Versions: Latest version	TLS	Private Endpoint	Not supported
Oracle Database@Azure Oracle Exadata Database Service *Registration through the Oracle Cloud Database Wizard*	Oracle Database software editions: • Enterprise Edition • Enterprise Edition High Performance • Enterprise Edition Extreme Performance Versions: 19c	TCP or TLS	Private endpoint	Supported
Oracle Database@Google Cloud Oracle Autonomous Database *Registration through the Autonomous Database Wizard*	Workload types: • Autonomous Data Warehouse • Autonomous Transaction Processing • Autonomous JSON Database* Versions: Latest version	TLS	Private Endpoint	Not supported
Oracle Database@Google Cloud Oracle Exadata Database Service *Registration through the Oracle Cloud Database Wizard*	Oracle Database software editions: • Enterprise Edition • Enterprise Edition High Performance • Enterprise Edition Extreme Performance Versions: 19c	TCP or TLS	Private endpoint	Supported

Table 3-2 (Cont.) Oracle database running in other cloud environments

Oracle Database	Supported Workload Types/Oracle Database Software Editions/ Versions	TCP/TLS Connection Protocol Options	Connectivity Options	Active Data Guard Support
Oracle Database on a compute instance in a non-Oracle cloud environment	Oracle Database software editions: • Standard Edition • Enterprise Edition Versions: 11.2.0.4, 12.1, 12.2.0.1 or later	TCP or TLS	• Private endpoint • On-premises connector (recommended)	Supported

* The Data Discovery and Data Masking features are not supported for JSON type columns.

Oracle Data Safe is a multi-tenant service running in a service tenancy owned by Oracle. Service data associated with the instance is stored in a back-end Oracle Autonomous Database Serverless database that's dedicated to the customer and region and is isolated from other customers' instances. For more information, refer to the Privacy and Security Feature Guidance for Oracle Autonomous Database Serverless available on My Oracle Support (Doc ID 114.2).

Security Levels for Target Databases

To use a database with Oracle Data Safe, you need to configure security in Oracle Cloud Infrastructure Identity and Access Management (IAM) and on the database.

There are two levels of security that you need to configure for a target database:

- **Policies in IAM** - You need to configure policies in IAM that allow users access to compartments, Oracle databases, network resources, and Oracle Data Safe resources. You may also need to update security lists and network security groups.
- **Roles on the target database** - You need to grant roles to the Oracle Data Safe service account on your database. The roles determine the Oracle Data Safe features that you can use with your database.

Where to Register Target Databases

You can register target databases from the following locations:

- Register any target database via a wizard from the **Overview** page for the Oracle Data Safe service in the Oracle Cloud Infrastructure Console.
- Register any target database from the **Target Databases** page for the Oracle Data Safe service in the Oracle Cloud Infrastructure Console. You can manually register a target database (for advanced users) or use a wizard.
- Register an Autonomous Database with Oracle Data Safe from an Autonomous Database's Console in Oracle Cloud Infrastructure.

Connectivity Options for Target Databases

Oracle Data Safe can connect to Oracle databases that have public or private IP addresses. To connect to databases with private IP addresses, you can use either an Oracle Data Safe

private endpoint or an Oracle Data Safe on-premises connector. Oracle Data Safe supports TLS and TCP protocols.

Public Versus Private Endpoints

If your database's IP address is public, the IP address is referred to as a *public endpoint*, and the IP address is accessible from the internet through an internet gateway. If your database's IP address is private (within a private subnet), the IP address is referred to as a *private endpoint*, and internet traffic cannot access the database.

Oracle Data Safe can connect to target databases with public or private IP addresses. For Autonomous Databases that have public IP addresses, you can configure a direct connection to them without using any special resources. For databases with private IP addresses, databases on compute instances, and databases outside of Oracle Cloud Infrastructure, you need to connect to them via an Oracle Data Safe private endpoint or Oracle Data Safe on-premises connector.

Oracle Data Safe Private Endpoints

You can create Oracle Data Safe private endpoints in your virtual cloud network (VCN) in Oracle Cloud Infrastructure to connect Oracle Data Safe to target databases with private IP addresses, target databases outside of Oracle Cloud Infrastructure, and target databases on compute instances. The private endpoint essentially represents the Oracle Data Safe service in your VCN and manifests as a VNIC with a private IP address in a subnet of your choice.

You typically create a private endpoint in the same virtual cloud network (VCN) as your target database. The only exception is if you are using VCN peering. In that case, you can select another VCN for which VCN peering with your database's VCN is set up. The private IP address does not need to be on the same subnet as your database, although, it does need to be on a subnet that can communicate with the database. You can create a maximum of one private endpoint per VCN. If a private endpoint already exists in the same VCN as your database, then you do not need to create a private endpoint.

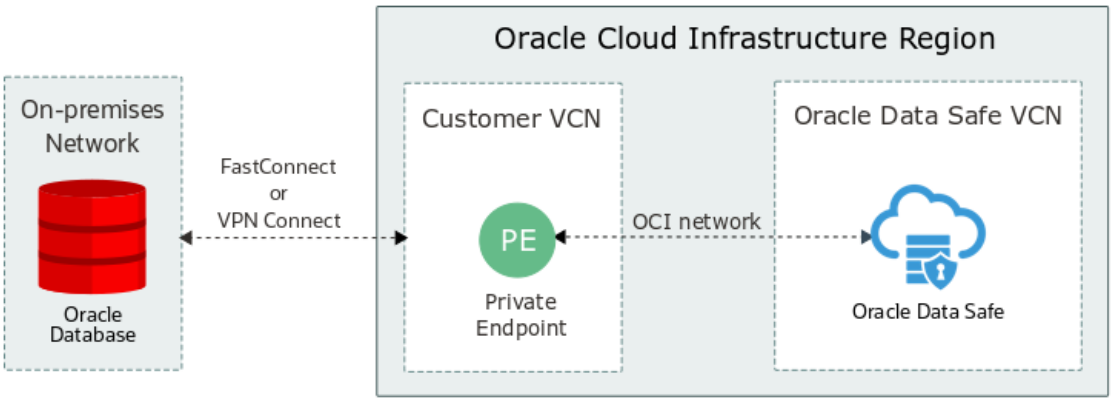
A security list and/or network security group for your database VCN is required when you set up a private endpoint. Both specify egress and ingress security rules at the IP address level. You can configure these in the target registration wizards. For more information about security lists and network security groups, see Access and Security in the Oracle Cloud Infrastructure documentation.

You can use a private endpoint with the following Oracle databases:

- Oracle Autonomous Database Serverless (with a private IP address)
- Autonomous Database on Dedicated Exadata Infrastructure
- DB System (with a private IP address)
- Oracle Database on a compute instance (with a private IP address) - Oracle recommends you use a private endpoint when the compute instance runs in the Oracle Cloud, as opposed to a non-Oracle cloud.
- On-premises Oracle Database (with a private IP address) - Requires FastConnect or VPN Connect
- Exadata Cloud@Customer - Requires FastConnect or VPN Connect
- Amazon RDS for Oracle

To use a private endpoint with a target database on your network outside of Oracle Cloud Infrastructure, you need to have FastConnect or VPN Connect set up between your outside network and a virtual cloud network (VCN) in Oracle Cloud Infrastructure. FastConnect in Oracle Cloud Infrastructure is a secure connection between your outside network and Oracle Cloud Infrastructure over a private network. VPN Connect in Oracle Cloud Infrastructure is a site-to-site IPSec virtual private network that securely connects your outside network to Oracle Cloud Infrastructure, using your existing internet connection.

The following diagram shows an example of a private endpoint configured with an on-premises Oracle database. The private endpoint communicates with the database over a private connection via FastConnect or VPN Connect in Oracle Cloud Infrastructure. The private endpoint also communicates with the Oracle Data Safe service over the Oracle Cloud Infrastructure network.



Oracle Data Safe On-Premises Connectors

You can create an Oracle Data Safe on-premises connector in your Oracle Data Safe service in Oracle Cloud Infrastructure to connect target databases to Oracle Data Safe. Oracle recommends you use an on-premises connector to connect to target databases that run outside of Oracle Cloud Infrastructure. You can use a private endpoint, however, to do so you need an existing FastConnect or VPN Connect set up between Oracle Cloud Infrastructure and your non-Oracle cloud environment. The private endpoint then needs to be created in the VCN in Oracle Cloud Infrastructure that has access to your database. Without this setup, Oracle recommends that you use an on-premises connector instead.

The on-premises connector is supported with the following Oracle databases:

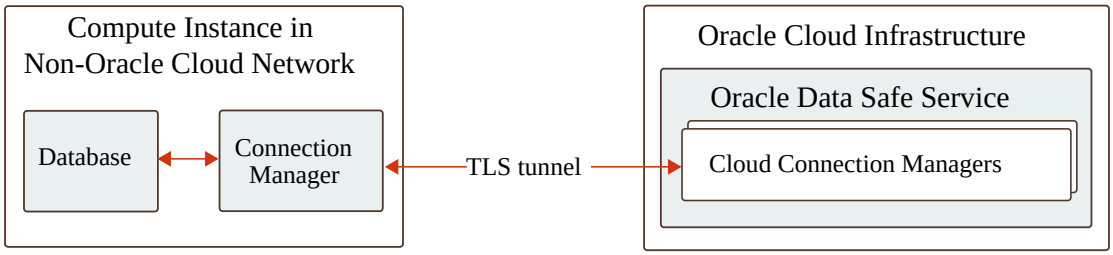
- Oracle Database on a compute instance in Oracle Cloud Infrastructure (recommended for target databases with public IP addresses)
- Oracle Database on a compute instance in a non-Oracle cloud environment, for example, in Amazon Web Services or Azure.
- On-premises Oracle Database
- Exadata Cloud@Customer Database
- Amazon RDS for Oracle

To use an on-premises connector, you first need to create the connector in Oracle Data Safe, either manually or in a target registration wizard. Next, you download an install bundle and then install an on-premises connector on a host machine on the same network as your target database. The on-premises connector establishes an encrypted TLS tunnel over the Internet to cloud Connection Managers in the Oracle Data Safe service tenancy. You can create one on-

premises connector in your Oracle Data Safe service in Oracle Cloud Infrastructure to connect to multiple Oracle databases.

The target registration wizards include the option to select or create an on-premises connector when applicable. If you defer the installation of the on-premises connector while working in the wizard, the wizard still registers the target database. In such case, the target database is placed in an inactive state and the on-premises connector is placed in "needs attention" mode until you install the on-premises connector. If you are manually registering a target database, then you need to complete the on-premises connector installation prior to registering the target database.

The following diagram shows an example of an on-premises connector with an Oracle database on a compute instance in a non-Oracle cloud network. The target database communicates with Connection Manager of the on-premises connector on the non-Oracle Cloud network. Connection Manager communicates with the cloud Connection Managers in Oracle Cloud Infrastructure through an encrypted TLS tunnel.



TLS and TCP Connection Protocols

During target database registration, you can configure a Transmission Control Protocol (TCP) or Transport Layer Security (TLS) connection between Oracle Data Safe and the database. Oracle Data Safe is considered a client of the target database. A TLS connection is a TCPS connection that uses TLS cryptographic protocol. Oracle Data Safe supports version 1.2 of the TLS protocol, but not the Secure Sockets Layer (SSL) cryptographic protocol.

Autonomous Databases, by default, have TLS encryption enabled with client authentication. During registration, Oracle Cloud Infrastructure automatically creates a TLS connection between the Autonomous Database and Oracle Data Safe and takes care of the registration details for you.

For non-Autonomous Databases, you can choose a TCP or TLS connection. If your target database has TLS configured on it, then you should choose TLS over TCP. A TLS connection to a target database provides privacy and data integrity, plus the identity of the communicating parties can be authenticated by using public key cryptography. Although authentication can be optional, the server typically requires it.

To establish a TCP connection between a non-Autonomous Database and Oracle Data Safe, the target database must have both the network encryption and data integrity features enabled. Network encryption is usually enabled by default. The supported encryption algorithm is AES256. Supported cryptographic hash functions for checksum are SHA1, SHA256, SHA384, and SHA512. Non-encrypted TCP connections are not supported.

Pre and Post Registration Tasks

Prior to and after registering a database, be sure to complete the necessary pre and post registration tasks. The tasks required depend on the type of database that you want to register.

Please refer to the target registration information for your target database to learn which pre and post registration tasks might be necessary.

This section has the following articles:

Create an Oracle Data Safe Service Account on Your Target Database

Every target database that you want to use with Oracle Data Safe requires an Oracle Data Safe service account on it. By default, Autonomous Databases already have this account. On non-Autonomous Databases, you need to create an account.

> **Note:**
>
> If you want to register a container database (CDB), please note that CDBs are supported on Oracle Database 19c and above.

Exception for Autonomous Databases

For all types of Oracle databases that you want to register with Oracle Data Safe, except for Autonomous Databases, you need to manually create an Oracle Data Safe service account. Create it with the least amount of privileges on the database.

An Autonomous Database comes with an Oracle Data Safe service account precreated on it so you do not need to create one. The account is named `DS$ADMIN` and is initially locked with the password expired. When you register an Autonomous Database with Oracle Data Safe, Oracle Cloud Infrastructure unlocks this account and resets its password. If you deregister the Autonomous Database, the account is locked again.

Create an Oracle Data Safe Service Account on a Target Database

Create the Oracle Data Safe service account with the least amount of privileges.

1. Log in to your database with an account that lets you create a user.
2. Create a user account with minimal privileges, for example:

```
CREATE USER DATASAFE_ADMIN identified by password
DEFAULT TABLESPACE "DATA"
TEMPORARY TABLESPACE "TEMP";
GRANT CONNECT, RESOURCE TO DATASAFE_ADMIN;
```

   - Replace *DATASAFE_ADMIN* and *password* with your own values.

> **Note:**
>
> The password must be at least 14 characters long and must contain at least one uppercase, one lowercase, one numeric, and one special character. See the Guidelines for Securing Passwords in the Security Guide for Oracle Database [19c] [23ai] for more details.

- Do not use `SYSTEM` or `SYSAUX` as the default tablespace. You cannot mask data if you use these tablespaces.
- Ensure that the `SESSIONS_PER_USER` for the Data Safe service account is at least 20. This is defined in the user profile. By default, the Data Safe service account is assigned the default user profile.

3. Grant roles to the Oracle Data Safe service account. See Grant Roles to the Oracle Data Safe Service Account on Your Target Database.

Grant Roles to the Oracle Data Safe Service Account on Your Target Database

The Oracle Data Safe features that you can use with your target database depend on the roles you grant to the Oracle Data Safe service account on that target database. You can grant and revoke roles as needed.

The roles are different for Autonomous Databases versus non-Autonomous Databases. For non-Autonomous databases, you can grant roles to the Oracle Data Safe service account prior to or after registering your database. For Autonomous Databases, you first need to register your database, which unlocks the Oracle Data Safe preseeded service account, and then grant and revoke roles as needed. By default, the Oracle Data Safe service account on an Autonomous Database is already granted some of the roles.

Roles for the Oracle Data Safe Service Account

> **Oracle Recommendation:**
>
> Grant only the roles needed to the Oracle Data Safe service on your target databases. How you grant roles depends on the type of target databases that you have.

The following table describes the roles for non-Autonomous Databases and Autonomous Databases. If you are registering a non-Autonomous Database (for example, a DB system, on-premises Oracle Database, or an Oracle Database on a compute instance), you can grant the roles in the first column. If you are registering an Autonomous Database, you can grant the roles in the second column. By default, some or most of the roles are granted by default so it is best to refer to each type of target registration.

Roles for Non-Autonomous Databases	Roles for Autonomous Databases	Description
`ASSESSMENT`	`DS$ASSESSMENT_ROLE`	Privileges required for the User Assessment and Security Assessment features
`AUDIT_COLLECTION`	`DS$AUDIT_COLLECTION_ROLE`	Privileges required for accessing audit trails for the target database
`DATA_DISCOVERY`	`DS$DATA_DISCOVERY_ROLE`	Privileges required for the Data Discovery feature (discovering sensitive data in the target database)
`MASKING`	`DS$DATA_MASKING_ROLE`	Privileges required for the Data Masking feature (masking sensitive data in the target database)

Roles for Non-Autonomous Databases	Roles for Autonomous Databases	Description
AUDIT_SETTING	DS$AUDIT_SETTING_ROLE	Privileges required for updating target database audit policies
SQL_FIREWALL	DS$SQL_FIREWALL_ROLE	Privileges required for the SQL Firewall feature (collect, monitor, and allow and block SQL traffic) Only for Oracle Database 23ai or later

Grant Roles to the Oracle Data Safe Service on an Autonomous Database

By default, an Autonomous Database comes with a database account specifically created for Oracle Data Safe named DS$ADMIN. The roles that you grant to this account determine the Oracle Data Safe features that you can use with your Autonomous Database.

For an Autonomous Database, all roles are already granted by default, except for DS$DATA_MASKING_ROLE and DS$SQL_FIREWALL_ROLE.

> **Note:**
>
> If Database Vault is enabled on your Autonomous Database, be aware that there are specific steps to take in the procedure below to get Oracle Data Safe to work with Database Vault.

To grant or revoke roles from the Oracle Data Safe service account on an Autonomous Database database, you can run the DS_TARGET_UTIL PL/SQL package on the Autonomous Database. You need to run this package as the PDB Admin user (ADMIN) or as a user that has execute permission on the DS_TARGET_UTIL PL/SQL package.

You can grant or revoke roles as often as needed.

1. To grant or revoke a role from the Oracle Data Safe service account, do the following:
   a. Using a tool like SQL*Plus or SQL Developer, log in to your Autonomous Database as the PDB Admin user (ADMIN) or as a user that has execute permission on the DS_TARGET_UTIL PL/SQL package.
   b. Run one of the following commands:
      - `EXECUTE DS_TARGET_UTIL.GRANT_ROLE('role_name');`

      > **Note:**
      >
      > If Database Vault is enabled on your database and you grant the DS$DATA_MASKING_ROLE role, expect an ORA-20001 error and proceed to step 3.

      or

- `EXECUTE DS_TARGET_UTIL.REVOKE_ROLE('role_name');`

  where *role_name* is the name of an Oracle Data Safe role. `role_name` must be in quotation marks.

2. If Database Vault is enabled on your database and you want to use the following features in Oracle Data Safe, do the following:
   - User Assessment or Security Assessment features: connect to your database as a user with the `DV_OWNER` role and grant the `DV_SECANALYST` role to the `DS$ADMIN` user.
   - Data Masking feature:
     a. Connect to the database as a user with the `DV_OWNER` role and authorize the `ADMIN` user to the **Oracle System Privilege and Role Management Realm**.
     b. Connect to the database as the `ADMIN` user and grant `UNLIMITED TABLESPACE` to the `DS$ADMIN` user.
   - SQL Firewall: If you granted the role as the PDB Admin user (`ADMIN`) or as a user that has the `DV_ADMIN` or `DV_OWNER` role, then this step is not necessary. However, if you did not, then connect to your database as a user with the `DV_ADMIN` or `DV_OWNER` role and run the following command as a user that has either the `DV_ADMIN` or `DV_OWNER` role:

     ```
     BEGIN
         DBMS_MACADM.AUTHORIZE_SQL_FIREWALL (
         uname => '<DATASAFE_ADMIN>',
         manage_dv_admins => 'N');
     END;
     /
     ```

     .

3. If Database Vault is enabled on your database and you want to revoke the following features in Oracle Data Safe, do the following:
   - User Assessment or Security Assessment feature: Connect to the database as the a user with the `DV_OWNER` role and revoke the `DV_SECANALYST` role from the `DS$ADMIN` user.
   - Data Masking feature:
     a. Connect to the database as the `ADMIN` user and revoke `UNLIMITED TABLESPACE` from the `DS$ADMIN` user.
     b. Connect to the database as a user with the `DV_OWNER` role and unauthorize the `ADMIN` user from the **Oracle System Privilege and Role Management Realm**.
   - SQL Firewall feature:
     a. Connect to your database as a user with the `DV_ADMIN` or `DV_OWNER` roles and run the following:

     ```
     BEGIN
         DBMS_MACADM.UNAUTHORIZE_SQL_FIREWALL (
             uname => '<DATASAFE_ADMIN>',
             manage_dv_admins => 'Y');
         END;
     /
     ```

- Revoke the `SQL_FIREWALL` role by following step one.

Grant Roles to the Oracle Data Safe Service on a Non-Autonomous Database

To grant or revoke roles from the Oracle Data Safe service account on a non-Autonomous Database, you need to run a SQL privileges script called `datasafe_privileges.sql`. You can download this script from Oracle Data Safe in Oracle Cloud Infrastructure. To run the script, you need to be connected to your database as the `SYS` user.

You can run the script as many times as needed. For example, suppose that in the beginning you only need to use the Activity Auditing feature in Oracle Data Safe. You can run the SQL privileges script to grant the database access to only Activity Auditing. Later, you decide you want to use the Data Discovery feature too. You can run the SQL privileges script again on the database to grant the database access to Data Discovery.

1. If Database Vault is enabled on your target database and you want to use the User Assessment or Security Assessment features or view audit data in Oracle Data Safe, connect to your database as a user with the `DV_OWNER` role and grant the `DV_SECANALYST` and `DV_MONITOR` roles to the Oracle Data Safe service account.
2. Download the SQL privileges script. This script is available within the wizards that assist with target database registration. You don't need to work through the wizard and register your target database at this time. Just start the wizard and you'll see the link to download the script on the first page. Download the script and exit the wizard.
   a. On the Overview page in the Oracle Data Safe service, find the tile for the wizard that corresponds to the type of database you are working with. Click **Start Wizard**.The wizard displays the Data Safe Target Information form.
   b. Click **Download Privilege Script** and save the `datasafe_privileges.sql` script to your computer.
   c. Click **Cancel**.
3. With SQL Developer or SQL*Plus, connect to your database as the `SYS` user, and then run the SQL privileges script with the following statement:

   ```
   @datasafe_privileges.sql <DATASAFE_ADMIN> <GRANT|REVOKE> <AUDIT_COLLECTION|
   AUDIT_SETTING|DATA_DISCOVERY|MASKING|ASSESSMENT|SQL_FIREWALL|ALL> [-
   RDSORACLE][-VERBOSE]
   ```

   - *<DATASAFE_ADMIN>* is the name of the Oracle Data Safe service account that you created on your database. It is case-sensitive and must match the account name in the `dba_users` data dictionary view in your database.
   - Specify `GRANT` or `REVOKE` depending on whether you want to add privileges to or remove privileges from the Oracle Data Safe service account.
   - You can specify only one feature per command, although `ALL` grants or revokes privileges for all features.
   - `-RDSORACLE` is **required** if you are registering Amazon RDS for Oracle, otherwise remove the parameter
   - `-VERBOSE` is optional.

4. If Database Vault is enabled on your database and you want to use the SQL Firewall feature in Data Safe, run the following as a user with either the `DV_ADMIN` or `DV_OWNER` role:

```
BEGIN
    DBMS_MACADM.AUTHORIZE_SQL_FIREWALL (
    uname => <DATASAFE_ADMIN>,
    manage_dv_admins => 'N');
END;
/
```

5. If Database Vault is enabled on your database and you want to stop using the SQL Firewall feature in Data Safe, perform the following as a user with either the `DV_ADMIN` or `DV_OWNER` role:

   a. Run the following:

```
BEGIN
    DBMS_MACADM.UNAUTHORIZE_SQL_FIREWALL (
        uname => '<DATASAFE_ADMIN>',
        manage_dv_admins => 'Y');
    END;
/
```

   b. Revoke the SQL Firewall privilege by following step three.

Example 3-1 Grant all privileges and make all Oracle Data Safe features available

```
@datasafe_privileges.sql <DATASAFE_ADMIN> GRANT ALL -VERBOSE
```

Example 3-2 Grant the privileges required to use the making feature

```
@datasafe_privileges.sql <DATASAFE_ADMIN> GRANT MASKING
```

Create a Wallet or Certificates for a TLS Connection

Prior to configuring a TLS connection to a non-Autonomous Database during target registration, you need to create one or more wallets or a certificate, depending on whether client authentication is enabled on your target database.

Create a PEM Certificate for a TLS Connection to a Database that has Server Authentication

1. Create a PEM Certificate for a TLS Connection. See Transport Layer Security Connections without a Client Wallet in the *Oracle Database Security Guide* for more information.
2. When you register the target database in Oracle Data Safe, make sure to do the following:
   - Select the connection type **TLS**.
   - Set the port number according to the port number you set in the `listener.ora` file. In this example, the port number is **1553**.
   - For the server distinguished name, enter the name you used when you created the self-signed certificate in the wallet. In this example, the name is **`CN=rootca`**.

- For the wallet or certificate type, select **PEM Certificate** and select the self-signed certificate that you exported from the wallet. In this example, the file is **`root1.crt`**.

Create Wallets for a TLS Connection to a Database that has Mutual Authentication

During target registration, you can configure a TLS connection between Oracle Data Safe and an Oracle database. You are required to upload two wallets: a TrustStore wallet and a KeyStore wallet.

> **Oracle Recommendation:**
>
> While self-signed certificates are fine for testing purposes, Oracle recommends that you use certificates signed by a trusted or internal certificate authority (CA) for production systems.

Part 1: Establish Mutually Authentication in Your Database

Configure mutual authentication on your target database. See Transport Layer Security Connections with a Client Wallet in the *Oracle Database Security Guide* for more information.

Part 2: Save the TrustStore and KeyStore Files

In this part, you copy the TrustStore and KeyStore files to your client machine.You do this because Oracle Data Safe requires a both wallets.

- Copy the TrustStore and KeyStore files to your client machine.

Part 3: Configure the TLS Connection During Target Registration in Oracle Data Safe

When you register the target database in Oracle Data Safe, make sure to do the following:

- Select the **TLS** connection type.
- Set the port number according to the port number you set in the `listener.ora` file. In this example, the port number is **1522**.
- For the server distinguished name, enter the name you used when you created the self-signed certificate for the target database. In this example, the name is `CN=CloudST2.debdev19.oraclecloud.internal`.
- Upload the TrustStore file. For example, upload `truststore.jks`.
- Upload the KeyStore file. For example, upload `keystore.jks`.

Configure a TLS Connection Between the On-Premises Connector on Your Host Machine and Your Oracle Database

Prior to configuring a TLS connection during target registration, you need to configure a TLS connection between the on-premises connector on your host machine and your target database.

1. Open a command prompt on the host machine that has the unzipped install bundle.

2. Find the distinguished name (DN) of the Connection Manager certificate from the on-premises connector wallet by running the following command:

   ```
   orapki wallet display -wallet <CMAN wallet location>
   ```

3. Export the Connection Manager certificate by running the following command:

   ```
   orapki wallet export -wallet <Connection Manager wallet location> -dn
   <distinguished name of the Connection Manager certificate> -cert
   <Connection Manager certificate file name>
   ```

4. Add the Connection Manager certificate to your on-premises Oracle database server's wallet by running the following command. Note that this step is not necessary for Exadata Cloud@Customer databases.

   ```
   orapki wallet add -wallet <database wallet location> -trusted_cert -cert
   <Connection Manager certificate file name>
   ```

5. Export the database server certificate by running the following command. For `<database server certificate file>`, enter the location where you want to store the certificate (the command below creates the certificate).

   ```
   orapki wallet export -wallet <database wallet location> -dn <db server DN>
   -cert <database server certificate file>
   ```

6. Import the database server certificate into the on-premises connector wallet by running the following command. When prompted, enter the wallet password. This is the password that you created when you downloaded and installed the install bundle.

   ```
   orapki wallet add -wallet <on-premises connector wallet location> -
   trusted_cert -cert <database server certificate file>
   ```

7. Restart the database listener and restart the on-premises connector.

Configure a TLS Connection Between the On-Premises Connector on Your Host Machine and an Autonomous Database on Exadata Cloud@Customer Database

You need to configure a TLS connection between the Oracle Data Safe on-premises connector on your host machine and Autonomous Database on Exadata Cloud@Customer.

Perform the following steps only once per Exadata Cloud@Customer cluster:

1. Download the Autonomous Database wallet.
2. Export the database server certificate by running the following command. For `-dn <db server DN>`, enter the first part of the database scan name, which you can find in the `tnsnames.ora` file. For `<database server certificate file>`, enter the location where you want to store the certificate (the command below creates the certificate).

   ```
   orapki wallet export -wallet <database wallet location> -dn <db server DN>
   -cert <database server certificate file>
   ```

3. For the *first* pluggable database (PDB) in the Exadata Cloud@Customer cluster (and only the first PDB - not the remaining PDBs in the cluster), import the database server certificate into the on-premises connector wallet. To do this, run the following command, and when prompted, enter the wallet password. The wallet password is the password that you created when you downloaded and installed the install bundle.

```
orapki wallet add -wallet <on-premises connector wallet location> -
trusted_cert -cert <database server certificate file>
```

Add the Security Certificate for the Amazon RDS Region

If registering an Amazon RDS for Oracle database with either a private endpoint or an on-premises connector, then you need to add the security certificate of the specific Amazon Web Services (AWS) region as a trusted certificate to the endpoint's or connector's wallets.

1. Download the certificate of the specific AWS region on which your Amazon RDS is present. See Using SSL/TLS to encrypt a connection to a DB instance from Amazon for more information.
2. Add the certificate to the on-premises connector or private endpoint:

```
 orapki wallet add -wallet <install location>/wallet -trusted_cert -cert
<certificate file>
```

Add Security Rules

If you plan to connect to your target database with an Oracle Data Safe private endpoint, prior to registering your target database, you need to add security rules to your virtual cloud network (VCN) to allow communication between your target database and Oracle Data Safe.

Overview

You can add the necessary security rules to your virtual cloud network's (VCN's) security lists or network security groups (NSGs). Both stateful and stateless security rules are allowed. In general, the security rules need to 1) allow your target database to receive incoming traffic from Oracle Data Safe, and 2) allow Oracle Data Safe to send requests to the target database.

There are two approaches that you can take when creating the security rules. The first approach is to allow communication between Oracle Data Safe and *all* IP addresses within the same subnet (0.0.0.0/0). With this configuration, Oracle Data Safe can connect to all of your target databases in the subnet.

The other approach is to be more specific by configuring separate ingress and egress rules as follows:

- **In the NSG or security list for your target database, add an ingress rule** that allows your target database's private endpoint IP address on the target database's port to receive incoming traffic from Oracle Data Safe's private endpoint IP address from all ports.
- **In the NSG or security list for your Oracle Data Safe private endpoint, add an egress rule** that allows Oracle Data Safe's private endpoint IP address on all ports to send requests to the target database's private endpoint IP address on the target database's port. If the target database has multiple IP addresses, you need configure an egress rule for each IP address. In the case of an Oracle On-Premises Database, you only need to configure an egress rule, and not an ingress rule.

For more information about security lists and network security groups, see Access and Security in the Oracle Cloud Infrastructure documentation.

Add Security Rules for an Oracle Autonomous Database Serverless with Private VCN Access

For an Oracle Autonomous Database Serverless with Private VCN Access, you need to create an ingress rule and an egress rule in the target database's virtual cloud network (VCN) in Oracle Cloud Infrastructure..

1. Obtain the private IP address and NSG or security list for your target database.

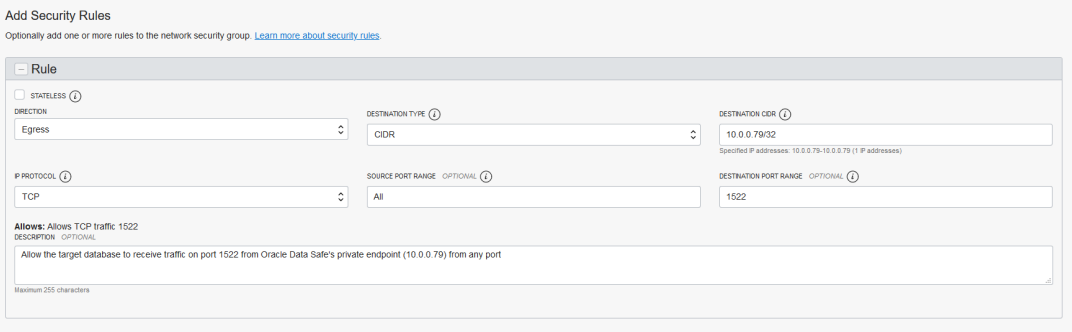
   You can find the network information on the **Autonomous Database Information** tab under **Network** in your database's Console in Oracle Cloud Infrastructure. For example, suppose your target database's private endpoint's IP address is 10.0.0.112 and the NSG name is nsg-atp.

2. Obtain the private IP address and NSG or security list for your Oracle Data Safe private endpoint.

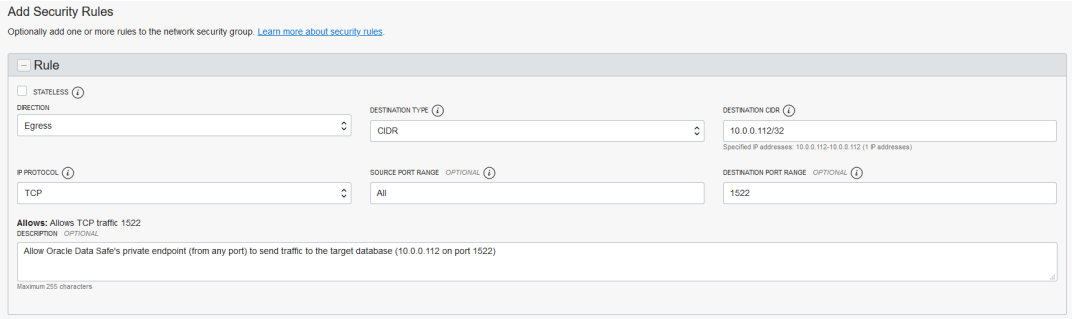
   You can find the network information for your Oracle Data Safe private endpoint on the **Private Endpoint Information** page in the Oracle Data Safe service in Oracle Cloud Infrastructure.

3. Open the VCN for your target database.

4. In your target database's NSG or security list, create an ingress rule that allows your target database's private endpoint IP address (for example, 10.0.0.112/32) on the target database's port (for example, 1522) to receive incoming traffic from Oracle Data Safe's private endpoint IP address (for example, 10.0.0.79/32) from all ports.



5. In your Oracle Data Safe private endpoint's NSG or security list, create an egress rule that allows Oracle Data Safe's private endpoint IP address (for example, 10.0.0.79/32) on all ports to send requests to the target database's private endpoint IP address (for example, 10.0.0.112/32) on the target database's port (for example, port 1522).



Add Security Rules for an Autonomous Database on Dedicated Exadata Infrastructure

For an Autonomous Database on Dedicated Exadata Infrastructure, you need to create an ingress rule and an egress rule in the target database's virtual cloud network (VCN) in Oracle Cloud Infrastructure.

1. Obtain the subnet (or floating IP addresses if known) and the name of the NSG or security list for your target database.

   An Autonomous Database on Dedicated Exadata Infrastructure can have up to 8 floating IP addresses for the database nodes.

2. Obtain the private IP address and the name of the NSG or security list for your Oracle Data Safe private endpoint.

   You can find this information on the **Private Endpoint Information** page in the Oracle Data Safe service in Oracle Cloud Infrastructure.

3. Open the VCN for your target database.

4. **In your target database's NSG or security list:** Create an ingress rule that allows your target database's private endpoint on port **2484** to receive incoming traffic from Oracle Data Safe's private endpoint IP address (from all ports).

5. **In your Oracle Data Safe private endpoint's NSG or security list,** do one of the following:

   - Create an egress rule that allows the Oracle Data Safe private endpoint (from all ports) to send requests to all IP addresses on the target database's subnet on port **2484**.
   - For each floating IP address, create an egress rule that allows the Oracle Data Safe private endpoint (from all ports) to send requests to the floating IP address on port **2484**.

Add Security Rules for an Oracle Cloud Database

For an Oracle Cloud Database, you need to create an ingress rule and an egress rule in the target database's virtual cloud network (VCN) in Oracle Cloud Infrastructure.

1. Obtain the IP address(es) and NSG name for your target database's private endpoint.

   - You can find your target database information in your target database's Console in Oracle Cloud Infrastructure.
   - A bare metal or vitual machine DB system has one private IP address.
   - An Exadata Cloud Service database can have multiple floating IP addresses for the database nodes. It can also have scan IP addresses for the database system. Oracle recommends that you use one of the scan IP addresses. You can find a scan IP address under Network on the DB System Information tab in Oracle Cloud Infrastructure. Alternatively, you can enter the private floating IP address of any one of the database nodes.

2. Obtain the private IP address and NSG name for the Oracle Data Safe private endpoint.

   You can find the Oracle Data Safe private endpoint information on the **Private Endpoint Information** page in the Oracle Data Safe service in Oracle Cloud Infrastructure.

3. Open the VCN for your target database.

4. In your target database's NSG, create an ingress rule that allows your target database's private endpoint IP address (for example, 10.0.0.112/32) on the target database's port (for example, **1521**) to receive incoming traffic from Oracle Data Safe's private endpoint IP address (for example, 10.0.0.79/32) from all ports.
5. In your Oracle Data Safe private endpoint's NSG, create an egress rule that allows Oracle Data Safe's private endpoint IP address (for example, 10.0.0.79/32) on all ports to send requests to the target database's private endpoint IP address (for example, 10.0.0.112/32) on the target database's port (for example, port **1521**).

   For an Exadata Cloud Database, create an egress rule for one of the scan IP addresses. Alternatively, you can use the private floating IP address of any one of the database nodes. The database port number is 1521.

Add Security Rules for an Oracle Database on Compute

If you plan to connect to your Oracle Database on Compute by using an Oracle Data Safe private endpoint, create an ingress rule and an egress rule on the target database's virtual cloud network (VCN) in Oracle Cloud Infrastructure. If the target database is in a non-Oracle cloud environment, configure the ingress rule in the non-Oracle Cloud environment.

1. Obtain the IP address and the name of the NSG or security list for your target database's private endpoint. You can find your target database information in your target database's Console in Oracle Cloud Infrastructure.
2. Obtain the IP address and the name of the NSG or security list for the Oracle Data Safe private endpoint. You can find the Oracle Data Safe private endpoint information on the **Private Endpoint Information** page in the Oracle Data Safe service in Oracle Cloud Infrastructure.
3. Open the VCN for your target database, either in Oracle Cloud Infrastructure or in a non-Oracle cloud environment. In the target database's NSG or security list, create an ingress rule that allows your target database's private endpoint IP address (for example, 10.0.0.112/32) on the target database's port (for example, **1521**) to receive incoming traffic from Oracle Data Safe's private endpoint IP address (for example, 10.0.0.79/32) from all ports.
4. In Oracle Cloud Infrastructure, open the VCN for your Oracle Data Safe private endpoint. In the Oracle Data Safe private endpoint's NSG or security list, create an egress rule that allows Oracle Data Safe's private endpoint IP address (for example, 10.0.0.79/32) on all ports to send requests to the target database's private endpoint IP address (for example, 10.0.0.112/32) on the target database's port (for example, port **1521**).

Add Security Rules for an Oracle On-Premises Database

For an Oracle On-Premises Database, you need to create an egress rule in the virtual cloud network (VCN) for your Oracle Data Safe private endpoint. You do not need to create an ingress rule.

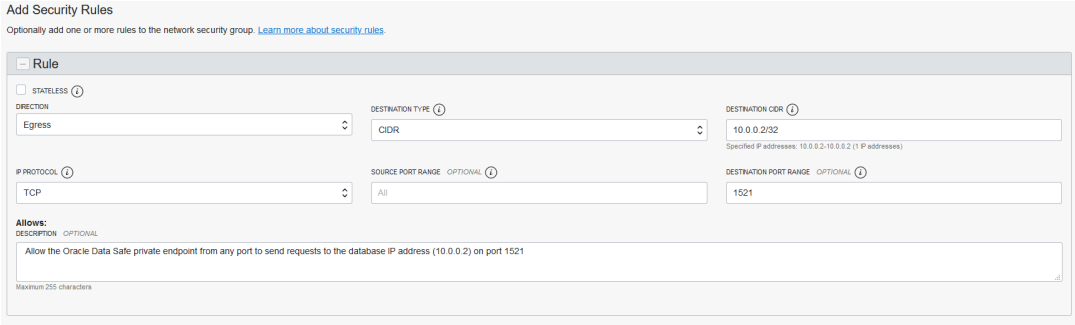
1. Obtain the private IP address of your target database. The IP address is where the listener is running. For example, suppose the Oracle database listener is running on 10.0.0.2.

   For a Real Application Cluster (RAC) database, you need to specify the IP addresses for the RAC database nodes and not the SCAN IP addresses. Whether you specify all the nodes in your RAC database depends on how you configured your pluggable databases (PDBs).

2. Obtain the private IP address and the name of the NSG or security list for your Oracle Data Safe private endpoint.

   You can find the Oracle Data Safe private endpoint information on the **Private Endpoint Information** page in the Oracle Data Safe service in Oracle Cloud Infrastructure.

3. Open the VCN for your Oracle Data Safe private endpoint. In your Oracle Data Safe private endpoint's NSG or security list, create an egress rule that allows Oracle Data Safe's private endpoint IP address (for example, 10.0.0.79/32) on all ports to send requests to the target database's private IP address (for example, 10.0.0.2/32) on the target database's port (for example, port **1521**).



Add Security Rules for an Exadata Cloud@Customer Database

Update the security list for your virtual cloud network (VCN) in Oracle Cloud Infrastructure, and if implemented, the network security group for your database subnet, to allow traffic from the Oracle Data Safe private endpoint to your database. This step allows Oracle Data Safe to access your database. A security list acts as a virtual firewall for your database and consists of a set of ingress and egress security rules that apply to all the VNICs in any subnet that the security list is associated with. Both stateful and stateless security rules in the security list are allowed. For more information about security lists and network security groups, see Access and Security in the Oracle Cloud Infrastructure documentation.

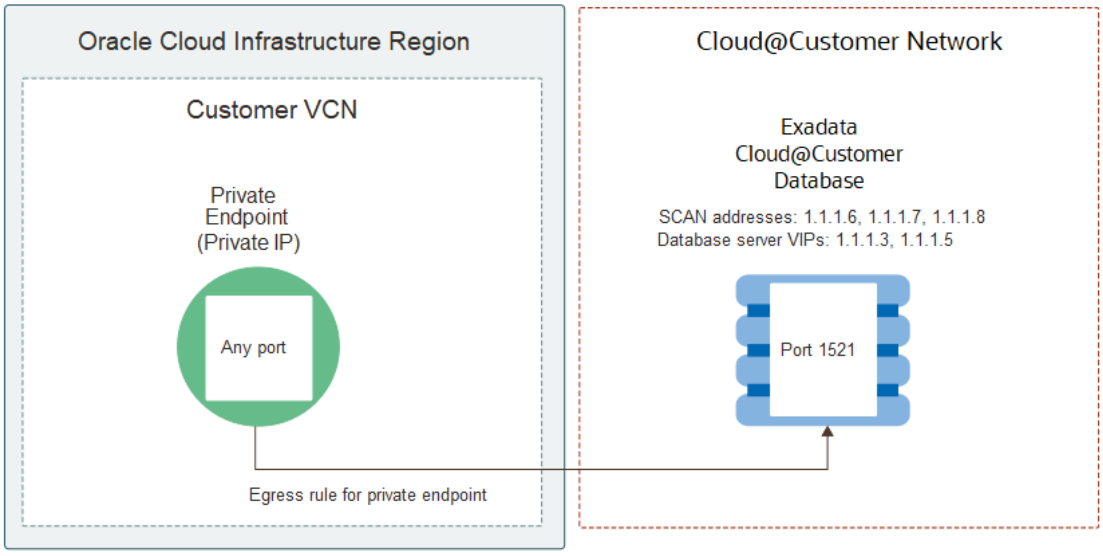
By default, every database deployment on Oracle Database Exadata Cloud@Customer is associated with a Single Client Access Name (SCAN), and the SCAN is associated with 3 IP addresses. Each Oracle Exadata Cloud@Customer system configuration contains compute nodes (database servers). In the Exadata Cloud@Customer infrastructure, there is one database server VIP address per compute node in the VM cluster.

When you use an Oracle Data Safe private endpoint to connect your Exadata Cloud@Customer database to Oracle Data Safe, you need to create an **egress security rule** for the Oracle Data Safe private endpoint. Configure the rule to allow communication between the Oracle Data Safe private endpoint (from any port) and all database server VIPs and SCAN addresses (all three).

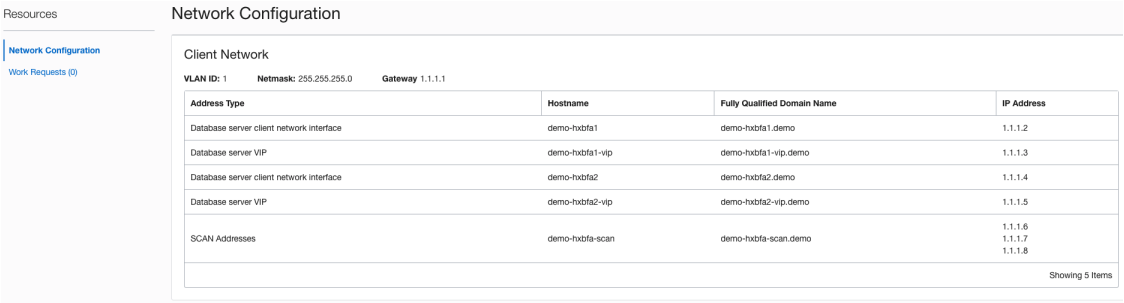
Example 3-3 Configure a stateful security rule for an Exadata Cloud@Customer database and an Oracle Data Safe private endpoint

This example shows a stateful security rule for an Exadata Cloud@Customer database and an Oracle Data Safe private endpoint. The egress security rule on the virtual cloud network (VCN) in Oracle Cloud Infrastructure allows the private endpoint (from any port) to send requests to two database server VIPs (1.1.1.3 and 1.1.1.5) and three SCAN addresses (1.1.1.6, 1.1.1.7, and 1.1.1.8) on port 1521. Always include the database server VIPs in the egress security rule.

The following diagram illustrates the Oracle Data Safe private endpoint, the Exadata Cloud@Customer database, and the egress security rule.



The following screenshot shows you the Exadata Cloud@Customer network configuration for the VM cluster in Oracle Cloud Infrastructure, where you can find the SCAN addresses and database server VIPs.



Register an Autonomous Database

You can register Autonomous Databases as target databases for Oracle Data Safe.

In Oracle Data Safe, use the **Autonomous Databases** wizard to register the following Autonomous Databases:

- Oracle Autonomous Database Serverless with Secure Access from Everywhere
- Oracle Autonomous Database Serverless with Secure Access from allowed IPs and VCNs only
- Oracle Autonomous Database Serverless with Private VCN Access (requires a Data Safe private endpoint)
- Oracle Autonomous Database on Dedicated Exadata Infrastructure (requires a Data Safe private endpoint)
- Oracle Database@Azure - Oracle Autonomous Database (requires a Data Safe private endpoint)
- Oracle Database@Google Cloud - Oracle Autonomous Database (requires a Data Safe private endpoint)

> **Note:**
>
> Be sure to complete the preregistration tasks before using the wizard and the post registration tasks after using the wizard.

Preregistration Tasks for an Autonomous Database

The following table lists the preregistration tasks.

Task Number	Task	Link to Instructions
1	Obtain permissions in Oracle Cloud Infrastructure Identity and Access Management (IAM) to register your target database.	Permissions to Register an Autonomous Database with Oracle Data Safe
2	(For Autonomous Database on Dedicated Exadata Infrastructure) • Obtain the `ADMIN` password for your target database because you need it during target database registration. • If Database Vault is enabled on the database, connect to your database as a user with the `DV_ACCTMGR` role and temporarily grant the `DV_ACCTMGR` role to the `ADMIN` user.	(none)

Run the Autonomous Databases Wizard

There is some variation in the workflow in the wizard, depending on whether the Autonomous Database you select is configured to run on serverless or dedicated Exadata infrastructure and (in the case of serverless infrastructure) if network access is via public or private IP. The wizard detects these configuration settings in the Autonomous Database you have selected and adjusts the steps accordingly. For example, if the database is configured with a public IP to be securely accessible from everywhere, then the steps to select a connectivity option and add a security rule are not needed and are skipped.

This is the Autonomous Database registration workflow:

Step 1: Select Database

1. On the Overview page in the Oracle Data Safe service, find the **Autonomous Databases** tile and click **Start Wizard**.

   The wizard displays the **Data Safe Target Information** form.

2. If your database does not reside in the compartment shown, click **CHANGE COMPARTMENT** and select the correct compartment.

3. Select the target database that you want to register.

   You can select only one target database.

   The wizard automatically fills in the **DATA SAFE TARGET DISPLAY NAME** and **COMPARTMENT** fields. If you want to register the database in a compartment other than

the OCI compartment where the database is stored, select a different compartment from the drop-down list.

4. Enter a target display name that is meaningful to you. Oracle Data Safe uses this name in its reports.
5. (Optional) In the **DESCRIPTION** field, add a description that is meaningful to you.
6. Optionally, click **Show advanced options** to tag the notification.
   a. Click **Add tag** to create an additional optional tag to organize and track resources in your tenancy.
   b. Select a **Tag namespace** from the drop-down list.
   c. Provide a **Tag key** and **Tag value**.
7. For an Autonomous Database on Dedicated Exadata Infrastructure only: At **DATABASE USERNAME** and **DATABASE PASSWORD**, enter the credentials of the database `ADMIN` user. This unlocks the Oracle Data Safe service account (`DS$ADMIN`) in the database. This step does not apply to Oracle Autonomous Database Serverless.

   > **Note:**
   >
   > The credentials requested here are for the database `ADMIN` user, not those of the Oracle Data Safe service account in the database.

8. Click **Next**.
   - If you are registering a target database that uses a private IP address, the **Next** button takes you to Step 2: **Connectivity Option**.
   - If you are registering an Oracle Autonomous Database Serverless with Secure Access from Everywhere, there is no need to choose a connectivity option or add a security rule. In this case, the wizard bypasses these steps and takes you directly to Step 4: **Review and Submit**.

Step 2: Connectivity Option

If you are registering a target database that is configured to use a private IP address, then an Oracle Data Safe private endpoint is required.

If an Oracle Data Safe private endpoint for the VCN of the database already exists, the wizard automatically selects it for you. If none exists, then in the **Private Endpoint Information** form the wizard prompts for the basic information in needs to create a new Oracle Data Safe private endpoint for the target database. The name, VCN, and subnet are preassigned. You can change any of the parameters entered into the form.

1. Review all of the parameter values and change them as needed.
2. Click **Next**.

   The wizard progresses to Step 3: **Add Security Rule**.

Step 3: Add Security Rule

In this step, add the required security rules. To allow communication from Oracle Data Safe to your database, you need to add two security rules:

- **Ingress rule for the database:** Allow the database to receive incoming traffic on its port from the private IP address of the Oracle Data Safe private endpoint (from any port).
- **Egress rule for the Oracle Data Safe private endpoint:** Allow the Oracle Data Safe private endpoint (from any port) to send requests to the database IP address(es) on the database's port.

The ingress and egress rules do not need to be stored within the same security list, network security group, or same compartment. If you already created the necessary security rules, you can choose to skip this step.

> **See Also:**
>
> For more information about security lists and network security groups, see Access and Security in the Oracle Cloud Infrastructure documentation.

1. At **Do you want to add the security rules now?** , select either **Yes** or **No**.

   If you select **No**, you can then click **Next** to bypass the security rules configuration and proceed to **Review and Submit**. You can configure the security rules later in the Oracle Cloud Infrastructure Console (under **Networking**). You may want to skip this step now if you already have security rules that you want to apply. Note that the target database remains inactive in Oracle Data Safe until the security rules are configured either in the Oracle Data Safe wizard or in the Oracle Cloud Infrastructure console.
2. If you select **Yes**, then at **Add Ingress Security Rule**, select either **Security List** or **Network Security Group**. Then use the drop-down menu to select the Security List or Network Security Group to which you want to add the ingress rule.

   In the **Ingress Rule** tile, the wizard shows you the ingress rule to be added to the security list or network security group you selected.
3. At **Add Egress Security Rule**, select either **Security List** or **Network Security Group**.
4. At the next prompt, select the security list or network security group where you want to add the rule.
5. Click **Next** to go to **Review and Submit**.

Step 4. Review and Submit

If you configured a target database that uses a private IP address, the **Review and Submit** page displays the configuration for **Target Database Information**, **Connectivity Option**, and **Security Rules**.

If you configured a target database that uses a public IP address, you did not need to configure a connectivity option or security rules, so this summary of the configuration shows only the following information, all of which you selected in Step 1:

- Display Name of Selected Database
- Compartment for Target
- Data Safe Target Display Name
- Description

To change any of these settings, click the **Edit** button on the right side of the corresponding tile.

1. Review the target database configuration.
2. If the information is correct, click **Register**. If not, click **Previous** to return to any of the earlier steps, or click **Cancel**.

Step 5. Registration Progress

After you click **Register** in Step 4: **Review and Submit**, Oracle Data Safe creates the configuration and registers the target database. The next and final step in the wizard is to monitor the registration progress. As part of the registration, if a new private endpoint is required or ingress/egress rules are added, the tasks required are listed and processed one-by-one. If there are any errors, they are reported here. You can click the **Previous** button to return to previous pages and correct the errors.

> **Important:**
>
> Do not click the **Close** button in the wizard, sign out of OCI, or close the browser tab until the wizard shows that all of the tasks listed are resolved. If you close prematurely, then the information for all of the tasks that have not yet been completed is lost and the target database is not registered. Use the **Close** button to exit the page if an error occurs in the registration process.

When Registration is Complete

The wizard presents the **Target Database Details** page when the registration is finished. On this page you can again review the registration details. Options on this page that are not available for the selected target database are grayed out. For Autonmous Database, the options available are on the **More Actions** tab. You can change the compartment where the registration is store, add tags, or deregister the target database.

The database icon on the left indicates the current status of the registration process.

Post Registration Tasks for an Autonomous Database

The following table lists tasks that you need to complete after you run the Autonomous Databases wizard.

Task Number	Task	Link to Instructions
1	(Optional) Change which features are allowed for the Oracle Data Safe service account on your target database by granting/revoking roles from the account. You need to be a PDB administrator (`ADMIN`) or a user that has execute permission on the `DS_TARGET_UTIL` package. **Note:** During target registration, all roles are already granted by default, except for `DS$DATA_MASKING_ROLE`.	Grant Roles to the Oracle Data Safe Service Account on Your Target Database
2	(Optional) Grant users access to Oracle Data Safe features with the target database by configuring policies in Oracle Cloud Infrastructure Identity and Access Management.	Create IAM Policies for Oracle Data Safe Users
3	(Autonomous Database on Dedicated Exadata Infrastructure only) If Database Vault is enabled on your target database, connect to your target database as a user with the `DV_ACCTMGR` role and revoke the `DV_ACCTMGR` role from the `ADMIN` user.	(none)

Register an Oracle Cloud Database

You can register Oracle cloud databases as target databases for Oracle Data Safe.

In Oracle Data Safe, use the **Oracle Cloud Databases** wizard to register the following databases:

- Oracle Base Database Service (DB system - Virtual Machine)
- Oracle Exadata Database Service on Dedicated Infrastructure (Exadata VM cluster)
- Oracle Database@AWS - Oracle Exadata Database Service
- Oracle Database@Azure - Oracle Exadata Database Service
- Oracle Database@Google Cloud - Oracle Exadata Database Service

> **Note:**
>
> Be sure to complete the preregistration tasks before using the wizard and the post registration tasks after using the wizard.

Preregistration Tasks for an Oracle Cloud Database

The following table lists the preregistration tasks.

Task Number	Task	Link to Instructions
1	In Oracle Cloud Infrastructure Identity and Access Management (IAM), obtain permissions to register your target database.	Permissions to Register an Oracle Cloud Database with Oracle Data Safe
2	Create an Oracle Data Safe service account on your target database and grant it Oracle Data Safe roles. Create the service account as the `SYS` user.	Create an Oracle Data Safe Service Account on Your Target Database Grant Roles to the Oracle Data Safe Service Account on Your Target Database
3	(Optional) If you plan to configure a TLS connection to your target database, create a wallet or certificate.	Create a Wallet or Certificates for a TLS Connection
4	If you're planning to register a database with Active Data Guard association: • Ensure that the primary and standby databases use the same private endpoint to connect to Oracle Data Safe. • Ensure that your Active Data Guard association follows the prerequisites of using Oracle Data Guard on a DB System	Use Oracle Data Guard on a DB System

Run the Oracle Cloud Databases Wizard

There is some variation in the workflow in the wizard, depending on whether you choose the TCP or TLS protocol.

This is the Oracle Cloud Database registration workflow in the wizard:

Step 1: Select Database

1. On the Overview page in the Oracle Data Safe service, find the **Oracle Cloud Databases** tile and click **Start Wizard**.

   The wizard displays the **Data Safe Target Information** form.
2. At **Cloud Database Type**, select your database type from the list.
3. Selecting a database or VM cluster:
   a. If you selected **Oracle Base Database Service** in the previous step: At **Select Database**, find and select the database.

b. If you selected an Oracle Exadata Database Service in the previous step: At **Select VM Cluster**, find and select the VM cluster.

c. If you selected **Oracle Exadata Database Service on Dedicated Infrastructure** earlier, select a database home from the **Select database** dropdown.

If your database or VM cluster does not reside in the compartment shown, click **Change Compartment**. If you want to register the database or VM cluster in a compartment other than the OCI compartment where the database or VM cluster is stored, then in the **Compartment** field, select a different compartment from the drop-down list.

> **Tip:**
>
> If you're registering a database with Active Data Guard, it is recommended to select the primary database for registration in this step and add the standby databases as peers in the following step, Step 2: Select Peer Databases.

4. Enter a target display name that is meaningful to you. Oracle Data Safe uses this name in its reports. All characters are accepted. The maximum number of characters is 255.
5. (Optional) In the **Description** box, add a description that is meaningful to you.
6. At **Database Service Name**, enter the service name of the PDB or CDB.
7. (Optional) At **Database Port Number**, the default port number is pre-filled. You may enter in a custom port number, otherwise the default will be used. For an Oracle Exadata Database Service on Dedicated Infrastructure database, enter the port number of the SCAN listener.
8. At **TCP/TLS**, select the network protocol.

   If you select the **TLS** protocol, you are presented with two options: **One way TLS** and **Mutual TLS**. If you select **One way TLS**, then do the following:

   - Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and optionally, enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database.

   If you select **Mutual TLS**, then do the following:

   - Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database.
   - When client authentication is enabled on your target database, upload the KeyStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet. This file is not required when client authentication is disabled.

   If you select `TCP` at **TCP/TLS**, you are not prompted for any additional details.
9. Perform this step if you did not already grant roles to the database user in the preregistration tasks.

   Click **Download Privilege Script** and save the `datasafe_privileges.sql` script to your computer. The script includes instructions on how to use it to grant privileges to the Oracle Data Safe service account on your target database. You should also refer to the preregistration task Grant Roles to the Oracle Data Safe Service on a Non-Autonomous Database for some additional details.
10. At **Database User Name** and **Database Password**, enter the name and password of the user you created in the preregistration tasks. If the user name is mixed case, enclose it in double-quotes (" ").

Oracle Data Safe uses this account to connect to the target database.

11. Optionally, click **Show advanced options** to tag the notification.
    a. Click **Add tag** to create an additional optional tag to organize and track resources in your tenancy.
    b. Select a **Tag namespace** from the drop-down list.
    c. Provide a **Tag key** and **Tag value**.
12. Click **Next**.

Step 2: Connectivity Option

An Oracle Data Safe private endpoint is required. Because you can only have one private endpoint in each VCN, if one already exists in the VCN (Virtual Cloud Network) of the database, Oracle Data Safe automatically selects it for you. You can then click **Next** to go directly to Step 4: **Add Security Rule**.
If no Oracle Data Safe private endpoint exists in the VCN, the wizard creates one and shows you the proposed configuration. You can change any of the parameters that are automatically entered in the form.

1. At **Name**, accept the given private endpoint name or provide a different one.
2. At **Compartment**, select the given compartment or use the drop-down menu to select a different one.

   The private endpoint does not need to be stored in the same compartment as the selected cloud database.
3. At **Virtual Cloud Network** accept the given compartment or use the drop-down menu to select the compartment where the VCN is stored. The private endpoint must run in the same VCN as the database or the VCN of the private endpoint must have VCN peering set up with the VCN of the target database.
4. At **Subnet**, accept the given compartment for the subnet or use the drop-down menu to select a different compartment. You can use any subnet. However, Oracle recommends that you use the same subnet as your database.
5. (Optional) At **Private IP**, enter the private IP address that should be assigned to the private endpoint. If you do not enter a private IP address, Oracle Data Safe assigns one automatically.
6. (Optional) Click **Show Advanced Options**.

   Use this option to attach OCI metadata tags to the private endpoint. Select the **Tag Namespace** and the **Tag Key** within the selected namespace. Then assign a value to this tag.
7. Click **Next**.

Step 3: Select Peer Database

If you're registering an Active Data Guard associated database then you can select the standby databases at this step. If you're not registering an Active Data Guard associated database, then skip this step by clicking **Next**.

1. On the **Select Additional Peer Database to Register (Optional)** page you will see a list of standby database that are associated with the primary database that you specified in the previous step. Select from the list which of the standby databases you would like to register as peers.

It is also possible to register standby databases after the primary database has been registered. See Manage Peer Databases Associated with a Registered Active Data Guard Primary Database for more information.

2. (Optional) Click **+** on a standby database to see the details for and edit any of the following if necessary:
   - Peer Display Name
   - Database Service Name
   - Database Port Number
   - TCP/TLS
3. Click **Next**.

Step 4: Add Security Rule

In this step, add the required security rules. To allow communication from Oracle Data Safe to your database, you need to add two security rules:

- **Ingress rule for the database:** Allow the database to receive incoming traffic on its port from the private IP address of the Oracle Data Safe private endpoint (from any port).
- **Egress rule for the Oracle Data Safe private endpoint:** Allow the Oracle Data Safe private endpoint (from any port) to send requests to the database IP address(es) on the database's port.

The ingress and egress rules do not need to be stored within the same security list, network security group, or same compartment. If you already created the necessary security rules, you can choose to skip this step.

> **See Also:**
>
> For more information about security lists and network security groups, see Access and Security in the Oracle Cloud Infrastructure documentation.

1. At **Do you want to add the security rules now?** , select either **Yes** or **No**.
   If you select **No**, you can then click **Next** to bypass the security rules configuration and proceed to **Review and Submit**. You can configure the security rules later in the Oracle Cloud Infrastructure Console (under **Networking**). You may want to skip this step now if you already have security rules that you want to apply. Note that the target database remains inactive in Oracle Data Safe until the security rules are configured either in the Oracle Data Safe wizard or in the Oracle Cloud Infrastructure console.
2. If you select **Yes**, then at **Add Ingress Security Rule**, select either **Security List** or **Network Security Group**. Then use the drop-down menu to select the Security List or Network Security Group to which you want to add the ingress rule.
   In the **Ingress Rule** tile, the wizard shows you the ingress rule to be added to the security list or network security group you selected.
3. At **Add Egress Security Rule**, select either **Security List** or **Network Security Group**.
4. At the next prompt, select the security list or network security group where you want to add the rule.
   If you are registering peer databases as part of an Active Data Guard associated database, then you will see an egress rule for each standby database that you selected to regiser as a peer database in Step 3: Select Peer Databases.

5. Click **Next** to go to **Review and Submit**.

Step 5: Review and Submit

If you configured a target database using an Oracle Data Safe private endpoint, the **Review and Submit** page displays the configuration for **Target Database Information**, **Connectivity Option**, and **Security Rules**.

If you are configured peer databases as part of an Active Data Guard enabled database, then you will review the **Peer Target Database Information** for each peer as well.

To change any of these settings, click the **Edit** button on the right side of the corresponding tile.

1. Review the target database configuration.
2. If the information is correct, click **Register**. If not, click **Previous** to return to any of the earlier steps, or click **Cancel**.

Step 6: Registration Progress

After you click **Register** in Step 5: **Review and Submit**, Oracle Data Safe creates the configuration and registers the target database. The next and final step in the wizard is to monitor the registration progress. The required tasks are listed and processed one-by-one.

> **Important:**
>
> Do not click the **Close** button in the wizard, sign out of OCI, or close the browser tab until the wizard shows that all of the tasks listed are resolved. If you exit prematurely, then the information for all of the tasks that have not yet been completed is lost and the target database is not registered.

After You Submit the Registration

The wizard presents the **Target Database Details** page when the registration submission is finished. On this page, you can again review the registration details. The wizard displays the `NEEDS_ATTENTION` icon if a task must be performed or corrected before the process is complete. A hint message indicates the pending task. You can make the necessary changes in the tabs that are available. When you save your changes, the `UPDATING` icon is displayed. If there is no further work to do, the registration completes.

Post Registration Tasks for an Oracle Cloud Database

The following table lists tasks that you need to complete after you run the Oracle Cloud Databases wizard.

Task Number	Task	Link to Instructions
1	(Optional) Change which features are allowed for the Oracle Data Safe service account on your target database by granting/revoking roles from the account. You need to be the `SYS` user.	Grant Roles to the Oracle Data Safe Service Account on Your Target Database

Task Number	Task	Link to Instructions
2	(Optional) Grant users access to Oracle Data Safe features with the target database by configuring policies in Oracle Cloud Infrastructure Identity and Access Management.	Create IAM Policies for Oracle Data Safe Users

Register an Oracle On-Premises Database

You can use the Oracle On-Premises Databases wizard to register an Oracle On-Premises database as an Oracle Data Safe target database.

> **Note:**
>
> Be sure to complete the preregistration tasks before using the wizard and the post registration tasks after using the wizard.

Preregistration Tasks for an Oracle On-Premises Database

The following table lists the preregistration tasks.

Task Number	Task	Link to Instructions
1	In Oracle Cloud Infrastructure Identity and Access Management (IAM), obtain permissions to register your target database.	Permissions to Register an On-Premises Oracle Database with Oracle Data Safe
2	Create an Oracle Data Safe service account on your target database and grant it Oracle Data Safe roles. Create the service account as the `SYS` user.	Create an Oracle Data Safe Service Account on Your Target Database Grant Roles to the Oracle Data Safe Service Account on Your Target Database
3	(Optional) If you plan to connect to the target database via an Oracle Data Safe private endpoint and want to configure a TLS connection, create a wallet or certificate.	Create a Wallet or Certificates for a TLS Connection.

Run the On-Premises Oracle Databases Wizard

This is the on-premises Oracle Database registration workflow in the wizard:

Step 1: Target Information

1. On the Overview page in the Oracle Data Safe service, find the **Register Oracle On-Premises Databases** tile and click **Start Wizard**.
   The wizard displays the **Data Safe Target Information** form.

2. At **DATA SAFE TARGET DISPLAY NAME**, enter a target display name that is meaningful to you. Data Safe uses this name in its reports. All characters are accepted. The maximum number of characters is 255.
3. At **COMPARTMENT**, use the drop-down menu to select the compartment where you want to store the target database.
4. (Optional) In the **DESCRIPTION** field, add a description that is meaningful to you.
5. At **DATABASE SERVICE NAME**, enter the service name of the PDB or CDB.
6. Perform this step if you did not already grant roles to the database user in the preregistration tasks.
   Click **Download Privilege Script** and save the `datasafe_privileges.sql` script to your computer. The script includes instructions on how to use it to grant privileges to the Oracle Data Safe service account on your target database. You should also refer to the preregistration task Grant Roles to the Oracle Data Safe Service on a Non-Autonomous Database for some additional details.
7. At **Database user name** and **Database password**, enter the name and password of the user you created in the preregistration tasks. If the user name is mixed case, enclose it in double-quotes (" "). Oracle Data Safe uses this account to connect to the target database.
8. Optionally, click **Show Advanced Options** to tag the notification.
   a. Click **+ Another Tag** to create an additional optional tag to organize and track resources in your tenancy.
   b. Select a **Tag Namespace** from the drop-down list.
   c. Provide a **Tag Key** and **Tag Value**.
9. Click **Next**.

Step 2: Connectivity Option

In this step, choose either an on-premises connector or Oracle Data Safe private endpoint for the connection to the target database.
If you have FastConnect or VPN Connect set up between your on-premises network and a virtual cloud network (VCN) in Oracle Cloud Infrastructure, you can register an on-premises Oracle database with Oracle Data Safe by using an Oracle Data Safe private endpoint.

1. At **Choose a connectivity option** click either `On-Premises Connector` or `Private Endpoint`.

> **Note:**
>
> If you select `Private Endpoint`, then if the database is configured with a private IP address and an Oracle Data Safe private endpoint is already configured for the VCN of the database, that private endpoint is automatically selected. (You can have only one Oracle Data Safe private endpoint per VCN.)

2. At **TCP/TLS**, select the network protocol.

   If you select the **TLS** and choose `Private Endpoint`, then you are presented with two options: **One way TLS** and **Mutual TLS**. If you select **One way TLS**, then do the following:

   - Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and optionally, enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database.

If you select **Mutual TLS**, then do the following:

- Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database.
- When client authentication is enabled on your target database, upload the KeyStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet. This file is not required when client authentication is disabled.

If you select `TCP` at **TCP/TLS**, you are not prompted for any additional details.

3. At **Database IP address**, enter the IP address of the database. If there are multiple IP addresses, use commas with no spaces to separate them.
4. At **Database port number**, enter the port number of your database listener.
5. If you chose `On-Premises Connector` in Step 1, then at **Do you want to use an existing on-premises connector?**, click **Yes** or **No**. If you select **Yes**, then from **Select on-premises connector**, use the drop-down menu to select the on-premises connector that you want to use. If you select **No**, the wizard prompts for basic information it needs to create a new on-premises connector for the target database.

   If instead you chose `Private Endpoint` in Step 1, then at **Do you want to use an existing private endpoint?**, click **Yes** or **No**. If you select **Yes**, then from **Select private endpoint**, use the drop-down menu to select the private endpoint that you want to use. The private endpoint needs to be in a VCN that can access your on-premises database. If you select **No**, the wizard prompts for basic information it needs to create a new private endpoint for the target database.

   At **Compartment** use the drop-down menu to select the compartment where you want to store the on-premises connector or private endpoint. At **Name**, provide a name of your choice. At **Description** you can opt to enter a description.
6. Click **Next**.

Step 3: Select Peer Database

If you're registering an Active Data Guard associated database then you can add the standby databases at this step. If you're not registering an Active Data Guard associated database, then skip this step by clicking **Next**.

1. Click **Add row** on the **Add additional Data Guard peer database(s) (Optional)** page. It is also possible to register standby databases after the primary database has been registered. See Manage Peer Databases Associated with a Registered Active Data Guard Primary Database for more information.
2. Enter the following information for the peer databases:
   - Peer display name
   - Database service name
   - Database IP address
   - Database port number
   - TCP/TLS
3. Add more peer databases by clicking **Add row**.
4. Click **Next**.
   If you selected `Private Endpoint` in Step 1, the wizard proceeds to Step 4: Add security rules.

If you selected `On-Premises Connector` in Step 1, the wizard takes you directly to Step 5: Review and submit.

Step 4: Add Security Rule

An egress rule is required if you configure an on-premises target database registration to use an Oracle Data Safe private endpoint. The egress rule allows the Oracle Data Safe private endpoint (from any port) to send requests to the database IP address(es) on the database's port.
An ingress rule is not needed in the Oracle Data Safe configuration for an on-premises target database. If you already created the necessary egress rule, you can choose to skip this step.

> **See Also:**
>
> For more information about security lists and network security groups, see Access and Security in the Oracle Cloud Infrastructure documentation.

1. At **Do you want to add the security rules now?**, select either **Yes** or **No**.

   If you select **No**, you can then click **Next** to bypass the egress rule selection and proceed to Step 5: **Review and Submit**. You can configure the egress rule later in the Oracle Cloud Infrastructure console (under **Networking**). Note that the target database remains inactive in Oracle Data Safe until the egress rule is configured either in the Oracle Data Safe wizard or on the Oracle Cloud Infrastructure Console.
2. If you select **Yes**, then at **Add egress security rule to**, select either **Security list** or **Network security group**.
3. Select the Security List or Network Security Group to which you want to add the egress rule.

   > **Note:**
   >
   > There will be an additional egress rule for each peer database that you have added as well.
4. Click **Next** to go to Step 5: **Review and Submit**.

Step 5: Review and Submit

In this step, the wizard displays the configuration you entered in Step 1: **Target Database Information**, Step 2: **Connectivity Option**, and Step 3: **Security Rules**.

To change any of these settings, click the **Edit** button on the right side of the corresponding tile.

1. Review the information on this page.
2. Click the checkbox, **I ACKNOWLEDGE THAT CHARGES MAY APPLY FOR THIS ON-PREMISES TARGET DATABASE**.
3. If all of the settings are correct, click **Register**. If not, click **Previous** to return to any of the earlier steps, or click **Cancel**.

Step 6: Registration Progress

After you click **Register** in Step 4: **Review and Submit**, Oracle Data Safe creates the configuration and registers the target database. The next and final step in the wizard is to monitor the registration progress. The tasks required are listed and processed one-by-one.

> **Important:**
>
> Do not click the **Close** button in the wizard, sign out of OCI, or close the browser tab until the wizard shows that all of the tasks listed are resolved. If you close prematurely, then the information for all of the tasks that have not yet been completed is lost and the target database is not registered.

After You Submit the Registration

The wizard presents the **Target Database Details** page when the registration submission is finished. On this page, you can again review the registration details. The wizard displays the `NEEDS_ATTENTION` icon if a task must be performed or corrected before the process is complete. A hint message indicates the pending task. You can make the necessary changes in the tabs that are available. When you save your changes, the `UPDATING` icon is displayed. If there is no further work to do, the registration completes.

Post Registration Tasks for an Oracle On-Premises Database

The following table lists tasks that you need to complete after you run the Oracle On-Premises Database wizard.

Task Number	Task	Link to Instructions
1	(If you are using an Oracle Data Safe on-premises connector) Download the install bundle for the on-premises connector and then install the on-premises connector on a host machine on your network.	Create an Oracle Data Safe On-Premises Connector
2	(If you are using a TLS connection and an Oracle Data Safe on-premises connector) Configure a TLS connection between the on-premises connector and your target database.	Configure a TLS Connection Between the On-Premises Connector on Your Host Machine and Your Oracle Database
3	(Optional) Change which features are allowed for the Oracle Data Safe service account on your target database by granting/revoking roles from the account. You need to be the `SYS` user.	Grant Roles to the Oracle Data Safe Service Account on Your Target Database
4	(Optional) Grant users access to Oracle Data Safe features with the target database by configuring policies in Oracle Cloud Infrastructure Identity and Access Management.	Create IAM Policies for Oracle Data Safe Users

Task Number	Task	Link to Instructions
5	Make sure to allow ingress traffic to your target database from the Oracle Data Safe private endpoint or Oracle Data Safe on-premises connector.	(none)
6	(If you are using an on-premises connector)	TCP.INVITED_NODES(Oracle Database Net Services Reference guide)

> **Note:**
>
> **Oracle Recommendation:** Ensure that only the on-premises client can connect to your on-premises Oracle database by specifying in `sqlnet.ora` parameter called `INVITED_NODES` the clients that are allowed to access your database.

Register an Oracle Cloud@Customer Database

You can register Oracle Cloud@Customer databases as target databases with Oracle Data Safe.

In Oracle Data Safe, use the **Oracle Cloud@Customer Databases** wizard to register the following Oracle Cloud@Customer databases:

- Exadata Database on Cloud@Customer
- Autonomous Database on Exadata Cloud@Customer

> **Note:**
>
> Be sure to complete the preregistration tasks before using the wizard and the post registration tasks after using the wizard.

Cloud@Customer Preregistration Tasks

The following table lists the preregistration tasks.

Task Number	Task	Link to Instructions
1	In Oracle Cloud Infrastructure Identity and Access Management (IAM), obtain permissions to register your target database.	Permissions to Register an Oracle Cloud@Customer Database with Oracle Data Safe
2	(Exadata Database on Cloud@Customer) Create an Oracle Data Safe service account on your target database and grant it Oracle Data Safe roles. Create the service account as the `SYS` user.	Create an Oracle Data Safe Service Account on Your Target Database
3	(Exadata Database on Cloud@Customer) Grant the Oracle Data Safe service account on your target database Oracle Data Safe roles.	Grant Roles to the Oracle Data Safe Service Account on Your Target Database
4	(Exadata Database on Cloud@Customer) If you plan to connect to the target database via an Oracle Data Safe private endpoint and want to configure a TLS connection, create a wallet or certificate.	Create a Wallet or Certificates for a TLS Connection.

Run the Oracle Cloud@Customer Databases Wizard

This is the registration workflow in the wizard:

Step 1: Target information

1. On the Overview page in the Oracle Data Safe service, find the **Oracle Cloud@Customer Databases** tile and click **Start Wizard**.

   The wizard displays the **Data Safe target information** form.
2. Select **Exadata Cloud@Customer** or **Autonomous Database on Exadata Cloud@Customer**.
3. At **Select VM Cluster** (for Exadata Database on Cloud@Customer) or **Select Database** (for Autonomous Database on Exadata Cloud@Customer), select the VM cluster or database respectively. If your VM cluster or database resides in a different compartment, click **Change compartment**, select the correct compartment, and then select your VM cluster or database.
4. At **Data Safe Target Display Name**, enter a target database name that is meaningful to you. Oracle Data Safe uses this name in its reports.
5. At **Compartment**, select the compartment where you want to store the Oracle Data Safe target database. Use the drop-down menu to select a different compartment if needed.

   The target database does not need to be stored in the same compartment as the VM cluster or database.
6. (Optional) In the **Description** field, enter a description that is meaningful to you.
7. (Exadata Database on Cloud@Customer) At **Database Service Name**, enter the service name of the CDB or PDB.
8. (Exadata Database on Cloud @Customer) Perform this step if you did not already grant roles to the database user in the preregistration tasks.

Click **Download privilege script** and save the `datasafe_privileges.sql` script to your computer. The script includes instructions on how to use it to grant privileges to the Oracle Data Safe service account on your target database.

> **See Also:**
>
> You should also refer to the Grant Roles preregistration task for some additional details. These instructions apply to target databases using Oracle Data Safe private endpoints and also those using on-premises connectors:
>
> Grant Roles to the Oracle Data Safe Service on a Non-Autonomous Database

9. (Exadata Database on Cloud@Customer) At **Database user name** and **Database password**, enter the credentials for the Oracle Data Safe user account that you created on your target database during the preregistration tasks. Oracle Data Safe uses this account to connect to the database. If the user name is mixed case, enclose it in double-quotes (" "). The password must be between 14 and 30 characters long and must contain at least 1 uppercase, 1 lowercase, 1 numeric, and 1 special character.
10. (Autonomous Database on Exadata Cloud@Customer) At **Database Admin User** and **Database password**, enter the credentials of the database `ADMIN` user to unlock the Oracle Data Safe user account that exists by default on the database.
11. Optionally, click **Show advanced options** to tag the notification.
    a. Click **Add tag** to create an additional optional tag to organize and track resources in your tenancy.
    b. Select a **Tag namespace** from the drop-down list.
    c. Provide a **Tag key** and **Tag value**.
12. Click **Next**.

Step 2: Connectivity Option

In this step, choose to connect to the target database through either an Oracle Data Safe on-premises connector or an Oracle Data Safe private endpoint. If you have FastConnect or VPN Connect set up between your network and a virtual cloud network (VCN) in Oracle Cloud Infrastructure, you can register your database with Oracle Data Safe by using an Oracle Data Safe private endpoint.

> **Note:**
>
> - **FastConnect** in Oracle Cloud Infrastructure is a secure connection between a customer's on-premises network and Oracle Cloud Infrastructure over a private network.
> - **VPN Connect** in Oracle Cloud Infrastructure is a site-to-site IPSec virtual private network that securely connects your on-premises network to Oracle Cloud Infrastructure, using your existing internet connection.

For an Exadata Database on Cloud@Customer, you can also choose the connectivity protocol (TCP or TLS). For an Autonomous Database on Exadata Cloud@Customer database, Oracle Data Safe automatically uses TLS.

1. Select **On-premises connector** or **Private endpoint**.
2. (Exadata Database on Cloud@Customer) For **TCP/TLS**, select **TCP** or **TLS**.
   - If you select **TCP** (the default), you are not prompted for any additional details.
   - If you are connecting via a private endpoint and select **TLS**, then you are presented with two options: **One way TLS** and **Mutual TLS**. If you select **One way TLS**, then do the following:
     – Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and optionally, enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database.

     If you select **Mutual TLS**, then do the following:
     – Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database.
     – When client authentication is enabled on your target database, upload the KeyStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet. This file is not required when client authentication is disabled.
3. (Autonomous Database on Exadata Cloud@Customer) If you selected **On-premises connector** in step 1, be sure to configure a TLS connection between the on-premises connector on your host machine and your target database. See Configure a TLS Connection Between the On-Premises Connector on Your Host Machine and an Autonomous Database on Exadata Cloud@Customer Database. If you selected **Private Endpoint** in step 1, no additional steps are needed for the TLS connection.
4. (Exadata Database on Cloud@Customer) If the database listener is not running on the default port, enter the custom port number; otherwise, leave this field blank.

> **Note:**
>
> For an Autonomous Database on Exadata Cloud@Customer, you cannot enter a port as it is automatically determined from the database.

5. For **Do you want to use an existing Private endpoint** (or **On-premises connector**): Select **Yes** to reuse or **No** to create an Oracle Data Safe on-premises connector or an Oracle Data Safe private endpoint, and then configure the following fields according to your selection.

- Yes
- No

Yes

Change compartment	If needed, click **Change compartment** to locate an existing on-premises connector or private endpoint.

Select Private Endpoint or **Select On-Premises Connector**	Select an existing Oracle Data Safe private endpoint or Oracle Data Safe on-premises connector. **Note:** If you chose **Private Endpoint** in step 1, the wizard automatically selects an existing private endpoint for you if your database has a private IP address and an Oracle Data Safe private endpoint is already configured for the VCN of the database. Be aware that you can have only one Oracle Data Safe private endpoint per VCN.

No

Compartment	Select the compartment where you want to store the on-premises connector or private endpoint.
Name	If required, enter a friendly name for your on-premises connector or private endpoint.
Description	(Optional) Enter a description for your on-premises connector or private endpoint.

6. Click **Next**.

   If you selected **On-premises connector**, the wizard will skip Step 4: **Add security rule**.

Step 3: Select Peer Database

If you're registering an Active Data Guard associated database then you can add the standby databases at this step. If you're not registering an Active Data Guard associated database, then skip this step by clicking **Next**.

1. On the **Select Additional Peer Database to Register (Optional)** page you will see a list of standby database that are associated with the primary database that you specified in the previous step. Select from the list which of the standby databases you would like to register as peers.
   It is also possible to register standby databases after the primary database has been registered. See Manage Peer Databases Associated with a Registered Active Data Guard Primary Database for more information.
2. (Optional) Click **+** on a standby database to see the details for and edit any of the following if necessary:
   - Peer Display Name
   - Database Service Name
   - Database Port Number
   - TCP/TLS
3. Click **Next**.

If you selected `On-premises connector` in Step 1, the wizard takes you directly to Step 5: **Review and submit**.

Step 4: Add Security Rule

> **Note:**
>
> This step applies only if you are configuring a private endpoint.

In this step, the wizard adds the required egress rules to enable communication between the Oracle Data Safe private endpoint and your target database. Egress rules do not need to be stored within the same security list, network security group, or same compartment. If you already created the necessary security rules, you can choose to skip this step. An ingress rule is not required.

> **See Also:**
>
> For more information about security lists and network security groups, see Access and Security in the Oracle Cloud Infrastructure documentation.

1. Choose to configure the security rules now or later.

   If you choose to configure later, click **Next** to bypass the security rule configuration and proceed to Step 4: **Review and Submit**. Later, you can configure the security rules under **Networking** in the Oracle Cloud Infrastructure Console. You may want to skip this step now if you already have security rules that you want to apply. Your target database remains inactive in Oracle Data Safe until the security rules are configured either in the Oracle Data Safe wizard or on the Oracle Cloud Infrastructure Console.
2. Choose to add egress security rules to a **Security List** or a **Network Security Group**, and then select the security list or network security group from the drop-down list.
3. Review the egress rules.

   If you are registering peer databases as part of an Active Data Guard associated database, then you will see an egress rule for each standby database that you selected to regiser as a peer database in Step 3: Select Peer Databases.

   The wizard creates an egress rule for each database server node's VIP (virtual IP address) in the VM cluster network.
4. Click **Next** to go to Step 5: **Review and Submit**.

Step 4: Review and Submit

If you configured a target database using an Oracle Data Safe private endpoint, the **Review and Submit** page displays the configuration for **Target Database Information**, **Connectivity Option**, and **Security Rules**.

If you configured a target database that uses an Oracle Data Safe on-premises connector, you did not need to configure security rules, so this summary shows information about your target database and connectivity.

To change any of these settings, click the **Edit** button on the right side of the corresponding tile.

1. Review the target database configuration.
2. If the information is correct, click **Register**. If not, click **Previous** to return to any of the earlier steps, or click **Cancel**.

Post Registration Tasks for an Oracle Cloud@Customer Database

The following table lists tasks that you need to complete after you run the Oracle Cloud@Customer Databases wizard.

Task Number	Task	Link to Instructions
1	(If you selected to create an Oracle Data Safe on-premises connector) Download the install bundle for the on-premises connector and then install the on-premises connector on a host machine on your network.	Create an Oracle Data Safe On-Premises Connector
2	(If you are using a TLS connection and an Oracle Data Safe on-premises connector) Configure a TLS connection between the on-premises connector and your target database.	• For **Autonomous Database on Exadata Cloud@Customer**: Configure a TLS Connection Between the On-Premises Connector on Your Host Machine and an Autonomous Database on Exadata Cloud@Customer Database • For **Exadata Database on Cloud@Customer**: Configure a TLS Connection Between the On-Premises Connector on Your Host Machine and Your Oracle Database
3	(Optional) Change which features are allowed for the Oracle Data Safe service account on your target database by granting/revoking roles from the account. You need to be the `SYS` user.	Grant Roles to the Oracle Data Safe Service Account on Your Target Database
4	(Optional) Grant users access to Oracle Data Safe features with the target database by configuring policies in Oracle Cloud Infrastructure Identity and Access Management.	Create IAM Policies for Oracle Data Safe Users
5	(If needed) Update the `ADMIN` credentials for your target database on the Target Database Details page.	Manage Target Databases - See the **Update the Database User** section
6	Make sure to allow ingress traffic to your target database from the Oracle Data Safe private endpoint or Oracle Data Safe on-premises connector.	(none)

Register an Oracle Database on a Compute Instance

You can use the Oracle Databases on Compute wizard to register an Oracle Database on a compute instance as Oracle Data Safe target databases.

Use the Oracle Databases on Compute wizard to register the following databases:

- Oracle Database on a compute instance in Oracle Cloud Infrastructure
- Oracle Database on a compute instance in a non-Oracle cloud environment

> **Note:**
>
> Be sure to complete the preregistration tasks before using the wizard and the post registration tasks after using the wizard.

Preregistration Tasks for an Oracle Database on Compute

The following table lists the preregistration tasks.

Task Number	Task	Link to Instructions
1	In Oracle Cloud Infrastructure Identity and Access Management (IAM), obtain permissions to register an Oracle Database on Compute.	Permissions to Register an Oracle Database on Compute with Oracle Data Safe
2	Create an Oracle Data Safe service account on your target database and grant it Oracle Data Safe roles. Create the service account as the `SYS` user.	Create an Oracle Data Safe Service Account on Your Target Database Grant Roles to the Oracle Data Safe Service Account on Your Target Database
3	(Optional) If you plan to connect to the target database via an Oracle Data Safe private endpoint and want to configure a TLS connection, create a wallet or certificate.	Create a Wallet or Certificates for a TLS Connection

Run the Oracle Databases on Compute Wizard

In the wizard, you can choose an Oracle Data Safe private endpoint or an Oracle Data Safe on-premises connector to connect to your target database. Consider the following recommendations:

- **For an Oracle Database on Compute in Oracle Cloud Infrastructure:** Oracle recommends that you use an Oracle Data Safe private endpoint to connect your target database to Oracle Data Safe.
- **For an Oracle Database on Compute in a non-Oracle cloud environment (for example, in Amazon Web Services or Azure):** Oracle recommends that you use an Oracle Data Safe on-premises connector to connect your target database to Oracle Data Safe. You can use a private endpoint, however, to do so you need an existing FastConnect or VPN Connect set up between Oracle Cloud Infrastructure and your non-Oracle cloud environment. The private endpoint then needs to be created in the Virtual Cloud Network (in Oracle Cloud Infrastructure) that has access to your target database. Without this setup, Oracle recommends that you use an on-premises connector instead.

This is the registration workflow in the wizard:

Step 1: Select Database

If you select ORACLE CLOUD INFRASTRUCTURE

1. On the Overview page in the Oracle Data Safe service, find the **Oracle Databases on Compute** tile and click **Start Wizard**. The wizard displays the **Data Safe Target Information** form.
2. Select either **ORACLE CLOUD INFRASTRUCTURE** or **AWS OR OTHER CLOUD ENVIRONMENT**.
3. If you selected **ORACLE CLOUD INFRASTRUCTURE** then at **SELECT COMPUTE INSTANCE**, select the OCI compute instance on which your database is running. If your compute instance does not reside in the compartment shown, click **CHANGE COMPARTMENT**, then locate and select the compute instance.

   This field does not appear if you select **OTHER CLOUD ENVIRONMENT**.
4. At **DATA SAFE TARGET DISPLAY NAME**, enter a target display name that is meaningful to you. Data Safe uses this name in its reports. All characters are accepted. The maximum number of characters is 255.
5. At **COMPARTMENT**, select the compartment where you want to store the target database. If you want to register the database in a compartment other than the OCI compartment where the database is stored, select a different compartment from the drop-down list.
6. (Optional) In the **DESCRIPTION** field, add a description that is meaningful to you.
7. At **DATABASE SERVICE NAME**, enter the service name of the PDB or CDB.
8. If you selected **AWS OR OTHER CLOUD ENVIRONMENT**, then at **DATABASE IP ADDRESS**, enter the IP address of the database.

   This field does not appear if you select **ORACLE CLOUD INFRASTRUCTURE**.
9. At **DATABASE PORT NUMBER**, enter the port number of your database listener.
10. Perform this step if you did not already grant roles to the database user in the preregistration tasks.

    Click **Download Privilege Script** and save the `datasafe_privileges.sql` script to your computer. The script includes instructions on how to use it to grant privileges to the Oracle Data Safe service account on your target database. You should also refer to the preregistration task Grant Roles to the Oracle Data Safe Service on a Non-Autonomous Database for some additional details.
11. At **Database user name** and **Database password**, enter the name and password of the user you created in the preregistration tasks. If the user name is mixed case, enclose it in double-quotes (" ").

    Oracle Data Safe uses this account to connect to the database.
12. Optionally, click **Show advanced options** to tag the notification.
    a. Click **Add tag** to create an additional optional tag to organize and track resources in your tenancy.
    b. Select a **Tag namespace** from the drop-down list.
    c. Provide a **Tag key** and **Tag value**.
13. Click **Next**.

Step 2: Connectivity Option

In this step choose to connect to the target database through either an on-premises connector or a through an Oracle Data Safe private endpoint.
If you have FastConnect or VPN Connect set up between your on-premises network and a virtual cloud network (VCN) in Oracle Cloud Infrastructure, you can register an on-premises Oracle database with Oracle Data Safe by using an Oracle Data Safe private endpoint.

1. At **Choose a connectivity option**, click either `On-Premises Connector` or `Private Endpoint`.

   > **Note:**
   >
   > If you select `Private Endpoint`, then if the database is configured with a private IP address and an Oracle Data Safe private endpoint is already configured for the VCN of the database, that private endpoint is automatically selected. (You can have only one Oracle Data Safe private endpoint per VCN.)

2. At **TCP/TLS**, select the network protocol.

   If you select the **TLS** protocol and choose `Private Endpoint`, then you are presented with two options: **One way TLS** and **Mutual TLS**. If you select **One way TLS**, then do the following:

   - Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and optionally, enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database.

   If you select **Mutual TLS**, then do the following:

   - Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database.
   - When client authentication is enabled on your target database, upload the KeyStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet. This file is not required when client authentication is disabled.

   If you select `TCP` at **TCP/TLS**, you are not prompted for any additional details.

3. If you chose `On-Premises Connector` in Step 1, then at **DO YOU WANT TO USE AN EXISTING ON-PREMISES CONNECTOR?**, click **YES** or **NO**. If you select **YES**, then from **SELECT ON-PREMISES CONNECTOR**, use the drop-down menu to select the on-premises connector that you want to use. If you select **NO**, the wizard prompts for basic information it needs to create a new on-premises connector for the target database.
4. If instead you chose `Private Endpoint` in Step 1, then at **DO YOU WANT TO USE AN EXISTING PRIVATE ENDPOINT?**, click **YES** or **NO**. If you select **YES**, then from **SELECT PRIVATE ENDPOINT**, use the drop-down menu to select the private endpoint that you want to use. If you select **NO**, the wizard prompts for basic information it needs to create a new private endpoint for the target database. The private endpoint needs to be in a VCN that can access your on-premises database.
5. At **COMPARTMENT** use the drop-down menu to select the compartment where you want to store the on-premises connector or private endpoint.
6. At **NAME**, provide a name of your choice.

7. At **DESCRIPTION**, enter a description.
8. Click **Next**.

   If you selected `Private Endpoint` in Step 1, the wizard proceeds to Step 3: **Add Security Rule**.

   If you selected `On-Premises Connector` in Step 1, the wizard bypasses Step 3: **Add Security Rule** and takes you directly to Step 4: **Review and Submit**.

Step 3: Add Peer Database

If you're registering an Active Data Guard associated database then you can add the standby databases at this step. If you're not registering an Active Data Guard associated database, then skip this step by clicking **Next**.

1. Click **Add row** on the **Add additional Data Guard peer database(s) (Optional)** page. It is also possible to register standby databases after the primary database has been registered. See Manage Peer Databases Associated with a Registered Active Data Guard Primary Database for more information.
2. Enter the following information for the peer databases:
   - Peer display name
   - Database service name
   - Database IP address
   - Database port number
   - TCP/TLS
3. Add more peer databases by clicking **Add row**.
4. Click **Next**.
   If you selected `Private Endpoint` in Step 1, the wizard proceeds to Step 4: Add security rules.

   If you selected `On-Premises Connector` in Step 1, the wizard takes you directly to Step 5: Review and submit.

Step 3: Add Security Rule

In this step, add the required security rules. To allow communication from Oracle Data Safe to your database, you need to add two security rules:

- **Ingress rule for the database:** Allow the database to receive incoming traffic on its port from the private IP address of the Oracle Data Safe private endpoint (from any port).
- **Egress rule for the Oracle Data Safe private endpoint:** Allow the Oracle Data Safe private endpoint (from any port) to send requests to the database IP address(es) on the database's port.

The ingress and egress rules do not need to be stored within the same security list, network security group, or same compartment. If you already created the necessary security rules, you can choose to skip this step.

> **See Also:**
>
> For more information about security lists and network security groups, see Access and Security in the Oracle Cloud Infrastructure documentation.

1. At **Do you want to add the security rules now?** , select either **Yes** or **No**.

   If you select **No**, you can then click **Next** to bypass the security rules configuration and proceed to **Review and Submit**. You can configure the security rules later in the Oracle Cloud Infrastructure Console (under **Networking**). You may want to skip this step now if you already have security rules that you want to apply. Note that the target database remains inactive in Oracle Data Safe until the security rules are configured either in the Oracle Data Safe wizard or in the Oracle Cloud Infrastructure console.
2. If you select **Yes**, then at **Add Ingress Security Rule**, select either **Security List** or **Network Security Group**. Then use the drop-down menu to select the Security List or Network Security Group to which you want to add the ingress rule.

   In the **Ingress Rule** tile, the wizard shows you the ingress rule to be added to the security list or network security group you selected.
3. At **Add Egress Security Rule**, select either **Security List** or **Network Security Group**.
4. At the next prompt, select the security list or network security group where you want to add the rule.

   > **Note:**
   >
   > The same egress rule is created for the database and for each peer database.
5. Click **Next** to go to **Review and Submit**.

Step 4: Review and Submit

In this step, the wizard displays the configuration you entered in Step 1: **Target Database Information**, Step 2: **Connectivity Option**, and Step 3: **Security Rules**.

1. Review the information on this page.
2. If all of the settings are correct, click **Register**. If not, you can click **Previous** to redo any of the earlier steps, or click **Cancel**.

Step 5: Registration Progress

After you click **Register** in Step 4: **Review and Submit**, Oracle Data Safe creates the configuration and registers the target database. The next and final step in the wizard is to monitor the registration progress. The tasks required are listed and processed one-by-one.

> **Important:**
>
> Do not click the **Close** button in the wizard, sign out of OCI, or close the browser tab until the wizard shows that all of the tasks listed are resolved. If you exit prematurely, then the information for all of the tasks that have not yet been completed is lost and the target database is not registered.

After You Submit the Registration

The wizard presents the **Target Database Details** page when the registration submission is finished. On this page, you can again review the registration details. Here you can you also review the status of peer databases, add more peer databases, and update the configuration of the peer databases as needed.

The wizard displays the `NEEDS_ATTENTION` icon if a task must be performed or corrected before the process is complete. A hint message indicates the pending task. You can make the necessary changes in the tabs that are available. When you save your changes, the `UPDATING` icon is displayed. If there is no further work to do, the registration completes.

Post Registration Tasks for an Oracle Database on Compute

The following table lists the tasks you need to complete after you run the Oracle Databases on Compute wizard.

Task Number	Task	Link to Instructions
1	(If you are using an Oracle Data Safe on-premises connector) Download the install bundle for the on-premises connector and then install the on-premises connector on a host machine on your network.	Create an Oracle Data Safe On-Premises Connector
2	(If you are using a TLS connection and an Oracle Data Safe on-premises connector) Configure a TLS connection between the on-premises connector and your target database.	Configure a TLS Connection Between the On-Premises Connector on Your Host Machine and Your Oracle Database
3	(Optional) Change which features are allowed for the Oracle Data Safe service account on your target database by granting/revoking roles from the account. You need to be the `SYS` user.	Grant Roles to the Oracle Data Safe Service Account on Your Target Database
4	(Optional) Grant users access to Oracle Data Safe features with the target database by configuring policies in Oracle Cloud Infrastructure Identity and Access Management.	Create IAM Policies for Oracle Data Safe Users
5	Make sure the firewall of the compute instance is configured to allow ingress traffic from the Oracle Data Safe private endpoint or Oracle Data Safe on-premises connector.	(none)

Register an Amazon RDS for Oracle database

You can use the Amazon RDS for Oracle Wizard to register an Amazon RDS for Oracle database as an Oracle Data Safe target database.

You can register your Amazon RDS for Oracle database with Oracle Data Safe through one of the following options:

- Register with an On-Premises Connector: Use this option if you have an Amazon RDS for Oracle database with private IP and don't have an established network peering connection, such as FastConnect or VPN Connect, between your Oracle Cloud Infrastructure (OCI) tenancy and your Amazon cloud environment
- Register with an Oracle Data Safe Private Endpoint: Use this option if you have an established network peering connection, such as FastConnect or VPN Connect, between your OCI tenancy and your Amazon cloud environment prior to registering your Amazon RDS for Oracle database with private IP with Oracle Data Safe.

> **Note:**
>
> Be sure to complete the preregistration tasks before using the wizard and the post registration tasks after using the wizard.

Register Amazon RDS for Oracle with an On-Premises Connector

Oracle recommends you use an on-premises connector to connect to target databases that run outside of Oracle Cloud Infrastructure.

Preregistration Tasks for Registering Amazon RDS for Oracle with an On-Premises Connector

The below topics should be completed before registering a target database with Oracle Data Safe with connection through an On-Premises Connector. One on-premises connector can be used to register multiple target databases. If you are establishing a TCP connection, you do not need to perform the steps to create a wallet for TLS connection.

Task Number	Task	Link to Instructions
1	In Oracle Cloud Infrastructure Identity and Access Management (IAM), obtain permissions to register a database with Oracle Data Safe	Permissions to Register a Target Database with Oracle Data Safe
2	In Oracle Cloud Infrastructure Identity and Access Management (IAM), obtain permissions to use an On-Premises Connector	Permissions for an Oracle Data Safe On-Premises Connector

Task Number	Task	Link to Instructions
3	Create an Oracle Data Safe service account on your target database and grant it Oracle Data Safe roles. Create the service account as the `SYS` user. Make sure to run the privilege script with the `-RDSORACLE` parameter as it is required if you are registering an Amazon RDS for Oracle database.	Create an Oracle Data Safe Service Account on Your Target Database Grant Roles to the Oracle Data Safe Service on a Non-Autonomous Database
4	Create an On-premises Connector	Create an Oracle Data Safe On-Premises Connector
5	Add the security certificate for the Amazon RDS specific region	Add the Security Certificate for the Amazon RDS Specific Region
6	TLS connection only: Configure a connection between the on-premises connector and your target database	Configure a TLS Connection Between the On-Premises Connector on Your Host Machine and Your Oracle Database

Run the Amazon RDS for Oracle Wizard

This is the Amazon RDS for Oracle registration workflow in the wizard:

Step 1: Target Information

1. On the Overview page in the Oracle Data Safe service, find the **Register Amazon RDS for Oracle** tile and click **Start Wizard**.
   The wizard displays the **Data Safe Target Information** form.
2. At **DATA SAFE TARGET DISPLAY NAME**, enter a target display name that is meaningful to you. Data Safe uses this name in its reports. All characters are accepted. The maximum number of characters is 255.
3. At **COMPARTMENT**, use the drop-down menu to select the compartment where you want to store the target database.
4. (Optional) In the **DESCRIPTION** field, add a description that is meaningful to you.
5. At **Database service name**, enter the service name of the CDB or PDB.
   You can use the database name on the Configuration tab of the RDS Amazon console for service name.
6. Enter the **Database IP address/endpoint**.
   The database endpoint can be found under the Connectivity and Security tab of the Amazon RDS console.
7. Enter the **Database port number**.
   The port number can be found under the Connectivity and Security tab of the Amazon RDS console.
8. Perform this step if you did not already grant roles to the database user in the preregistration tasks.
   Click **Download Privilege Script** and save the `datasafe_privileges.sql` script to your computer. The script includes instructions on how to use it to grant privileges to the Oracle Data Safe service account on your target database. You should also refer to the preregistration task Grant Roles to the Oracle Data Safe Service on a Non-Autonomous Database for some additional details.

9. At **Database user name** and **Database password**, enter the name and password of the user you created in the preregistration tasks. If the user name is mixed case, enclose it in double-quotes (" "). Oracle Data Safe uses this account to connect to the target database.
10. Optionally, click **Show Advanced Options** to tag the notification.
    a. Click **+ Another Tag** to create an additional optional tag to organize and track resources in your tenancy.
    b. Select a **Tag Namespace** from the drop-down list.
    c. Provide a **Tag Key** and **Tag Value**.
11. Click **Next**.

Step 2: Connectivity Option

1. Select **On-premises connector** as your connectivity option.
2. Select either **TCP** or **TLS** connection.
   If you select **TLS** connection:

> **Note:**
>
> In your AWS environment you will need to:
>
> - Configure SSL option group to enable SSL connection. After enabling the SSL connection, the certificate authority would show up. See Oracle Secure Sockets Layer and Creating an option group from Amazon to learn how to enable the SSL option.
> - Modify the inbound rules on port 2484 (opened by default) on Amazon RDS to allow for TLS connection
>
> .

3. From the **Select On-Premises Connector**, use the drop-down menu to select the on-premises connector that you want to use.
4. Click **Next**.

Step 3: Select Peer Database

If you're registering an Active Data Guard associated database then you can add the standby databases at this step. If you're not registering an Active Data Guard associated database, then skip this step by clicking **Next**.

1. Click **Add row** on the **Add additional Data Guard peer database(s) (Optional)** page.
   It is also possible to register standby databases after the primary database has been registered. See Manage Peer Databases Associated with a Registered Active Data Guard Primary Database for more information.
2. Enter the following information for the peer databases:
   - Peer display name
   - Database service name
   - Database IP address
   - Database port number

- TCP/TLS

3. Add more peer databases by clicking **Add row**.
4. Click **Next**.

> **Note:**
>
> Because you are using an `On-Premises Connector`, the wizard takes you directly to Step 5: Review and submit. If you use a `Private Endpoint`, the wizard takes you to Step 4: Add security rules.

Review and Submit

In this step, the wizard displays the configuration you entered in the previous steps. To change any of these settings, click the **Edit** button on the right side of the corresponding title.

1. Review the information on this page.
2. Click the checkbox, **I acknowledge that charges in Data Safe will apply for the Amazon RDS for Oracle database**.
3. Click **Register**.

Registration Process

After you click **Register** in **Review and Submit**, Oracle Data Safe creates the configuration and registers the target database. The next and final step in the wizard is to monitor the registration progress. The tasks required are listed and processed one-by-one.

> **Important:**
>
> Do not click the **Close** button in the wizard, sign out of OCI, or close the browser tab until the wizard shows that all of the tasks listed are resolved. If you close prematurely, then the information for all of the tasks that have not yet been completed is lost and the target database is not registered.

After You Submit the Registration

The wizard presents the **Target Database Details** page when the registration submission is finished. On this page, you can again review the registration details. The wizard displays the `NEEDS_ATTENTION` icon if a task must be performed or corrected before the process is complete. A hint message indicates the pending task. You can make the necessary changes in the tabs that are available. When you save your changes, the `UPDATING` icon is displayed. If there is no further work to do, the registration completes.

Post Registration Tasks

Oracle Recommendation:

Ensure that only the on-premises client can connect to your Amazon RDS for Oracle database by specifying in `sqlnet.ora` parameter called `INVITED_NODES` the clients that are allowed to access your database. See TCP.INVITED_NODES (Oracle Database Net Services Reference guide) for more information.

Register Amazon RDS for Oracle with an Oracle Data Safe Private Endpoint

If you intend to connect through a Data Safe private endpoint, you must have an established network peering connection, such as FastConnect or VPNConnect, between your Oracle Cloud Infrastructure (OCI) tenancy and your Amazon cloud environment prior to registering your target database.

Preregistration Tasks for Registering Amazon RDS for Oracle with an Oracle Data Safe Private Endpoint

The below topics should be completed before registering a target database with Oracle Data Safe with connection through a Data Safe Private Endpoint. One private endpoint can be used to register multiple target databases, but there can only be one private endpoint per Virtual Cloud Network (VCN). If you are establishing a TCP connection, you do not need to perform the steps to create a wallet for TLS connection.

Task Number	Task	Link to Instructions
1	In Oracle Cloud Infrastructure Identity and Access Management (IAM), obtain permissions to register a database with Oracle Data Safe	Permissions to Register a Target Database with Oracle Data Safe
2	In Oracle Cloud Infrastructure Identity and Access Management (IAM), obtain permissions to use an Oracle Data Safe Private Endpoint	Permissions for an Oracle Data Safe Private Endpoint
3	In Oracle Cloud Infrastructure Identity and Access Management (IAM), obtain permissions to use the underlying virtual networking resources of the private endpoint.	Virtual Cloud Networking Resources
4	Create an Oracle Data Safe service account on your target database and grant it Oracle Data Safe roles. Create the service account as the `SYS` user. Make sure to run the privilege script with the `-RDSORACLE` parameter as it is required if you are registering an Amazon RDS for Oracle database.	Create an Oracle Data Safe Service Account on Your Target Database Grant Roles to the Oracle Data Safe Service on a Non-Autonomous Database
5	Create an Oracle Data Safe private endpoint.	Create an Oracle Data Safe Private Endpoint
6	Add the security certificate for the Amazon RDS specific region	Add the Security Certificate for the Amazon RDS Specific Region
7	TLS connection only: Create a wallet or certificate	Create a Wallet or Certificates for a TLS Connection

Run the Amazon RDS for Oracle Wizard

This is the Amazon RDS for Oracle registration workflow in the wizard:

Step 1: Target Information

1. On the Overview page in the Oracle Data Safe service, find the **Register Amazon RDS for Oracle** tile and click **Start Wizard**.
   The wizard displays the **Data Safe Target Information** form.

2. At **DATA SAFE TARGET DISPLAY NAME**, enter a target display name that is meaningful to you. Data Safe uses this name in its reports. All characters are accepted. The maximum number of characters is 255.
3. At **COMPARTMENT**, use the drop-down menu to select the compartment where you want to store the target database.
4. (Optional) In the **DESCRIPTION** field, add a description that is meaningful to you.
5. At **Database service name**, enter the service name of the CDB or PDB.
   You can use the database name on the Configuration tab of the RDS Amazon console for service name.
6. Enter the **Database IP address/endpoint**.

   > **Tip:**
   >
   > For registration via private endpoint, an IP address should be provided.

7. Enter the **Database port number**.
   The port number can be found under the Connectivity and Security tab of the Amazon RDS console.
8. Perform this step if you did not already grant roles to the database user in the preregistration tasks.
   Click **Download Privilege Script** and save the `datasafe_privileges.sql` script to your computer. The script includes instructions on how to use it to grant privileges to the Oracle Data Safe service account on your target database. You should also refer to the preregistration task Grant Roles to the Oracle Data Safe Service on a Non-Autonomous Database for some additional details.
9. At **Database user name** and **Database password**, enter the name and password of the user you created in the preregistration tasks. If the user name is mixed case, enclose it in double-quotes (" "). Oracle Data Safe uses this account to connect to the target database.
10. Optionally, click **Show Advanced Options** to tag the notification.
    a. Click **+ Another Tag** to create an additional optional tag to organize and track resources in your tenancy.
    b. Select a **Tag Namespace** from the drop-down list.
    c. Provide a **Tag Key** and **Tag Value**.
11. Click **Next**.

Step 2: Connectivity Option

If you have already setup network peering, such as through FastConnect or VPN Connect, that allows you to access your Amazon RDS for Oracle database from a virtual cloud network (VCN) in OCI, then you can leverage that connection and register your database via a Data Safe private endpoint. The private endpoint essentially represents the Oracle Data Safe service in your VCN with a private IP address in a subnet of your choice.

1. Select **Private endpoint** as your connectivity option.

> **Note:**
>
> If you select **Private Endpoint**, then if the database is configured with a private IP address and an Oracle Data Safe private endpoint is already configured for the VCN of the database, that private endpoint is automatically selected. (You can have only one Oracle Data Safe private endpoint per VCN.)

2. Select either **TCP** or **TLS** connection.

   If you select **TLS** connection, you are presented with two options: **One way TLS** and **Mutual TLS**. If you select **One way TLS**, then do the following:

   - Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and optionally, enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database.

   If you select **Mutual TLS**, then do the following:

   - Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database.
   - When client authentication is enabled on your target database, upload the KeyStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet. This file is not required when client authentication is disabled.

   If you select `TCP` at **TCP/TLS**, you are not prompted for any additional details.

> **Note:**
>
> In your AWS environment you will need to:
>
> - Configure SSL option group to enable SSL connection. After enabling the SSL connection, the certificate authority would show up. See Oracle Secure Sockets Layer and Creating an option group from Amazon to learn how to enable the SSL option.
> - Modify the inbound rules on port 2484 (opened by default) on Amazon RDS to allow for TLS connection
>
> .

3. From the **Select Private Endpoint**, use the drop-down menu to select the private endpoint that you want to use.
4. Click **Next**.

Step 3: Select Peer Database

If you're registering an Active Data Guard associated database then you can add the standby databases at this step. If you're not registering an Active Data Guard associated database, then skip this step by clicking **Next**.

1. Click **Add row** on the **Add additional Data Guard peer database(s) (Optional)** page. It is also possible to register standby databases after the primary database has been registered. See Manage Peer Databases Associated with a Registered Active Data Guard Primary Database for more information.
2. Enter the following information for the peer databases:

- Peer display name
- Database service name
- Database IP address
- Database port number
- TCP/TLS

3. Add more peer databases by clicking **Add row**.
4. Click **Next**.

> **Note:**
>
> Because you are using a `Private Endpoint`, the wizard takes you to Step 4: Add security rules. If you use an `On-Premises Connector`, the wizard takes you directly to Step 5: Review and submit.

Step 3: Add Security Rule

An egress rule is required if you configure Amazon RDS for Oracle to use an Oracle Data Safe private endpoint. The egress rule allows the Oracle Data Safe private endpoint (from any port) to send requests to the database IP address(es) on the database's port.

1. At **Do you want to add the security rules now?** , select **Yes**.
   If you select **No**, you can then click **Next** to bypass the egress rule selection and proceed to Step 4: **Review and Submit**. You can configure the egress rule later in the Oracle Cloud Infrastructure console (under **Networking**). Note that the target database remains inactive in Oracle Data Safe until the egress rule is configured either in the Oracle Data Safe wizard or on the Oracle Cloud Infrastructure Console.
2. Select either **Security List** or **Network Security Group** (recommended) for where the egress security rule should be added to.
3. Select the security list or network security group from the drop down.
   The registration wizard will create the displayed egress rule in the selected list or group.
4. Click **Next**.

> **See Also:**
>
> For more information about security lists and network security groups, see Access and Security in the Oracle Cloud Infrastructure documentation.

Review and Submit

In this step, the wizard displays the configuration you entered in the previous steps. To change any of these settings, click the **Edit** button on the right side of the corresponding title.

1. Review the information on this page.
2. Click the checkbox, **I acknowledge that charges in Data Safe will apply for the Amazon RDS for Oracle database**.
3. Click **Register**.

Registration Process

After you click **Register** in **Review and Submit**, Oracle Data Safe creates the configuration and registers the target database. The next and final step in the wizard is to monitor the registration progress. The tasks required are listed and processed one-by-one.

> **Important:**
>
> Do not click the **Close** button in the wizard, sign out of OCI, or close the browser tab until the wizard shows that all of the tasks listed are resolved. If you close prematurely, then the information for all of the tasks that have not yet been completed is lost and the target database is not registered.

After You Submit the Registration

The wizard presents the **Target Database Details** page when the registration submission is finished. On this page, you can again review the registration details. The wizard displays the `NEEDS_ATTENTION` icon if a task must be performed or corrected before the process is complete. A hint message indicates the pending task. You can make the necessary changes in the tabs that are available. When you save your changes, the `UPDATING` icon is displayed. If there is no further work to do, the registration completes.

Manually Register a Target Database

You can manually register all supported target databases with Oracle Data Safe from the Target Databases page in Oracle Cloud Infrastructure.

Overview

Advanced users may prefer to register target databases manually with Oracle Data Safe instead of using a wizard. Manual registration requires that you're familiar with target registration concepts and know how to fulfill all of the preregistration tasks without the assistance of the wizard.

You can also choose to register an Autonomous Database directly from the database's details page in Oracle Cloud Infrastructure. If your Autonomous Database has a public IP address, you simply click the **Register** link and you are done. If you are registering an Autonomous Database with a private IP address, you need have an Oracle Data Safe private endpoint created beforehand. When registering an Autonomous Database on Dedicated Exadata Infrastructure, you need to provide the `ADMIN` database user credentials.

Preregistration Tasks for Manual Target Database Registration

Before manually registering a database as an Oracle Data Safe target database, be sure to complete the following preregistration tasks.

- Obtain permissions in Oracle Cloud Infrastructure Identity and Access Management (IAM) for registering your target database. See the following:
  - Permissions to Register an Autonomous Database with Oracle Data Safe
  - Permissions to Register an Oracle Cloud Database with Oracle Data Safe

  - Permissions to Register an On-Premises Oracle Database with Oracle Data Safe
  - Permissions to Register an Oracle Database on Compute with Oracle Data Safe
  - Permissions to Register an Oracle Cloud@Customer Database with Oracle Data Safe
- If needed, create an Oracle Data Safe private endpoint or an Oracle Data Safe on-premises connector to connect Oracle Data Safe to your target database. See the following:
  - Create an Oracle Data Safe Private Endpoint
  - Create an Oracle Data Safe On-Premises Connector
- If you are using an Oracle Data Safe private endpoint to connect your target database to Oracle Data Safe, create the necessary ingress and/or egress security rules. See Add Security Rules.
- (Non-Autonomous Databases only) Create an Oracle Data Safe service account on your database. See Create an Oracle Data Safe Service Account on Your Target Database.
- Grant and revoke roles from the Oracle Data Safe service account on your target database to allow or disallow Oracle Data Safe features on the database. See Grant Roles to the Oracle Data Safe Service Account on Your Target Database.
- (Non-Autonomous Databases only) If you plan to configure a TLS connection to your target database, then you need to do the following:
  - If you are connecting to your target database via an Oracle Data Safe private endpoint, create a wallet or certificate. See Create a Wallet or Certificates for a TLS Connection.
  - If you are connecting to your target database via an Oracle Data Safe on-premises connector, configure the TLS connection between your on-premises database and the on-premises connector on your host machine. See Configure a TLS Connection Between the On-Premises Connector on Your Host Machine and Your Oracle Database.
- (Autonomous Database on Dedicated Exadata Infrastructure) If Database Vault is enabled on the database, connect to your database as a user with the `DV_ACCTMGR` role and temporarily grant the c role to the `ADMIN` user.
- (Autonomous Database on Exadata Cloud@Customer) Configure a TLS connection between the on-premises connector on your host machine and your Autonomous Database. See Configure a TLS Connection Between the On-Premises Connector on Your Host Machine and an Autonomous Database on Exadata Cloud@Customer Database.

Manually Register an Autonomous Database

Oracle recommends using the Oracle Data Safe registration wizard for Autonomous Databases; however, advanced users can also use the manual registration option as described below. Be sure to complete the pre-registration tasks beforehand and the post-registration tasks afterward.

1. Sign in to Oracle Cloud Infrastructure (OCI).
2. From the navigation menu in Oracle Cloud Infrastructure, select **Oracle Database**, and then **Data Safe - Database Security**.
3. Under **Data Safe** on the left, click **Target Databases**.
4. Click **Register Database**.
5. For **Database Type**, select **Autonomous Database**.

6. Configure the fields as described in the following table.

Field	Instruction
Select Database	Select the name of your database. If needed, click **Change Compartment**, select a different compartment, and then select the name of your database.
Data Safe Target Display Name	Enter a friendly name for your target database.This name can be any name you want, and all characters are accepted. The maximum number of characters is 255. This name is displayed in all of the Oracle Data Safe reports that pertain to your target database.
Description	(Optional) Enter a description that is meaningful to you.
Compartment	Select the compartment where you want to store the target database registration information. The compartment doesn't have to be the same compartment in which the actual database resides. You cannot change the compartment after the target database is registered.

7. Optionally, click **Show advanced options** to tag the notification.
   a. Click **Add tag** to create an additional optional tag to organize and track resources in your tenancy.
   b. Select a **Tag namespace** from the drop-down list.
   c. Provide a **Tag key** and **Tag value**.
8. Click **Register**.

Manually Register an Oracle Cloud Database

Oracle recommends using the Oracle Data Safe registration wizard for Oracle Cloud Databases; however, advanced users can also use the manual registration option as described below. Be sure to complete the pre-registration tasks beforehand and the post-registration tasks afterward.

1. Sign in to Oracle Cloud Infrastructure (OCI).
2. From the navigation menu in Oracle Cloud Infrastructure, select **Oracle Database**, and then **Data Safe - Database Security**.
3. Under **Data Safe** on the left, click **Target Databases**.
4. Click **Register Database**.
5. For **Database Type**, select **Oracle Cloud Database**.
6. Configure the fields as described in the following table.

Field	Instruction
Cloud Database type	Select **Oracle Base Database Service**, **Oracle Exadata Database Service on Dedicated Infrastructure**, or **Oracle Exadata Database Service on Exascale Infrastructure**.
Select Database	Select the name of your database. If needed, click **Change Compartment**, select a different compartment, and then select your database name.
Data Safe Target Display Name	Enter a friendly name for your target database. This name can be any name you want, and all characters are accepted. The maximum number of characters is 255. This name is displayed in all of the Oracle Data Safe reports that pertain to your target database.

Field	Instruction
Description	(Optional) Enter a description that is meaningful to you.
Compartment	Select the compartment where you want to store the target database registration information. The compartment doesn't have to be the same compartment in which the actual database resides. You cannot change the compartment after the target database is registered.
Select Private Endpoint	Select an Oracle Data Safe private endpoint. If needed, click **Change Compartment** to browse to a different compartment and select a private endpoint. If you do not have a private endpoint created, exit manual registration and create one.
TCP/TLS	Select **TCP** or **TLS** as the connection protocol. If you select TLS, you are presented with two options: **One way TLS** and **Mutual TLS**. If you select **One way TLS**, then do the following: Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and optionally, enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database. If you select **Mutual TLS**, then do the following: Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database. When client authentication is enabled on your target database, upload the KeyStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet. This file is not required when client authentication is disabled.
Database Service Name	Enter the long version of the database service name for the target database; for example, `abc_prod.subnetad3.tttvcn.companyvcn.com`. You can find the database service name in the `tnsnames.ora` file for your target database, or by running the following statement when connected to the PDB via SQL Plus: `select sys_context('userenv','service_name') from dual;`
Database Port Number	Enter a custom port number; otherwise the default, pre-filled port number is used. For an Oracle Exadata Database Service on Dedicated Infrastructure database, enter the port number of the SCAN listener.
Data Safe User and Database Password	Enter the credentials for the Oracle Data Safe user account on your target database. A default Oracle Data Safe user name is displayed if it exists on your target database (for example, `DATASAFE$ADMIN`). The user name is case-insensitive, unless you enclose it in quotation marks. You cannot specify database roles, such as `SYSDBA` or `SYSKM`, and you cannot specify `SYS` as the user.
Download Privilege Script	To grant roles to the Oracle Data Safe user account on your target database, click **Download Privilege Script** and save the `datasafe_privileges.sql` script to your computer. The script includes instructions. Also see Grant Roles to the Oracle Data Safe Service on a Non-Autonomous Database.

7. Optionally, click **Show advanced options** to tag the notification.
   a. Click **Add tag** to create an additional optional tag to organize and track resources in your tenancy.
   b. Select a **Tag namespace** from the drop-down list.
   c. Provide a **Tag key** and **Tag value**.
8. Click **Register**.

Manually Register an Oracle On-Premises Database

Oracle recommends using the Oracle Data Safe registration wizard for Oracle On-Premises Databases; however, advanced users can also use the manual registration option as described below. Be sure to complete the pre-registration tasks beforehand and the post-registration tasks afterward.

1. Sign in to Oracle Cloud Infrastructure (OCI).
2. From the navigation menu in Oracle Cloud Infrastructure, select **Oracle Database**, and then **Data Safe - Database Security**.
3. Under **Data Safe** on the left, click **Target Databases**.
4. Click **Register Database**.
5. For **Database Type**, select **Oracle On-Premises Database**.
6. Configure the fields as described in the following table.

Field	Instruction
Data Safe Target Display Name	Enter a friendly name for your target database.This name can be any name you want, and all characters are accepted. The maximum number of characters is 255. This name is displayed in all of the Oracle Data Safe reports that pertain to your target database.
Description	(Optional) Enter a description that is meaningful to you.
Compartment	Select the compartment where you want to store the target database registration information. The compartment doesn't have to be the same compartment in which the actual database resides. You cannot change the compartment after the target database is registered.
Choose a connectivity option	Select **On-Premises Connector** or **Private Endpoint**.
Select Private Endpoint	(If you chose private endpoint) Select the name of an existing Oracle Data Safe private endpoint. If needed, click **Change Compartment** to browse to a different compartment and select a private endpoint.
Select On-Premises Connector	(If you chose on-premises connector) Select the name of an existing Oracle Data Safe on-premises connector. If needed, click **Change Compartment** to browse to a different compartment and select an on-premises connector.
Connection Protocol	Select **TCP** or **TLS** as the connection protocol. If you select TLS, you are presented with two options: **One way TLS** and **Mutual TLS**. If you select **One way TLS**, then do the following: Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and optionally, enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database. If you select **Mutual TLS**, then do the following: Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database. When client authentication is enabled on your target database, upload the KeyStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet. This file is not required when client authentication is disabled.

Field	Instruction
Database Service Name	Enter the long version of the database service name for the target database; for example, `abc_prod.subnetad3.tttvcn.companyvcn.com`. You can find the database service name in the `tnsnames.ora` file for your target database, or by running the following statement when connected to the PDB via SQL Plus: `select sys_context('userenv','service_name') from dual;`
Database IP Address	Enter the database IP addresses for each database node listener. Separate the IP addresses with a comma. For a RAC database, enter the IP addresses for the RAC database nodes.
Database Port Number	Enter a custom port number; otherwise the default, pre-filled port number is used. All node listeners have to run on the same port for on-premises databases.
Data Safe User and Database Password	Enter the credentials for the Oracle Data Safe user account on your target database. A default Oracle Data Safe user name is displayed (`DATASAFE$ADMIN`). The user name is case-insensitive, unless you enclose it in quotation marks. You cannot specify database roles, such as `SYSDBA` or `SYSKM`, and you cannot specify `SYS` as the user.
Download Privilege Script	To grant roles to the Oracle Data Safe user account on your target database, click **Download Privilege Script** and save the `datasafe_privileges.sql` script to your computer. The script includes instructions. Also see Grant Roles to the Oracle Data Safe Service on a Non-Autonomous Database.

7. Optionally, click **Show advanced options** to tag the notification.
   a. Click **Add tag** to create an additional optional tag to organize and track resources in your tenancy.
   b. Select a **Tag namespace** from the drop-down list.
   c. Provide a **Tag key** and **Tag value**.
8. Click **Register**.

Manually Register an Oracle Database on Compute

Oracle recommends using the Oracle Data Safe registration wizard for an Oracle Database on Compute; however, advanced users can also use the manual registration option as described below. Be sure to complete the pre-registration tasks beforehand and the post-registration tasks afterward.

1. Sign in to Oracle Cloud Infrastructure (OCI).
2. From the navigation menu in Oracle Cloud Infrastructure, select **Oracle Database**, and then **Data Safe - Database Security**.
3. Under **Data Safe** on the left, click **Target Databases**.
4. Click **Register Database**.
5. For **Database Type**, select **Oracle Database on Compute**.
6. Configure the fields as described in the following table.

Field	Instruction
Cloud environment	Select **Oracle Cloud Infrastructure** if your database runs in Oracle Cloud Infrastructure, or select **Other cloud environment** if your target database runs in a non-Oracle cloud environment.
Select Database	(If your target database runs in Oracle Cloud Infrastructure) Select the name of your database. If needed, click **Change Compartment**, select a different compartment, and then select your database name.
Data Safe Target Display Name	Enter a friendly name for your target database. This name can be any name you want, and all characters are accepted. The maximum number of characters is 255. This name is displayed in all of the Oracle Data Safe reports that pertain to your target database.
Description	(Optional) Enter a description that is meaningful to you.
Compartment	Select the compartment where you want to store the target database registration information. The compartment doesn't have to be the same compartment in which the actual database resides. You cannot change the compartment after the target database is registered.
Choose a connectivity option	Select **On-Premises Connector** or **Private Endpoint**. If your target database runs in Oracle Cloud Infrastructure, Oracle recommends you use a private endpoint. If your target database runs in a non-Oracle cloud environment, Oracle recommends you use an on-premises connector.
Select Private Endpoint	(If you chose private endpoint) Select the name of an existing Oracle Data Safe private endpoint. If needed, click **Change Compartment** to browse to a different compartment and select a private endpoint.
Select On-Premises Connector	(If you chose on-premises connector) Select the name of an existing Oracle Data Safe on-premises connector. If needed, click **Change Compartment** to browse to a different compartment and select an on-premises connector.
Connection Protocol	Select **TCP** or **TLS** as the connection protocol. If you select TLS, you are presented with two options: **One way TLS** and **Mutual TLS**. If you select **One way TLS**, then do the following: Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and optionally, enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database. If you select **Mutual TLS**, then do the following: Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database. When client authentication is enabled on your target database, upload the KeyStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet. This file is not required when client authentication is disabled.
Database Service Name	Enter the long version of the database service name for the target database; for example, `abc_prod.subnetad3.tttvcn.companyvcn.com`. You can find the database service name in the `tnsnames.ora` file for your target database, or by running the following statement when connected to the PDB via SQL Plus: `select sys_context('userenv','service_name') from dual;`
Database IP Address	(Non-Oracle cloud environments) Enter the database IP address for your target database.
Database Port Number	Enter a port number.

Field	Instruction
Data Safe User and Database Password	Enter the credentials for the Oracle Data Safe user account on your target database. A default Oracle Data Safe user name is displayed (`DATASAFE$ADMIN`). The user name is case-insensitive, unless you enclose it in quotation marks. You cannot specify database roles, such as `SYSDBA` or `SYSKM`, and you cannot specify `SYS` as the user.
Download Privilege Script	To grant roles to the Oracle Data Safe user account on your target database, click **Download Privilege Script** and save the `datasafe_privileges.sql` script to your computer. The script includes instructions. Also see Grant Roles to the Oracle Data Safe Service on a Non-Autonomous Database.

7. Optionally, click **Show advanced options** to tag the notification.
   a. Click **Add tag** to create an additional optional tag to organize and track resources in your tenancy.
   b. Select a **Tag namespace** from the drop-down list.
   c. Provide a **Tag key** and **Tag value**.
8. Click **Register**.

Manually Register a Cloud@Customer Database

Oracle recommends using the Oracle Data Safe registration wizard for Oracle Cloud@Customer Databases; however, advanced users can also use the manual registration option as described below. Be sure to complete the pre-registration tasks beforehand and the post-registration tasks afterward.

1. Sign in to Oracle Cloud Infrastructure (OCI).
2. From the navigation menu in Oracle Cloud Infrastructure, select **Oracle Database**, and then **Data Safe - Database Security**.
3. Under **Data Safe** on the left, click **Target Databases**.
4. Click **Register Database**.
5. For **Database Type**, select **Oracle Cloud@Customer Database**.
6. For **Choose a target type**, select **Exadata Cloud@Customer** or **Autonomous Database on Exadata Cloud@Customer**, configure the fields for your target type, and then click **Register**.

- Exadata Cloud@Customer database
- Autonomous Database on Exadata Cloud@Customer

Exadata Cloud@Customer database

Select VM Cluster	Select a VM cluster. If needed, click **Change Compartment**, select a different compartment, and then select a VM cluster.
Data Safe Target Display Name	Enter a friendly name for your target database. This name can be any name you want, and all characters are accepted. The maximum number of characters is 255. This name is displayed in

	all of the Oracle Data Safe reports that pertain to your target database.
Description	(Optional) Enter a description that is meaningful to you.
Compartment	Select the compartment where you want to store the target database registration information. The target database does not need to be stored in the same compartment as the VM cluster or database. You cannot change the compartment after the target database is registered.
Choose a connectivity option	Select **On-Premises Connector** or **Private Endpoint**, and then select the name of an existing Oracle Data Safe private endpoint or Oracle Data Safe on-premises connector. If needed, click **Change Compartment**, browse to a different compartment, and then make your selection.
Connection Protocol	Select **TCP** or **TLS** as the connection protocol. If you select TLS, you are presented with two options: **One way TLS** and **Mutual TLS**. If you select **One way TLS**, then do the following: Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and optionally, enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database. If you select **Mutual TLS**, then do the following: Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database. When client authentication is enabled on your target database, upload the KeyStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet. This file is not required when client authentication is disabled.
Database Service Name	Enter the long version of the database service name for the target database; for example, `abc_prod.subnetad3.tttvcn.companyvcn.com`. You can find the database service name in the `tnsnames.ora` file for your target database, or by running the following statement when connected to the PDB via SQL Plus: `select sys_context('userenv','service_name') from dual;`
Database Port Number	(Optional) If the database listener is not running on the default port, enter the custom port number; otherwise, leave this field blank.
Data Safe User and Database Password	Enter the credentials for the Oracle Data Safe user account on your target database. A default Oracle Data Safe user name is displayed (`DATASAFE$ADMIN`). The user name is case-insensitive, unless you enclose it in quotation marks. The password must be between 14 and 30 characters long and must contain at least 1 uppercase, 1 lowercase, 1 numeric, and 1 special character. You cannot specify database roles, such as `SYSDBA` or `SYSKM`, and you cannot specify `SYS` as the user.
Download Privilege Script	To grant roles to the Oracle Data Safe user account on your target database, click **Download Privilege Script** and save the

	`datasafe_privileges.sql` script to your computer. The script includes instructions. Also see Grant Roles to the Oracle Data Safe Service on a Non-Autonomous Database.

Autonomous Database on Exadata Cloud@Customer

Select Database	Select a database. If needed, click **Change Compartment**, select a different compartment, and then select your database name.
Data Safe Target Display Name	Enter a friendly name for your target database. This name can be any name you want, and all characters are accepted. The maximum number of characters is 255. This name is displayed in all of the Oracle Data Safe reports that pertain to your target database.
Description	(Optional) Enter a description that is meaningful to you.
Compartment	Select the compartment where you want to store the target database registration information. The compartment doesn't have to be the same compartment in which the actual database resides. You cannot change the compartment after the target database is registered.
Choose a connectivity option	Select **On-Premises Connector** or **Private Endpoint**, and then select the name of an existing Oracle Data Safe private endpoint or Oracle Data Safe on-premises connector. If needed, click **Change Compartment**, browse to a different compartment, and then make your selection. If you choose on-premises connector, be sure to configure a TLS connection between the Connection Manager of the on-premises connector on your host machine and your target database. See Configure a TLS Connection Between the On-Premises Connector on Your Host Machine and Your Oracle Database.
Database Admin User and Database Password	Enter the credentials for the `ADMIN` user account on your target database. This is required to unlock the Oracle Data Safe user account that already exists on your database.

7. Optionally, click **Show advanced options** to tag the notification.
   a. Click **Add tag** to create an additional optional tag to organize and track resources in your tenancy.
   b. Select a **Tag namespace** from the drop-down list.
   c. Provide a **Tag key** and **Tag value**.
8. Click **Register**.

Manually Register an Amazon RDS for Oracle database

Oracle recommends using the Oracle Data Safe registration wizard however, advanced users can also use the manual registration option as described below. Be sure to complete the pre-registration tasks beforehand and the post-registration tasks afterward.

Preregistration Tasks for Registering Amazon RDS for Oracle with Private IP

The below topics should be completed before registering an Amazon RDS for Oracle database. Select the tab for registering with an Oracle Data Safe private endpoint if you have an established FastConnect or VPNConnect connection between your OCI tenancy and your Amazon cloud environment. If you are establishing a TCP connection, you do not need to perform the steps to create a wallet for TLS connection.

- On-Premises Connector
- Private Endpoint

On-Premises Connector

Task Number	Task	Link to Instructions
1	In Oracle Cloud Infrastructure Identity and Access Management (IAM), obtain permissions to register a database with Oracle Data Safe	Permissions to Register a Target Database with Oracle Data Safe
2	In Oracle Cloud Infrastructure Identity and Access Management (IAM), obtain permissions to use an On-Premises Connector	Permissions for an Oracle Data Safe On-Premises Connector
3	Create an Oracle Data Safe service account on your target database and grant it Oracle Data Safe roles. Create the service account as the `SYS` user. Make sure to run the privilege script with the `-RDSORACLE` parameter as it is required if you are registering an Amazon RDS for Oracle database.	Create an Oracle Data Safe Service Account on Your Target Database Grant Roles to the Oracle Data Safe Service on a Non-Autonomous Database
4	Create an On-premises Connector	Create an Oracle Data Safe On-Premises Connector

Task Number	Task	Link to Instructions
5	Add the security certificate for the Amazon RDS specific region	Add the Security Certificate for the Amazon RDS Specific Region
6	TLS connection only: Configure a connection between the on-premises connector and your target database	Configure a TLS Connection Between the On-Premises Connector on Your Host Machine and Your Oracle Database

Private Endpoint

Task Number	Task	Link to Instructions
1	In Oracle Cloud Infrastructure Identity and Access Management (IAM), obtain permissions to register a database with Oracle Data Safe	Permissions to Register a Target Database with Oracle Data Safe
2	In Oracle Cloud Infrastructure Identity and Access Management (IAM), obtain permissions to use an Oracle Data Safe Private Endpoint	Permissions for an Oracle Data Safe Private Endpoint
3	In Oracle Cloud Infrastructure Identity and Access Management (IAM), obtain permissions to use the underlying virtual networking resources of the private endpoint.	Virtual Cloud Networking Resources
4	Create an Oracle Data Safe service account on your target database and grant it Oracle Data Safe roles. Create the service account as the `SYS` user. Make sure to run the privilege script with the `-RDSORACLE` parameter as it is required if you are registering an Amazon RDS for Oracle database.	Create an Oracle Data Safe Service Account on Your Target Database Grant Roles to the Oracle Data Safe Service on a Non-Autonomous Database
5	Create an Oracle Data Safe private endpoint.	Create an Oracle Data Safe Private Endpoint
6	Add the security certificate for the Amazon RDS specific region	Add the Security Certificate for the Amazon RDS Specific Region
7	TLS connection only: Create a wallet or certificate	Create a Wallet or Certificates for a TLS Connection

Manually Register Amazon RDS for Oracle

Oracle recommends using the Oracle Data Safe registration wizard however, advanced users can also use the manual registration option as described below. Be sure to complete the pre-registration tasks beforehand and the post-registration tasks afterward.

1. Sign in to Oracle Cloud Infrastructure (OCI).
2. From the navigation menu in Oracle Cloud Infrastructure, select **Oracle Database**, and then **Data Safe - Database Security**.

3. Under **Data Safe** on the left, click **Target Databases**.
4. Click **Register Database**.
5. For **Database Type**, select **Amazon RDS for Oracle**.
6. At **DATA SAFE TARGET DISPLAY NAME**, enter a target display name that is meaningful to you. Data Safe uses this name in its reports. All characters are accepted. The maximum number of characters is 255.
7. (Optional) In the **DESCRIPTION** field, add a description that is meaningful to you.
8. At **COMPARTMENT**, use the drop-down menu to select the compartment where you want to store the target database.
9. Select either **Private endpoint** or **On-premises connector** as the connectivity option.
10. Select an existing private endpoint or on-premises connector from the appropriate compartment.
11. Select either **TCP** or **TLS** connection.

    If you select **TLS** connection, you are presented with two options: **One way TLS** and **Mutual TLS**. If you select **One way TLS**, then do the following:

    - Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and optionally, enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database.

    If you select **Mutual TLS**, then do the following:

    - Upload the TrustStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet and enter the wallet password. This file is required whether client authentication is enabled or disabled on your target database.
    - When client authentication is enabled on your target database, upload the KeyStore of your database in the format of PEM file, PKCS#12 wallet, or JKS wallet. This file is not required when client authentication is disabled.

    If you select `TCP` at **TCP/TLS**, you are not prompted for any additional details.

    > **Note:**
    >
    > In your AWS environment you will need to:
    >
    > - Configure SSL option group to enable SSL connection. After enabling the SSL connection, the certificate authority would show up. See Oracle Secure Sockets Layer and Creating an option group from Amazon to learn how to enable the SSL option.
    > - Modify the inbound rules on port 2484 (opened by default) on Amazon RDS to allow for TLS connection
    >
    > .

12. At **Database service name**, enter the service name of the CDB or PDB.
    You can use the database name on the Configuration tab of the RDS Amazon console for service name.
13. Enter the **Database IP address/endpoint**.

> **Tip:**
>
> For registration via private endpoint, an IP address should be provided.

14. Enter the **Database port number**.
    The port number can be found under the Connectivity and Security tab of the Amazon RDS console.
15. Perform this step if you did not already grant roles to the database user in the preregistration tasks.
    Click **Download Privilege Script** and save the `datasafe_privileges.sql` script to your computer. The script includes instructions on how to use it to grant privileges to the Oracle Data Safe service account on your target database. You should also refer to the preregistration task Grant Roles to the Oracle Data Safe Service on a Non-Autonomous Database for some additional details.
16. At **Database user name** and **Database password**, enter the name and password of the user you created in the preregistration tasks. If the user name is mixed case, enclose it in double-quotes (" "). Oracle Data Safe uses this account to connect to the target database.
17. Optionally, click **Show Advanced Options** to tag the notification.
    a. Click **+ Another Tag** to create an additional optional tag to organize and track resources in your tenancy.
    b. Select a **Tag Namespace** from the drop-down list.
    c. Provide a **Tag Key** and **Tag Value**.
18. Click **Register**.

Post Registration Tasks for Manual Target Database Registration

After you complete the manual target database registration, perform the following post registration tasks as needed:

- (Optional) Grant users access to Oracle Data Safe features with the target database by configuring IAM policies. See Create IAM Policies for Oracle Data Safe Users.
- (Optional) Change which features are allowed for the Oracle Data Safe service account on your target database by granting/revoking roles from the account. See Grant Roles to the Oracle Data Safe Service Account on Your Target Database.
- For an Autonomous Database on Dedicated Exadata Infrastructure only: If Database Vault is enabled on your target database, connect to your target database as a user with the `DV_ACCTMGR` role and revoke the `DV_ACCTMGR` role from the `ADMIN` user.
- For Oracle Database on a compute instance, make sure the firewall of the compute instance is configured to allow ingress traffic from the Oracle Data Safe private endpoint or Oracle Data Safe on-premises connector.
- For an Oracle On-Premises database or an Oracle Cloud@Customer database, make sure to allow ingress traffic to your target database from the Oracle Data Safe private endpoint or Oracle Data Safe on-premises connector.

Manage Target Databases

As your target databases and their environments evolve, you may need to perform various life-cycle management activities.

View Registration Details for a Target Database

You can view registration details from the Target Database Details page in the Oracle Data Safe service in Oracle Cloud Infrastructure.

1. From the navigation menu in Oracle Cloud Infrastructure, select **Oracle Database**, and then select **Data Safe - Database Security**.

   The **Overview** page for the Oracle Data Safe service is displayed.
2. Under **Data Safe** on the left, click **Target databases**.
3. Under **List scope** on the left, select the compartment that contains the target databases that you want to view.
4. (Optional) To list all of the target databases in the child compartments too, select the **Include child compartments** check box.
5. Click the name of the target database for which you want to view registration details.

   The **Target database information** page is displayed.
6. View the registration details for the selected target database on the **Target database information** tab. The details vary depending on the database type.

Update Connection Details for a Target Database

From the **Target Database Details** page, you can update connection details for a target database. The connection details vary depending on the database type; for example, TCP/TLS, database service name, database port number, and so on.

For example, for some target databases you can change the Oracle Data Safe private endpoint or Oracle Data Safe on-premises connector configuration for a target database.

1. From the navigation menu in Oracle Cloud Infrastructure, select **Oracle Database**, and then select **Data Safe - Database Security**.

   The **Overview** page for the Oracle Data Safe service is displayed.
2. Under **Data Safe** on the left, click **Target Databases**.
3. Under **List Scope** on the left, select the compartment that contains the target databases that you want to view.
4. (Optional) To list all of the target databases in the child compartments too, select the **Include Child Compartments** check box.
5. Click the name of the target database that you want to update.

   The **Target Database Details** page is displayed.
6. Click **Edit Connection Details**.

   The **Edit Connection Details** window is displayed.
7. Modify the connection details as needed, and then click **Save Changes**.

Update a Target Database Name and Description

You can update the name and description for your target database.

1. From the navigation menu in Oracle Cloud Infrastructure, select **Oracle Database**, and then select **Data Safe - Database Security**.

The **Overview** page for the Oracle Data Safe service is displayed.

2. Under **Data Safe** on the left, click **Target Databases**.
3. Under **List Scope** on the left, select the compartment that contains your target database.
4. (Optional) To list all of the target databases in the child compartments too, select the **INCLUDE CHILD COMPARTMENTS** check box.
5. Click the name of the target database that you want to update.

   The **Target Database Details** page is displayed.
6. To modify the target database name, click the pencil icon next to the **Name** field, modify the name, and then click the save icon.
7. To modify the target database description, click the pencil icon next to the **Description** field, modify the description, and then click the save icon.

Update the Database User

You can use the **Update Database User** feature on the **Target Database Details** page to update the user credentials on your target database that Oracle Data Safe requires.

For a non-Autonomous Database, you can update the credentials for the Oracle Data Safe service account. For an Autonomous Database, you can update the credentials for the `ADMIN` account, which is required to unlock the Oracle Data Safe user account that already exists on the database.

1. From the navigation menu in Oracle Cloud Infrastructure, select **Oracle Database**, and then select **Data Safe - Database Security**.

   The **Overview** page for the Oracle Data Safe service is displayed.
2. Under **Data Safe** on the left, click **Target Databases**.
3. Under **List Scope** on the left, select the compartment that contains the target databases that you want to view.
4. (Optional) To list all of the target databases in the child compartments too, select the **INCLUDE CHILD COMPARTMENTS** check box.
5. Click the name of the target database.

   The **Target Database Details** page is displayed.
6. Click **Update Database User**.

   The **Update Database User** panel is displayed.
7. Modify the credentials as needed, and then click **Save Changes**.

Manage Peer Databases Associated with a Registered Active Data Guard Primary Database

When you register a target database that is the primary database in an Active Data Guard association, you can manage the associated standby databases from the **Target database information** page of the primary database. Managing the standby databases can include, adding them as peer databases, refreshing their connection details, editing their connection details, or deregistering them from Oracle Data Safe.

1. From the navigation menu in Oracle Cloud Infrastructure, select **Oracle Database**, and then select **Data Safe - Database Security**.

The **Overview** page for the Oracle Data Safe service is displayed.

2. Under **Data Safe** on the left, click **Target databases**.
3. Under **List scope** on the left, select the compartment that contains the target databases that you want to view.
4. (Optional) To list all of the target databases in the child compartments too, select the **Include child compartments** check box.
5. Click the name of the target database for which you want to add peer databases to or refresh peer database connections for.
   The **Target database information** page is displayed.

Add Peer Databases

1. Click **Add peer database** in the **Active Data Guard peer databases** section.
2. For a cloud target database and Cloud@Customer database:
   a. In the side pane you will see a list of standby database that are associated with the selected primary database. Select from the list which of the standby databases you would like to register as peers.
   b. (Optional) Click **+** on a standby database to see the details for and edit any of the following if necessary:
      - Peer Display Name
      - Database Service Name
      - Database Port Number
      - TCP/TLS
   c. Click **Add peer database**
3. For an on-premises target database:
   a. In the side pane enter in the information for the peer database:
      - Peer display name
      - Database service name
      - Database IP address
      - Database port number
      - TCP/TLS
   b. Click **Add row** to add an additional peer database.
   c. Click **Add peer database**

Manually Refresh Peer Database Connections

Click **Refresh**.

> **Note:**
>
> Oracle Data Safe automatically checks and refreshes the peer database connection details every hour.

Edit Connection Details

1. Click on the name of the peer database from the **Active Data Guard peer databases** section.
   This will bring you to the **Peer database information** page.
2. To edit connection details, click **Edit connection details**, edit the information as necessary, and click **Save changes**.

> **Note:**
>
> If the peer database is the root database, the connection details can't be edited. The **Secondary key** value for a root database is 0.

Deregister a Peer Database

1. Click on the name of the peer database from the **Active Data Guard peer databases** section.
   This will bring you to the **Peer database information** page.
2. Click **Deregister**.

What to Do in Data Safe After Performing a Manual Switch Over of Active Data Guard Associated Target Databases?

If you have registered Active Data Guard associated target databases in Data Safe, you are able to see the role (primary or standby) of the databases. If you perform a manual switchover of the databases, you may not see the changes in the roles reflected immediately in Data Safe.

As a result of this, it's possible that a data masking job will fail because the proper read and write permissions are not associated with the database.

To prevent this from occurring, after performing a manual switchover, refresh the database connections. See Manage Peer Databases Associated with a Registered Active Data Guard Primary Database for more information.

Move a Target Database to a Different Compartment

1. From the navigation menu in Oracle Cloud Infrastructure, select **Oracle Database**, and then select **Data Safe - Database Security**.

   The **Overview** page for the Oracle Data Safe service is displayed.
2. Under **Data Safe** on the left, click **Target Databases**.
3. Under **List Scope** on the left, select the compartment that contains your target database.
4. (Optional) To list all of the target databases in the child compartments too, select the **INCLUDE CHILD COMPARTMENTS** check box.
5. Click the name of the target database that you want to update.

   The **Target Database Details** page is displayed.
6. From the **More Actions** menu, select **Move Resource**.

   A **Move Resource to a Different Compartment** dialog box is displayed.

7. From the drop-down list, select a different compartment, and then click **Move Resource**.

   The target database is immediately moved to the compartment.

Activate or Deactivate a Target Database

The activate and deactivate features are available for Oracle Cloud Databases only. When you deactivate a target database, it can no longer be used in Oracle Data Safe and audit data collection is stopped for the target database. Users who have access to the target database can still view existing reports and assessments.

1. From the navigation menu in Oracle Cloud Infrastructure, select **Oracle Database**, and then select **Data Safe - Database Security**.

   The **Overview** page for the Oracle Data Safe service is displayed.
2. Under **Data Safe** on the left, click **Target Databases**.
3. Under **List Scope** on the left, select the compartment that contains the target database that you want to activate or deactivate.
4. (Optional) To list all of the target databases in the child compartments too, select the **INCLUDE CHILD COMPARTMENTS** check box.
5. Click the name of the target database that you want to activate or deactivate.

   The **Target Database Details** page is displayed.
6. From the **More Actions** menu, select **Activate** or **Deactivate**.
7. To confirm, click **Activate** or **Deactivate**.

   Your target database is activated or deactivated from Oracle Data Safe.

Deregister a Target Database

When you deregister a target database, the target database is no longer available in Oracle Data Safe. If your target database is connected via a private endpoint, the private endpoint is not automatically deleted during deregistration. You can still view collected audit data in the audit reports for a deregistered target database as long as the audit data retention period is not expired.

1. From the navigation menu in Oracle Cloud Infrastructure, select **Oracle Database**, and then select **Data Safe - Database Security**.

   The **Overview** page for the Oracle Data Safe service is displayed.
2. Under **Data Safe** on the left, click **Target Databases**.
3. Under **List Scope** on the left, select the compartment that contains the target database that you want to deregister.
4. (Optional) To list all of the target databases in the child compartments too, select the **INCLUDE CHILD COMPARTMENTS** check box.
5. Click the name of the target database that you want to deregister.

   The **Target Database Details** page is displayed.
6. From the **More Actions** menu, select **Deregister**.
7. To confirm, click **Deregister**.

   Your target database is deregistered from Oracle Data Safe.

For non-billed target databases the database will be in a `DELETED` state for one day. During this time, the metadata about your target database is kept in Oracle Data Safe. After one day, Oracle Data Safe permanently removes all metadata about your target database and your target database is no longer listed in the user interface.

For billed target databases the database will be in a `DELETED` state for 45 days. During this time, the metadata about your target database is kept in Oracle Data Safe. After 45 days, Oracle Data Safe permanently removes all metadata about your target database and your target database is no longer listed in the user interface.

Related Topics

- Resources That Are Automatically Deleted When a Target Database is De-registered
- What Resources Can Be Deleted While a Target Database is Active

Resources That Are Automatically Deleted When a Target Database is De-registered

When you de-register a target database there are a number of resources that are automatically deleted. However, there are also some resources that can't be deleted. See the below list to learn what happens to certain resources when a target database is de-registered.

Table 3-3 Resources that are automatically deleted when a target database is de-registered

Functional Area	Data Safe Resource	Data Safe Resource Name in OCI IAM	Comments
Activity Auditing	Audit Profile*	data-safe-audit-profiles	In a cleanup job once there are no more audit events for the target
Activity Auditing	Audit Trail	data-safe-audit-trails	
Activity Auditing	Audit Event	data-safe-audit-events	Once the retention policy is over
Activity Auditing	Audit Policy*	data-safe-audit-policies	
Activity Auditing/Alerts	Target Alert Policy Associations	data-safe-target-alert-policy-associations	
Activity Auditing/Alerts	Report	data-safe-reports	Reports that are older than 90 days will be deleted in a routine cleanup job
Activity Auditing	Archive Retrievals	data-safe-archive-retrievals	Yes - After the retrieved data has been online for 30 days
User Assessment	User Assessment	user-assessments	In a routine cleanup job
Security Assessment	Security Assessment	security-assessments	In a routine cleanup job
SQL Firewall	Database Security Config	data-safe-database-security-configs	In a routine cleanup job
SQL Firewall	Security Policy	data-safe-security-policies	In a routine cleanup job
SQL Firewall	Security Policy Deployment	data-safe-security-policy-deployments	In a routine cleanup job
SQL Firewall	Firewall Policy	data-safe-sql-firewall-policies	In a routine cleanup job
SQL Firewall	SQL Collection	data-safe-sql-collections	In a routine cleanup job

Table 3-3 (Cont.) Resources that are automatically deleted when a target database is de-registered

Functional Area	Data Safe Resource	Data Safe Resource Name in OCI IAM	Comments
SQL Firewall	Violation Logs	data-safe-sql-firewall-violations	Yes-After the 12 month retention period has passed
SQL Firewall	SQL Firewall Allowed SQL	data-safe-sql-firewall-allowed-sqls	In a routine cleanup job

*When a target database is de-registered, the target database's audit policies and audit profiles are scheduled for deletion in an automatic cleanup job. Following the first run of the cleanup job, the policies are visible and marked as FAILED. Following the second run of the clean up job, the policies are visible and marked as DELETED. The policies are hard deleted following the third run of the clean up job and then are no longer be visible.

> **Note:**
>
> A maximum of 100 policies are cleaned up per day. So, in cases where more than 100 policies need to be cleaned up, the remaining policies are queued up for the next day's cleanup job.

The routine cleanup job runs frequently and deletes a number of resources whenever it runs. If you have many resources in the queue to be deleted, it may take several runs of the cleanup job to empty the queue.

Resources associated with or used by the target database (for example, sensitive data models, masking policies, and reports) are not deleted when the target database is de-registered. You need to manually delete these items. See What Resources Can Be Deleted While a Target Database is Active for more information.

Related Topics

- What Resources Can Be Deleted When a Target Database is Active

Resources That Are Automatically Deleted When a Target Database is De-registered

When you de-register a target database there are a number of resources that are automatically deleted. However, there are also some resources that can't be deleted. See the below list to learn what happens to certain resources when a target database is de-registered.

Table 3-4 Resources that are automatically deleted when a target database is de-registered

Functional Area	Data Safe Resource	Data Safe Resource Name in OCI IAM	Comments
Activity Auditing	Audit Profile*	data-safe-audit-profiles	In a cleanup job once there are no more audit events for the target

Table 3-4 (Cont.) Resources that are automatically deleted when a target database is de-registered

Functional Area	Data Safe Resource	Data Safe Resource Name in OCI IAM	Comments
Activity Auditing	Audit Trail	data-safe-audit-trails	
Activity Auditing	Audit Event	data-safe-audit-events	Once the retention policy is over
Activity Auditing	Audit Policy*	data-safe-audit-policies	
Activity Auditing/Alerts	Target Alert Policy Associations	data-safe-target-alert-policy-associations	
Activity Auditing/Alerts	Report	data-safe-reports	Reports that are older than 90 days will be deleted in a routine cleanup job
Activity Auditing	Archive Retrievals	data-safe-archive-retrievals	Yes - After the retrieved data has been online for 30 days
User Assessment	User Assessment	user-assessments	In a routine cleanup job
Security Assessment	Security Assessment	security-assessments	In a routine cleanup job
SQL Firewall	Database Security Config	data-safe-database-security-configs	In a routine cleanup job
SQL Firewall	Security Policy	data-safe-security-policies	In a routine cleanup job
SQL Firewall	Security Policy Deployment	data-safe-security-policy-deployments	In a routine cleanup job
SQL Firewall	Firewall Policy	data-safe-sql-firewall-policies	In a routine cleanup job
SQL Firewall	SQL Collection	data-safe-sql-collections	In a routine cleanup job
SQL Firewall	Violation Logs	data-safe-sql-firewall-violations	Yes-After the 12 month retention period has passed
SQL Firewall	SQL Firewall Allowed SQL	data-safe-sql-firewall-allowed-sqls	In a routine cleanup job

*When a target database is de-registered, the target database's audit policies and audit profiles are scheduled for deletion in an automatic cleanup job. Following the first run of the cleanup job, the policies are visible and marked as FAILED. Following the second run of the clean up job, the policies are visible and marked as DELETED. The policies are hard deleted following the third run of the clean up job and then are no longer be visible.

> **Note:**
>
> A maximum of 100 policies are cleaned up per day. So, in cases where more than 100 policies need to be cleaned up, the remaining policies are queued up for the next day's cleanup job.

The routine cleanup job runs frequently and deletes a number of resources whenever it runs. If you have many resources in the queue to be deleted, it may take several runs of the cleanup job to empty the queue.

Resources associated with or used by the target database (for example, sensitive data models, masking policies, and reports) are not deleted when the target database is de-registered. You need to manually delete these items. See What Resources Can Be Deleted While a Target Database is Active for more information.

Related Topics

- What Resources Can Be Deleted When a Target Database is Active

Manage Network Access Changes for an Oracle Autonomous Database Serverless

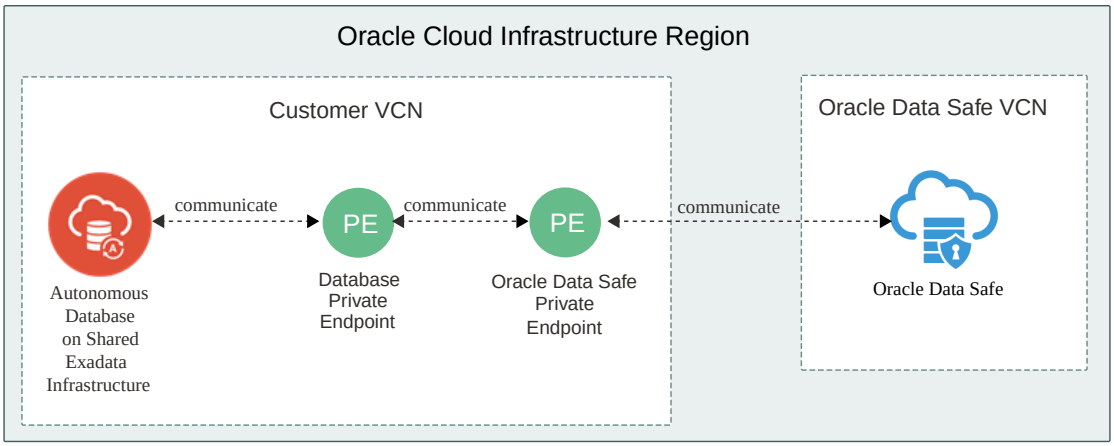
You can change the network access type for your Oracle Autonomous Database Serverless from **Secure Access from Anywhere** to **Virtual cloud network**, and vice versa. When making a network access change, you may need to perform tasks to maintain the database's registration with Oracle Data Safe.

Overview

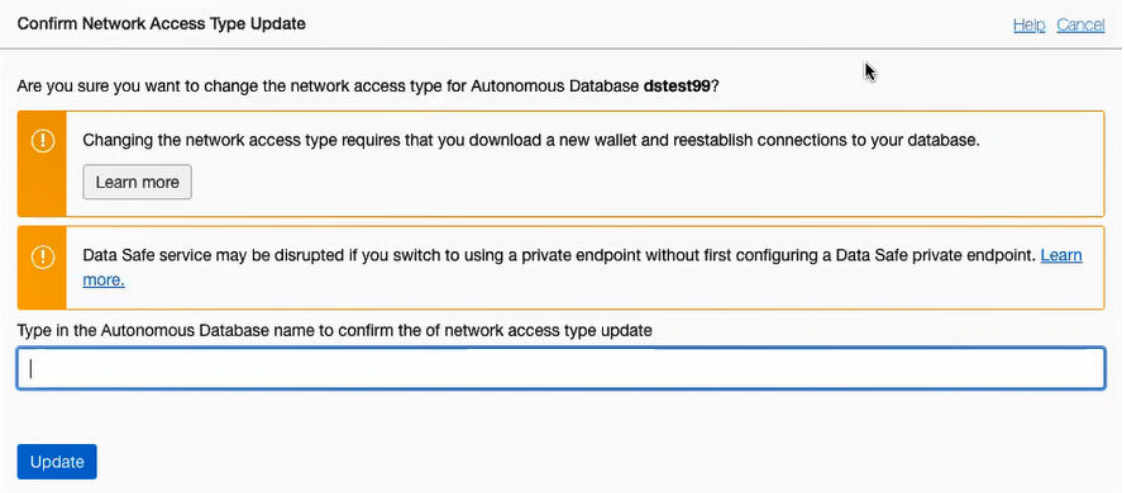
If you plan to switch the network access for your Oracle Autonomous Database Serverless from **Secure Access from Anywhere** (public endpoint) to **Virtual cloud network** (private endpoint), prior to making the network access change, you need to create an Oracle Data Safe private endpoint on the same virtual cloud network (VCN) and subnet as your database. If you plan to switch from a private endpoint to a public endpoint, you do not need to do anything other than make the network switch. You do not need to deregister your Autonomous Database with Oracle Data Safe beforehand. Your database will have a public IP address after you make the change and you can view that IP address from the database's Console. You may want to delete the Oracle Data Safe private endpoint previously used because it is no longer needed.

> **Note:**
>
> If your Oracle Autonomous Database Serverless is not yet registered with Oracle Data Safe, first make the network access change and then register your database.

When you switch the network access type for your Autonomous Database from **Secure Access from Anywhere** to **Virtual cloud network**, the database's private endpoint communicates with Oracle Data Safe's private endpoint. The two private endpoints allow Oracle Data Safe to communicate with your database. This scenario is illustrated in the diagram below.



If there is no Oracle Data Safe private endpoint available and you attempt to make the network access change, you will get a message stating that the "Data Safe service may be disrupted if you switch to using a private endpoint without first configuring a Data Safe private endpoint.", as shown in the screenshot below. In this case, the switch will fail.



Workflow

If your Oracle Autonomous Database Serverless is already registered with Oracle Data Safe and you want to switch the database's network access type from **Secure Access from Anywhere** to **Virtual cloud network**, then follow the general steps listed in the table below.

Step	Description	Reference
1	Create an Oracle Data Safe private endpoint.	Create an Oracle Data Safe Private Endpoint
2	Switch the network access type to VCN for your Oracle Autonomous Database Serverless.	Change from Public to Private Endpoints with Autonomous Database
3	Update the security rules to allow communication between Oracle Data Safe and your Autonomous Database.	Update the Security Rules to Allow Communication Between Oracle Data Safe and Your Database

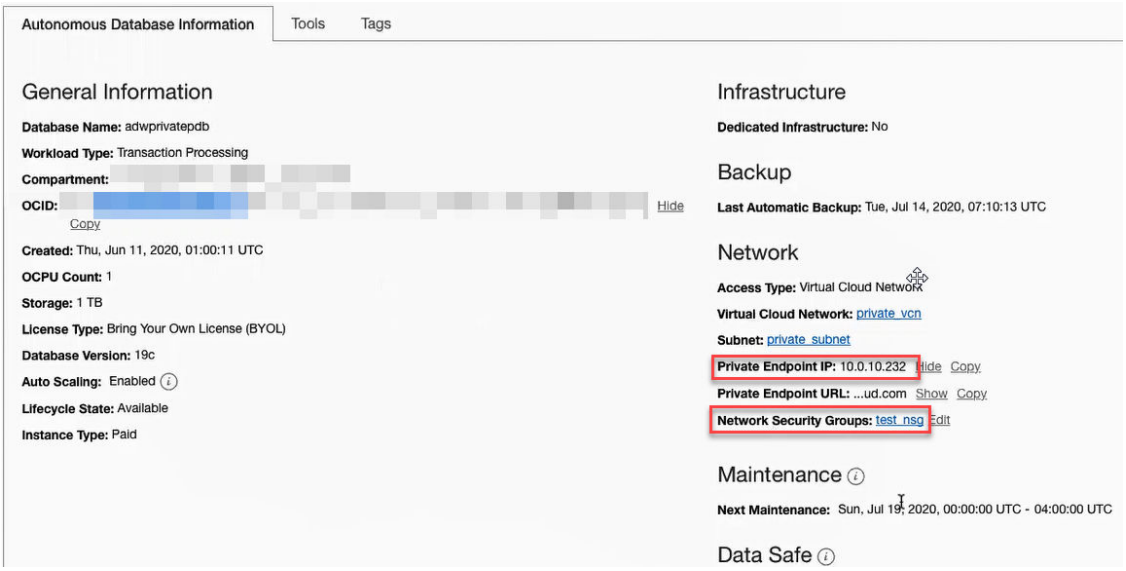
Update the Security Rules to Allow Communication Between Oracle Data Safe and Your Database

Update the ingress and egress security rules for the Network Security Groups (NSGs) on your private VCN in Oracle Cloud Infrastructure to allow traffic from Oracle Data Safe's private endpoint to your Autonomous Database's private endpoint. While both an NSG and a security list act as virtual firewalls for your database, Oracle recommends that you use NSGs. For more information, see Network Security Groups.

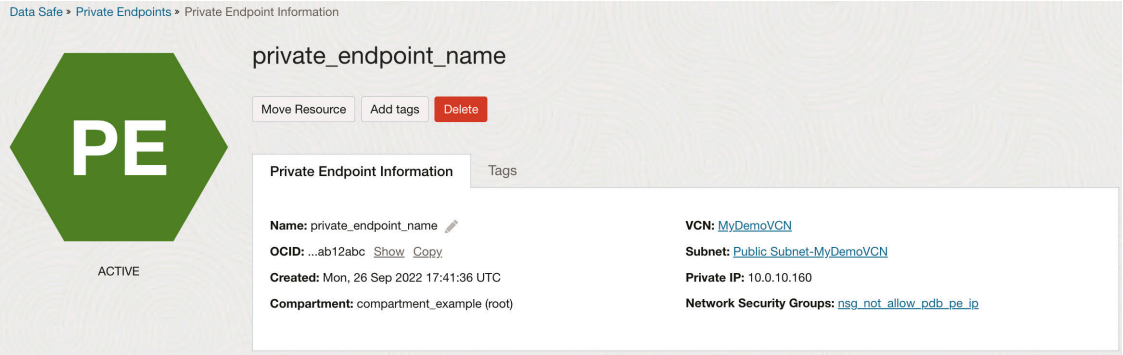
Example 3-4 Configure security rules for an Oracle Autonomous Database Serverless with private VCN access

Suppose you provision an Oracle Autonomous Database Serverless with private VCN access in Oracle Cloud Infrastructure. During provisioning, Oracle Cloud Infrastructure automatically creates a private endpoint for your database and you associate an NSG with your database.

To obtain the private IP address for your database's private endpoint and view the NSG name, you access the **Autonomous Database Information** tab in your database's Console in Oracle Cloud Infrastructure. As shown in the following screenshot, under **Network**, the private endpoint's IP address is **10.0.10.232** and the NSG name is **test_nsg**.



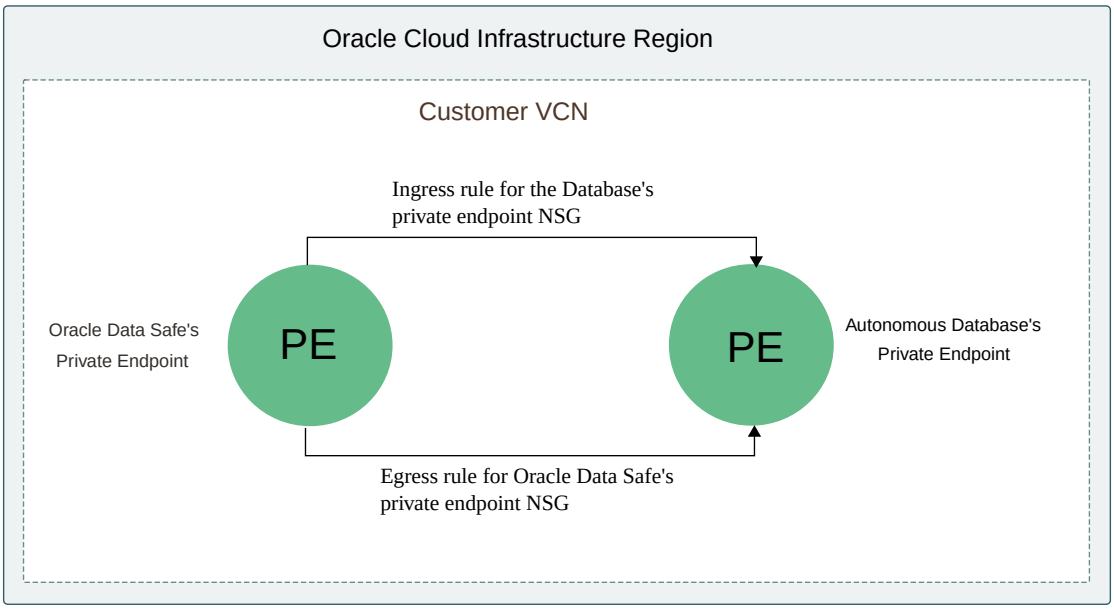
To obtain the private IP address and NSG for Oracle Data Safe's private endpoint, you access the **Private Endpoint Information** tab on the **Data Safe** page in Oracle Cloud Infrastructure. As shown in the following screenshot, the IP address is **10.0.10.160** and the NSG name is **nsg_not_allow_pdb_pe_ip**.



Next, you create a security rule for each of the NSGs the following way:

- **Ingress rule for the database private endpoint NSG:** The database's private endpoint IP address, 10.0.10.232 (on port 1522), can receive incoming traffic from Oracle Data Safe's private endpoint IP address, 10.0.0.6 (from any port).
- **Egress rule for the Oracle Data Safe private endpoint NSG:** Oracle Data Safe's private endpoint IP address, 10.0.0.6 (from any port), can send requests to the database's private endpoint IP address, 10.0.10.232 (on port 1522).

The following diagram illustrates the security rules.



What to Do if an Autonomous Database Name Changes

If you rename your Autonomous Database from the database's Console in Oracle Cloud Infrastructure, the change is automatically propagated to Oracle Data Safe. Oracle recommends that you update the target database name in Oracle Data Safe to best match your database name.

Each target database name must be unique in Oracle Data Safe. By updating your target database name, you can avoid name conflicts in the future.

To update the name of your target database:

1. From the navigation menu in Oracle Cloud Infrastructure, select **Oracle Database**, and then select **Data Safe - Database Security**.

The **Overview** page for the Oracle Data Safe service is displayed.

2. Under **Data Safe** on the left, click **Target Databases**.
3. Under **List Scope** on the left, select the compartment that contains your target database.
4. (Optional) To list all of the target databases in the child compartments too, select the **INCLUDE CHILD COMPARTMENTS** check box.
5. Click the name of the target database that you want to update.

   The **Target Database Details** page is displayed.
6. Click the edit button (pencil icon) next to the target database name, modify the name, and then click the save button (disk icon).

Create an Oracle Data Safe Private Endpoint

You can create an Oracle Data Safe private endpoint to connect Oracle Data Safe to an Oracle Cloud Database (with a private IP address), Oracle On-Premises Database, and Oracle Database on Compute. Create the Oracle Data Safe private endpoint on the Private Endpoints page in the Oracle Data Safe service in Oracle Cloud Infrastructure.

Prerequisites Tasks for Creating an Oracle Data Safe Private Endpoint

Prior to creating an Oracle Data Safe private endpoint, be sure to complete the following prerequisite tasks:

- Obtain permission to create virtual networking resources in Oracle Cloud Infrastructure. See the section called **Target Registration Resources** in OCI Resources for Oracle Data Safe.
- Obtain permission to create an Oracle Data Safe private endpoint in Oracle Cloud Infrastructure. See the section called **Target Registration Resources** in OCI Resources for Oracle Data Safe.

Create an Oracle Data Safe Private Endpoint

1. Refer to the following table to obtain the network information for your database.

Database	How to Find Network Information for the Database
Oracle Autonomous Database Serverless (private IP address)	a. From the navigation menu in Oracle Cloud Infrastructure, select **Oracle Database**, and then **Autonomous Data Warehouse** or **Autonomous Transaction Processing**. b. From the **Compartment** drop-down list, select the compartment that contains your Autonomous Database. c. On the right, click the name of your Autonomous Database. d. Under **Network** on the the **Autonomous Database Information** tab, make note of the VCN and subnet names.

Database	How to Find Network Information for the Database
Autonomous Database on Dedicated Exadata Infrastructure (private IP address)	a. From the navigation menu in Oracle Cloud Infrastructure, select **Oracle Database**, and then **Autonomous Dedicated Infrastructure**. b. Click **Autonomous Exadata Infrastructure**. c. On the right, in the **Autonomous Exadata Infrastructure** table, click the name of the infrastructure in which your database exists. d. Under **Network**, make note of the VCN and subnet names.
DB system (private IP address)	a. From the navigation menu in Oracle Cloud Infrastructure, select **Oracle Database**, and then **Bare Metal, VM, and Exadata**. b. Click the name of your DB system. c. On the **DB System Information** tab, under **Network**, make note of the VCN and subnet names.
Oracle Database on a compute instance in Oracle Cloud Infrastructure	a. From the navigation menu in Oracle Cloud Infrastructure, select **Compute**, and then **Instances**. b. Click the name of your compute instance. c. On the **Instance Information** tab, make note of the VCN and subnet names.
Oracle Database on a compute instance in a non-Oracle cloud environment	a. From the navigation menu in Oracle cloud Infrastructure, select **Networking**, and then **Site-to-Site VPN (IPSec)** or **FastConnect**. b. Select the VCN and subnet in Oracle Cloud Infrastructure that has connectivity via FastConnect or VPN Connect to your database. c. If you do not have FastConnect or VPN Connect set up, Oracle recommends that you use an Oracle Data Safe on-premises connector instead. See Create an Oracle Data Safe On-Premises Connector.
On-Premises Oracle Database	Obtain the name of the virtual cloud network and subnet on which your on-premises Oracle database can be accessed.
Amazon RDS for Oracle	Obtain the name of the virtual cloud network and subnet on which your Amazon RDS for Oracle database can be accessed.

2. From the navigation menu in Oracle Cloud Infrastructure, select **Oracle Database**, and then **Data Safe - Database Security**.

   The **Overview** page is displayed.

3. On the left under **Data Safe**, click **Target Databases**.

4. On the left under **Connectivity Options**, click **Private Endpoints**.

   The **Private Endpoints** page is displayed.

5. Click **Create Private Endpoint**.

   The **Create Private Endpoint** panel is displayed.

6. In the **NAME** field, enter a name for your private endpoint.

7. Select a compartment in which to store your private endpoint.

8. Scroll down to the **Private Endpoint Information** section.

9. From the **VIRTUAL CLOUD NETWORK** drop-down list, select the VCN on which your database can be accessed. If needed, click **CHANGE COMPARTMENT** and select the compartment that stores your VCN.

10. From the **SUBNET** drop-down list, select a subnet within the selected VCN. If needed, click **CHANGE COMPARTMENT** and select the compartment that stores the subnet that you want to use.

    The subnet can be in a different compartment than the VCN. The subnet that you select needs to have access to the database's subnet.

11. (Optional) In the **PRIVATE IP** field, specify a private IP address.

    If you do not specify a private IP address, Oracle Cloud Infrastructure automatically generates one for you in the selected subnet.

12. (Optional) Select a network security group to which your database belongs.

13. (Optional) To add another network security group, click **+ Another Network Security Group**, and select another network security group.

14. Click **Create Private Endpoint**.

    A private endpoint for Oracle Data Safe is provisioned in your database's VCN.

15. To view details for your private endpoint, click its name. Take note of the Private IP address that was assigned to the Private Endpoint (or that you assigned to it). It is needed for configuring security rules.

Create an Oracle Data Safe On-Premises Connector

You can create an Oracle Data Safe on-premises connector to connect Oracle Data Safe to an Oracle On-Premises Database, or Oracle Database on Compute. You can create up to five Oracle Data Safe on-premises connectors on the On-Premises Connectors page in the Oracle Data Safe service in Oracle Cloud Infrastructure. One on-premises connector instance can support up to 192 active connections.

Prerequisites for Creating an Oracle Data Safe On-Premises Connector

Prior to creating an Oracle Data Safe on-premises connector, be sure to complete the following prerequisite tasks:

- Obtain permission for creating an Oracle Data Safe on-premises connector. See the section called **Target Registration Resources** in OCI Resources for Oracle Data Safe.
- Ensure that the host(s) on which you plan to install the Oracle Data Safe on-premises connector meets the hardware and software requirements.

Hardware Requirements

Oracle recommends that you install the on-premises connector on a host machine other than your Oracle database host machine. You can, however, install it on the database host machine if needed. In a production environment, Oracle recommends that you install the same on-premises connector on two Linux hosts for high availability. If one of your hosts goes down due to system failure or maintenance, Oracle Data Safe connections automatically fail over to the on-premises connector running on the other host, and the on-going Oracle Data Safe operations are not affected.

Be sure that the host machine on which you are going to install the on-premises connector meets the following hardware requirements:

- Minimum CPU: 2
- Minimum RAM: 16GB
- Minimum local disk storage:
  - 5GB, where the on-premises connection software plus log space takes 100 MB
  - `/tmp` space: 100 MB
- Network interface bandwidth: 1Gbps
- Network connectivity:
  - Outbound connectivity to Oracle Data Safe (`accesspoint.datasafe.<region>.oci.oraclecloud.com:443`). Replace `<region>` with your region; for example, `accesspoint.datasafe.us-ashburn-1.oci.oraclecloud.com`.
  - Local connectivity to target database listener hosts/ports

Software Requirements

Be sure that the host machine on which you are going to install the on-premises connector meets the following software requirements:

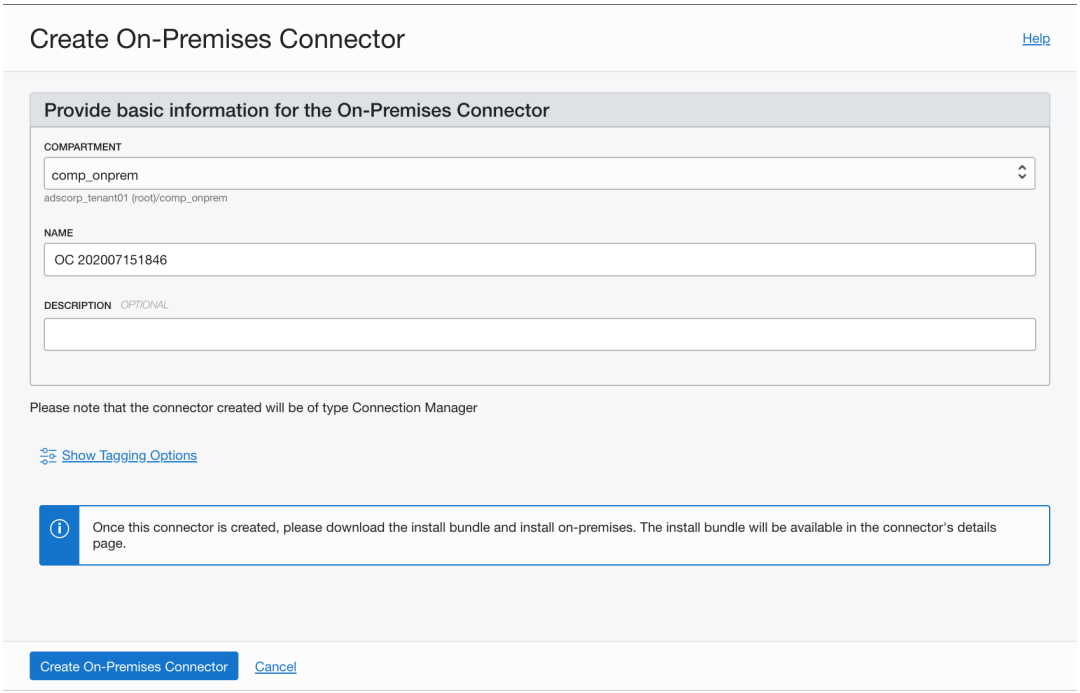
- Operating system:
  - Oracle Linux 7 or higher (Linux x86-64) or
  - Red Hat Enterprise Linux (RHEL) 8
- Python 3.5 or higher - If you have multiple versions of Python installed, make sure that you set the default to Python 3.5 or higher, or explicitly provide the Python path when running the commands.
- Java version 7 or higher with a valid Java Home (`JAVA_HOME`)

> **Note:**
>
> For instructions on how to uninstall, update, stop, and show the status, please refer to the `README` file that comes with the install bundle.

Create an Oracle Data Safe On-Premises Connector

1. Sign in to the Oracle Cloud Infrastructure Console and select the appropriate region in your tenancy.
2. From the navigation menu, select **Oracle Database**, and then **Data Safe - Database Security**.
3. On the left under **Data Safe**, click **Target Databases**.
4. On the left under **Connectivity Options**, click **On-Premises Connectors**.
5. On the right, click **Create On-Premises Connector**.

   The **Create On-Premises Connector** panel is displayed.
6. From the drop-down list, select the compartment in which you want to store the on-premises connector.
7. Enter a name for the on-premises connector.
8. (Optional) Enter a description for the on-premises connector.
9. (Optional) To configure tagging, click **Show Tagging Options**, and then configure a tag.



10. Click **Create On-Premises Connector**.

    The on-premises connector is created and listed in the table. The initial life-cycle state of the on-premises connector is set to `INACTIVE`.

Download the Install Bundle for the Oracle Data Safe On-Premises Connector

You can download the install bundle for the on-premises connector from the **Connector Detail** page in the Oracle Data Safe service.

1. Access the **Overview** page for Oracle Data Safe.
2. On the left under **Data Safe**, click **Target Databases**.
3. Under **Connectivity Options** on the left, click **On-Premises Connectors**.
4. Click the on-premises connector that you created.
5. Click **Download Install Bundle**.

   The **Download Install Bundle** dialog box is displayed.
6. Enter a password for the install bundle, confirm it, and then click **Download**.

   Keep this password on hand as you need it later when you install the on-premises connector on a host on your network.

   The install bundle is downloaded to your browser's default download location.
7. Copy the install bundle ZIP file to a host machine on your network.
8. Unzip the file and confirm that you have the following files:
   - `README` - Readme file with installation instructions
   - `connector.conf` - Connection Manager configuration file
   - `downloads/orapki.zip` - ZIP file containing an `orapki` script and required JAR files
   - `downloads/cman.zip` - ZIP file containing Connection Manager binaries
   - `downloads/cmanora.template` - Connection Manager configuration template
   - `util/datasafe_privileges.sql` - Oracle Data Safe privileges SQL script. You can also download this script from the Oracle Data Safe service in Oracle Cloud Infrastructure.
   - `wallet/ewallet.p12` - P12 wallet
   - `setup.py` - Python setup script to install the on-premises connector

Install an Oracle Data Safe On-Premises Connector

The Connection Manager, as part of your on-premises connector installation, establishes a TLS tunnel to a cloud Connection Manager. You can control outgoing traffic from your host machine to the IP address of the cloud Connection Manager, which listens on port 443. The address of a cloud Connection Manager is `accesspoint.datasafe.REGIONNAME.oci.oraclecloud.com`. For example, for the Ashburn region, the address is `accesspoint.datasafe.us-ashburn-1.oci.oraclecloud.com`. You can obtain the IP address of the cloud Connection Manager by doing a DNS lookup.

The following items are also installed. For more information about these items, see the Database Administrator's Guide.

- Listener control utility (`lsnrctl`)
- Connection testing utility (`tnsping`)

1. Open a command prompt on a host machine where you want to install the on-premises connector.
2. As a user different from the `root` user, enter the following command to install the on-premises connector.

   Do not run the installer as the `root` user.

Provide a port number for the on-premises connector. The `https-proxy` argument is optional. You can skip the `https-proxy` argument if the deploying host has public internet access. The on-premises connector does not support a proxy username and password. The HTTP proxy may not be enough depending on your organization's network configuration and security policies. For example, some networks require a username and password for the HTTP proxy. In such cases contact your network administrator to open outbound connections to hosts in the `accesspoint.oraclecloud.com` domain using port 443 without going through an HTTP proxy.

The `create-osservice` argument is optional as well. By setting this to `Yes` you will designate the on-premises connector as an operating system service. This designation will ensure that the on-premises connector gets automatically restarted whenever the OS of the host machine is rebooted. If this argument is not included or set to no, the on-premises connector will have to be manually restarted whenever the OS of the host machine is rebooted.

The install script automatically starts the on-premises connector.

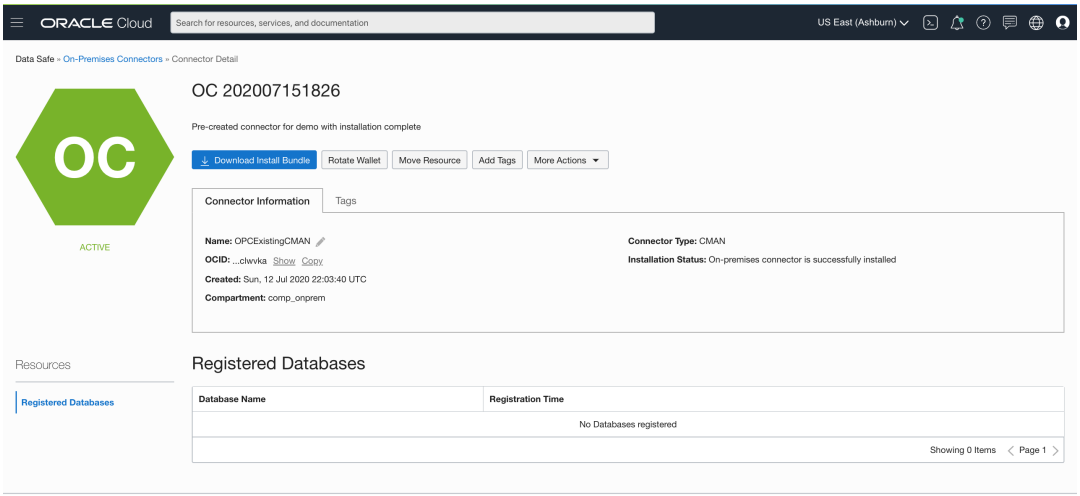
```
$ python setup.py install --connector-port=<port> [--https-
proxy=<proxy:port> --create-osservice=<Yes or No>]
```

Examples:

```
$ python setup.py install --connector-port=1560
$ python setup.py install --connector-port=1560 --https-proxy=https://www-
proxy.exampledomain.com:80 --create-osservice=Yes
```

3. At the prompt, enter the password that you created when you downloaded the install bundle.

   The on-premises connector is installed in the current directory and automatically started. The status for the on-premises connector in the Oracle Data Safe service in Oracle Cloud Infrastructure is now set to `ACTIVE`.



4. (Optional) To diagnose installation issues or execute additional commands (such as uninstall, update, start, stop, and status), please refer to the `README` file that comes with the install bundle.

High Availability of an On-Premises Connector

If you wish to increase the resilience of your on-premises connector and make it highly available, install another instance of the connector using the same install bundle you downloaded for the first installation on a different host or VM. Up to three instances of the same on-premises connector can be started or installed. Each connector will check in with Oracle Data Safe, and if one connector instance fails or is unreachable, Data Safe will automatically try one of the remaining connectors. You may have up to three copies of the connector running simultaneously.

Related Topics

- Install an Oracle Data Safe On-Premises Connector

Check the Status of an On-Premises Connector

To check the status of an on-premises connector, enter the following command:

```
python setup.py status
```

Restart an On-Premises Connector

To restart an on-premises connector, run the following command:

```
python setup.py restart
```

Creating OS User Service for Existing On-Premises Connectors

By designating the on-premises connector as an operating system(OS) service, you can prevent the on-premises connector from requiring a manual restart after an OS reboot of the on-premises connector's host machine.

To designate an existing on-premises connector as an OS service, run the following command on the on-premises connector:

```
setup.py osservice --command=create
```

This command will ensure that the on-premises connector is restarted whenever the OS of the host machine is rebooted.

Update an Oracle Data Safe On-Premises Connector

You can update an Oracle Data Safe On-Premises Connector by downloading a new copy of the install bundle and then running the setup script to perform the update.

The download procedure for creating and updating on-premises connectors is the same and the bundle includes the same set of files. However, in the update procedure you must unzip the bundle files into the same directory where the connector is already installed, overwriting the existing files. Also, to perform an update pass the `update` argument to the `setup.py` script instead of the `install` argument.

> **Note:**
>
> During the update, the on-premises connector is not able to connect to target databases that may be using it. Connection is reestablished when the update is complete.

1. Download the install bundle to your local computer from the **Connector Detail** page in the Oracle Data Safe service.
   See Download the Install Bundle for the Oracle Data Safe On-Premises Connector for the download instructions.
2. Upload the bundle to the host where you want to update the connector.
3. Unzip the bundle into the directory where the on-premises connector is installed. This overwrites the current files.
4. As a user other than `root`, run `setup.py` with the `update` argument.

   ```
   $ python setup.py update
   ```

5. Enter the bundle password when prompted for it.

   ```
   Enter bundle password:
   ```

You should see the following messages:

```
Data Safe on-premises connector update in progress...
Updating wallet...
Data Safe on-premises connector successfully updated
```

This completes the update of the on-premises connector.

If you encounter errors during the update, see Troubleshooting Install or Update Issues.

Uninstall an Oracle Data Safe On-Premises Connector

You can use the `setup.py` script to uninstall an Oracle Data Safe on-premises connector.

1. Log on to the host where the on-premises connector is installed.
2. Navigate to the directory where the on-premises connector is installed. Find the `setup.py` script.
3. As a user other than root, run `setup.py` with the `uninstall` argument.

   ```
   $ python setup.py uninstall
   ```

   At the prompt, confirm that you want to uninstall the connector:

   ```
   This will remove the Data Safe on-premises connector, please confirm (Yes/
   No): yes

   Data Safe on-premises connector successfully uninstalled
   ```

Find the Log Files for an On-Premises Connector

An on-premises connector's setup and manage logs can be found at:

```
<script_directory>/log/
```

An on-premises connector's runtime log can be found at:

```
<script_directory>/oracle_cman_home/log/diag/netcman/<hostName>/cust_cman/
trace/cust_cman.log
```

Troubleshooting Install or Update Issues

- Error message: `Failed to create the tunnels to Data Safe connection manager - for more details check <log file name>`
  After installation or update, the Oracle Data Safe on-premises connector attempts to connect (or re-connect) to the Oracle Data Safe Connection Manager. This message may not indicate an actual error. It can appear if tunnel creation is slow. To confirm that the connector is working, run the `show tunnels` command. If one or more tunnels (connections) exist, then the on-premises connector can communicate with the Connection Manager and you can ignore this message.

  ```
  $ ./oracle_cman_home/bin/cmctl show tunnels -c cust_cman


  CMCTL for Linux: Version 20.0.0.0.0 - Production on 09-OCT-2021
      10:45:34
  Copyright (c) 1996, 2020, Oracle. All rights reserved.
  Current instance cust_cman is already started
  Connecting to (address_list=(address=(protocol=TCPS)(host=localhost)
  (port=1520)))
  Number of connections: 12.
  The command completed successfully.
  ```

- If an error occurs during an `update` (for example if `show tunnels` shows that no tunnels exist), try rerunning the `update` command. Run `uninstall` and then rerun `install` only if `update` fails again. This is because after running `uninstall` you may need to reimport the database certificates if TCPS configuration was part of the original installation.

Troubleshoot Target Registration

If your target database has the status `NEEDS_ATTENTION` or `INACTIVE`, you need to troubleshoot target registration. You can refer here for help to resolve error messages.

Error Message: ORA-17292: No valid logon method found

Make sure `SQLNET.ALLOWED_LOGON_VERSION` is `11G` or above in `sqlnet.ora` and the database parameter `SEC_CASE_SENSITIVE_LOGON` is set to `TRUE` on the target database. See the Database Net Services Reference guide for more information about the `SQLNET.ALLOWED_LOGON_VERSION` and `SEC_CASE_SENSITIVE_LOGON` settings.

Error Message: ORA-12650: No common encryption or data integrity algorithm

To resolve this error, make sure the `ENCRYPTION_TYPES_SERVER` parameter is set to `AES256` and `SQLNET.ENCRYPTION_SERVER` is not set to `rejected` in the database configuration. See Configuration of Data Encryption and Integrity for more information about data encryption and data integrity settings.

Target Database Turns `INACTIVE` If In `NEEDS_ATTENTION` Status for 15 Days

Oracle Data Safe is actively monitoring the connection status of the target databases by initiating connection every hour. If the connection is successful, the target database will remain `ACTIVE` or turn `ACTIVE` if it wasn't before. When the connection is unsuccessful, the target database will be put into a `NEEDS_ATTENTION` status with a message stating why the connection failed.

Even when the target database is in `NEEDS_ATTENTION`, Oracle Data Safe will keep monitoring the connection status and recover the target database to the `ACTIVE` status if the connection succeeds. However, if the target database is stuck in `NEEDS_ATTENTION` status for over 15 days, Oracle Data Safe will consider the target database unreachable with the provided connection details and stop monitoring the target database. This will show as the target database being in the `INACTIVE` status. A message will show saying that the target database is unreachable and has been unreachable since the time the target database turned to `NEEDS_ATTENTION` status.

If you are no longer interested in the target, deregister the target database from Oracle Data Safe. If you want to recover the target from the `NEEDS_ATTENTION` state, check the failure reason and address the problem.

An update of the target database in Oracle Data Safe is required to bring it back to the `ACTIVE` status. Even if the existing details are correct, re-enter the existing details to update and recover the database. Once the target database is updated, Oracle Data Safe will resume monitoring the database. This includes any audit trails that changed to the `NEEDS_ATTENTION` status when the target database connection failed. It may take up to two hours for an audit trail to become `ACTIVE` again.

Please Choose the Right Database Category Error Message

You may encounter this error when registering a target database.

After attempting to register a target database with Oracle Data Safe, if you encounter an error message that says `Please choose the right database category` this indicates that you have selected the incorrect combination of infrastructure type and database type.

To correct this error if you are registering an Amazon RDS for Oracle database, choose the `NON_ORACLE_CLOUD` infrastrusture type and `CLOUD_DATABASE_SERVICE` database type. If you are registering a different target database type, choose the correct combination of infrastrusture type and database type.

4

Events

Oracle Cloud Infrastructure Events enables you to create automation based on the state changes of resources throughout your tenancy, including Oracle Data Safe resources.

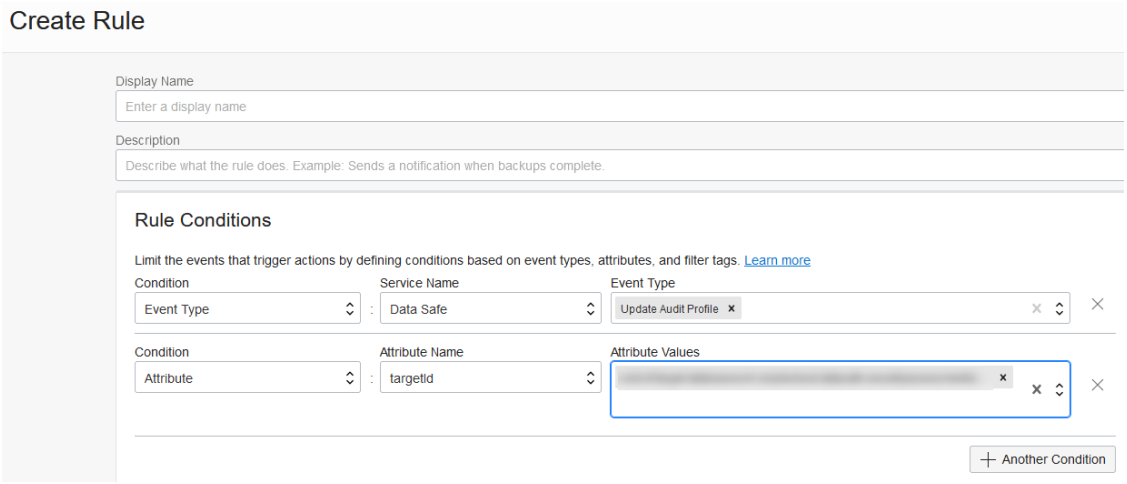
Overview of Oracle Data Safe Events

Administrators can configure the Oracle Data Safe service to emit events in Oracle Cloud Infrastructure, which are structured messages that indicate changes in resources.

Rule Conditions

When you create a rule, you start by configuring a condition. The first condition specifies the event type(s) for which you want to be notified. If you want to set filters on the event types, you can add more conditions that specify attributes and tags.

Let's look at a simple example. Suppose you want to be notified when an audit profile is updated in Oracle Data Safe. To do this, in the event rule, you select the **Update Audit Profile** event type for the first condition. Because you are interested in a particular database, you add a second condition to the rule with a filter on the attribute **targetId**. For its value, you enter the OCID of your target database. Now, if a user updates the audit profile for your target database, you will be notified. The following screenshot shows you the **Create Rule** page in Oracle Cloud Infrastructure with these conditions configured.



Notification Text

Notification text is in JSON format. From the **Create Rule** page in Oracle Cloud Infrastructure, you can preview the text. Simply click the **View example events (JSON)** link and select an

Oracle Data Safe event type. The following is an example for the **Create Audit Archive retrieval - Begin** event type:

```
{
  "eventType": "com.oraclecloud.datasafe.createarchiveretrieval.begin",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2021-11-18T12:06:46.588Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID",
    "compartmentName": "example-compartment",
    "resourceName": "auditArchiveRetrievals",
    "resourceId": "ocid1.coreservicesworkrequest.oc1..unique_ID",
    "availabilityDomain": "ad1",
    "additionalDetails": {
      "targetId": "ocid1.datasafetargetdatabase.oc1..unique_ID",
      "startDate": "2021-02-01T00:00:00.000Z",
      "endDate": "2021-05-01T00:00:00.000Z"
    }
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID"
  }
}
```

Each event type has its own set of additional details, and some do not have any. In the example above, the `additionalDetails` node shows you target database name, start date, and end date.

About Oracle Data Safe Events

To configure events, you create rules that specify which events can trigger actions. Actions include publishing messages to a stream via the Streaming service, broadcasting a notification message to subscribers via the Notifications service, or invoking functions in Oracle Functions. For example, you can trigger a notification message when a user registers a target database with Oracle Data Safe.

> **Note:**
>
> Any Oracle Data Safe event for User Assessment or Security Assessment that you created in the past that uses an old event type name, for example, `com.oraclecloud.datasafe.securityassessmentrefresh.begin`, needs to be dropped and recreated so that it uses the new friendly name, for example, `Security Assessment Refresh Begin`; otherwise, the event will not work.

To learn more about events, see Overview of Events in the Oracle Cloud Infrastructure documentation.

Event Types for Oracle Data Safe

Oracle Data Safe has events types for Security Assessment, User Assessment, Alerts, Activity Auditing, Data Discovery, Data Masking, SQL Firewall, Oracle Data Safe on-premises connectors, Oracle Data Safe private endpoints, and target databases.

Target Database Event Types

The following table describes event types for target databases in Oracle Data Safe.

Friendly Name	Event Type and Description
Create Target Database - Begin	`com.oraclecloud.datasafe.createtargetdatabase.begin` The event type emits when a user creates a target database with Oracle Data Safe.
Create Target Database - End	`com.oraclecloud.datasafe.createtargetdatabase.end` The event type emits when target database creation is completed.
Delete Target Database - Begin	`com.oraclecloud.datasafe.deletetargetdatabase.begin` The event type emits when a user deletes a target database.
Delete Target Database - End	`com.oraclecloud.datasafe.deletetargetdatabase.end` The event type emits when a target database is deleted.
Register Target Database - Begin	`com.oraclecloud.datasafe.registerdatasafetarget.begin` The event type emits when a user registers a target database with Oracle Data Safe.
Register Target Database - End	`com.oraclecloud.datasafe.registerdatasafetarget.end` The event type emits when target database registration is completed.
Deregister Target Database - Begin	`com.oraclecloud.datasafe.deregisterdatasafetarget.begin` The event type emits when a user deregisters a target database with Oracle Data Safe.
Deregister Target Database - End	`com.oraclecloud.datasafe.deregisterdatasafetarget.end` The event type emits when a target deregistration is completed.
Target Database State Change	`com.oraclecloud.datasafe.statechangetargetdatabase` The event type emits when there is a change in a target database's state.
Alert Policy Target Association Patch Begin	`com.oraclecloud.datasafe.patchtargetalertpolicyassociation.begin` The event type emits when a user triggers an alert policy target association patch with Oracle Data Safe.
Alert Policy Target Association Patch End	`com.oraclecloud.datasafe.patchtargetalertpolicyassociation.end` The event type emits when an alert policy target association patch is completed.
Disabled Target Alert Policy Association	`com.oraclecloud.datasafe.disabledtargetalertpolicyassociation` The event type emits when a target alert policy association is generating more alerts than the threshold permits.

Example 4-1 Notification Text for a Create Target Database - End Event Type

```
{
  "eventType": "com.oraclecloud.datasafe.createtargetdatabase.end",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2021-02-23T19:15:20.264Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID",
    "compartmentName": "example-compartment",
    "resourceName": "targetDatabase",
    "resourceId": "ocid1.coreservicesworkrequest.oc1..unique_ID",
    "availabilityDomain": "<availability-domain>"
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID"
  },
  "serviceName": "Data Safe",
  "displayName": "Create Target Database - End",
  "additionalDetails": [
    {"name": "targetId", "type": "string"},
    {"name": "targetType", "type": "string"}
    ],
  "timeCreated": "2021-02-23T19:15:20.264Z",
  "activationTime": "2021-03-15T00:00:00.000Z"
}
```

Oracle Data Safe On-Premises Connector Event Types

The following table describes event types for Oracle Data Safe on-premises connectors.

Friendly Name	Event Type and Description
Create On-Prem Connector - Begin	`com.oraclecloud.datasafe.createonpremconnector.begin` The event type emits when an Oracle Data Safe on-premises connector creation request is triggered by a user.
Create On-Prem Connector - End	`com.oraclecloud.datasafe.createonpremconnector.end` The event type emits when an on-premises connector creation request is completed.
Delete On-Prem Connector - Begin	`com.oraclecloud.datasafe.deleteonpremconnector.begin` The event type emits when an Oracle Data Safe on-premises connector deletion request is triggered by a user.
Delete On-Prem Connector - End	`com.oraclecloud.datasafe.deleteonpremconnector.end` The event type emits when the on-premises connector deletion request is completed.
On-Prem Connector State Change	`com.oraclecloud.datasafe.statechangeonpremconnector` The event type emits when the state of an Oracle Data Safe on-premises connector changes.

Friendly Name	Event Type and Description
Rotate On-Prem Connector - Begin	`com.oraclecloud.datasafe.updateonpremconnectorwallet.begin` The event type emits when a wallet rotation request for an Oracle Data Safe on-premises connector is triggered by a user.
Rotate On-Prem Connector - End	`com.oraclecloud.datasafe.updateonpremconnectorwallet.end` The event type emits when a wallet rotation request for an Oracle Data Safe on-premises connector is completed.

Example 4-2 Notification Text for the Create On-Prem Connector - Begin Event Type

```
{
  "eventType": "com.oraclecloud.datasafe.createonpremconnector.begin",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2020-09-10T22:06:46.588Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID",
    "compartmentName": "example-compartment",
    "resourceName": "onPremConnectors",
    "resourceId": "ocid1.coreservicesworkrequest.oc1..unique_ID",
    "availabilityDomain": "ad1"
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID"
  }
  "serviceName": "Data Safe",
  "displayName": "Create On-Prem Connector - Begin",
  "additionalDetails": [],
  "timeCreated": "2020-09-10T22:06:48.011Z"
}
```

Oracle Data Safe Private Endpoint Event Types

The following table describes event types for Oracle Data Safe private endpoints.

Friendly Name	Event Type and Description
Create Private Endpoint - Begin	`com.oraclecloud.datasafe.createdatasafeprivateendpoint.begin` The event type emits when an Oracle Data Safe private endpoint creation request is triggered by a user.
Create Private Endpoint - End	`com.oraclecloud.datasafe.createdatasafeprivateendpoint.end` The event type emits when an Oracle Data Safe private endpoint creation request is completed.

Friendly Name	Event Type and Description
Delete Private Endpoint - Begin	`com.oraclecloud.datasafe.deletedatasafeprivateendpoint.begin` The event type emits when an Oracle Data Safe private endpoint deletion request is triggered by a user.
Delete Private Endpoint - End	`com.oraclecloud.datasafe.deletedatasafeprivateendpoint.end` The event type emits when an Oracle Data Safe private endpoint deletion request is completed.

Example 4-3 Notification Text for the Create Private Endpoint - End Event Type

```
{
  "eventType": "com.oraclecloud.datasafe.createdatasafeprivateendpoint.end",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2020-09-10T22:07:10.809Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID",
    "compartmentName": "example-compartment",
    "resourceName": "privateEndpoints",
    "resourceId": "ocid1.coreservicesworkrequest.oc1..unique_ID",
    "availabilityDomain": "ad1"
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID"
  },
  "serviceName": "Data Safe",
  "displayName": "Create Private Endpoint - End",
  "additionalDetails": [],
  "timeCreated": "2020-09-10T22:06:48.011Z"
}
```

Security Assessment Event Types

The following table describes event types for Security Assessment in Oracle Data Safe.

Friendly Name	Event Type and Description
Security Assessment Create Begin	`com.oraclecloud.datasafe.createsecurityassessment.begin` The event type is emitted when a user triggers a security assessment.
Security Assessment Create End	`com.oraclecloud.datasafe.createsecurityassessment.end` The event type is emitted when a security assessment is finished.
Security Assessment Refresh Begin	`com.oraclecloud.datasafe.refreshsecurityassessment.begin` The event type is emitted when a user refreshes a security assessment.

Friendly Name	Event Type and Description
Security Assessment Refresh End	`com.oraclecloud.datasafe.refreshsecurityassessment.end` The event type is emitted when a security assessment is finished refreshing.
Security Assessment Baseline Set Begin	`com.oraclecloud.datasafe.setsecurityassessmentbaseline.begin` The event type is emitted when a user sets a security assessment as a baseline.
Security Assessment Baseline Set End	`com.oraclecloud.datasafe.setsecurityassessmentbaseline.end` The event type is emitted when a set baseline operation on a security assessment is finished.
Security Assessment Baseline Unset Begin	`com.oraclecloud.datasafe.unsetsecurityassessmentbaseline.begin` The event type is emitted when a user unsets a security assessment as a baseline.
Security Assessment Baseline Unset End	`com.oraclecloud.datasafe.unsetsecurityassessmentbaseline.end` The event type is emitted when an unset baseline operation on a security assessment is finished.
Security Assessment Compare Begin	`com.oraclecloud.datasafe.comparesecurityassessment.begin` The event type is emitted when a user compares two security assessments.
Security Assessment Compare End	`com.oraclecloud.datasafe.comparesecurityassessment.end` The event type is emitted when a compare operation for two security assessments is finished.
Security Assessment Drift From Baseline	`com.oraclecloud.datasafe.securityassessmentdriftfrombaseline` The event type is emitted when a security assessment is compared with a baseline assessment and a difference is found.
Security Assessment Report Generate Begin	`com.oraclecloud.datasafe.generatesecurityassessmentreport.begin` The event type is emitted when a user requests to generate a security assessment report.
Security Assessment Report Generate End	`com.oraclecloud.datasafe.generatesecurityassessmentreport.end` The event type is emitted when an operation to generate a security assessment report is finished.
Security Assessment Report Download	`com.oraclecloud.datasafe.downloadsecurityassessmentreport` The event type is emitted when a user requests to download a security assessment report.
Security Assessment Finding Risk Update Begin	`com.oraclecloud.datasafe.updatefinding.begin` The event type is emitted when a user begins changing the risk for a finding.
Security Assessment Finding Risk Update End	`com.oraclecloud.datasafe.updatefinding.end` The event type is emitted when changing the risk for a finding is finished.

> **Note:**
>
> Any Oracle Data Safe event for User Assessment or Security Assessment that you created in the past that uses an old event type name, for example, `com.oraclecloud.datasafe.securityassessmentrefresh.begin`, needs to be dropped and recreated so that it uses the new friendly name, for example, `Security Assessment Refresh Begin`; otherwise, the event will not work.

Example 4-4 Notification Text for a Security Assessment Drift From Baseline Event Type

```
{
  "eventType": "com.oraclecloud.datasafe.securityassessmentdriftfrombaseline",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2020-09-10T22:06:46.588Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID",
    "compartmentName": "example-compartment",
    "resourceName": "securityAssessment",
    "resourceId": "ocid1.coreservicesworkrequest.oc1..unique_ID",
    "availabilityDomain": "ad1"
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID"
  },
  "serviceName": "Data Safe",
  "displayName": "Security Assessment Drift From Baseline",
  "additionalDetails": [{"name":"targetNames","value":["target1", "target2"]},
{"name":"comparisonId","value": "<baseline_assessment_ID>"} ],
  "timeCreated": "2020-09-10T22:06:48.011Z"
}
```

User Assessment Event Types

The following table describes event types for User Assessment in Oracle Data Safe.

Friendly Name	Event Type and Description
User Assessment Create Begin	`com.oraclecloud.datasafe.createuserassessment.begin` The event type is emitted when a user triggers a user assessment.
User Assessment Create End	`com.oraclecloud.datasafe.createuserassessment.end` The event type is emitted when a user assessment is finished creating.
User Assessment Refresh Begin	`com.oraclecloud.datasafe.refreshuserassessment.begin` The event type is emitted when a user refreshes a user assessment.

Friendly Name	Event Type and Description
User Assessment Refresh End	com.oraclecloud.datasafe.refreshuserassessment.end The event type is emitted when a user assessment is finished refreshing.
User Assessment Baseline Set Begin	com.oraclecloud.datasafe.setuserassessmentbaseline.begin The event type is emitted when a user sets a user assessment as a baseline assessment.
User Assessment Baseline Set End	com.oraclecloud.datasafe.setuserassessmentbaseline.end The event type is emitted when a set baseline operation on a user assessment is finished.
User Assessment Baseline Unset Begin	com.oraclecloud.datasafe.unsetuserassessmentbaseline.begin The event type is emitted when a user unsets a user assessment as a baseline assessment.
User Assessment Baseline Unset End	com.oraclecloud.datasafe.unsetuserassessmentbaseline.end The event type is emitted when an unset baseline operation on a user assessment is finished.
User Assessment Compare Begin	com.oraclecloud.datasafe.compareuserassessment.begin The event type is emitted when a user compares two user assessments.
User Assessment Compare End	com.oraclecloud.datasafe.compareuserassessment.end The event type is emitted when a compare operation for two user assessments is finished.
User Assessment Drift From Baseline	com.oraclecloud.datasafe.userassessmentdriftfrombaseline The event type is emitted when a user assessment is compared with a baseline and a difference is found.
User Assessment Report Generate Begin	com.oraclecloud.datasafe.generateuserassessmentreport.begin The event type is emitted when a user requests to generate a user assessment report.
User Assessment Report Generate End	com.oraclecloud.datasafe.generateuserassessmentreport.end The event type is emitted when a user assessment report is generated.
User Assessment Report Download	com.oraclecloud.datasafe.downloaduserassessmentreport The event type is emitted when a user requests to download a user assessment report.
Security Policy Report Create Begin	com.oraclecloud.datasafe.createsecuritypolicyreport.begin The event type is emitted when a security policy report is being created.
Security Policy Report Create Complete	com.oraclecloud.datasafe.createsecuritypolicyreport.end The event type is emitted when security policy report creation is completed.
Security Policy Report Delete Begin	com.oraclecloud.datasafe.deletesecuritypolicyreport.begin The event type is emitted when a security policy report is being deleted by the system.

Friendly Name	Event Type and Description
Security Policy Report Delete Complete	`com.oraclecloud.datasafe.deletesecuritypolicyreport.end` The event type is emitted when a security policy report deletion is completed.
Security Policy Report Refresh Begin	`com.oraclecloud.datasafe.refreshsecuritypolicyreport.begin` The event type is emitted when a security policy report is being refreshed.
Security Policy Report Refresh Complete	`com.oraclecloud.datasafe.refreshsecuritypolicyreport.end` The event type is emitted when a security policy report is refreshed.
User Assessment Password Expiry Date	`com.oraclecloud.datasafe.userassessmentpasswordexpirydate` This event is triggered twice: first when the user has fewer than 90 days remaining until password expiration, and again when fewer than 30 days remain.

Note:

Any Oracle Data Safe event for User Assessment or Security Assessment that you created in the past that uses an old event type name, for example, `com.oraclecloud.datasafe.securityassessmentrefresh.begin`, needs to be dropped and recreated so that it uses the new friendly name, for example, `Security Assessment Refresh Begin`; otherwise, the event will not work.

Example 4-5 Notification Text for a User Assessment Drift From Baseline Event Type

```
{
  "eventType": "com.oraclecloud.datasafe.userassessmentdriftfrombaseline",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2020-09-10T22:06:46.588Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID",
    "compartmentName": "example-compartment",
    "resourceName": "userAssessment",
    "resourceId": "ocid1.coreservicesworkrequest.oc1..unique_ID",
    "availabilityDomain": "ad1"
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID"
  },
  "serviceName": "Data Safe",
  "displayName": "User Assessment Drift From Baseline",
  "additionalDetails": [{"name":"targetNames","value":["target1", "target2"]},
{"name":"comparisonId","value": "<baseline_assessment_ID>"} ],
```

```
  "timeCreated": "2020-09-10T22:06:48.011Z"
}
```

Activity Auditing Event Types

The following table describes event types for Activity Auditing in Oracle Data Safe.

Friendly Name	Event Type and Description
Audit Archive Retrieval Create Begin	`com.oraclecloud.datasafe.createarchiveretrieval.begin` An event is emitted when an archive retrieval is started.
Audit Archive Retrieval Create End	`com.oraclecloud.datasafe.createarchiveretrieval.end` An event is emitted when an archive retrieval is finished.
Audit Archive Retrieval Delete Begin	`com.oraclecloud.datasafe.deletearchiveretrieval.begin` An event is emitted when an archive retrieval delete is started.
Audit Archive Retrieval Delete End	`com.oraclecloud.datasafe.deletearchiveretrieval.end` An event is emitted when an archive retrieval delete is finished.
Audit Events Post Retention Purge	`com.oraclecloud.datasafe.purgeretention` An event is emitted when the retention period for audit records is reached and the audit events are being deleted from Data Safe.
Audit Policy Provision Begin	`com.oraclecloud.datasafe.provisionauditpolicy.begin` An event is emitted when an audit policy provisioning is started.
Audit Policy Provision End	`com.oraclecloud.datasafe.provisionauditpolicy.end` An event is emitted when an audit policy provisioning ends.
Audit Profile Retention Update Begin	`com.oraclecloud.datasafe.changeretention.begin` An event is emitted when an audit retention update is started. Example, when online/offline audit data retention settings are being updated.
Audit Profile Retention Update End	`com.oraclecloud.datasafe.changeretention.end` An event is emitted when an audit retention update is completed. Example, when online/offline audit data retention settings are successfully updated.
Audit Policy Retrieve Begin	`com.oraclecloud.datasafe.retrieveauditpolicies.begin` An event is emitted when an audit policy retrieval is started.
Audit Policy Retrieve End	`com.oraclecloud.datasafe.retrieveauditpolicies.end` An event is emitted when an audit policy retrieval is finished.
Audit Profile Update Begin	`com.oraclecloud.datasafe.updateauditprofile.begin` An event is emitted when an audit profile update is started.
Audit Profile Update End	`com.oraclecloud.datasafe.updateauditprofile.end` An event is emitted when an audit profile update is completed.
Audit Trail Collection Free Limit Warning	`com.oraclecloud.datasafe.auditcollectionwarning` An event is emitted when an audit collection reaches 80% of the free limit.
Audit Trail Resume Begin	`com.oraclecloud.datasafe.resumeaudittrail.begin` An event is emitted when an audit trail resume begins.
Audit Trail Resume End	`com.oraclecloud.datasafe.resumeaudittrail.end` An event is emitted when an audit trail resume ends.

Friendly Name	Event Type and Description
Audit Trail Start Begin	com.oraclecloud.datasafe.startauditrail.begin An event is emitted when an audit trail start begins.
Audit Trail Start End	com.oraclecloud.datasafe.startauditrail.end An event is emitted when an audit trail start ends.
Audit Trail Stop Begin	com.oraclecloud.datasafe.stopauditrail.begin An event is emitted when an audit trail stop begins.
Audit Trail Stop End	com.oraclecloud.datasafe.stopauditrail.end An event is emitted when an audit trail is stopped automatically or manually.
Audit Trail Update Begin	com.oraclecloud.datasafe.updateauditrail.begin An event is emitted when audit trail update is started.
Audit Trail Update End	com.oraclecloud.datasafe.updateauditrail.end An event is emitted when audit trail update is finished.
Report Generate Begin	com.oraclecloud.datasafe.generatereport.begin An event is emitted when a report generation is started.
Report Generate End	com.oraclecloud.datasafe.generatereport.end An event is emitted when a report generation is completed.
Report Schedule Begin	com.oraclecloud.datasafe.schedulereport.begin An event is emitted when a new report schedule is being created.
Report Schedule End	com.oraclecloud.datasafe.schedulereport.end An event is emitted when a new report schedule is created successfully.
Report Schedule Delete Begin	com.oraclecloud.datasafe.removeschedulereport.begin An event is emitted when report schedule delete is started.
Report Schedule Delete End	com.oraclecloud.datasafe.removeschedulereport.end An event is emitted when report schedule delete is completed.
Scheduled Report Generated	com.oraclecloud.datasafe.scheduledreportcomplete An event is emitted when a scheduled report is generated successfully.

Example 4-6 Notification text for the event type Audit Policy Provision Begin

```
{
  "eventType": "com.oraclecloud.datasafe.provisionauditpolicy.begin",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2021-11-18T11:06:46.588Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID",
    "compartmentName": "example-compartment",
    "resourceName": "auditPolicies",
    "resourceId": "ocid1.coreservicesworkrequest.oc1..unique_ID",
    "availabilityDomain": "ad1",
    "additionalDetails": {
      "targetId": "ocid1.datasafetargetdatabase.oc1..unique_ID"
    }
```

```
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID"
  }
}
```

Alert Event Types

The following table describes event types for alerts in Oracle Data Safe.

Friendly Name	Event Type and Description
Alert Generated	`com.oraclecloud.datasafe.generateauditalert` An event is emitted when an audit alert is generated.
Alert Generation Throttled	`com.oraclecloud.datasafe.throttlealertgeneration` An event is emitted when alert generation has been temporarily disabled for the alert policy because it generated more alerts than the threshold of 1,000 per ten minutes.
Alert Policy Target Association Patch Begin	`com.oraclecloud.datasafe.patchtargetalertpolicyassociation.begin` An event is emitted when target alert policy associations are created or updated.
Alert Policy Target Association Patch End	`com.oraclecloud.datasafe.patchtargetalertpolicyassociation.end` An event is emitted when target alert policy associations updates have completed.
Alert UpdateAll Begin	`com.oraclecloud.datasafe.alertsupdate.begin` An event is emitted when Alert updateAll is started.
Alert UpdateAll End	`com.oraclecloud.datasafe.alertsupdate.end` An event is emitted when Alert updateAll is completed.
Create Alert Policy Begin	`com.oraclecloud.datasafe.createalertpolicy.begin` An event is emitted when creation of a custom alert policy is started.
Create Alert Policy End	`com.oraclecloud.datasafe.createalertpolicy.end` An event is emitted when creation of a custom alert policy is finished.
Create Alert Policy Rule Begin	`com.oraclecloud.datasafe.createalertpolicyrule.begin` An event is emitted when creation of a custom alert policy rule is started.
Create Alert Policy Rule End	`com.oraclecloud.datasafe.createalertpolicyrule.end` An event is emitted when creation of a custom alert policy rule is finished.
Delete Alert Policy Begin	`com.oraclecloud.datasafe.deletealertpolicy.begin` An event is emitted when deletion of a custom alert policy is started.
Delete Alert Policy End	`com.oraclecloud.datasafe.deletealertpolicy.end` An event is emitted when deletion of a custom alert policy is finished.
Delete Alert Policy Rule Begin	`com.oraclecloud.datasafe.deletealertpolicyrule.begin` An event is emitted when deletion of a custom alert policy rule is started.

Friendly Name	Event Type and Description
Delete Alert Policy Rule End	com.oraclecloud.datasafe.deletealertpolicyrule.end An event is emitted when deletion of a custom alert policy rule is finished.
Update Alert Policy Begin	com.oraclecloud.datasafe.updatealertpolicy.begin An event is emitted when a custom alert policy update is started.
Update Alert Policy End	com.oraclecloud.datasafe.updatealertpolicy.end An event is emitted when a custom alert policy update is finished.
Update Alert Policy Rule Begin	com.oraclecloud.datasafe.updatealertpolicyrule.begin An event is emitted when a custom alert policy rule update is started.
Update Alert Policy Rule End	com.oraclecloud.datasafe.updatealertpolicyrule.end An event is emitted when a custom alert policy rule update is finished.

Example 4-7 Notification Text for an Audit Alert Generated Event Type


```
{
  "eventType": "com.oraclecloud.datasafe.generateauditalert",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2020-09-29T16:03:41.293Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.compartment.oc1..unique_ID",
    "compartmentName": "example_compartment",
    "resourceName": "alerts",
    "resourceId": "ocid1.datasafealert.oc1.phx.unique_ID",
    "availabilityDomain": "availability_domain",
    "additionalDetails": {
      "status": "OPEN",
      "displayName": "Failed logon by Admin user",
      "description": "Failed logon by Admin user was detected",
      "severity": "HIGH",
      "targetId": "ocid1.datasafetarget.oc1.phx.unique_ID",
      "targetName": "target_sa",
      "policyId": "ocid1.datasafealertpolicy.oc1.iad.unique_ID",
      "timeCreated": "2020-09-29T16:03:31.293Z",
      "timeUpdated": "2020-09-29T16:03:42.736Z",
      "osUserName": "dscs",
      "operationTime": "2020-09-29T15:29:51.404Z",
      "operation": "Login on target database",
      "operationStatus": "Success",
      "clientHostname": "jobsvm3002.jobsvm.stestvcn.oraclevcn.com",
      "clientIPs": "10.0.4.15,10.0.4.16,10.0.4.14",
      "clientId": "ORACLE$_DATA_SAFE#",
      "clientProgram": "JDBC Thin Client",
      "userName": "user1",
      "objectType": "UNIFIED_AUDIT_TRAIL",
      "commandText": "SELECT * FROM AUDSYS.UNIFIED_AUDIT_TRAIL WHERE
\"EVENT_TIMESTAMP\"<=:1 AND \"EVENT_TIMESTAMP\">:2 \u0000",
      "commandParam": " #1(31):02-JUL-21 12.42.15.044000000 PM #2(31):02-
```

```
JUL-21 12.34.22.509000000 PM"
    }
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.compartment.oc1..unique_ID"
  }
}
```

Data Discovery Event Types

The following table describes event types for Data Discovery in Oracle Data Safe.

Friendly Name	Event Type and Description
Create Sensitive Type Group Begin	`com.oraclecloud.datasafe.createsensitivetypegroup.begin` The event type emits when a sensitive type group creation request is triggered.
Create Sensitive Type Group End	`com.oraclecloud.datasafe.createsensitivetypegroup.end` The event type emits when a sensitive type group creation request is completed
Delete Sensitive Type Group Begin	`com.oraclecloud.datasafe.deletesensitivetypegroup.begin` The event type emits when a sensitive type group delete request is triggered.
Delete Sensitive Type Group End	`com.oraclecloud.datasafe.deletesensitivetypegroup.end` The event type emits when a sensitive type group delete request is completed.
Patch Grouped Sensitive Types Begin	`com.oraclecloud.datasafe.patchgroupedsensitivetypes.begin` The event type emits when the request for a sensitive type to be added to or to be removed from a sensitive type group is triggered.
Patch Grouped Sensitive Types End	`com.oraclecloud.datasafe.patchgroupedsensitivetypes.end` The event type emits when the request for a sensitive type to be added to or to be removed from a sensitive type group is completed.
Referential Relations Create Begin	`com.oraclecloud.datasafe.CreateReferentialRelation.begin` The event type emits when a referential relation creation request in a sensitive data model is triggered.
Referential Relations Create End	`com.oraclecloud.datasafe.CreateReferentialRelation.end` The event type emits when a referential relation creation request in a sensitive data model is completed.
Referential Relations Delete Begin	`com.oraclecloud.datasafe.DeleteReferentialRelation.begin` The event type emits when a referential relation deletion request in a sensitive data model is triggered.
Referential Relations Delete End	`com.oraclecloud.datasafe.DeleteReferentialRelation.end` The event type emits when a referential relation deletion request in a sensitive data model is completed.
Sensitive Column Create Begin	`com.oraclecloud.datasafe.createsensitivecolumn.begin` The event type emits when a sensitive column creation request is triggered.

Friendly Name	Event Type and Description
Sensitive Column Create End	com.oraclecloud.datasafe.createsensitivecolumn.end The event type emits when a sensitive column creation request is completed.
Sensitive Column Delete Begin	com.oraclecloud.datasafe.deletesensitivecolumn.begin The event type emits when a sensitive column delete request is triggered.
Sensitive Column Delete End	com.oraclecloud.datasafe.deletesensitivecolumn.end The event type emits when a sensitive column delete request is completed.
Sensitive Data Model Create Begin	com.oraclecloud.datasafe.createsensitivedatamodel.begin The event type emits when a sensitive data model creation request is triggered.
Sensitive Data Model Create End	com.oraclecloud.datasafe.createsensitivedatamodel.end The event type emits when a sensitive data model creation request is completed.
Sensitive Data Model Delete Begin	com.oraclecloud.datasafe.deletesensitivedatamodel.begin The event type emits when a sensitive data model deletion request is triggered.
Sensitive Data Model Delete End	com.oraclecloud.datasafe.deletesensitivedatamodel.end The event type emits when a sensitive data model deletion request is triggered.
Sensitive Data Model Update Begin	com.oraclecloud.datasafe.updatesensitivedatamodel.begin The event type emits when a sensitive data model update request is triggered.
Sensitive Data Model Update End	com.oraclecloud.datasafe.updatesensitivedatamodel.end The event type emits when a sensitive data model update request is completed.
Sensitive Discovery Job Create Begin	com.oraclecloud.datasafe.creatediscoveryjob.begin The event type emits when an incremental discovery job creation request is triggered.
Sensitive Discovery Job Create End	com.oraclecloud.datasafe.creatediscoveryjob.end The event type emits when an incremental discovery job creation request is completed.
Sensitive Type Create Begin	com.oraclecloud.datasafe.createsensitivetype.begin The event type emits when a sensitive type request is triggered.
Sensitive Type Create End	com.oraclecloud.datasafe.createsensitivetype.end The event type emits when a sensitive type creation request is completed.
Sensitive Type Delete	com.oraclecloud.datasafe.deletesensitivetype The event type emits when a sensitive type delete request is completed.
Sensitive Types Export Create Begin	com.oraclecloud.datasafe.createsensitivetypesexport.begin The event type is emitted when a sensitive types export resource creation request is triggered.

Friendly Name	Event Type and Description
Sensitive Types Export Create End	com.oraclecloud.datasafe.createsensitivetypesexport.end The event type emits when a sensitive types export resource creation request is completed.
Sensitive Types Export Update Begin	com.oraclecloud.datasafe.updatesensitivetypesexport.begin The event type is emitted when a sensitive types export resource update request is triggered.
Sensitive Types Export Update End	com.oraclecloud.datasafe.updatesensitivetypesexport.end The event type is emitted when a sensitive types export resource update request is completed.
Sensitive Type Update Begin	com.oraclecloud.datasafe.updatesensitivetype.begin The event type emits when a sensitive type update request is triggered.
Sensitive Type Update End	com.oraclecloud.datasafe.updatesensitivetype.end The event type emits when a sensitive type update request is completed.
Update Sensitive Type Group Begin	com.oraclecloud.datasafe.updatesensitivetypegroup.begin The event type emits when a sensitive type group update request is triggered.
Update Sensitive Type Group End	com.oraclecloud.datasafe.updatesensitivetypegroup.end The event type emits when a sensitive type group update request is completed.

Example 4-8 Notification text for the event type Sensitive Type Create Begin

```
{
  "eventType": "com.oraclecloud.datasafe.createsensitivetype.begin",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2021-11-18T11:06:46.588Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID",
    "compartmentName": "example-compartment",
    "resourceName": "sensitiveTypes",
    "resourceId": "ocid1.coreservicesworkrequest.oc1..unique_ID",
    "availabilityDomain": "ad1",
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID"
  }
}
```

Data Masking Event Types

The following table describes event types for Data Masking in Oracle Data Safe.

Friendly Name	Event Type and Description
Masking Column Delete	`com.oraclecloud.datasafe.deletemaskingcolumn` The event type emits when a masking column delete request is completed.
Masking Columns Patch Begin	`com.oraclecloud.datasafe.patchmaskingcolumns.begin` The event type emits when a masking columns patch request is triggered by a user.
Masking Columns Patch End	`com.oraclecloud.datasafe.patchmaskingcolumns.end` The event type emits when a masking columns patch request is completed.
Masking Health Check Begin	`com.oraclecloud.datasafe.generatehealthreport.begin` The event type emits when a masking policy health report creation request is triggered by a user.
Masking Health Check Delete Begin	`com.oraclecloud.datasafe.deletemaskingpolicyhealthreport.begin` The event type emits when a masking policy health report deletion request is triggered by a user.
Masking Health Check Delete End	`com.oraclecloud.datasafe.deletemaskingpolicyhealthreport.end` The event type emits when a masking policy health report deletion request is completed.
Masking Health Check End	`com.oraclecloud.datasafe.generatehealthreport.end` The event type emits when a masking policy health report creation request is completed.
Masking Job Begin	`com.oraclecloud.datasafe.mask.begin` The event type emits when a masking job creation request is triggered by a user.
Masking Job End	`com.oraclecloud.datasafe.mask.end` The event type emits when a masking job creation request is completed.
Masking Library Format Create Begin	`com.oraclecloud.datasafe.createlibrarymaskingformat.begin` The event type emits when a library masking format creation request is triggered by a user.
Masking Library Format Create End	`com.oraclecloud.datasafe.createlibrarymaskingformat.end` The event type emits when a library masking format creation request is completed.
Masking Library Format Delete	`com.oraclecloud.datasafe.deletelibrarymaskingformat` The event type emits when a library masking format delete request is completed.
Masking Library Format Update Begin	`com.oraclecloud.datasafe.updatelibrarymaskingformat.begin` The event type emits when a library masking format update request is triggered by a user.
Masking Library Format Update End	`com.oraclecloud.datasafe.updatelibrarymaskingformat.end` The event type emits when a library masking format update request is completed.

Friendly Name	Event Type and Description
Masking Policy Create Begin	com.oraclecloud.datasafe.createmaskingpolicy.begin The event type emits when a masking policy creation request is triggered by a user.
Masking Policy Create End	com.oraclecloud.datasafe.createmaskingpolicy.end The event type emits when a masking policy creation request is completed.
Masking Policy Delete Begin	com.oraclecloud.datasafe.deletemaskingpolicy.begin The event type emits when a masking policy deletion request is triggered by a user.
Masking Policy Delete End	com.oraclecloud.datasafe.deletemaskingpolicy.end The event type emits when a masking policy deletion request is completed.
Masking Policy Update Begin	com.oraclecloud.datasafe.updatemaskingpolicy.begin The event type emits when a masking policy update request is triggered by a user.
Masking Policy Update End	com.oraclecloud.datasafe.updatemaskingpolicy.end The event type emits when a masking policy update request is completed.
Masking Report Delete Begin	com.oraclecloud.datasafe.deletemaskingreport.begin The event type emits when a masking report delete request is triggered by a user.
Masking Report Delete End	com.oraclecloud.datasafe.deletemaskingreport.end The event type emits when a masking report delete request is completed.

Example 4-9 Notification text for the event type Masking Library Format Create Begin

```
{
  "eventType": "com.oraclecloud.datasafe.createlibrarymaskingformat.begin",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2021-11-18T11:06:46.588Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID",
    "compartmentName": "example-compartment",
    "resourceName": "libraryMaskingFormats",
    "resourceId": "ocid1.coreservicesworkrequest.oc1..unique_ID",
    "availabilityDomain": "ad1",
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID"
  }
}
```

SQL Firewall Event Types

The following table describes event types for SQL Firewall in Oracle Data Safe.

Friendly Name	Event Type and Description
Database Security Config Cleanup	`com.oraclecloud.datasafe.cleanupdatabasesecurityconfig` The event is emitted when a database security configuration is deleted.
Database Security Config Create Begin	`com.oraclecloud.datasafe.createdatabasesecurityconfig.begin` The event is emitted when a database security configuration is started.
Database Security Config Create End	`com.oraclecloud.datasafe.createdatabasesecurityconfig.end` The event is emitted when a database security configuration is finished.
Database Security Config Refresh Begin	`com.oraclecloud.datasafe.refreshdatabasesecurityconfig.begin` The event is emitted when a database security configuration refresh is started.
Database Security Config Refresh End	`com.oraclecloud.datasafe.refreshdatabasesecurityconfig.end` The event is emitted when a database security configuration refresh is finished.
Database Security Config Update Begin	`com.oraclecloud.datasafe.updatedatabasesecurityconfig.begin` The event is emitted when a database security configuration update is started.
Database Security Config Update End	`com.oraclecloud.datasafe.updatedatabasesecurityconfig.end` The event is emitted when a database security configuration update is finished.
Security Policy Auto Create	`com.oraclecloud.datasafe.autocreatesecuritypolicy` The event is emitted when a security policy is created by the system.
Security Policy Cleanup	`com.oraclecloud.datasafe.cleanupsecuritypolicy` The event is emitted when a security policy is deleted by the system.
Security Policy Deployment Auto Create	`com.oraclecloud.datasafe.autocreatesecuritydeploymentpolicy` The event is emitted when a security policy deployment is created by the system.
Security Policy Deployment Cleanup	`com.oraclecloud.datasafe.cleanupsecuritydeploymentpolicy` The event is emitted when a security policy deployment is deleted.
Security Policy Deployment Update Begin	`com.oraclecloud.datasafe.updatesecuritydeploymentpolicy.begin` This event is emitted when a security policy deployment update is started.
Security Policy Deployment Update End	`com.oraclecloud.datasafe.updatesecuritydeploymentpolicy.end` This event is emitted when a security policy deployment update is finished.
Security Policy Update Begin	`com.oraclecloud.datasafe.updatesecuritypolicy.begin` The event is emitted when a security policy update is started.

Friendly Name	Event Type and Description
Security Policy Update End	com.oraclecloud.datasafe.updatesecuritypolicy.end This event is emitted when a security policy update is finished.
SQL Firewall Collection Auto Create	com.oraclecloud.datasafe.autocreatesqlcollection The event is emitted when a SQL Firewall collection is created by the system.
SQL Firewall Collection Cleanup	com.oraclecloud.datasafe.cleanupsqlcollection The event is emitted when a SQL Firewall collection is deleted by the system.
SQL Firewall Collection Create Begin	com.oraclecloud.datasafe.createsqlcollection.begin The event is emitted when creation of a SQL Firewall collection is started.
SQL Firewall Collection Create End	com.oraclecloud.datasafe.createsqlcollection.end The event is emitted when creation of a SQL Firewall collection is finished.
SQL Firewall Collection Delete Begin	com.oraclecloud.datasafe.deletesqlcollection.begin The event is emitted when deletion of a SQL Firewall collection is started.
SQL Firewall Collection Delete End	com.oraclecloud.datasafe.deletesqlcollection.end The event is emitted when deletion of a SQL Firewall collection is finished.
SQL Firewall Collection Insights Refresh Begin	com.oraclecloud.datasafe.refreshsqlcollectionloginsights.begin The event is emitted when a SQL Firewall collection insights refresh is started.
SQL Firewall Collection Insights Refresh End	com.oraclecloud.datasafe.refreshsqlcollectionloginsights.end The event is emitted when a SQL Firewall collection insights refresh is finished.
SQL Firewall Collection Logs Purge Begin	com.oraclecloud.datasafe.purgesqlcollectionlogs.begin The event is emitted when a SQL Firewall collection logs purge is started.
SQL Firewall Collection Logs Purge End	com.oraclecloud.datasafe.purgesqlcollectionlogs.end The event is emitted when a SQL Firewall collection logs purge is finished.
SQL Firewall Collection Start Begin	com.oraclecloud.datasafe.startsqlcollection.begin The event is emitted when a SQL Firewall collection is started.
SQL Firewall Collection Start End	com.oraclecloud.datasafe.startsqlcollection.end The event is emitted when a SQL Firewall collection is finished.
SQL Firewall Collection Stop Begin	com.oraclecloud.datasafe.stopsqlcollection.begin The event is emitted when a SQL Firewall collection stop is started.
SQL Firewall Collection Stop End	com.oraclecloud.datasafe.stopsqlcollection.end The event is emitted when a SQL Firewall collection stop is finished.
SQL Firewall Collection Update Begin	com.oraclecloud.datasafe.updatesqlcollection.begin This event is emitted when a SQL firewall collection update is started.
SQL Firewall Collection Update End	com.oraclecloud.datasafe.updatesqlcollection.end This event is emitted when a SQL Firewall collection update is finished.
SQL Firewall Policy Auto Create	com.oraclecloud.datasafe.autocreatesqlfirewallpolicy The event is emitted when a SQL Firewall policy is created by a system.

Friendly Name	Event Type and Description
SQL Firewall Policy Cleanup	`com.oraclecloud.datasafe.cleanupsqlfirewallpolicy` The event is emitted when a SQL Firewall policy is deleted.
SQL Firewall Policy Delete Begin	`com.oraclecloud.datasafe.deletesqlfirewallpolicy.begin` The event is emitted when deletion for a SQL Firewall policy is started.
SQL Firewall Policy Delete End	`com.oraclecloud.datasafe.deletesqlfirewallpolicy.end` The event is emitted when deletion for a SQL Firewall policy is finished.
SQL Firewall Policy Generate Begin	`com.oraclecloud.datasafe.generatesqlfirewallpolicy.begin` The event is emitted when generation of a SQL Firewall policy is started.
SQL Firewall Policy Generate End	`com.oraclecloud.datasafe.generatesqlfirewallpolicy.end` The event is emitted when generation of a SQL Firewall policy is finished.
SQL Firewall Policy Update Begin	`com.oraclecloud.datasafe.updatesqlfirewallpolicy.begin` This event is emitted when a SQL Firewall policy update is started.
SQL Firewall Policy Update End	`com.oraclecloud.datasafe.updatesqlfirewallpolicy.end` This event is emitted when a SQL Firewall policy update is finished.

Event Notifications in Data Safe

Instead of working in OCI Events and Notifications to create rules and subscribe to topics, Data Safe allows you to create event notifications and subscriptions directly. This allows you to remain in the context of Data Safe while creating and modifying notifications for OCI Events.

Through the **Notifications** tab available in Data Safe's features, you can create OCI Event notifications using predefined templates or an advanced set up. In one simple workflow you create the event, rule, topic, and subscription necessary to receive OCI Event notifications. In addition, you can set up Alarm notifications for Alerts which can be configured to notify you if a specific trigger happens a set number of times in a specified time frame.

The simplified notification workflow allows you to focus on the available events for the feature that you're working within and retain the context of your specific resources. For example, if you'd like to be notified whenever a masking job is completed, you can create that notification directly within Data masking. The notifications workflow is available within all of Data Safe's features and you can find more specific information in the below topics:

- Create and Modify Event Notifications for Targets and Connectivity Options
- Create and Modify Event Notifications in Security Assessment
- Create and Modify Event Notifications in User Assessment
- Create and Modify Event Notifications in Activity Auditing
- Create and Modify Event and Alarm Notifications in Alerts
- Create and Modify Event Notifications in Data Discovery
- Create and Modify Event Notifications in Data Masking
- Create and Modify Event Notifications in SQL Firewall

Related Topics

- OCI Events
- OCI Notifications
- OCI Monitoring

Create and Modify Event Notifications for Targets and Connectivity Options

You can create and modify event notifications in context in the Target databases, Private endpoints, and On-premises connectors sections.

Creating Event Notifications for Target Registration

In Data Safe you can create event notifications for target registration related events. You can use the quickstart template for common events or the advanced event notification workflows to create notifications.

Prerequisites:

Ensure you have the necessary IAM permissions to create event notifications. For more information, see Permissions to Use Contextual Event Notifications in the *Administering Oracle Data Safe* guide.

To create notifications:

1. In Data Safe, click **Target databases**.
2. Click the **Notifications** tab.
3. Click **Create notification**.
   If you don't have any notifications created for the selected resource then you will see a list of available quickstart templates. You may click on one of these instead.

   The **Create notification** side panel will appear.
4. Select to create an event notification from either a **Quickstart** template or an **Advanced event notification**.
   A Quickstart template allows you to select from a list of common event scenarios. When you create a notification from a quickstart template, the Rule and Event is created automatically.

   > **Note:**
   >
   > The Rule and Event are created in the compartment that you were working in when you started the Notification workflow. Rules and Events will only trigger for the compartment and any child-compartments of the compartment that they were created in.

5. If you selected **Quickstart** in the previous step, make a quickstart **Template selection**.
   If you selected **Advanced event notification** in the previous step, type in a **Rule name** and select an **Event type**.

   See Target Database Event Types in the *Administering Oracle Data Safe* guide for more information on events.
6. Select to either **Create new topic** or to **Select existing topic**.
7. Select a **Compartment**.

> **Note:**
>
> This compartment is where the topic will be created, not where the rule and event will be monitored in.

8. If you're creating a new topic, type the topic name or, if you're using an existing topic, select the topic name.
9. Select a **Subscription protocol**.
10. Provide the necessary inputs for the selected subscription protocol.
11. Optionally, click **Show Advanced Options** to tag the notification.
    a. Click **+ Another Tag** to create an additional optional tag to organize and track resources in your tenancy.
    b. Select a **Tag Namespace** from the drop-down list.
    c. Provide a **Tag Key** and **Tag Value**.
12. Click **Create notification**.

Modifying Event Notifications For Target Registration

After creating event notifications in target registration in Oracle Data Safe, you can modify the notifications you created.

To modify the event and rule:

1. In Data Safe, click **Target databases**.
2. Click the **Notifications** tab.
3. Click on an existing event from the **Name** column.

> **Note:**
>
> You will only see the Events that were created directly within Data Safe.

This will bring you to the Rule details page which is part of Oracle Cloud Infrastructure (OCI) Events Service. For more information, see the Events section of the OCI Documentation.

To modify the topic and subscription:

1. In Data Safe, click **Target databases**.
2. Click the **Notifications** tab.
3. Click on an existing topic from the **Topic** column.

> **Note:**
>
> You will only see the Topics that were created directly within Data Safe.

This will bring you to the Topic Details page which is part of Oracle Cloud Infrastructure (OCI) Notifications. For more information, see the Notifications section of the OCI Documentation.

Creating Event Notifications for Private Endpoints

In Data Safe you can create event notifications for Private Endpoint related events. You can use the quickstart template for common events or the advanced event notification workflows to create notifications.

Prerequisites:

Ensure you have the necessary IAM permissions to create event notifications. For more information, see Permissions to Use Contextual Event Notifications in the *Administering Oracle Data Safe* guide.

To create notifications:

1. In Data Safe, click **Target databases**.
2. Under **Connectivity options**, click **Private endpoint**.
3. Click the **Notifications** tab.
4. Click **Create notification**.
   If you don't have any notifications created for the selected resource then you will see a list of available quickstart templates. You may click on one of these instead.

   The **Create notification** side panel will appear.
5. Select to create an event notification from either a **Quickstart** template or an **Advanced event notification**.
   A Quickstart template allows you to select from a list of common event scenarios. When you create a notification from a quickstart template, the Rule and Event is created automatically.

   > **Note:**
   >
   > The Rule and Event are created in the compartment that you were working in when you started the Notification workflow. Rules and Events will only trigger for the compartment and any child-compartments of the compartment that they were created in.
6. If you selected **Quickstart** in the previous step, make a quickstart **Template selection**.
   If you selected **Advanced event notification** in the previous step, type in a **Rule name** and select an **Event type**.

   See Oracle Data Safe Private Endpoint Event Types in the *Administering Oracle Data Safe* guide for more information on events.
7. Select to either **Create new topic** or to **Select existing topic**.
8. Select a **Compartment**.

> **Note:**
>
> This compartment is where the topic will be created, not where the rule and event will be monitored in.

9. If you're creating a new topic, type the topic name or, if you're using an existing topic, select the topic name.
10. Select a **Subscription protocol**.
11. Provide the necessary inputs for the selected subscription protocol.
12. Optionally, click **Show Advanced Options** to tag the notification.
    a. Click **+ Another Tag** to create an additional optional tag to organize and track resources in your tenancy.
    b. Select a **Tag Namespace** from the drop-down list.
    c. Provide a **Tag Key** and **Tag Value**.
13. Click **Create notification**.

Modifying Event Notifications For Private Endpoints

After creating event notifications in the Private Endpoint section in Oracle Data Safe, you can modify the notifications you created.

To modify the event and rule:

1. In Data Safe, click **Target databases**.
2. Under **Connectivity options**, click **Private endpoint**.
3. Click the **Notifications** tab.
4. Click on an existing event from the **Name** column.

> **Note:**
>
> You will only see the Events that were created directly within Data Safe.

This will bring you to the Rule details page which is part of Oracle Cloud Infrastructure (OCI) Events Service. For more information, see the Events section of the OCI Documentation.

To modify the topic and subscription:

1. In Data Safe, click **Target databases**.
2. Under **Connectivity options**, click **Private endpoint**.
3. Click the **Notifications** tab.
4. Click on an existing topic from the **Topic** column.

> **Note:**
>
> You will only see the Topics that were created directly within Data Safe.

This will bring you to the Topic Details page which is part of Oracle Cloud Infrastructure (OCI) Notifications. For more information, see the Notifications section of the OCI Documentation.

Creating Event Notifications for On-Premises Connectors

In Data Safe you can create event notifications for On-Premises Connector related events. You can use the quickstart template for common events or the advanced event notification workflows to create notifications.

Prerequisites:

Ensure you have the necessary IAM permissions to create event notifications. For more information, see Permissions to Use Contextual Event Notifications in the *Administering Oracle Data Safe* guide.

To create notifications:

1. In Data Safe, click **Target databases**.
2. Under **Connectivity options**, click **On-premises connectors**.
3. Click the **Notifications** tab.
4. Click **Create notification**.
   If you don't have any notifications created for the selected resource then you will see a list of available quickstart templates. You may click on one of these instead.

   The **Create notification** side panel will appear.
5. Select to create an event notification from either a **Quickstart** template or an **Advanced event notification**.
   A Quickstart template allows you to select from a list of common event scenarios. When you create a notification from a quickstart template, the Rule and Event is created automatically.

   > **Note:**
   >
   > The Rule and Event are created in the compartment that you were working in when you started the Notification workflow. Rules and Events will only trigger for the compartment and any child-compartments of the compartment that they were created in.
6. If you selected **Quickstart** in the previous step, make a quickstart **Template selection**.
   If you selected **Advanced event notification** in the previous step, type in a **Rule name** and select an **Event type**.

   See Oracle Data Safe On-premises Connector Event Types in the *Administering Oracle Data Safe* guide for more information on events.
7. Select to either **Create new topic** or to **Select existing topic**.
8. Select a **Compartment**.

> **Note:**
>
> This compartment is where the topic will be created, not where the rule and event will be monitored in.

9. If you're creating a new topic, type the topic name or, if you're using an existing topic, select the topic name.
10. Select a **Subscription protocol**.
11. Provide the necessary inputs for the selected subscription protocol.
12. Optionally, click **Show Advanced Options** to tag the notification.
    a. Click **+ Another Tag** to create an additional optional tag to organize and track resources in your tenancy.
    b. Select a **Tag Namespace** from the drop-down list.
    c. Provide a **Tag Key** and **Tag Value**.
13. Click **Create notification**.

Modifying Event Notifications For On-Premises Connectors

After creating event notifications in the On-Premises Connector section of Oracle Data Safe, you can modify the notifications you created.

To modify the event and rule:

1. In Data Safe, click **Target databases**.
2. Under **Connectivity options**, click **On-premises connectors**.
3. Click the **Notifications** tab.
4. Click on an existing event from the **Name** column.

> **Note:**
>
> You will only see the Events that were created directly within Data Safe.

This will bring you to the Rule details page which is part of Oracle Cloud Infrastructure (OCI) Events Service. For more information, see the Events section of the OCI Documentation.

To modify the topic and subscription:

1. In Data Safe, click **Target databases**.
2. Under **Connectivity options**, click **On-premises connectors**.
3. Click the **Notifications** tab.
4. Click on an existing topic from the **Topic** column.

> **Note:**
>
> You will only see the Topics that were created directly within Data Safe.

This will bring you to the Topic Details page which is part of Oracle Cloud Infrastructure (OCI) Notifications. For more information, see the Notifications section of the OCI Documentation.

5

Reference

This section contains reference materials.

Target Database Information Stored in Oracle Data Safe

As an Oracle Data Safe service consumer, you control what data is retrieved and stored by Oracle Data Safe.

Typical types of data are:

- **Audit data and metadata about database users, including username, privileges and role assignments** - If configured to do so, Oracle Data Safe collects audit data and user metadata from the target databases for analysis, alerting, and reporting.
- **Metadata about audit policies** - If configured to do so, Oracle Data Safe collects information about unified audit policies within the database, including the policy name, policy condition, and policy state (enabled/disabled).
- **Metadata about the database's security configuration, including users and their privileges** - If configured to do so, Oracle Data Safe collects configuration information from the database to identify areas where the configuration does not match common practices or may introduce additional risk, or where security features are not enabled.
- **Metadata about database users, including username, privileges and role assignments, and account status** - If configured to do so, Oracle Data Safe collects information about users to assess user risk.
- **Metadata about data stored within the database** - If configured to do so, Oracle Data Safe scans the target database for sensitive data and retrieves the schema, table, and column names, as well as the number of rows of data involved. The database schema names, table names, and column names are collected within Oracle Data Safe and associated with the appropriate sensitive data type.
- **Metadata about database structures** - If configured to do so, Oracle Data Safe masks sensitive data within the database. As part of that operation, Oracle Data Safe collects information about table structures, including primary and foreign key relationships, column names and data types, and the names and types of indexes.
- **Data** - During the data discovery process, users can select "Collect, display, and store sample data." Enabling this option will retrieve and store one (1) sample value for each discovered item of sensitive data to assist Oracle Data Safe users in validating the discovery results. This option is turned off by default. Oracle Data Safe automatically deletes the collected sample data when the user deletes the sensitive data model.
- **Metadata about the database** - To provide supported features, Oracle Data Safe collects metadata about the database, including database edition and version.
- **Database connection details, including database credentials** - When a database is registered in Oracle Data Safe, Oracle Data Safe collects database connection details and the Oracle Data Safe database account credentials, as provided through user inputs, to be able to access the database and provide the Oracle Data Safe features.

Oracle Data Safe is a multi-tenant service running in a service tenancy owned by Oracle. Service data associated with the instance is stored in a back-end Oracle Autonomous

Database Serverless database that's dedicated to the customer and region and is isolated from other customers' instances. For more information, refer to the Privacy and Security Feature Guidance for Oracle Autonomous Database Serverless available on My Oracle Support (Doc ID 114.2).

Service Limits

Oracle Data Safe has usage and service activation limits.

Usage Limits

Usage limits are as follows:

- The combined number of security assessment, user assessment, data discovery, data masking, and audit report work requests that you can run is limited to 1000 per month per target database. If you exceed this limit, you cannot run any additional work requests for the remainder of the month. You can, however, still access Security Center and view existing reports.
- You can create up to 100 Oracle Data Safe private endpoints per tenancy and region, provided the number of unused private endpoints is below 5.*
- You can create up to five Oracle Data Safe on-premises connectors per tenancy and region.*
- Up to 1 million audit records per month per target database are included in Oracle Data Safe at no additional cost. If you exceed this limit, you may be charged for audit records over the limit. It depends on your settings in Security Center. See View and Manage Audit Profiles.
- Audit records generated by the Oracle Data Safe service user are not counted towards the monthly quota.
- Audit records are retained for up to twelve months online in Oracle Data Safe. Audit records can be archived for an additional six years (a total of seven years) in Oracle Data Safe. You can configure audit data retention periods in Oracle Data Safe.
- You can retrieve up to twelve months of audit data from the archive if archiving is configured for your target database.
- You can retrieve audit data from the archive up to six times per month per target database.

* You can create a service request to increase the limit.

Free Trial

During a free trial, the following additional limits apply:

- You can register up to one paid on-premises Oracle Database or one paid Oracle Database on a compute instance.
- You can create up to two Oracle Data Safe private endpoints.
- You can create one Oracle Data Safe on-premises connector.

For more information about using Oracle Data Safe during a free trial, see Try Oracle Data Safe for Free.