Oracle® Cloud

Using Oracle Database Autonomous Recovery Service

F47893-13
February 2024

Oracle Cloud Using Oracle Database Autonomous Recovery Service,

F47893-13

Primary Author: Ramya P

Contributing Authors: Glenn Maxey, Prakash Jashnani, Nirmal Kumar, Jean-Francois Verrier

Contributors: Angelo Rajadurai, Kelly Smith, Alex Goldblatt, Andrew Babb, Shariful Haque, Fuad Arshad, Harini Gavisiddappa, Deepika Muthukumar, Shravan Kumar Kodam, Dileep Thiagarajan, Sam Corso

Contents

Preface

This guide describes how to use Autonomous Recovery Service to protect Oracle Cloud databases.

Audience

This guide is intended for database administrators responsible for the following tasks:

- Managing backup and restore for Oracle Cloud databases
- Maintaining backups

To use this document, you must be familiar with:

- Oracle Cloud Infrastructure concepts as described in Getting Started with Oracle Cloud Infrastructure
- Oracle Database concepts, basic database administration including backup and recovery concepts.

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.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry

standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

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.

1

Overview of Oracle Database Autonomous Recovery Service

Oracle Database Autonomous Recovery Service is a fully managed, standalone, and centralized cloud backup solution for Oracle Cloud Infrastructure (OCI) databases. Learn about the key concepts and benefits of using Oracle Database Autonomous Recovery Service.

- About Oracle Database Autonomous Recovery Service
  Oracle Database Autonomous Recovery Service is an Oracle Cloud service that protects Oracle databases.
- Recovery Service Terminology
  Before using Recovery Service, familiarize yourself with the following key terms and concepts, including some terms related to Oracle Cloud Infrastructure Networking.
- Recovery Service Components
  Access Recovery Service components using the Oracle Cloud Infrastructure Console.
- Supported Oracle Database Releases
  Review the list of Oracle Database releases supported by Recovery Service.

About Oracle Database Autonomous Recovery Service

Oracle Database Autonomous Recovery Service is an Oracle Cloud service that protects Oracle databases.

With backup automation and enhanced data protection capabilities for OCI databases, you can offload all backup processing and storage requirements to Oracle Database Autonomous Recovery Service, thereby eliminating backup infrastructure costs and manual administration overhead.

The OCI Console provides a unified interface to configure your backup strategy. The options available in the Console centralize backup administration and monitoring for Oracle Cloud databases in your tenancy.

> **Note:**
>
> - The terms *Oracle Database Autonomous Recovery Service* and *Recovery Service* are used interchangeably throughout this documentation. Both the terms refer to the same service.
> - The term *protected database* refers to an Oracle Cloud database that uses Recovery Service for backup operations.

Recovery Service is designed to leverage the combined capabilities of the Oracle Zero Data Loss Recovery Appliance and Oracle Recovery Manager (RMAN).

RMAN enables a protected database to send backups to Recovery Service, and maintains the recovery window.

The recovery window is the period of time (in days) for which Recovery Service ensures backup retention for a protected database. The retention period (in days) is defined in a Recovery Service protection policy. You can recover a protected database to any time during the recovery window period. The interval always ends with the current time and extends backwards in time for the number of days defined in a protection policy.

Recovery Service processes backups, provides automated recovery validation, end-to-end encryption, and policy-driven backup retention. The continuous transfer of redo logs from a protected database to Recovery Service is called **Real-time data protection**. Recovery Service offers real-time data protection so that you can minimize the possibility of data loss and enhance database protection.

Protection policies and Recovery Service subnets simplify backup administration tasks. Each protected database must be associated with a Recovery Service subnet and a protection policy.

Protection policies enforce backup retention rules and enable efficient storage utilization. A protection policy can be a Oracle-defined policy or a custom policy defined by you as per your internal storage requirements. You can associate multiple protected databases to a single protection policy.

Recovery Service subnets provide network isolation for backup traffic between databases and Recovery Service in each virtual cloud network.

To summarize, you can leverage Recovery Service to:

- Significantly reduce dependencies on backup infrastructure
- Develop a centralized backup management strategy for all the supported OCI database services
- Retain backups with Recovery Service for a maximum period of 95 days
- Leverage real-time data protection capabilities to eliminate data loss
- Significantly reduce backup processing overhead for your production databases
- Implement a dedicated network for Recovery Service operations in each virtual cloud network (VCN)
- Automate backup validation to ensure recoverability
- Implement a policy-driven backup life-cycle management

You can select Autonomous Recovery Service as the backup destination for OCI managed automatic backups which is the preferred method for backing up Oracle Cloud databases.

Recovery Service Terminology

Before using Recovery Service, familiarize yourself with the following key terms and concepts, including some terms related to Oracle Cloud Infrastructure Networking.

Level 0 Incremental Backup
A level 0 incremental backup performs the same function as a full backup in that they both back up all blocks that have ever been used. The difference is that a full backup

does not affect blocks backed up by subsequent incremental backups, whereas an incremental backup affects blocks backed up by subsequent incremental backups.

Level 1 Backup or Incremental Backup
Incremental backups at level 1 back up only blocks that have changed since previous incremental backups. Blocks that have not changed are not sent again, because they are represented already in the level 0 or previous level 1 backups.

Protected Database
An Oracle Cloud database that sends backups to Recovery Service.

Protection Policy
A mechanism used by Recovery Service to control backup retention for protected databases. A protection policy defines the length of time, expressed as a window of time extending backward from the present, that backups are retained. Recovery Service retains database backups for a minimum period of 14 days and maximum period of 95 days. Each protected database must be assigned with one protection policy. A protection policy can be a Oracle-defined policy or a custom policy defined by you as per your internal storage requirements. You can associate multiple protected databases to a single protection policy.

Recovery point objective (RPO)
The data-loss tolerance of a business process or an organization. The RPO is often measured in terms of time, for example, five hours or two days worth of data loss.

Real-time Data Protection
The continuous transfer of redo changes from a protected database to Recovery Service. Real-time data protection helps to achieve a recovery point objective (RPO) near the last sub-second.

Recovery Service Catalog
A metadata database containing information about backups. Metadata views are stored in Oracle Cloud and managed by Recovery Service.

Recovery Service subnet
A Recovery Service subnet identifies a private subnet that is dedicated to backup operations within a virtual cloud network (VCN) in your tenancy. The OCI Console provides an easy-to-use interface to register Recovery Service subnets.

Recovery window
The maximum length of time, counting backward from the current time, that a database can be recovered.

Retention Period
The length of time, expressed as a window of time extending backward from the present, that backups are retained by Recovery Service. Recovery Service can retain database backups for a minimum period of 14 days and a maximum period of 95 days.

RMAN
Recovery Manager (RMAN) is the primary utility for backup and recovery of Oracle databases. RMAN enables a protected database to send backups to Recovery Service.

Subnet
A subnet is a networking component and a subdivision in a VCN. You must designate a private subnet for Recovery Service to access OCI databases in a VCN.

Virtual Cloud Network (VCN)
A virtual, private network that you set up in Oracle data centers.

Virtual Level 0
A complete database image as of one distinct point in time, maintained efficiently through the indexing of incremental backups from a protected database. The virtual full backups contain individual blocks from multiple incremental backups.

Recovery Service Components

Access Recovery Service components using the Oracle Cloud Infrastructure Console.

Table 1-1 Components of Recovery Service

Component	Description	More Information
Recovery Service subnets	Provides the interface to register a private subnet required to allow Recovery Service to access databases in a VCN.	Managing Recovery Service Subnets
Protection policies	Provides the interface to set up backup retention period.	Managing Protection Policies
Protected databases	The component that represents an Oracle Cloud Database in Recovery Service. A protected database resource is created when you enable the Oracle-managed automatic backups option for a database, and set Autonomous Recovery Service as the backup destination.	Managing Protected Databases

Supported Oracle Database Releases

Review the list of Oracle Database releases supported by Recovery Service.

You can use Oracle Database Autonomous Recovery Service as the backup destination for Oracle Cloud databases provisioned with the following Oracle Database releases.

Oracle Database Edition and Version	More Information
Oracle Database 19c Release 16 (19.16) or later	To use the Real-time data protection feature, your database must be provisioned with: Oracle Database 19c Release 18 (19.18) or later
Oracle Database 21c Release 7 (21.7) or later	To use the Real-time data protection feature, your database must be provisioned with: Oracle Database 21c Release 8 (21.8) or later

Related Topics

- Real-time Data Protection
  Recovery Service offers the real-time data protection feature that enables protected databases to minimize the possibility of data loss.

2

Configuring your Tenancy for Recovery Service

Review OCI and networking requirements to prepare to use Recovery Service in your tenancy.

- Groups and Users for Recovery Service
  Create Oracle Cloud Infrastructure (OCI) user accounts, and a group to which the user accounts belong. You can then assign policies to the group and enable all operations on Recovery Service and related resources.
- Policies to Enable Access to Recovery Service and Related Resources
  Create policy statements such that the supported OCI database services can use Recovery Service for data protection.
- Configuring Network Resources for Recovery Service
  Review the network requirements and configurations required to backup your Oracle Cloud databases to Recovery Service.
- Review Protection Policies for Database Backup Retention
  Recovery Service provides predefined protection policies to suit common use cases for backup retention. You can optionally create custom protection policies to suit your internal data retention requirements.
- Ways to Manage Recovery Service Resources
  In Oracle Cloud Infrastructure (OCI), you can create and manage Recovery Service resources using a variety of interfaces provided to fit your different management use cases.

Groups and Users for Recovery Service

Create Oracle Cloud Infrastructure (OCI) user accounts, and a group to which the user accounts belong. You can then assign policies to the group and enable all operations on Recovery Service and related resources.

Table 2-1 Creating Groups and Users for Recovery Service

Task	More Information
Create a group	To create a group
Create users	To create a user
Add users to a group	To add a user to a group

Policies to Enable Access to Recovery Service and Related Resources

Create policy statements such that the supported OCI database services can use Recovery Service for data protection.

In the Console, use the Policy Builder to quickly create the policies required to use Recovery Service in your tenancy. In the Policy Builder, select **Autonomous Recovery Service** as the **Policy Use Case**, and then select these predefined policy templates:

- Ability to do all things with Autonomous Recovery Service
- Let users manage protection policies in Autonomous Recovery Service
- Let users manage Autonomous Recovery Service subnets

Ability to do all things with Autonomous Recovery Service

The **Ability to do all things with Autonomous Recovery Service** policy template includes all the policy statements required to provide permissions for the supported database services to use Recovery Service, and for Recovery Service to use the network resources to access databases in a VCN.

You can either select the policy template or add these policy statements using the manual editor in the Policy Builder.

Table 2-2 Policy Statements Required for Using Recovery Service

Policy Statement	Create In	Purpose
`Allow service database to manage recovery-service-family in tenancy`	Root compartment	Enables the OCI Database Service to access protected databases, protection policies, and Recovery Service subnets within your tenancy.
`Allow service database to manage tagnamespace in tenancy`	Root compartment	Enables the OCI Database Service to access the tag namespace in a tenancy.
`Allow service rcs to manage recovery-service-family in tenancy`	Root compartment	Enables Recovery Service to access and manage protected databases, Recovery Service subnets, and protection policies within your tenancy.
`Allow service rcs to manage virtual-network-family in tenancy`	Root compartment	Enables Recovery Service to access and manage the private subnet in each database VCN within your tenancy. The private subnet defines the network path for backups between a database and Recovery Service.

Table 2-2 (Cont.) Policy Statements Required for Using Recovery Service

Policy Statement	Create In	Purpose
`Allow group admin to manage recovery-service-family in tenancy`	Root compartment	Enables users in a specified group to access all Recovery Service resources. Users belonging to the specified group can manage protected databases, protection policies, and Recovery Service subnets.

Let users manage protection policies in Autonomous Recovery Service

The **Let users manage protection policies in Autonomous Recovery Service** policy template grants permissions for users in a specified group to create, update, and delete protection policy resources in Recovery Service.

You can either select the policy template or add this policy statement using the manual editor in the Policy Builder.

Table 2-3 Policy Statement for Managing Protection Policies

Policy Statement	Create In	Purpose
`Allow group {group name} to manage recovery-service-policy in compartment {location}`	Compartment that owns the protection policies.	Enables all users in a specified group to create, update, and delete protection policies in Recovery Service.

Consider this example.

```
RecoveryServiceUserABC

Allow group RecoveryServiceUser to manage recovery-service-policy in
compartment ABC
```

Let users manage Autonomous Recovery Service subnets

The **Let users manage Autonomous Recovery Service subnets** policy template grants permissions for users in a specified group to create, update, and delete Recovery Service subnet resources.

You can either select the policy template or add this policy statement in the Policy Builder.

Table 2-4 Policy Statement for Managing Recovery Service subnets

Policy Statement	Create In	Purpose
`Allow Group {group name} to manage recovery-service-subnet in compartment {location}`	Compartment that owns the Recovery Service subnets.	Enables all users in a specified group to create, update, and delete Recovery Service subnets.

Consider this example.

```
RecoveryServiceAdminABC

Allow group RecoveryServiceAdmin to manage recovery-service-subnet in
compartment ABC
```

Related Topics

- Recovery Service Resource Types and Policies
  Learn how to develop policies required to control Recovery Service resources.
- How Policies Work
- Writing Policy Statements with the Policy Builder
- To create a policy
- Recovery Service Family Resource Types
  Each Recovery Service resource-type verb grants different levels of access.

Configuring Network Resources for Recovery Service

Review the network requirements and configurations required to backup your Oracle Cloud databases to Recovery Service.

- About Using a Private Subnet for Recovery Service
  Recovery Service uses a private subnet inside a virtual cloud network (VCN) where your database resides. The private subnet defines the network path for backups between your database and Recovery Service.
- Networking Service Permissions to Configure a Private Subnet
  Review the policies that provide permissions to create and manage the networking components required to enable Recovery Service.
- Subnet Size Requirements and Security Rules for Recovery Service Subnet
  In the database VCN, include a security list with ingress rules defined to allow backup traffic between a database and Recovery Service. You must associate the security list with the private subnet used by Recovery Service.
- Creating a Recovery Service Subnet in the Database VCN
  In the OCI Console, configure a private subnet for Recovery Service in your database VCN. You must then register the Recovery Service subnet.

About Using a Private Subnet for Recovery Service

Recovery Service uses a private subnet inside a virtual cloud network (VCN) where your database resides. The private subnet defines the network path for backups between your database and Recovery Service.

Oracle recommends that your database VCN must have a single private subnet dedicated for backups to Recovery Service. Your Oracle Cloud database can reside in the same private subnet used by Recovery Service, or in a different subnet within the same VCN.

Use a private subnet with a minimum size of /24 (256 IP addresses). You can either create a subnet, or use a preexisting subnet in your database VCN.

> **Note:**
>
> Select an IPv4-only subnet for Recovery Service in your database VCN. Do not select an IPv6-enabled subnet as Oracle does not support using an IPv6-enabled subnet for Recovery Service operations. See Creating a Subnet to learn more.

Associate security lists with the private subnet. The security list must include stateful ingress rules to allow destination ports 8005 and 2484.

You must register the private subnet as a Recovery Service subnet to control backup traffic between your database and Recovery Service.

> **Note:**
>
> Oracle recommends using a private subnet for your backups, but it is possible to use a public subnet.

Networking Service Permissions to Configure a Private Subnet

Review the policies that provide permissions to create and manage the networking components required to enable Recovery Service.

Table 2-5 Networking Service Permissions Required to Create Subnets, Security Lists, Service Gateway, and Route Tables

Operation	Required IAM Policies
Configure a private subnet in a database VCN	• `use vcns` for the compartment which the VCN is in • `use subnets` for the compartment which the VCN is in • `manage private-ips` for the compartment which the VCN is in • `manage vnics` for the compartment which the VCN is in • manage vnics for the compartment which the database is provisioned or is to be provisioned in

Alternatively, you can create a policy that allows a specified group with broader access to networking components.

For example, use this policy to allow a `NetworkAdmin` group to manage all networks in any compartment in a tenancy.

Example 2-1 Policy for Network Administrators

```
Allow group NetworkAdmin to manage virtual-network-family in tenancy
```

Subnet Size Requirements and Security Rules for Recovery Service Subnet

In the database VCN, include a security list with ingress rules defined to allow backup traffic between a database and Recovery Service. You must associate the security list with the private subnet used by Recovery Service.

> **Note:**
>
> Select an IPv4-only subnet for Recovery Service in your database VCN. Do not select an IPv6-enabled subnet as Oracle does not support using an IPv6-enabled subnet for Recovery Service operations. See Creating a Subnet to learn more.

Table 2-6 Subnet size requirements and ingress rules for private subnet used by Recovery Service

Item	Requirements
Minimum subnet size	/24 (256 IP addresses)
General ingress rule 1: Allow HTTPS traffic from Anywhere	This rule allows backup traffic from your Oracle Cloud Infrastructure Database to Recovery Service. • **Stateless**: No (all rules must be stateful) • **Source Type**: CIDR • **Source CIDR**: CIDR of the VCN where the database resides • **IP Protocol**: TCP • **Source Port Range**: All • **Destination Port Range**: 8005
General ingress rule 2: Allows SQLNet Traffic from Anywhere	This rule allows recovery catalog connections and real-time data protection from your Oracle Cloud Infrastructure Database to Recovery Service. • **Stateless**: No (all rules must be stateful) • **Source Type**: CIDR • **Source CIDR**: CIDR of the VCN where the database resides • **IP Protocol**: TCP • **Source Port Range**: All • **Destination Port Range**: 2484

> **Note:**
>
> If your database VCN restricts network traffic between subnets, then ensure to add an egress rule for ports 2484 and 8005 from the database subnet to the Recovery Service subnet that you create.

Creating a Recovery Service Subnet in the Database VCN

In the OCI Console, configure a private subnet for Recovery Service in your database VCN. You must then register the Recovery Service subnet.

1. In the navigation menu, select **Networking**, and then select **Virtual Cloud Networks** to display the Virtual Cloud Networks page.
2. Select the VCN in which your database resides.
3. Under **Resources**, select **Security Lists**.
4. Select the security list that is used for the VCN, and add two ingress rules to allow destination ports 8005 and 2484.
5. Click **Add Ingress Rule**, and add these details to set up a rule that allows HTTPS traffic from anywhere:
   a. **Source Type**: `CIDR`
   b. **Source CIDR**: Specify the CIDR of the VCN where the database resides.
   c. **IP Protocol**: `TCP`.
   d. **Source Port Range**: `All`
   e. **Destination Port Range**: `8005`.
   f. **Description**: Specify an optional description of the ingress rule to help manage the security rules.

   See: Subnet Size Requirements and Security Rules for Recovery Service Subnet.
6. Click **Add Ingress Rule**, and add these details to set up a rule that allows SQLNet traffic from anywhere:
   a. **Source Type**: `CIDR`
   b. **Source CIDR**: Specify the CIDR of the VCN where the database resides.
   c. **IP Protocol**: `TCP`.
   d. **Source Port Range**: `All`
   e. **Destination Port Range**: `2484`.
   f. **Description**: Specify an optional description of the ingress rule to help manage the security rules.

   See: Subnet Size Requirements and Security Rules for Recovery Service Subnet.
7. In the Virtual Cloud Networks Details page, click **Create Subnet**. Create a private subnet with a minimum subnet size of /24 (256 IP addresses). See, Overview of VCN and Subnets.

   Alternatively, select a suitable private subnet that already exists in the VCN.

> **Note:**
>
> Select an IPv4-only subnet for Recovery Service in your database VCN. Do not select an IPv6-enabled subnet as Oracle does not support using an IPv6-enabled subnet for Recovery Service operations. See Creating a Subnet to learn more.

8. Associate the security list with the private subnet. The security list must include ingress rules to allow destination ports 8005 and 2484.

   See: Security Lists.

9. Register the private subnet in Recovery Service. See: Register Recovery Service Subnets.

   Oracle recommends that you register a single Recovery Service subnet per VCN.

> **Note:**
>
> If your database VCN restricts network traffic between subnets, then ensure to add an egress rule for ports 2484 and 8005 from the database subnet to the Recovery Service subnet that you create.

For additional configuration details, refer the relevant database service documentation.

Review Protection Policies for Database Backup Retention

Recovery Service provides predefined protection policies to suit common use cases for backup retention. You can optionally create custom protection policies to suit your internal data retention requirements.

1. In the navigation menu, select **Oracle Database**, and then select **Database Backups** to view the Database Backups page.
2. Click **Protection Policies**.
3. Recovery Service provides four Oracle-defined protection policies based on typical use cases for backup retention. You cannot modify these policies:
   - **Platinum**: 95 days
   - **Gold**: 65 days
   - **Silver**: 35 days
   - **Bronze**: 14 days
4. Optionally, create a custom policy to suit your backup retention requirements. See: Creating a Protection Policy .

Related Topics

- Policy-Based Data Protection Management
  Recovery Service simplifies backup management through protection policies.

Ways to Manage Recovery Service Resources

In Oracle Cloud Infrastructure (OCI), you can create and manage Recovery Service resources using a variety of interfaces provided to fit your different management use cases.

Interface	More Information
OCI Console	Using the Console

Interface	More Information
Application Programming Interfaces (APIs)	Oracle Database Autonomous Recovery Service API
Command-Line Interfaces (CLIs)	Using the CLI

Related Topics

- Using Recovery Service to Backup and Recover Oracle Cloud Databases
  Learn how to configure Recovery Service as the backup destination for Oracle Cloud Infrastructure (OCI) managed automatic backups.
- Using the API to Manage Recovery Service Resources
  Review the list of APIs that you can use for managing Recovery Service resources.

3

Recovery Service Concepts

Recovery Service is designed to leverage the combined capabilities of the Oracle Zero Data Loss Recovery Appliance and Oracle Recovery Manager (RMAN).

- Backup Automation and Storage in Oracle Cloud
  You can store database backups in Oracle Cloud and eliminate dependencies on backup storage infrastructure.
- Network Isolation for Backup Operations
  Recovery Service requires a private subnet for backup and recovery operations in each database virtual cloud network (VCN) within your tenancy.
- Centralized Backup Management
  Centralize your database backup strategy in Oracle Cloud Infrastructure (OCI).
- Policy-Based Data Protection Management
  Recovery Service simplifies backup management through protection policies.
- Real-time Data Protection
  Recovery Service offers the real-time data protection feature that enables protected databases to minimize the possibility of data loss.
- Typical Workflow for Recovery Service Administrators
  Review the workflow as a guide to configure Recovery Service for backing up your Oracle Cloud databases.

Backup Automation and Storage in Oracle Cloud

You can store database backups in Oracle Cloud and eliminate dependencies on backup storage infrastructure.

Recovery Service centralizes backup storage in Oracle Cloud. A protection policy based mechanism controls your backup storage demands. You do not need to perform any manual tasks to address storage utilization or monitoring.

OCI-managed automatic backups is the preferred backup method for Oracle Cloud databases because you can easily configure backup settings using the Console.

When you enable the automatic backups for an Oracle Cloud database, such as an Exadata Cloud Service instance database or Oracle Base Database DB Systems, you can set Autonomous Recovery Service as the backup destination. The database can then transfer backups to Recovery Service for complete and secure data protection.

Your Oracle Cloud databases may have varied demands for backup retention. Recovery Service simplifies this process by enforcing a single protection policy for each database. A protection policy defines the number of days to retain database backups for recoverability.

As a backup administrator for your Oracle Cloud databases, you can use the Oracle Cloud Infrastructure (OCI) Console to create and apply protection policies in your backup strategy. You can attach multiple databases to a single protection policy.

Recovery Service includes a group of Oracle-defined protection policies that cover typical use-cases for backup retention. Optionally, you can create custom policies to suit your internal storage demands.

Custom policies allow the flexibility to retain backups for a period ranging from a minimum period of 14 days to a maximum period of 95 days. You can recover a database from backups up to until the retention period expires.

Network Isolation for Backup Operations

Recovery Service requires a private subnet for backup and recovery operations in each database virtual cloud network (VCN) within your tenancy.

An important part of your backup strategy is network isolation and access control for transferring backups over the network. Recovery Service simplifies this process using Recovery Service subnets.

Oracle recommends that your database VCN includes at least one private subnet dedicated for backups to Recovery Service. You can then register a Recovery Service subnet to enable Recovery Service to access databases in the VCN.

You can implement access control by assigning Oracle Cloud Infrastructure (OCI) policies that permit Recovery Service to access databases only in a chosen VCN.

Centralized Backup Management

Centralize your database backup strategy in Oracle Cloud Infrastructure (OCI).

The OCI Console provides a unified interface to centralize your backup strategy for all Oracle Cloud databases in your tenancy. You can use the **Database Backups** page to configure Recovery Service resources, monitor backups of protected databases, and analyze your backup storage utilization for individual databases.

In the OCI Console, select the **Oracle Databases** menu, and click **Database Backups** to view and configure the following Recovery Service resources:

Protected Databases
The Protected databases page lists each Oracle Cloud database protected by Recovery Service. Oracle Cloud databases must use the OCI-managed automatic backups feature to send backups to Recovery Service. When you enable the automatic backups option for a database, Recovery Service creates a protected database resource associated with the database.

Recovery Service Subnets
A Recovery Service subnet resource defines the network path between Recovery Service and Oracle Cloud databases in a VCN. You can use the Recovery service subnets page to register a private subnet in the VCN where your databases resides.

Protection Policies
The Protection policies page lists both the **Oracle-defined** policies and any **User-defined** policies that you create. Use the Protection policies page to centrally manage policies, and to know the protected databases attached to each policy.

Policy-Based Data Protection Management

Recovery Service simplifies backup management through protection policies.

- Backup Retention
  Recovery Service retains protected database backups for a minimum period of 14 days and a maximum period of 95 days.
- Recovery Window
  Recovery window is the maximum length of time, counting backward from the current time, that a protected database can be recovered.
- Retention Lock
  Retention lock is an optional feature to safeguard your protected database backups from inadvertent changes or malicious damages, such as ransomware attacks.

Backup Retention

Recovery Service retains protected database backups for a minimum period of 14 days and a maximum period of 95 days.

Recovery Service protection policies control the length of time for which protected database backups are retained for recovery purposes. A protection policy defines the backup retention period in days.

For a protected database, Recovery Service ensures that the backups are retained for the period defined in the assigned protection policy, so that database recovery is possible to any point in time within this interval, counting backward from the current time.

For example, the Oracle-defined **Silver** protection policy has a predefined 35-day backup retention period. A protected database that is assigned with the **Silver** policy can recover from backups within the 35-day interval, counting backward from the current time.

Recovery Window

Recovery window is the maximum length of time, counting backward from the current time, that a protected database can be recovered.

You must assign each protected database exactly one protection policy that determines the maximum period that Recovery Service will retain backup data to support recovery. For each protected database in a protection policy, Recovery Service attempts to ensure that the oldest backup is able to support a point-in-time recovery to any time within the specified interval (for example, the past 7 days), counting backward from the current time.

Retention Lock

Retention lock is an optional feature to safeguard your protected database backups from inadvertent changes or malicious damages, such as ransomware attacks.

Retention lock applies to the backup retention period defined in a protection policy. Recovery Service mandates a minimum delay of 14-days for the retention lock to take effect. During the scheduled delay, you can either increase or decrease the backup retention period or disable the retention lock, if necessary.

After the scheduled delay ends, the retention period is permanently locked. You are only allowed to increase the retention period. Recovery Service prevents the modification or deletion of backups until the backup retention period ends. For example, assume that a custom protection policy retains backups for 50 days. When the retention lock is in effect, you are only allowed to increase the backup retention period to a maximum 95 days, and Recovery Service prohibits the deletion of protected database backups during the 50 day retention period.

See, *Using Retention Lock to Protect Backups* for additional information.

Related Topics

- Using Retention Lock to Protect Backups
  Retention lock applies to the backup retention period defined in a protection policy.

Real-time Data Protection

Recovery Service offers the real-time data protection feature that enables protected databases to minimize the possibility of data loss.

You can backup multiple Oracle Cloud databases to Recovery Service. You can also configure each database to use real-time data protection.

When you enable real-time data protection, a protected database can continuously transfer redo logs to Recovery Service and achieve a recovery point objective (RPO) near the last sub-second.

Real-time data protection is an extra cost option.

Related Topics

- Enable Real-time Data Protection for Protected Databases
  Recovery Service offers the ability to use Real-time data protection, a premium capability to help minimize the possibility of data loss and enhance protection for your Oracle Cloud databases.

Typical Workflow for Recovery Service Administrators

Review the workflow as a guide to configure Recovery Service for backing up your Oracle Cloud databases.

- General OCI-Related Tasks
  An administrator at your organization must set up an Oracle Cloud Infrastructure (OCI) account, configure the tenancy, create groups, users, and assign permissions to the groups to manage Recovery Service related tasks.
- OCI Database-Related Tasks
  A database administrator must ensure recommended network configuration to allow Oracle Cloud Infrastructure (OCI) databases in a virtual cloud network (VCN) to connect with Recovery Service.
- Recovery Service Related Tasks to Enable OCI-Managed Automatic Backups
  You must configure Recovery Service subnets and protection policies (optional) to define your automatic backup strategy.

General OCI-Related Tasks

An administrator at your organization must set up an Oracle Cloud Infrastructure (OCI) account, configure the tenancy, create groups, users, and assign permissions to the groups to manage Recovery Service related tasks.

Table 3-1 General OCI-Related Tasks

Task	Description	More Information
Create OCI groups and user accounts	Create groups and add users to the groups.	Groups and Users for Recovery Service
Create policies to assign permissions to use Recovery Service.	The IAM user groups must be assigned the required permissions using policies to use Recovery Service	Policies to Enable Access to Recovery Service and Related Resources Recovery Service Resource Types and Policies

Related Topics

- Getting Started with Oracle Cloud

OCI Database-Related Tasks

A database administrator must ensure recommended network configuration to allow Oracle Cloud Infrastructure (OCI) databases in a virtual cloud network (VCN) to connect with Recovery Service.

Table 3-2 OCI Database-Related Tasks

Tasks	Description	More Information
Provision your OCI databases in a VCN and configure a single private subnet dedicated for backups to Recovery Service	Create a private subnet in the VCN.	VCN and Subnets
Assign service permissions	Recovery Service must be able to access OCI databases provisioned in a specific VCN and compartment.	Policies to Enable Access to Recovery Service and Related Resources
Enable communication between your Oracle Cloud database and Recovery Service	Configure networking service resources to enable connectivity between your database and Recovery Service	Configuring Network Resources for Recovery Service

Recovery Service Related Tasks to Enable OCI-Managed Automatic Backups

You must configure Recovery Service subnets and protection policies (optional) to define your automatic backup strategy.

Table 3-3 Tasks for Enabling OCI Managed Automatic Backups to Recovery Service

Task	Description	More Information
Register Recovery Service subnet	Recovery service subnets provide network isolation for Recovery Service operations in a database VCN.	Managing Recovery Service Subnets
Review Oracle-defined protection policies or create custom protection policies	Oracle-defined protection policies provide common use cases for backup retention. Optionally, create custom policies to suit your internal backup storage demands.	Managing Protection Policies
Enable automatic backups	Select Recovery Service as the backup destination for automatic backups.	Using Recovery Service to Backup and Recover Oracle Cloud Databases

4

Using Recovery Service to Backup and Recover Oracle Cloud Databases

Learn how to configure Recovery Service as the backup destination for Oracle Cloud Infrastructure (OCI) managed automatic backups.

- About Using Recovery Service to Backup and Recover Oracle Cloud Databases
  Learn how to automate backups using Recovery Service.
- Prerequisites for Using Recovery Service as a Automatic Backup Destination
  Ensure that your tenancy is configured to use Recovery Service.
- Backing Up Oracle Cloud Databases to Recovery Service
  Learn how to use the Oracle-managed automatic backups feature to backup an Oracle Cloud database to Recovery Service.
- Recovering a Database Using Recovery Service
  Learn how to recover a database using backups created by Recovery Service.
- Backup Retention for a Terminated Database
  Recovery Service supports data recovery from accidental or malicious damages, and also provides you with options to retain backups after terminating a database.

Related Topics

- Ways to Manage Recovery Service Resources
  In Oracle Cloud Infrastructure (OCI), you can create and manage Recovery Service resources using a variety of interfaces provided to fit your different management use cases.

About Using Recovery Service to Backup and Recover Oracle Cloud Databases

Learn how to automate backups using Recovery Service.

The OCI Console managed automatic backups feature is the preferred method for backing up Oracle Cloud databases because you can easily configure backup settings using the console.

The automatic backups feature supports Recovery Service as the backup destination to provide you with a fully automated cloud backup solution. You do not need to perform any manual backups or backup storage administration tasks.

Use the Console to configure automatic backups and set Autonomous Recovery Service as the backup destination. By default, the Oracle-defined Silver (35-day retention period) protection policy is applied for backup retention. Alternatively, you can assign a different Oracle-defined policy or a custom policy to suit your internal storage demands.

When you enable automatic backups, OCI automatically sends an initial full (RMAN level 0) backup and successive incremental (RMAN level 1) backups to Recovery Service. Backups are retained for the period defined in the assigned protection policy.

After you enable automatic backups, Recovery Service creates an associated protected database resource. The Protected databases page provides you an unified interface to view a list of all the protected databases in your tenancy. You can select a protected database to view the list of backups, monitor database protection and backup status, and analyze storage utilization.

You can use the console to restore a database using a backup created by Recovery Service. You can also create a new database by using a protected database backup.

> **Note:**
>
> For more information, refer your Oracle Cloud Database Service documentation.

Related Topics

- Backing Up a Database

Prerequisites for Using Recovery Service as a Automatic Backup Destination

Ensure that your tenancy is configured to use Recovery Service.

Table 4-1 Review the prerequisite tasks before you use Recovery Service as the automatic backup destination

Task	More Information	Required or Optional
Create IAM policies	Policies to Enable Access to Recovery Service and Related Resources	Required
Configure network resources and register a Recovery Service subnet	Creating a Recovery Service Subnet in the Database VCN	Required
Create protection policies	Review Protection Policies for Database Backup Retention	Optional

Backing Up Oracle Cloud Databases to Recovery Service

Learn how to use the Oracle-managed automatic backups feature to backup an Oracle Cloud database to Recovery Service.

- About Backing Up an Oracle Cloud Database to Recovery Service
  Backing up your Oracle Cloud Database to Recovery Service offers the advantage of enhanced data protection and simplified backup management.
- Enable Automatic Backups to Recovery Service
  Use this procedure to enable the Oracle-managed automatic backups feature and set Recovery Service as the backup destination for an Oracle Clouddatabase in your tenancy.

- Viewing the Protection Details of a Database
  A protected database is an Oracle Cloud database that uses Recovery Service for backups and data protection. Use this procedure to review the details of a protected database resource.
- Viewing the Backups List for a Protected Database
  In the OCI Console, view the protected database backups from the Database Details page.

About Backing Up an Oracle Cloud Database to Recovery Service

Backing up your Oracle Cloud Database to Recovery Service offers the advantage of enhanced data protection and simplified backup management.

You must use the Oracle-managed backups feature, also called automatic backups, to protect a database using Recovery Service. Use the console to configure automatic backups and set Autonomous Recovery Service as the backup destination. You can then access and monitor the protected databases and backups using the console.

When you create a database, such as an Exadata Cloud Infrastructure instance, you can enable automatic backups and set Autonomous Recovery Service as the backup destination. You can also enable automatic backups to Recovery Service after the database is created.

Enable Automatic Backups to Recovery Service

Use this procedure to enable the Oracle-managed automatic backups feature and set Recovery Service as the backup destination for an Oracle Clouddatabase in your tenancy.

Ensure that you have met all the prerequisites as described in Configuring your Tenancy for Recovery Service.

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, select the relevant database service, and navigate to the required database system page.

   Choose a compartment containing the database you want to view, and click the name of the required database.

   For example, follow these steps to navigate to the cloud VM cluster containing the database that you want to backup to Recovery Service.

   a. Open the navigation menu, click **Oracle Database**, then click **Exadata on Oracle Public Cloud**.
   b. Under **Oracle Exadata Database Service on Dedicated Infrastructure**, click **Exadata VM Clusters**.
   c. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

   Follow these steps to access DB systems:

   a. Open the navigation menu, and select **Oracle Base Database (VM, BM)**.
   b. Click **DB Systems**.
   c. In the list of DB systems, find the Exadata DB system you want to access, and then click its name to display details about it.

   The details section indicates whether the database is configured to use automatic backups. If the automatic backups option is enabled, then the Backups section also

indicates the backup destination, the backup retention period, and the health of database backups, among other details.

3. In the Database Details page, click **Configure automatic backups**.
4. In the **Configure automatic backups** dialog, select **Enable automatic backups**.
5. Select these options to configure automatic backups:
   a. **Backup scheduling (UTC)** - Select a two-hour scheduling window to control when backup operations begin. If you do not specify a window, the six-hour default window of 00:00 to 06:00 (in the time zone of the DB system's region) is used for your database.
   b. **Backup destination** - Select **Autonomous Recovery Service** as the backup destination for the database.
   c. **Protection policy** - Defines the retention period for backups created by Recovery Service. The **Protection policy** field defaults to the Oracle-defined **Silver** policy which has a backup retention period of 35 days. You can optionally select a different Oracle-defined protection policy or a custom protection policy that you have created.

      Recovery Service retains database backups for the period defined in the selected protection policy. For example, if you have assigned a **Silver** policy, then backups for the database will be available for a maximum period of 35 days.
6. **Real-time data protection** - Real-time data protection enhances database protection, minimizes data loss, and supports a recovery point up to the last sub-second. This is an extra cost option.

   See: Supported Oracle Database Releases for information about the Oracle Database versions that support using Real-time data protection for your database.
7. **Deletion options after database termination** - Options that you can use to retain protected database backups after the database is terminated. These options can also help restore the database from backups in case of accidental or malicious damages to the database.
   a. **Retain backups according to the protection policy retention period** - Select this option if you want to retain database backups for the entire period defined in the protection policy after the database is terminated.
   b. **Retain backups for 72 hours, then delete** - Select this option to retain backups for a period of 72 hours after you terminate the database.
8. Click **Save changes**.

   After you enable automatic backups, Recovery Service automatically creates an associated protected database resource to represent the database in Recovery Service.

   In the Database Details page, the Backups section indicates **Autonomous Recovery Service** as the **Backup destination**. This page also displays these fields to provide additional details about database protection:

   - **Automatic backup**: Indicates whether the database uses automatic backups.
   - **Health** - Indicates the protection status of the database in Recovery Service. The allowed values are: **Protected**, **Warning**, and **Alert**.
     – A **Protected** status indicates that Recovery Service can ensure database recovery to any point in time within the entire recovery window, and the potential data loss exposure since the last backup is less than 10 seconds

(if real-time data protection is enabled) or less than 70 minutes (if real-time data protection is disabled).

  - A **Warning** status indicates that Recovery Service can ensure database recovery within the current recovery window, and the potential data loss exposure since the last backup is greater than 10 seconds (if real-time data protection is enabled) or greater than 70 minutes, (if real-time data protection is disabled).
  - An **Alert** status indicates that Recovery Service cannot recover the database within the current recovery window, and the latest backup has failed.

- **Data loss exposure**: Time for potential data loss since the last backup was taken.
- **Last failed backup**: The date and time of the most recent failed backup
- **Last completed backup**: The date and time of the most recent successful backup
- **Next scheduled backup**: The date and time of the next scheduled backup
- **Space used for recovery window**: The amount of storage space that is currently used to meet the recovery window goal for the protected database
- **Backup destination**: Indicates that the database sends backups to Recovery Service.
- **Real-time protection**: Indicates whether the real-time redo data is sent from the protected database to Recovery Service. Real-time data protection minimizes the possibility of data loss and enhances data protection. This is an extra-cost option.
- **Protection policy**: The protection policy that defines the maximum period to retain the backups created for the database. Click **Edit Policy** to view the Configure automatic backups pane and change the protection policy.

.

9. In the **Backup destination** field, click the **Autonomous Recovery Service** link to view the protected database details page.

Related Topics

- Managing Protected Databases
  A protected database is an Oracle Cloud database that sends backups to Recovery Service. Learn how to use the Oracle Cloud Infrastructure (OCI) Console to view and monitor the protected databases in your tenancy.
- Enable Real-time Data Protection for Protected Databases
  Recovery Service offers the ability to use Real-time data protection, a premium capability to help minimize the possibility of data loss and enhance protection for your Oracle Cloud databases.

Viewing the Protection Details of a Database

A protected database is an Oracle Cloud database that uses Recovery Service for backups and data protection. Use this procedure to review the details of a protected database resource.

1. Log in to your OCI tenancy.
2. Do one of the following to view the protected database details page:
   - In the navigation menu, click **Oracle Database**, select the relevant database service, and navigate to the required database system page. Choose a compartment

containing the database you want to view, and click the name of the required database.
In the **Backup Destination** field, click the **Autonomous Recovery Service** link.

- In the navigation menu, click **Oracle Database**, and select **Database Backups**. Under **Protected Databases**, find the protected database you want to access, and then click the name to display the details.

Consider the following examples:

Exadata VM Clusters:
Under **Oracle Exadata Database Service on Dedicated Infrastructure**, click **Exadata VM Clusters**. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster. In the Database Details page, under **Backup Destination**, click **Autonomous Recovery Service**.

DB Systems:
Under **Oracle Base Database Service**, click **DB Systems**, find the Exadata DB system you want to access, and then click its name to display details about it. In the Database Details page, under **Backup Destination**, click **Autonomous Recovery Service** .

3. Review the fields displayed in the Protected database information section:

   - **Protection summary**:
     - **Health** - Indicates the protection status of the database in Recovery Service. The allowed values are: **Protected**, **Warning**, and **Alert**.
       * A **Protected** status indicates that Recovery Service can ensure database recovery to any point in time within the entire recovery window, and the potential data loss exposure since the last backup is less than 10 seconds (if real-time data protection is enabled) or less than 70 minutes (if real-time data protection is disabled).
       * A **Warning** status indicates that Recovery Service can ensure database recovery within the current recovery window, and the potential data loss exposure since the last backup is greater than 10 seconds (if real-time data protection is enabled) or greater than 70 minutes, (if real-time data protection is disabled).
       * An **Alert** status indicates that Recovery Service cannot recover the database within the current recovery window, and the latest backup has failed.

       For an **Active** protected database, its details page automatically refreshes the **Health** field at an interval of one minute. This ensures that you are viewing the latest **Health** status.
     - **Real-time protection**: Indicates whether the real-time redo data is sent from the protected database to Recovery Service. Real-time data protection minimizes the possibility of data loss and enhances data protection. This is an extra-cost option.
     - **Data loss exposure**: Indicates the time elapsed since the last valid backup or the period of potential data loss exposure.
       For an **Active** protected database, its details page automatically refreshes the **Data loss exposure** field at an interval of one minute. This ensures that you are viewing the latest data about a potential data loss exposure.

  - **Protection policy**: The protection policy that defines the maximum period to retain the backups created for the database.
  - **Current recovery window**: Indicates how far back in time, starting from the current time, the database can be recovered. If data loss exposure occurs during the said period, then the recovery window decreases by as much. The database can be restored to any point in time, counting backward from the beginning of the data loss exposure period, if any.
- **Space usage**
  - **Space used for recovery window**: The amount of storage space that is currently used to meet the recovery window goal for the protected database.
  - **Protected database size**: The size of the database that is being protected.
- **Database backup summary**
  - **Last failed backup**: The date and time of the most recent failed backup
  - **Last completed backup**: The date and time of the most recent successful backup
  - **Next scheduled backup**: The date and time of the next scheduled backup
- **Protected database**:
  - **Database details**: The Oracle Cloud database that is being protected by Recovery Service. Click the link to view the associated Database Details page.
  - **DB unique name**: The user-specified database name and a system-generated suffix. For example: `dbtst_phx1cs`.
  - **Database version**: The Oracle database release version.
  - **Compartment**: The compartment that contains the protected database.
- **General information**:
  - **OCI Show**: Click **Show** to view the OCID of the protected database
  - **OCI Copy**: Click **Copy** to copy the OCID of the protected database
  - **Compartment**: The compartment that contains the protected database resource
  - **Backup configuration created**: The date and time when the database was configured to backup to Recovery Service
  - **Backup configuration updated**: The date and time when the database backup configuration was last updated

4. Click **Metrics** to view the default metric charts that help you to monitor the protected database. See, Available Metrics: oci_recovery_service.
5. Click **Network Details** to view and manage the Recovery Service subnets associated with the protected database.
6. Click **Work requests** to view the work requests associated with the protected database.
7. Select the **Tags** section to view the tags applied to the protected database resource item.

Viewing the Backups List for a Protected Database

In the OCI Console, view the protected database backups from the Database Details page.

1. Log in to your OCI tenancy.

2. In the navigation menu, click **Oracle Database**, select the relevant database service, and navigate to the required database system page. Choose a compartment containing the database you want to view, and click the name of the required database.

   Consider the following examples:

   Exadata VM Clusters: Under **Oracle Exadata Database Service on Dedicated Infrastructure**, click **Exadata VM Clusters**. In the list of VM clusters, find the VM cluster you want to access and click its highlighted name to view the details page for the cluster.

   DB Systems: Under **Oracle Base Database (VM, BM)**, click **DB Systems**, find the Exadata DB system you want to access, and then click its name to display details about it.

   The database details page is displayed.
3. Under **Resources**, click **Backups**.
4. The Backups list displays detailed information about each backup, and provides options you can use to perform specific actions using backups.

Recovering a Database Using Recovery Service

Learn how to recover a database using backups created by Recovery Service.

- About Recovering a Database from Recovery Service
  Use the OCI Console to restore an Oracle Cloud Database.
- Recovering a Database
  Use this procedure to recover a database using backups created by Recovery Service.

About Recovering a Database from Recovery Service

Use the OCI Console to restore an Oracle Cloud Database.

Use the Console to restore a database from backups created by Recovery Service. You can restore to the last known good state of the database, or you can specify a point in time or an existing System Change Number (SCN). You can also create a new database by using a standalone backup.

Recovering a Database

Use this procedure to recover a database using backups created by Recovery Service.

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, select the relevant database service, and navigate to the required database system page.
3. Choose a compartment containing the database you want to view.
4. Click the name of the required database.

   For example, to restore a bare metal or virtual machine DB system database, click **Oracle Database**, select **Oracle Base Database (VM, BM)**, select a DB system, and then select the database that you want to restore.

5. In the Database Details page, click **Restore**.
6. Select one of the following options:
   - **Restore to the latest** - Restores the database to the last known good state with the least possible data loss.
   - **Restore to a timestamp** - Restores the database to the timestamp specified.
   - **Restore to SCN** - Restores the database using the System Change Number (SCN) specified. This SCN must be valid.
7. Click **Restore database** and confirm the action.

Backup Retention for a Terminated Database

Recovery Service supports data recovery from accidental or malicious damages, and also provides you with options to retain backups after terminating a database.

In the OCI Console, while enabling automatic backups for a database, you can choose any one of the following options to retain protected database backups prior to terminating your database.

- **Retain backups according to the protection policy retention period** - After you terminate a database, Recovery Service will continue to retain backups for period defined in the associated protection policy.
- **Retain backups for 72 hours, then delete** - Recovery Service will retain backups for a period of 72 hours (3-days) after you terminate a database.

In the case of accidental or malicious damages to a database, Recovery Service supports recovery from backups for a period of 72 hours (3-days).

When you terminate a source database or if you disable automatic backups for the database, Recovery Service automatically schedules the deletion of the associated protected database resource and its backups.

After you terminate a source database, the associated protected database resource enters the **Delete Scheduled** state, and remains in this state for a period of 72 hours (default delay) or until the retention period expires, depending on the option that you have selected to retain backups.

If you disable automatic backups for a database, Recovery Service schedules the deletion of the associated protected database resource and its backups after a 72 hour delay. The protected database enters the **Delete Scheduled** state.

Recovery Service automatically deletes the protected database resource and the database backups after the scheduled delay ends.

> **Note:**
>
> If the retention lock is enabled for the protection policy, then when you terminate a database or disable its automatic backups, Recovery Service will delete the protected database resource and its backups only after the retention period ends. See, Using Retention Lock to Protect Backups to learn about using policy retention lock.

Related Topics

- Using Retention Lock to Protect Backups
  Retention lock applies to the backup retention period defined in a protection policy.
- Life Cycle States of Recovery Service Resources
  Learn how Recovery Service resources progress through different life cycle states based on specific events.

5

Managing Protected Databases

A protected database is an Oracle Cloud database that sends backups to Recovery Service. Learn how to use the Oracle Cloud Infrastructure (OCI) Console to view and monitor the protected databases in your tenancy.

- Filter Protected Databases by Compartment
  Use this procedure to find protected databases specific to an individual compartment.
- Filter Protected Databases by State
  Use this procedure to filter protected databases by their life cycle state.
- Filter Protected Databases by Health
  Use this procedure to find a protected database based on the protection status or health status of the database in Recovery Service.
- Viewing Protected Database Details
  Each protected database uniquely identifies an Oracle Cloud database that sends backups to Recovery Service.
- Enable Real-time Data Protection for Protected Databases
  Recovery Service offers the ability to use Real-time data protection, a premium capability to help minimize the possibility of data loss and enhance protection for your Oracle Cloud databases.
- Downloading Protected Database Network Connection Details
  Use this procedure to download the network configuration details for a protected database.
- Access the Network Connection Details for a Protected Database
  Use this procedure to view the details about the Recovery Service subnet associated with a protected database.
- Moving a Protected Database to a Different Compartment
  Use this procedure to relocate a protected database to a different compartment.
- Applying Tags to a Protected Database
  You can apply tags to organize and group protected databases based on their specific purpose.

Filter Protected Databases by Compartment

Use this procedure to find protected databases specific to an individual compartment.

You must have the following permissions to view protected databases in a selected compartment:

```
RECOVERY_SERVICE_PROTECTED_DATABASE_INSPECT
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the **Database Backups** page.

3. The **Protected databases** list populates in the page.
4. Under **List scope**, select a compartment from the list.

Filter Protected Databases by State

Use this procedure to filter protected databases by their life cycle state.

You must have the following permissions to view protected databases in a selected compartment:

```
RECOVERY_SERVICE_PROTECTED_DATABASE_INSPECT
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. The **Protected databases** list populates in the page.
4. Under **List scope**, select a compartment from the list.
5. Under **Filters**, select a state from the list.
   - **Creating**
   - **Active**
   - **Updating**
   - **Failed**
   - **Delete Scheduled**
   - **Deleting**
   - **Deleted**

   See *Life Cycle States of Recovery Service Resources* for detailed information about the transition of a protected database through the different life cycle states.

Related Topics

- Life Cycle States of Recovery Service Resources
  Learn how Recovery Service resources progress through different life cycle states based on specific events.

Filter Protected Databases by Health

Use this procedure to find a protected database based on the protection status or health status of the database in Recovery Service.

You must have the following permissions to view protected databases in a selected compartment:

```
RECOVERY_SERVICE_PROTECTED_DATABASE_INSPECT
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the **Database Backups** page.

3. The **Protected databases** list populates in the page.
4. Under **List scope**, select a compartment from the list.
5. Under **Health**, select a health status.
   - **Any health**
   - **Protected**:
     A **Protected** status indicates that Recovery Service can ensure database recovery to any point in time within the entire recovery window, and the potential data loss exposure since the last backup is less than 10 seconds (if real-time data protection is enabled) or less than 70 minutes (if real-time data protection is disabled).
   - **Warning**:
     A **Warning** status indicates that Recovery Service can ensure database recovery within the current recovery window, and the potential data loss exposure since the last backup is greater than 10 seconds (if real-time data protection is enabled) or greater than 70 minutes, (if real-time data protection is disabled).
   - **Alert**:
     An **Alert** status indicates that Recovery Service cannot recover the database within the current recovery window, and the latest backup has failed.

Viewing Protected Database Details

Each protected database uniquely identifies an Oracle Cloud database that sends backups to Recovery Service.

When you enable automatic backups for an Oracle Cloud database and set Recovery Service as the backup destination, Recovery Service creates an associated protected database resource.

Required IAM Policy

```
RECOVERY_SERVICE_PROTECTED_DATABASE_READ
```

1. Log in to your OCI tenancy.
2. For information about the different ways to access protected databases and review the details, see: Viewing the Protection Details of a Database.

Related Topics

- Viewing the Backups List for a Protected Database
  In the OCI Console, view the protected database backups from the Database Details page.
- Enable Automatic Backups to Recovery Service
  Use this procedure to enable the Oracle-managed automatic backups feature and set Recovery Service as the backup destination for an Oracle Clouddatabase in your tenancy.

Enable Real-time Data Protection for Protected Databases

Recovery Service offers the ability to use Real-time data protection, a premium capability to help minimize the possibility of data loss and enhance protection for your Oracle Cloud databases.

Use this procedure to enable Real-time data protection (extra-cost option) for a protected database.

> **Note:**
>
> Recovery Service supports Real-time data protection for Oracle Cloud databases provisioned with these Oracle Database versions:
>
> - Oracle Database 19c Release 18 (19.18) or later
> - Oracle Database 21c Release 8 (21.8) or later

Required IAM Policy

```
RECOVERY_SERVICE_PROTECTED_DATABASE_UPDATE
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. Use the **List Scope** option to choose a compartment containing the required protected database.
4. In the **Protected databases** list, click the Action menu, and select **View details**.
5. Perform one of these steps in the Protected database details page:
   - The page displays an alert message with instructions to enable real-time data protection. Click **View Source Database** in the alert message.
   - In the **Protected database** section, click the name of the database in the **Database details** field.

   The source database details page is displayed.
6. Click **Configure automatic backups**.
7. Select **Real-time data protection**.
8. Click **Save changes**.

Downloading Protected Database Network Connection Details

Use this procedure to download the network configuration details for a protected database.

Required IAM Policy

```
RECOVERY_SERVICE_PROTECTED_DATABASE_READ
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. Use the **List scope** option to choose a compartment containing the protected database you want to view.
   - In the Protected databases list, click the Action menu, and select **View details**.
   - Alternatively, click the name of the required protected database.

   The Protected database details page is displayed.
4. Click **Download configuration** to save the configuration zip file.

   By default, the file name is `dbrsconfig.zip`. You can rename the zip file with a name of your choice.

Oracle recommends that you protect the downloaded configuration files to prevent unauthorized access to the protected database.

5. Unzip `dbrsconfig.zip` to extract the following files:
   - `dbrsnames.ora` - This file includes connect descriptors or network identification information required for the protected database client to connect with Recovery Service.
   - `certChainPem` - This file stores the trusted certificate (CA Bundle) specific to your region and tenancy.
   - `cabundle.txt`
   - `hosts.txt`

Access the Network Connection Details for a Protected Database

Use this procedure to view the details about the Recovery Service subnet associated with a protected database.

Required IAM Policies

```
RECOVERY_SERVICE_PROTECTED_DATABASE_UPDATE
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.

3. Use the **List scope** option to choose a compartment containing the required protected database.
   - In the Protected databases list, click the Action menu, and select **View details**.
   - Alternatively, click the name of the required protected database.
4. In the Protected database details page, navigate to the **Resources** section, and click **Network details**.
5. Click **Show** and then click **Copy** to copy the network connection string.

Moving a Protected Database to a Different Compartment

Use this procedure to relocate a protected database to a different compartment.

Before you move a protected database to a different compartment, ensure that the associated resources, which includes the database, Recovery Service subnet, and protection policy can access the protected database in the new compartment.

Required IAM Policy

```
RECOVERY_SERVICE_PROTECTED_DATABASE_MOVE
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. Use the **List scope** option to choose a compartment containing the protected database you want to relocate. Perform one of these actions:
   - In the Protected databases list, click the Action menu, and select **Move resource**.
   - Click the name of the required resource. In the Protected database details page, click **Move resource**.
4. Choose a new destination compartment, and click **Move resource**.

Related Topics

- Managing Compartments

Applying Tags to a Protected Database

You can apply tags to organize and group protected databases based on their specific purpose.

You must have the following permissions to apply tags to a protected database:

```
RECOVERY_SERVICE_PROTECTED_DATABASE_UPDATE
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.

3. Use the **List scope** option to choose a compartment containing the protected database to which you want to apply tags.
4. In the Protected databases list, click the Action menu for the required resource, and select **Add tags**.

   Alternatively, click the name of the required protected database. In the Protected database details page, click **Add tags**.

   The **Add tags** dialog box is displayed.
5. In the **Tag namespace** field, consider adding a tag namespace (an identifying text string applied to a set of compartments), or tagging the protection policy with an existing tag namespace.
6. Click **Add tags**.

Related Topics

- Resource Tags

6

Managing Protection Policies

Protection policies provide automated backup retention management. Learn how to set up protection policies using a centralized interface within the Oracle Cloud Infrastructure (OCI) Console.

- About Configuring Protection Policies
  Recovery Service uses protection policies to control database backup retention in Oracle Cloud. Learn how to use the OCI Console to configure and manage protection policies.
- Using Retention Lock to Protect Backups
  Retention lock applies to the backup retention period defined in a protection policy.
- Filter Protection Policies by Compartment
  Use this procedure to find protection policies specific to an individual compartment.
- Filter Protection Policies by State
  Use this procedure to find protection policies by their life cycle state.
- Creating a Protection Policy
  Use this procedure to create a custom protection policy.
- Viewing Protection Policy Details
  Use this procedure to access information about a protection policy.
- Updating a Protection Policy
  Use this procedure to update an existing user-defined protection policy.
- Moving a Protection Policy to a Different Compartment
  Use this procedure to relocate a protection policy to a different compartment.
- Applying Tags to a Protection Policy
  Use this procedure to apply tags to an existing user-defined protection policy.
- Deleting a Protection Policy
  You can delete only user-defined protection policies that you no longer use.

About Configuring Protection Policies

Recovery Service uses protection policies to control database backup retention in Oracle Cloud. Learn how to use the OCI Console to configure and manage protection policies.

Protection Policies provide automatic backup retention for protected databases. Each protected database must be associated with one protection policy.

A protection policy determines the maximum period (in days) allowed to retain backups created by Recovery Service. Based on your business requirements, you can assign separate policies for each protected database or use a single policy across all protected databases in a VCN.

You can use two types of protection policies:

Oracle-defined
There are four Oracle-defined protection policies based on typical use cases for backup retention. You cannot modify these policies.

- **Platinum**: The **Platinum** policy retains backups for 95 days
- **Gold**: The **Gold** policy retains backups for 65 days
- **Silver**: The **Silver** policy retains backups for 35 days
- **Bronze**: The **Bronze** policy retains backups for 14 days

User-defined
These are custom protection policies that you can create based on your business requirements. Custom policies limit backup retention period to a minimum period of 14 days and to a maximum period of 95 days.

The OCI Console is the primary interface to configure protection polices for all databases in your tenancy.

Using Retention Lock to Protect Backups

Retention lock applies to the backup retention period defined in a protection policy.

Locking the backup retention period enables Recovery Service to prevent the modification of backups for the duration defined in the policy. Use the retention lock feature to protect backups from accidental modifications or malicious damages, such as ransomware.

When you enable the retention lock, you must also set a date for the lock to take effect. Recovery Service mandates a minimum delay of 14 days to permanently lock the retention period defined in a policy.

For example, assuming that you enable the retention lock on August 1, you can set the lock date as August 15 or later.

During the specified delay period, you can either increase or decrease the backup retention period or disable the retention lock, if necessary.

When the specified delay ends, the retention period is permanently locked. Recovery Service strictly prohibits the modification or deletion of backups until the retention period expires.

Be aware of these restrictions that apply (to all users including tenancy administrators) if the retention period is permanently locked for a protection policy.

- You cannot disable the retention lock
- You are only allowed to increase the backup retention period for the policy (maximum 95 days)
- You cannot assign a different protection policy to a protected database if the retention period is permanently locked for the existing policy

> **Note:**
>
> If you assign a database to a policy where the retention period is permanently locked, then Recovery Service does not immediately enforce the retention lock for the newly added database. You can leverage the 14 day (minimum) grace period before the retention lock can take permanent effect for the newly added database. For example, assume that the retention period is permanently locked for a policy on August 15. If you assign the same policy to another database on August 16, then the retention lock would take effect only August 30 for the newly added database.

Filter Protection Policies by Compartment

Use this procedure to find protection policies specific to an individual compartment.

Required IAM Policy

```
RECOVERY_SERVICE_POLICY_INSPECT
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. Click **Protection Policies**.
4. Under **List Scope**, select a compartment from the list.

Filter Protection Policies by State

Use this procedure to find protection policies by their life cycle state.

Required IAM Policy

```
RECOVERY_SERVICE_POLICY_INSPECT
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. Click **Protection Policies**.
4. Under **List scope**, select a compartment from the list.
5. Under **Filters**, select a state from the list.
   - **Any State**
   - **Creating**
   - **Active**
   - **Updating**
   - **Failed**
   - **Deleting**

- **Deleted**

  See *Life Cycle States of Recovery Service Resources* for detailed information about each life cycle state.

Related Topics

- Life Cycle States of Recovery Service Resources
  Learn how Recovery Service resources progress through different life cycle states based on specific events.

Creating a Protection Policy

Use this procedure to create a custom protection policy.

Required IAM Policy

```
RECOVERY_SERVICE_POLICY_CREATE
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. Click **Protection Policies**.
4. Click **Create protection policy**.

   The **Create protection policy** panel is displayed.
5. In the **Name** field, specify a name for the policy.
6. In the **Create in compartment** field, select the compartment where you want to create the protection policy.
7. In the **Backup retention period (in days)** field, specify the maximum number of days to retain backups using this policy.

You can specify a minimum period of 14 days and a maximum period of 95 days for retaining backups using this policy.

8. (Optional) Use these steps to lock the backup retention period.
   a. Select **Enable retention lock**.
   b. In the **Scheduled lock time** field, select a date that occurs at least 14 days after the current date.

      Recovery Service mandates a minimum delay of 14 days to permanently lock the retention period. During the delay period, you can either increase or decrease the retention period or disable the lock, if necessary. At the end of the specified time delay, the backup retention period is permanently locked. You are only allowed to increase the retention period.
9. To specify additional features, select **Show advanced options**. In the **Tag namespace** field, consider adding a tag namespace (an identifying text string applied to a set of compartments), or tagging the control with an existing tag namespace.
10. Click **Create**.

The protection policy is created.

Related Topics

- Using Retention Lock to Protect Backups
  Retention lock applies to the backup retention period defined in a protection policy.

Viewing Protection Policy Details

Use this procedure to access information about a protection policy.

Required IAM Policy

```
RECOVERY_SERVICE_POLICY_READ
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. Click **Protection Policies**.
4. In the Protection policies page, use the **List scope** option to find the policy you want to view.
   - In the **Protection policies** list, click the Action menu, and select **View details**.
   - Alternatively, click the name of the required protection policy.

   The Protection policy details page is displayed.
5. The Protection policy information section displays different options that you can use to view the detailed information about a policy.
   - **OCID Show** - Click **Show** to view the protection policy's OCID
   - **OCID Copy** - Click **Copy** to copy the protection policy's OCID
   - **Compartment** - The compartment to which the policy belongs
   - **Created** - When the policy was created
   - **Updated** - When the policy was last updated
   - **Policy type** - Indicates whether the policy is Oracle-defined or a user-defined custom policy.
   - **Backup retention period** - The retention period (in days) defined in the policy.
6. Under **Resources**, click **Protected databases** to view all the protected databases using this policy.

Updating a Protection Policy

Use this procedure to update an existing user-defined protection policy.

You can edit a user-defined protection policy to change the policy name and modify the backup retention period.

Required IAM Policy

```
RECOVERY_SERVICE_POLICY_UPDATE
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. Click **Protection Policies**.
4. Use the **List scope** option to find the protection policy you want to edit.
   - In the **Protection policies** list, click the Action menu, and select **Edit**.
   - Alternatively, click the name of the required protection policy, and click **Edit**.

   The Edit protection policy panel is displayed.
5. In the **Name** field, update the name as necessary.
6. In the **Backup retention period (in days)** field, you can choose to update the retention period. You can specify a value ranging from 14 days to 95 days.

   If you have enabled the retention lock and if the scheduled lock date is earlier than the current date, it indicates that the retention period is permanently locked. In this case, you can only increase the backup retention period for the policy.
7. If the scheduled lock date is greater than the current date, then you can clear the **Enable retention lock** option to disable the lock. See, Using Retention Lock to Protect Backups for more information.
8. Click **Save changes**.

Moving a Protection Policy to a Different Compartment

Use this procedure to relocate a protection policy to a different compartment.

Required IAM Policy

```
RECOVERY_SERVICE_POLICY_MOVE
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. Click **Protection Policies**.
4. Use the **List scope** option to find the protection policy you want to move to a different compartment.
   - In the **Protection Policies** list, click the Action menu, and select **Move resource**.
   - Alternatively, click the name of the required protection policy. In the Protection policy details page, click **Move resource**.

   The Move resource dialog box is displayed.
5. Choose a compartment and click **Move resource**.

Applying Tags to a Protection Policy

Use this procedure to apply tags to an existing user-defined protection policy.

Required IAM Policy

```
RECOVERY_SERVICE_POLICY_UPDATE
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. Click **Protection Policies**.
4. Use the **List scope** option to find the protection policy to which you want to apply tags.
   - In the **Protection policies** list, click the Action menu, and select **Add tags**.
   - Alternatively, click the name of the required protection policy. In the Protection policy details page, click **Add tags**.

   The Add tags dialog box is displayed.
5. In the **Tag namespace** field, consider adding a tag namespace (an identifying text string applied to a set of compartments), or tagging the protection policy with an existing tag namespace.
6. Click **Add tags**.

Deleting a Protection Policy

You can delete only user-defined protection policies that you no longer use.

Required IAM Policy

```
RECOVERY_SERVICE_POLICY_DELETE
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. Click **Protection Policies**.
4. Use the **List scope** option to find the protection policy you want to delete.
   - In the **Protection policies** list, click the Action menu, and select **Delete**.
   - Alternatively, click the name of the required protection policy. In the Protection policy details page, click **Delete**.

   The Delete protection policy dialog box is displayed.
5. Click **Remove** to confirm your action.

7

Managing Recovery Service Subnets

Recovery Service subnets define the network path for backup operations between a database and Recovery Service in each database VCN. Learn how to use the Oracle Cloud Infrastructure (OCI) Console to register and manage Recovery Service subnets in your tenancy.

- About Configuring Recovery Service Subnets
  Recovery service subnets enable network isolation for Recovery Service operations in a VCN.
- Filter Recovery Service Subnets by Compartment
  Use this procedure to find Recovery Service subnets specific to an individual compartment.
- Filter Recovery Service Subnets by State
  Use this procedure to find Recovery Service subnets based on their life cycle state.
- Register Recovery Service Subnets
  After you have created a private subnet for Recovery Service in your database VCN, use this procedure to register the subnet in Recovery Service.
- Viewing Recovery Service Subnet Details
  Use this procedure to access detailed information about a Recovery Service subnet.
- Renaming a Recovery Service Subnet
  Use this procedure to modify the name of an existing Recovery Service subnet.
- Moving a Recovery Service Subnet to a Different Compartment
  Use this procedure to relocate a Recovery Service subnet to a different compartment.
- Applying Tags to a Recovery Service Subnet
  You can apply tags to organize and group Recovery Service subnets based on their purpose.
- Deleting a Recovery Service Subnet
  Use this procedure to delete a Recovery Service subnet that you no longer use.

About Configuring Recovery Service Subnets

Recovery service subnets enable network isolation for Recovery Service operations in a VCN.

Recovery Service connects with your Oracle Cloud databases provisioned in a virtual cloud network (VCN) within your tenancy. Recovery Service subnets establish network presence for Recovery Service in each VCN.

Your database VCN must include a single private subnet dedicated for backups to Recovery Service.

In the Oracle Cloud Infrastructure (OCI) Console, the **Recovery Service Subnets** page provides the interface to quickly register a recovery service subnet by selecting an existing subnet in your database VCN.

You can register only a single Recovery Service subnet per VCN in your tenancy.

Related Topics

- Register Recovery Service Subnets
  After you have created a private subnet for Recovery Service in your database VCN, use this procedure to register the subnet in Recovery Service.
- About Using a Private Subnet for Recovery Service
  Recovery Service uses a private subnet inside a virtual cloud network (VCN) where your database resides. The private subnet defines the network path for backups between your database and Recovery Service.
- Creating a Recovery Service Subnet in the Database VCN
  In the OCI Console, configure a private subnet for Recovery Service in your database VCN. You must then register the Recovery Service subnet.

Filter Recovery Service Subnets by Compartment

Use this procedure to find Recovery Service subnets specific to an individual compartment.

Required IAM Policy

```
RECOVERY_SERVICE_SUBNET_INSPECT
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. Click **Recovery Service Subnets**.
4. Under **List Scope**, select a compartment from the list.

Filter Recovery Service Subnets by State

Use this procedure to find Recovery Service subnets based on their life cycle state.

Required IAM Policy

```
RECOVERY_SERVICE_SUBNET_INSPECT
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. Click **Recovery Service Subnets**.
4. Under **List Scope**, select a compartment from the list.
5. Under **Filters** field, select a state from the list.
   - **Any state**
   - **Creating**
   - **Active**

- **Updating**
- **Failed**
- **Deleting**
- **Deleted**

See *Life Cycle States of Recovery Service Resources* for detailed information about each life cycle state.

Related Topics

- Life Cycle States of Recovery Service Resources
  Learn how Recovery Service resources progress through different life cycle states based on specific events.

Register Recovery Service Subnets

After you have created a private subnet for Recovery Service in your database VCN, use this procedure to register the subnet in Recovery Service.

Multiple protected databases can use the same Recovery Service subnet. In order to ensure that the required number of IP addresses are available to support the Recovery Service private endpoints, you can assign multiple subnets to a Recovery Service subnet that is used by more than one protected database.

> **Note:**
>
> Select an IPv4-only subnet for Recovery Service in your database VCN. Do not select an IPv6-enabled subnet as Oracle does not support using an IPv6-enabled subnet for Recovery Service operations. See Creating a Subnet to learn more.

Ensure that you have completed all the networking service configuration tasks as described in Configuring Network Resources for Recovery Service.
Required IAM Policy

```
RECOVERY_SERVICE_SUBNET_CREATE
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. Click **Recovery Service Subnets**.
4. In the **Compartment** field, select a compartment where you want to create the Recovery Service subnet.
5. Click **Register Recovery Service subnet**, and specify the details.
6. In the **Name** field, enter a name for the Recovery Service subnet.
7. In the **Compartment** field, select the compartment where you want to create the Recovery Service subnet.
8. In the **Virtual cloud network** field, select the database VCN.

   Click **Change Compartment** to select a VCN belonging to a different compartment.

9. In the **Subnet** field, select a private subnet that you have configured for Recovery Service operations in your database VCN.

   Click **Change Compartment** to select a private subnet from a different compartment.

10. (Optional) Click **+Another Subnet** to assign an additional subnet to the Recovery Service subnet.

    If a single subnet does not contain enough IP addresses to support the Recovery Service private endpoints, then you can assign multiple subnets.

11. (Optional) To specify additional features, select **Show Advanced Options**. In the **Tag Namespace** field, consider adding a tag namespace, or tagging the control with an existing tag namespace.

12. Click **Register**.

You can replace a subnet or add more subnets to support the required number of private endpoints.

13. Use these steps to update a Recovery Service subnet:

    a. In the **Subnets** section of the Recovery Service subnet details page, click **Add subnet** and select the subnets you want to add.

    b. To replace an existing subnet, click the Action menu, and select **Remove subnet**. You can then add another subnet.

> **Note:**
>
> A Recovery Service subnet must be associated with at least one subnet belonging to your database VCN.

Related Topics

- About Configuring Recovery Service Subnets
  Recovery service subnets enable network isolation for Recovery Service operations in a VCN.
- About Configuring Recovery Service Subnets
  Recovery service subnets enable network isolation for Recovery Service operations in a VCN.
- Configuring Network Resources for Recovery Service
  Review the network requirements and configurations required to backup your Oracle Cloud databases to Recovery Service.
- Configuring your Tenancy for Recovery Service
  Review OCI and networking requirements to prepare to use Recovery Service in your tenancy.
- VCN and Subnets

Viewing Recovery Service Subnet Details

Use this procedure to access detailed information about a Recovery Service subnet.

Required IAM Policy

```
RECOVERY_SERVICE_SUBNET_READ
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. Click **Recovery Service Subnets**.
4. Use the **List scope** option to choose a compartment containing the Recovery Service subnet you want to view.
5. In the **Recovery Service subnets** list, click the Action menu, and select **View details**. Alternatively, click the name of the required subnet.
6. The Recovery Service subnet details page displays different options that you can use to access detailed information about the selected resource item.
   - **OCID Show** - Click **Show** to view the Recovery Service subnet's OCID.
   - **OCID Copy** - Click **Copy** to copy the Recovery Service subnet's OCID.
   - **VCN** - The VCN in which the Recovery Service subnet exists. Click the link to view the virtual cloud network (VCN) details page.
   - **Subnet** - The private subnet used for backup operations in the database VCN. Click the link to view the subnet details page.
   - **Created** - The date and time when the resource was created.
   - **Updated** - The date and time when the resource was last updated.
7. In the **Subnets** section, click **Add subnets** and select an additional subnet you want to add. Use the **+Another subnet** option to select new subnets.

Renaming a Recovery Service Subnet

Use this procedure to modify the name of an existing Recovery Service subnet.

Required IAM Policy

```
RECOVERY_SERVICE_SUBNET_UPDATE
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. Click **Recovery Service Subnets**.
4. Use the **List scope** option to choose a compartment containing the Recovery Service subnet you want to rename.

5. In the **Recovery Service subnet** list, click the Action menu, and select **Rename**. Alternatively, click the name of the required resource, and then click **Rename**.

   The Rename Recovery Service subnet dialog box is displayed.
6. Specify a new name for the subnet.
7. Click **Save changes**.

Moving a Recovery Service Subnet to a Different Compartment

Use this procedure to relocate a Recovery Service subnet to a different compartment.

Required IAM Policy

```
RECOVERY_SERVICE_SUBNET_MOVE
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. Click **Recovery Service Subnets**.
4. Use the **List scope** option to choose a compartment containing the Recovery Service subnet you want to move.
5. In the **Recovery Service subnets** list, click the Action menu and select **Move resource**. Alternatively, click the name of the required resource item, and then click **Move resource**.

   The Move resource dialog box is displayed.
6. Choose a new compartment and then click **Move resource**.

Related Topics

- Managing Compartments

Applying Tags to a Recovery Service Subnet

You can apply tags to organize and group Recovery Service subnets based on their purpose.

Required IAM Policy

```
RECOVERY_SERVICE_SUBNET_UPDATE
```

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. Click **Recovery Service Subnets**.
4. Use the **List scope** option to choose a compartment containing the required subnet.

5. In the **Recovery Service subnets** list, click the Action menu, and select **Add tags**. Alternatively, click the name of the required resource item, and then click **Add tags**.

   The Add tags dialog box is displayed.

6. In the **Tag namespace** field, consider adding a tag namespace (an identifying text string applied to a set of compartments), or tagging the Recovery Service subnet with an existing tag namespace.
7. Click **Add tags**.

Related Topics

- Tagging Overview

Deleting a Recovery Service Subnet

Use this procedure to delete a Recovery Service subnet that you no longer use.

Required IAM Policy

```
RECOVERY_SERVICE_SUBNET_DELETE
```

.

1. Log in to your OCI tenancy.
2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. Click **Recovery Service Subnets**.
4. Use the **List scope** option to choose a compartment containing the subnet you want to delete.
5. In the **Recovery Service subnets** list, click the Action menu, and select **Delete**. Alternatively, click the name of the required subnet, and click **Delete**.
6. Click **Remove** to confirm your action.

8

Using the API to Manage Recovery Service Resources

Review the list of APIs that you can use for managing Recovery Service resources.

Recovery Service application programming interface (API) assist to manage protected databases, Recovery Service subnets, and protection policies.

- Using the API to Manage Protected Databases
  Review the list of REST API endpoints to manage protected databases.
- Using the API to Manage Protection Policies
  Review the list of REST API endpoints to create and manage protection policies.
- Using the API to Manage Recovery Service Subnets
  Review the list of REST API endpoints to register and manage Recovery Service subnets.

Related Topics

- Ways to Manage Recovery Service Resources
  In Oracle Cloud Infrastructure (OCI), you can create and manage Recovery Service resources using a variety of interfaces provided to fit your different management use cases.

Using the API to Manage Protected Databases

Review the list of REST API endpoints to manage protected databases.

For information about using the API and signing requests, see *REST APIs* and *Security Credentials*. For information about SDKs, see *Software Development Kits and Command Line Interface*

Use the following REST API endpoints to manage protected databases.

- **Create a protected database:** `CreateProtectedDatabase`
  You can perform a dry run of the `CreateProtectedDatabase` API in order to verify that all the prerequisites are met before actually creating a protected database.

  See, *Performing a Dry Run to Check the Preparedness for Creating a Protected Database*.
- **Delete a protected database:** `DeleteProtectedDatabase`
- **View the details of a protected database:** `GetProtectedDatabase`
- **Retrieve the protected database configuration details:** `FetchProtectedDatabaseConfiguration`
- **Modify a protected database:** `UpdateProtectedDatabase`
- **Change the protected database compartment:** `ChangeProtectedDatabaseCompartment`
- **Cancel the deletion of a protected database:**`CancelProtectedDatabaseDeletion`

- **Schedule the deletion of a protected database:** `ScheduleProtectedDatabaseDeletion`

Performing a Dry Run to Check the Preparedness for Creating a Protected Database

When you run the `CreateProtectedDatabase` API with the `opc-dry-run` option set as `TRUE`, it indicates that the request is a dry run to check for any missing prerequisites before creating a protected database. During a dry-run, the `CreateProtectedDatabase` API returns error messages to warn you about any missing requirements, without actually creating a protected database. If an errors occurs, you can review, correct, and repeat the dry-run until the `CreateProtectedDatabase` request does not return any errors.

These are the common issues that you can identify by performing a dry run of the `CreateProtectedDatabase` API:

- The Recovery Service subnet has insufficient free IP addresses to support the required number of private endpoints.
  Ensure that sufficient unallocated IP addresses remain available in the subnet used for Recovery Service operations in the database VCN.

  See, Register Recovery Service Subnets
- Recovery Service does not have permissions to manage the network resources in a chosen compartment.
  Review and assign the required policies. See, Policies to Enable Access to Recovery Service and Related Resources
- Recovery Service is out of capacity.
  Review the service limits for your tenancy and request for an increase

  See, Autonomous Recovery Service Limits
- Recovery Service resources exceed quota limits
  Review and manage Recovery Service resource consumption within compartments. See, Autonomous Recovery Quotas .
- A protected database, having the same database ID, already exists
  Select a different database to use Recovery Service
- The specified protection policy does not exist, or it is not in an **Active** state
  See, Managing Protection Policies
- The prerequisite of registering a Recovery Service subnet is not met
  Ensure that you register a Recovery Service subnet before enabling automatic backups to Recovery Service

  See, Register Recovery Service Subnets

Example 8-1 Dry Run Request of the `CreateProtectedDatabase` API

This example is a sample dry run request.

```
CreateProtectedDatabaseRequest createProtectedDatabaseRequest =
CreateProtectedDatabaseRequest.builder()
.createProtectedDatabaseDetails(createProtectedDatabaseDetails)
.opcRetryToken("EXAMPLE-opcRetryToken-Value")
.opcDryRun(true)
.opcRequestId("UCCBPPQDHXIF5I7A11SS<unique_ID>").build();
```

This is a sample output of the dry run.

```
Status Code : 409
Service Code: IncorrectState
Error Message:
Authorization failed. Autonomous Recovery Service does not have the required security
policies to
manage virtual-network-family in the chosen compartment.
See, 'Prerequisites for Using Recovery Service as a Automatic Backup Destination' in
the
Recovery Service documentation.

The following compartment quotas were exceeded:
protected-database-backup-storage-gb in policy 'example-policy' by 1.

The prerequisite of registering a Recovery Service subnet is not met.
Ensure that you register a Recovery Service subnet before enabling automatic backups.
See, 'Register Recovery Service Subnet' in the Recovery Service documentation.
```

Ensure that you review and perform all the prerequisite tasks described in Configuring your Tenancy for Recovery Service.

Related Topics

- REST APIs
- Security Credentials
- Software Development Kits and Command Line Interface
- CreateProtectedDatabase
- DeleteProtectedDatabase
- GetProtectedDatabase
- FetchProtectedDatabaseConfiguration
- UpdateProtectedDatabase
- ChangeProtectedDatabaseCompartment

Using the API to Manage Protection Policies

Review the list of REST API endpoints to create and manage protection policies.

For information about using the API and signing requests, see *REST APIs* and *Security Credentials*. For information about SDKs, see *Software Development Kits and Command Line Interface*

Use the following REST API endpoints to manage Protection policies.

- **Create a Protection policy:** `CreateProtectionPolicy`
- **Delete a Protection policy:** `DeleteProtectionPolicy`
- **View the details of a Protection policy:** `GetProtectionPolicy`
- **Modify a Protection policy:** `UpdateProtectionPolicy`
- **Change Protection policy compartment:** `ChangeProtectionPolicyCompartment`

Related Topics

- REST APIs
- Security Credentials

- Software Development Kits and Command Line Interface
- CreateProtectionPolicy
- DeleteProtectionPolicy
- GetProtectionPolicy
- UpdateProtectionPolicy
- ChangeProtectionPolicyCompartment

Using the API to Manage Recovery Service Subnets

Review the list of REST API endpoints to register and manage Recovery Service subnets.

For information about using the API and signing requests, see *REST APIs* and *Security Credentials*. For information about SDKs, see *Software Development Kits and Command Line Interface*.

Use the following REST API endpoints to manage Recovery Service subnets.

- **Create a Recovery service subnet:** `CreateRecoveryServiceSubnet`
- **Delete a Recovery service subnet:** `DeleteRecoveryServiceSubnet`
- **View the details of a Recovery service subnet:** `GetRecoveryServiceSubnet`
- **Modify a Recovery service subnet:** `UpdateRecoveryServiceSubnet`
- **Change Recovery service subnet compartment:** `ChangeRecoveryServiceSubnetCompartment`

Related Topics

- REST APIs
- Security Credentials
- Software Development Kits and Command Line Interface
- CreateRecoveryServiceSubnet
- DeleteRecoveryServiceSubnet
- GetRecoveryServiceSubnet
- UpdateRecoveryServiceSubnet
- ChangeRecoveryServiceSubnetCompartment

9

Recovery Service Resource Types and Policies

Learn how to develop policies required to control Recovery Service resources.

- About Recovery Service Resource Types
  Review the list of resource types you can use to create policies for Recovery Service.
- Supported Variables for Recovery Service
  Use variables when adding conditions to a policy. Recovery Service supports only the general variables.
- Details of Verb+Resource-Type Combinations
  Review the list of permissions and API operations covered by each verb for Recovery Service.
- Permissions Required for Each API Operation
  Review the list of permissions for Recovery Service resources in a logical order, grouped by resource-type.

Related Topics

- Policies to Enable Access to Recovery Service and Related Resources
  Create policy statements such that the supported OCI database services can use Recovery Service for data protection.

About Recovery Service Resource Types

Review the list of resource types you can use to create policies for Recovery Service.

You can use two types of resources, individual and family, to define policies.

An individual resource-type controls access to a specific resource. For example, the `recovery-service-policy` resource-type represents the protection policy resource. Use the following individual resource-types to control Recovery Service resources.

```
recovery-service-protected-database
recovery-service-policy
recovery-service-subnet
recovery-service-work-request
```

A family resource-type includes multiple individual resource-types. If you want to write a policy to grant access to all the Recovery Service resources, then use the family resource-type called `recovery-service-family`.

Related Topics

- How Policies Work

Supported Variables for Recovery Service

Use variables when adding conditions to a policy. Recovery Service supports only the general variables.

Related Topics

- General Variables for All Requests

Details of Verb+Resource-Type Combinations

Review the list of permissions and API operations covered by each verb for Recovery Service.

- Recovery Service Family Resource Types
  Each Recovery Service resource-type verb grants different levels of access.
- recovery-service-family
  Review the list of permissions and API operations for the `recovery-service-family` resource type.
- recovery-service-protected-database
  Review the list of permissions and API operations for the `recovery-service-protected-database` resource-type.
- recovery-service-subnet
  Review the list of permissions and API operations for the `recovery-service-subnet` resource-type.
- recovery-service-policy
  Review the list of permissions and API operations for the `recovery-service-policy` resource type.
- recovery-service-work-request
  Review the list of permissions and API operations for the `recovery-service-work-request` resource type.

Related Topics

- Permissions
- Verbs
- Resource-Types

Recovery Service Family Resource Types

Each Recovery Service resource-type verb grants different levels of access.

The level of access is cumulative as you go from `inspect` to `read`, to `use`, and to `manage`. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

To govern control to a specific resource, you must define at least one policy that follows this syntax:

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

```
RecoveryServiceAdminGroup
Allow RecoveryServiceAdminGroup to manage recovery-service-protected-database in
tenancy
```

recovery-service-family

Review the list of permissions and API operations for the `recovery-service-family` resource type.

Table 9-1 recovery-service-family

Permissions	APIs Fully Covered	APIs Partially Covered
RECOVERY_SERVICE_PROTECTED_DATABASE_INSPECT RECOVERY_SERVICE_POLICY_INSPECT RECOVERY_SERVICE_SUBNET_INSPECT RECOVERY_SERVICE_WORK_REQUEST_INSPECT	ListProtectedDatabases ListProtectionPolicies ListRecoveryServiceSubnets ListWorkRequests	*none*

Table 9-2 recovery-service-family

Permissions	APIs Fully Covered	APIs Partially Covered
INSPECT+ RECOVERY_SERVICE_PROTECTED_DATABASE_READ RECOVERY_SERVICE_POLICY_READ RECOVERY_SERVICE_SUBNET_READ RECOVERY_SERVICE_WORK_REQUEST_READ	GetProtectedDatabase GetProtectionPolicy GetRecoveryServiceSubnet GetWorkRequest	*none*

Table 9-3 recovery-service-family

Permissions	APIs Fully Covered	APIs Partially Covered
READ+ RECOVERY_SERVICE_PROTECTED_DATABASE_UPDATE RECOVERY_SERVICE_POLICY_UPDATE RECOVERY_SERVICE_SUBNET_UPDATE	UpdateProtectedDatabase UpdateProtectionPolicy UpdateRecoveryServiceSubnet	*none*

Table 9-4 recovery-service-family

Permissions	APIs Fully Covered	APIs Partially Covered
USE+ RECOVERY_SERVICE_PROTECTED_DATABASE_CREATE RECOVERY_SERVICE_PROTECTED_DATABASE_DELETE RECOVERY_SERVICE_PROTECTED_DATABASE_MOVE RECOVERY_SERVICE_POLICY_CREATE RECOVERY_SERVICE_POLICY_DELETE RECOVERY_SERVICE_POLICY_MOVE RECOVERY_SERVICE_SUBNET_CREATE RECOVERY_SERVICE_SUBNET_DELETE RECOVERY_SERVICE_SUBNET_MOVE	CreateProtectedDatabase DeleteProtectedDatabase ChangeProtectedDatabaseCompartment CreateProtectionPolicy DeleteProtectionPolicy ChangeProtectionPolicyCompartment CreateRecoveryServiceSubnet DeleteRecoveryServiceSubnet ChangeRecoveryServiceSubnetCompartment	*none*

recovery-service-protected-database

Review the list of permissions and API operations for the `recovery-service-protected-database` resource-type.

Table 9-5 recovery-service-protected-database

Permission	APIs Fully Covered	APIs Partially Covered
RECOVERY_SERVICE_PROTECTED_DATABASE_INSPECT	ListProtectedDatabases	*none*

Table 9-6 recovery-service-protected-database

Permissions	APIs Fully Covered	APIs Partially Covered
INSPECT+ RECOVERY_SERVICE_PROTECTED_DATABASE_READ	GetProtectedDatabase	*none*

Table 9-7 recovery-service-protected-database

Permissions	APIs Fully Covered	APIs Partially Covered
READ+ RECOVERY_SERVICE_PROTECTED_DATABASE_UPDATE	UpdateProtectedDatabase	*none*

Table 9-8 recovery-service-protected-database

Permissions	APIs Fully Covered	APIs Partially Covered
USE+ RECOVERY_SERVICE_PROTECTED_DATABASE_CREATE RECOVERY_SERVICE_PROTECTED_DATABASE_DELETE RECOVERY_SERVICE_PROTECTED_DATABASE_MOVE	CreateProtectedDatabase DeleteProtectedDatabase ChangeProtectedDatabaseCompartment	*none*

recovery-service-subnet

Review the list of permissions and API operations for the `recovery-service-subnet` resource-type.

Table 9-9 recovery-service-subnet

Permissions	APIs Fully Covered	APIs Partially Covered
RECOVERY_SERVICE_SUBNET_INSPECT	ListRecoveryServiceSubnets	*none*

Table 9-10 recovery-service-subnet

Permissions	APIs Fully Covered	APIs Partially Covered
INSPECT+ RECOVERY_SERVICE_SUBNET_READ	GetRecoveryServiceSubnet	*none*

Table 9-11 recovery-service-subnet

Permissions	APIs Fully Covered	APIs Partially Covered
READ+ RECOVERY_SERVICE_SUBNET_UPDATE	UpdateRecoveryServiceSubnet	*none*

Table 9-12 recovery-service-subnet

Permissions	APIs Fully Covered	APIs Partially Covered
USE+ RECOVERY_SERVICE_SUBNET_CREATE RECOVERY_SERVICE_SUBNET_DELETE RECOVERY_SERVICE_SUBNET_MOVE	CreateRecoveryServiceSubnet DeleteRecoveryServiceSubnet ChangeRecoveryServiceSubnetCompartment	*none*

recovery-service-policy

Review the list of permissions and API operations for the `recovery-service-policy` resource type.

Table 9-13 recovery-service-policy

Permissions	APIs Fully Covered	APIs Partially Covered
RECOVERY_SERVICE_POLICY_INSPECT	ListProtectionPolicies	*none*

Table 9-14 recovery-service-policy

Permissions	APIs Fully Covered	APIs Partially Covered
INSPECT+ RECOVERY_SERVICE_POLICY_READ	GetProtectionPolicy	*none*

Table 9-15 recovery-service-policy

Permissions	APIs Fully Covered	APIs Partially Covered
READ+ RECOVERY_SERVICE_POLICY_UPDATE	UpdateProtectionPolicy	*none*

Table 9-16 recovery-service-policy

Permissions	APIs Fully Covered	APIs Partially Covered
USE+ RECOVERY_SERVICE_POLICY_CREATE RECOVERY_SERVICE_POLICY_DELETE RECOVERY_SERVICE_POLICY_MOVE	CreateProtectionPolicy DeleteProtectionPolicy ChangeProtectionPolicyCompartment	*none*

recovery-service-work-request

Review the list of permissions and API operations for the `recovery-service-work-request` resource type.

Table 9-17 recovery-service-work-request

Permissions	APIs Fully Covered	APIs Partially Covered
RECOVERY_SERVICE_WORK_REQUEST_INSPECT	ListWorkRequests	*none*

Table 9-18 recovery-service-work-request

Permissions	APIs Fully Covered	APIs Partially Covered
INSPECT+ RECOVERY_SERVICE_WORK_REQUEST_READ	GetWorkRequest ListWorkRequestErrors ListWorkRequestLogs	*none*

Permissions Required for Each API Operation

Review the list of permissions for Recovery Service resources in a logical order, grouped by resource-type.

Table 9-19 Resource Type and Permissions

Resource Type	Permissions
recovery-service-family	RECOVERY_SERVICE_PROTECTED_DATABASE_INSPECT RECOVERY_SERVICE_PROTECTED_DATABASE_READ RECOVERY_SERVICE_PROTECTED_DATABASE_CREATE RECOVERY_SERVICE_PROTECTED_DATABASE_UPDATE RECOVERY_SERVICE_PROTECTED_DATABASE_DELETE RECOVERY_SERVICE_PROTECTED_DATABASE_MOVE RECOVERY_SERVICE_POLICY_INSPECT RECOVERY_SERVICE_POLICY_READ RECOVERY_SERVICE_POLICY_CREATE RECOVERY_SERVICE_POLICY_UPDATE RECOVERY_SERVICE_POLICY_DELETE RECOVERY_SERVICE_POLICY_MOVE RECOVERY_SERVICE_SUBNET_INSPECT RECOVERY_SERVICE_SUBNET_READ RECOVERY_SERVICE_SUBNET_CREATE RECOVERY_SERVICE_SUBNET_UPDATE RECOVERY_SERVICE_SUBNET_DELETE RECOVERY_SERVICE_SUBNET_MOVE RECOVERY_SERVICE_WORK_REQUEST_INSPECT RECOVERY_SERVICE_WORK_REQUEST_READ
recovery-service-protected-database	RECOVERY_SERVICE_PROTECTED_DATABASE_INSPECT RECOVERY_SERVICE_PROTECTED_DATABASE_READ RECOVERY_SERVICE_PROTECTED_DATABASE_CREATE RECOVERY_SERVICE_PROTECTED_DATABASE_UPDATE RECOVERY_SERVICE_PROTECTED_DATABASE_DELETE RECOVERY_SERVICE_PROTECTED_DATABASE_MOVE

Table 9-19 (Cont.) Resource Type and Permissions

Resource Type	Permissions
recovery-service-policy	RECOVERY_SERVICE_POLICY_INSPECT RECOVERY_SERVICE_POLICY_READ RECOVERY_SERVICE_POLICY_CREATE RECOVERY_SERVICE_POLICY_UPDATE RECOVERY_SERVICE_POLICY_DELETE RECOVERY_SERVICE_POLICY_MOVE
recovery-service-subnet	RECOVERY_SERVICE_SUBNET_INSPECT RECOVERY_SERVICE_SUBNET_READ RECOVERY_SERVICE_SUBNET_CREATE RECOVERY_SERVICE_SUBNET_UPDATE RECOVERY_SERVICE_SUBNET_DELETE RECOVERY_SERVICE_SUBNET_MOVE
recovery-service-work-request	RECOVERY_SERVICE_WORK_REQUEST_INSPECT RECOVERY_SERVICE_WORK_REQUEST_READ

Table 9-20 API Operations and Permissions

API Operation	Permissions Required for the Operation
CreateProtectedDatabase	RECOVERY_SERVICE_PROTECTED_DATABASE_CREATE
DeleteProtectedDatabase	RECOVERY_SERVICE_PROTECTED_DATABASE_DELETE
GetProtectedDatabase	RECOVERY_SERVICE_PROTECTED_DATABASE_READ
ListProtectedDatabases	RECOVERY_SERVICE_PROTECTED_DATABASE_INSPECT
UpdateProtectedDatabase	RECOVERY_SERVICE_PROTECTED_DATABASE_UPDATE
ChangeProtectedDatabaseCompartment	RECOVERY_SERVICE_PROTECTED_DATABASE_MOVE
CreateProtectionPolicy	RECOVERY_SERVICE_POLICY_CREATE
DeleteProtectionPolicy	RECOVERY_SERVICE_POLICY_DELETE
GetProtectionPolicy	RECOVERY_SERVICE_POLICY_READ
ListProtectionPolicies	RECOVERY_SERVICE_POLICY_INSPECT
UpdateProtectionPolicy	RECOVERY_SERVICE_POLICY_UPDATE
ChangeProtectionPolicyCompartment	RECOVERY_SERVICE_POLICY_MOVE
CreateRecoveryServiceSubnet	RECOVERY_SERVICE_SUBNET_CREATE
DeleteRecoveryServiceSubnet	RECOVERY_SERVICE_SUBNET_DELETE

Table 9-20 (Cont.) API Operations and Permissions

API Operation	Permissions Required for the Operation
GetRecoveryServiceSubnet	RECOVERY_SERVICE_SUBNET_READ
ListRecoveryServiceSubnets	RECOVERY_SERVICE_SUBNET_INSPECT
UpdateRecoveryServiceSubnet	RECOVERY_SERVICE_SUBNET_UPDATE
ChangeRecoveryServiceSubnetCompartment	RECOVERY_SERVICE_SUBNET_MOVE

10

Recovery Service Metrics

Learn how to access Recovery Service metrics and monitor protected database backups.

- About Recovery Service Metrics
  Learn about the metrics emitted by the metric namespace: `oci_recovery_service` (Oracle Database Autonomous Recovery Service).
- Available Metrics: oci_recovery_service
  This topic describes the Recovery Service performance metrics available for every protected database resource. You do not need to enable monitoring on the resource to view the default metrics.
- Using the Console to View Protected Database Metrics
  Learn how to use the console to view the metric charts for Recovery Service and monitor your protected databases.
- Using Alarms to Monitor Protected Databases
  You can create alarms for metrics emitted by the `oci_recovery_service` namespace.

About Recovery Service Metrics

Learn about the metrics emitted by the metric namespace: `oci_recovery_service` (Oracle Database Autonomous Recovery Service).

A protected database is an Oracle Cloud database that uses Recovery Service for backups and data protection.

Use Recovery Service metrics to monitor the backup performance of your protected databases. For example, you can use metrics to monitor the protection status or health of your database, the amount of backup storage space utilized to meet the recovery window goal, etc.

In the OCI Console, use the Protected database details page to view the default metric charts for a single protected database. Use the Oracle Cloud Infrastructure Monitoring service to view metrics for multiple protected databases.

You can also use the Oracle Cloud Infrastructure Monitoring service to build metric queries and create alarms to be notified when the metrics meet alarm-specified triggers.

The following terms are helpful for understanding metrics:

- **Namespace**: A container for Recovery Service metrics. `oci_recovery_service` is the Recovery Service namespace.
- **Metrics**: The fundamental concept in telemetry and monitoring. Metrics define a time-series set of datapoints. Each metric is uniquely defined by namespace, metric name, compartment identifier, a set of one or more dimensions, and a unit of measure. Each datapoint has a timestamp, a value, and a count associated with it.
- **Dimensions**: A key-value pair that defines the characteristics associated with the metric. For example, `resourceId`, which is the protected database OCID.

- **Statistics**: Metric data aggregations over specified periods of time. Aggregations are done using the namespace, metric name, dimensions, and the datapoint unit of measure within the time period specified.
- **Alarms**: Used to automate operations monitoring and performance. An alarm keeps track of changes that occur over a specific period of time. It also performs one or more defined actions, based on the rules defined for the metric.

To monitor resources, you must have the required type of access to Recovery Service resources in a policy written by an administrator.

Available Metrics: oci_recovery_service

This topic describes the Recovery Service performance metrics available for every protected database resource. You do not need to enable monitoring on the resource to view the default metrics.

Table 10-1 Recovery Service Metric Dimensions

Dimension	Description
`resourceId`	The OCID of a protected database.
`dBUniqueName`	The unique name identifying the protected database in Recovery Service.

Default Metrics

These default metric charts are available for each protected database from the Protected database details page.

Table 10-2 Default metrics for protected databases

Metric	Metric Display Name	Unit	Description and Metric Chart Defaults	Dimensions
`SpaceUsedForRecoveryWindow`	Space used for recovery window	GB	The amount of storage space that is currently used to meet the recovery window goal for the protected database. Statistic: Max Interval: 1 day	resourceId dBUniqueName
`ProtectedDatabaseSize`	Protected database size	GB	The total storage space consumed by a database protected by Recovery Service. Statistic: Max Interval: 1 day	resourceId dBUniqueName

Table 10-2 (Cont.) Default metrics for protected databases

Metric	Metric Display Name	Unit	Description and Metric Chart Defaults	Dimensions
`ProtectedDatabaseHealth`	Protected database health	Count	Indicates the current protection status or health of the database. • A value of **0** indicates that the database is **Protected** • A value of **1** indicates a **Warning** status due to a potential data loss exposure • A value of **2** indicates an **Alert** status if the latest backup has failed Statistic: Max Interval: 30 minutes	resourceId dBUniqueName
`DataLossExposure`	Data loss exposure	Mean	Indicates the time since the last valid backup, or the amount of time for potential data loss. Statistic: Mean Interval: 30 minutes	resourceId dBUniqueName

Related Topics

- Using the Console to View Protected Database Metrics
  Learn how to use the console to view the metric charts for Recovery Service and monitor your protected databases.

Using the Console to View Protected Database Metrics

Learn how to use the console to view the metric charts for Recovery Service and monitor your protected databases.

To view the default metric charts for a single protected database:

1. Log in to your OCI tenancy.

2. In the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database Backups page.
3. In the **Compartment** field, select the compartment that contains the protected database you want to view.
4. In the **Protected databases** list, click the name of the protected database you want to monitor.
5. In the Protected database details page, under **Resources**, click **Metrics**.

To view the default metric chart for multiple protected databases

1. Open the navigation menu and click **Observability & Management**. Under **Monitoring**, click **Service Metrics**.
2. Choose the **Compartment** that contains the protected databases you want to monitor.
3. In the **Metric namespace** field, select **oci_recovery_service**.
4. The Service Metrics page dynamically updates the page to show charts for each metric that is emitted by the selected metric namespace.

To view custom query metric charts using Metrics Explorer

1. Open the navigation menu and click **Observability & Management**. Under **Monitoring**, click **Metrics Explorer**. The **Metrics Explorer** page displays an empty chart with fields to build a query.
2. Select a **Compartment**.
3. In the **Metric namespace** field, select **oci_recovery_service**.
4. In the **Metric name** field, select a metric. For example, select **DataLossExposure** to create a metric chart that displays data loss exposure information for protected databases.
5. Refine your query. For instructions, see: *Building Metric Queries*.
6. Click **Update Chart**.
7. The chart shows the results of your new query. You can optionally add more queries by clicking **Add Query** below the chart.
8. Optionally, click **Create Alarm** to create an alarm from the query.

Related Topics

- Available Metrics: oci_recovery_service
  This topic describes the Recovery Service performance metrics available for every protected database resource. You do not need to enable monitoring on the resource to view the default metrics.
- Building Metric Queries
- Monitoring

Using Alarms to Monitor Protected Databases

You can create alarms for metrics emitted by the `oci_recovery_service` namespace.

Use the Oracle Cloud Infrastructure Monitoring service alarms feature to passively monitor your protected databases resources and notify you when metrics meet alarm-specified triggers.

From each metric displayed in the Protected database details page, you can set an alarm and be notified when a condition is met. For example, you can create an alarm to notify you when the space used for recovery window is more than 70%, or when the protected database health status changes to **1** (warning).

To set an alarm from the Protected database details page

1. Open the navigation menu, click **Oracle Database**, and select **Database Backups** to display the Database backups page.
2. Choose the compartment that contains the protected databases you want to monitor, and then select a protected database from the list.
3. In the Protected database details page, under **Resources**, click **Metrics**.
4. From any of the available metric charts, click the **Options** menu, and select **Create an alarm on this query**. The Oracle Cloud Infrastructure Monitoring service Create Alarm page is displayed.
5. Specify the alarm settings. For detailed instructions to create an alarm, see *Managing Alarms*.

To set an alarm from the Alarm Definitions page of the Monitoring service

1. Open the navigation menu and click **Observability & Management**. Under **Monitoring**, click **Alarm Definitions**.
2. Click **Create Alarm**.
3. Specify the alarm settings. In the **Metric description** section, select the `oci_recovery_service` namespace. In the **Metric name** field, and select any one of the metrics emitted by the `oci_recovery_service` namespace. For detailed instructions to create an alarm, see *Managing Alarms*.

Related Topics

- Available Metrics: oci_recovery_service
  This topic describes the Recovery Service performance metrics available for every protected database resource. You do not need to enable monitoring on the resource to view the default metrics.
- Managing Alarms
- Monitoring
- Best Practices for your Alarms

11

Recovery Service Events

The Recovery Service resources emit events, which are structured messages that indicate changes in resources.

- About Recovery Service Events and Event Types
  You can create rules in the Events service for Recovery Service event types.
- Protected Databases Event Types
  Review details about the events emitted by the Recovery Service protected databases resource.
- Recovery Service Subnets Event Types
  Review details about the events emitted by the Recovery Service subnets resource.
- Protection Policies Event Types
  Review details about the events emitted by the Recovery Service protection policies resource.
- Viewing Audit Log Events
  Audit provides records of API operations performed against supported services as a list of log events.

About Recovery Service Events and Event Types

You can create rules in the Events service for Recovery Service event types.

Recovery Service emits events for these resources:

- Protected Databases
- Recovery Service Subnets
- Protection Policies

Related Topics

- Overview of Events

Protected Databases Event Types

Review details about the events emitted by the Recovery Service protected databases resource.

Table 11-1 Recovery Service: Protected Database Event Types

Friendly Name	Event Type
Protected Database - Change Billing Compartment Begin	`com.oraclecloud.autonomousrecoveryservice.changeprotecteddatabasebillingcompartment.begin`

Table 11-1 (Cont.) Recovery Service: Protected Database Event Types

Friendly Name	Event Type
Protected Database - Change Billing Compartment End	com.oraclecloud.autonomousrecoveryservice.changeprotecteddatabasebillingcompartment.end
Protected Database - Change Compartment Begin	com.oraclecloud.autonomousrecoveryservice.changeprotecteddatabasecompartment.begin
Protected Database - Change Compartment End	com.oraclecloud.autonomousrecoveryservice.changeprotecteddatabasecompartment.end
Protected Database - Create Begin	com.oraclecloud.autonomousrecoveryservice.createprotecteddatabase.begin
Protected Database - Create End	com.oraclecloud.autonomousrecoveryservice.createprotecteddatabase.end
Protected Database - Delete Begin	com.oraclecloud.autonomousrecoveryservice.deleteprotecteddatabase.begin
Protected Database - Delete End	com.oraclecloud.autonomousrecoveryservice.deleteprotecteddatabase.end
Get Protected Database Configuration Begin	com.oraclecloud.autonomousrecoveryservice.fetchprotecteddatabaseconfiguration.begin
Get Protected Database Configuration End	com.oraclecloud.autonomousrecoveryservice.fetchprotecteddatabaseconfiguration.end
Protected Database - Update Begin	com.oraclecloud.autonomousrecoveryservice.updateprotecteddatabase.begin
Protected Database - Update End	com.oraclecloud.autonomousrecoveryservice.updateprotecteddatabase.end

Example 11-1 Reference Event for Protected Databases

Here's a reference event for protected databases:

```
{
    "eventType":
"com.oraclecloud.autonomousrecoveryservice.updateprotecteddatabase.begi
n",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "autonomousRecoveryService",
    "eventTime": "2022-09-08T20:39:38.446Z",
    "contentType": "application/json",
    "eventID": "unique_ID",
    "data": {
      "compartmentId": "ocid1.compartment.oc1..unique_ID",
      "compartmentName": "example_compartment",
      "resourceName": "example protected database",
```

```
      "resourceId":
"ocid1.recoveryserviceprotecteddatabase.oc1.phx.unique_ID",
      "availabilityDomain": "availability_domain",
      "freeFormTags": {},
      "definedTags": {
        "Oracle-Tags": {
          "CreatedBy": "oracleidentitycloudservice/example_email",
          "CreatedOn": "2022-09-08T20:38:53.109Z"
        }
      },
      "additionalDetails": {
        "X-Real-Port": 35739
      }

    }
  },
```


Recovery Service Subnets Event Types

Review details about the events emitted by the Recovery Service subnets resource.

Table 11-2 Recovery Service Subnets Event Types

Friendly Name	Event Type
Recovery Service Subnet - Change Compartment Begin	`com.oraclecloud.autonomousrecoveryservice.changerecoveryservicesubnetcompartment.begin`
Recovery Service Subnet - Change Compartment End	`com.oraclecloud.autonomousrecoveryservice.changerecoveryservicesubnetcompartment.end`
Recovery Service Subnet - Create Begin	`com.oraclecloud.autonomousrecoveryservice.createrecoveryservicesubnet.begin`
Recovery Service Subnet - Create End	`com.oraclecloud.autonomousrecoveryservice.createrecoveryservicesubnet.end`
Recovery Service Subnet - Delete Begin	`com.oraclecloud.autonomousrecoveryservice.deleterecoveryservicesubnet.begin`
Recovery Service Subnet - Delete End	`com.oraclecloud.autonomousrecoveryservice.deleterecoveryservicesubnet.end`
Recovery Service Subnet - Update Begin	`com.oraclecloud.autonomousrecoveryservice.updaterecoveryservicesubnet.begin`
Recovery Service Subnet - Update End	`com.oraclecloud.autonomousrecoveryservice.updaterecoveryservicesubnet.end`

Example 11-2 Reference Event for Recovery Service Subnets

Here's a reference event for Recovery Service subnets:


```
{
      "eventType":
"com.oraclecloud.autonomousrecoveryservice.createrecoveryservicesubnet.begin"
```

```
,
      "cloudEventsVersion": "0.1",
      "eventTypeVersion": "2.0",
      "source": "autonomousRecoveryService",
      "eventTime": "2022-09-08T20:39:38.446Z",
      "contentType": "application/json",
      "eventID": "unique_ID",
      "data": {
        "compartmentId": "ocid1.compartment.oc1..unique_ID",
        "compartmentName": "example_compartment",
        "resourceName": "example recovery service subnet",
        "resourceId": "ocid1.recoveryservicesubnet.oc1.phx.unique_ID",
        "availabilityDomain": "availability_domain",
        "freeFormTags": {},
        "definedTags": {
          "Oracle-Tags": {
            "CreatedBy": "oracleidentitycloudservice/example_email",
            "CreatedOn": "2022-09-08T20:38:53.109Z"
          }
        },
        "additionalDetails":{
          "X-Real-Port": 35739
        }
      }
    },
```

Protection Policies Event Types

Review details about the events emitted by the Recovery Service protection policies resource.

Table 11-3 Recovery Service: Protection Policies Event Types

Friendly Name	Event Type
Protection Policy - Change Compartment Begin	com.oraclecloud.autonomousrecoveryservice.changeprotectionpolicycompartment.begin
Protection Policy - Change Compartment End	com.oraclecloud.autonomousrecoveryservice.changeprotectionpolicycompartment.end
Protection Policy - Create Begin	com.oraclecloud.autonomousrecoveryservice.createprotectionpolicy.begin
Protection Policy - Create End	com.oraclecloud.autonomousrecoveryservice.createprotectionpolicy.end
Protection Policy - Delete Begin	com.oraclecloud.autonomousrecoveryservice.deleteprotectionpolicy.begin
Protection Policy - Delete End	com.oraclecloud.autonomousrecoveryservice.deleteprotectionpolicy.end
Protection Policy - Update Begin	com.oraclecloud.autonomousrecoveryservice.updateprotectionpolicy.begin

Table 11-3 (Cont.) Recovery Service: Protection Policies Event Types

Friendly Name	Event Type
Protection Policy - Update End	`com.oraclecloud.autonomousrecoveryservice.updateprotectionpolicy.end`

Example 11-3 Reference Event for Protection Policies

Here's a reference event for protection policies:

```
{
      "eventType":
"com.oraclecloud.autonomousrecoveryservice.updateprotectionpolicy.end",
      "cloudEventsVersion": "0.1",
      "eventTypeVersion": "2.0",
      "source": "autonomousRecoveryService",
      "eventTime": "2022-09-08T20:39:38.446Z",
      "contentType": "application/json",
      "eventID": "unique_ID",
      "data": {
        "compartmentId": "ocid1.compartment.oc1..unique_ID",
        "compartmentName": "example_compartment",
        "resourceName": "example protection policy",
        "resourceId": "ocid1.recoveryservicepolicy.oc1.phx.unique_ID",
        "availabilityDomain": "availability_domain",
        "freeformTags": null,
        "definedTags": null,
        "additionalDetails": null
      }
    },
    "additionalDetails": []
  }
```

Viewing Audit Log Events

Audit provides records of API operations performed against supported services as a list of log events.

Use the console to view Recovery Service events logged by Audit.

For more information on searching logs, see *Using the Console*.

Related Topics

- Overview of Audit
- View Audit Log Events
- Using the Console

A
Troubleshooting

Learn how to address typical issues and errors that you may encounter while working with Recovery Service.

- Troubleshoot Backup Failures to Recovery Service
  If your database fails to backup to Recovery Service, use the information in this topic to troubleshoot the issue.
- Getting Help for Recovery Service
  You can collect diagnostics to analyze an issue. If you need help to resolve the issue, raise a service request with My Oracle Support and share the diagnostics.

Troubleshoot Backup Failures to Recovery Service

If your database fails to backup to Recovery Service, use the information in this topic to troubleshoot the issue.

Typically, automatic backups to Recovery Service may fail because of configuration issues in the database VCN, or due to network connectivity problems between your database and Recovery Service.

These sections describe the common errors associated with backup failures, and provides troubleshooting information.

Connection timed out

Backups to Recovery Service may fail if the connection from a database client to Recovery Service could not be completed within the time out period.

How to Diagnose

Run the `tnsping` command from the database client to verify connectivity between your database and Recovery Service.

For example:

```
tnsping dbrs
```

This message indicates that a connection could not be established with Recovery Service.

```
TNS Ping Utility for Linux: Version 19.0.0.0.0 - Production on 26-APR-2023 06:09:46
Used parameter files:

/u01/app/oracle/product/19.0.0.0/dbhome_1/network/admin/sqlnetdb.ora

Used TNSNAMES adapter to resolve the alias
Attempting to contact (DESCRIPTION = (FAILOVER = on) (CONNECT_TIMEOUT = 3)
(RETRY_COUNT = 3) (TRANSPORT_CONNECT_TIMEOUT = 3) (ADDRESS_LIST = (LOAD_BALANCE = on)
(ADDRESS = (PROTOCOL = TCPS)(HOST = sales-server)(PORT = 1421)) (ADDRESS = (PROTOCOL =
TCPS)(HOST = sales-server)(PORT = 1421))) (CONNECT_DATA = (SERVER = DEDICATED)
```

```
(SERVICE_NAME = sales.example.com)))
TNS-12535: TNS:operation timed out
```

Probable Cause 1
Port 8005 is not open to allow HTTP traffic.

Solution
Add an ingress rule to allow HTTP traffic from **Destination Port Range** 8005. You must add this rule to the security list used by the VCN in which your database resides.

See, Subnet Size Requirements and Security Rules for Recovery Service Subnet

Probable Cause 2
Port 2484 is not open to allow SQL Net traffic

Solution
Add an ingress rule to allow SQL Net traffic from **Destination Port Range** 2484. You must add this ingress rule to the security list used by the VCN in which your database resides.

See, Subnet Size Requirements and Security Rules for Recovery Service Subnet

Probable Cause 3
An egress rule may be preventing network traffic on ports 8005 and 2484.

Solution
If your database VCN restricts network traffic between subnets, then ensure to add an egress rule for ports 2484 and 8005 from the database subnet to the Recovery Service subnet that you create.

See, Subnet Size Requirements and Security Rules for Recovery Service Subnet

Probable Cause 4
You could be using a custom DNS setup, which will lead to incorrect IP address resolution.

Solution
Perform a `nslookup` on the host names provided in the `dbrsnames.ora` file. You can also obtain the host names when you run the `tnsping` command. The IP address must match the IP addresses provided in the protected database `hosts.txt` file. You can download the `hosts.txt` file from the protected database details page in the OCI Console.
See, Downloading Protected Database Network Connection Details.

Subnet does not have any more available IP addresses

While creating a protected database, the work request may report a failed state for the associated Recovery Service subnet.

Probable Cause
There are insufficient unallocated IP addresses in the subnet used for Recovery Service operations in the database VCN.

Solution
To prevent a recurrence of this issue, ensure that sufficient unallocated IP addresses remain available in the subnet, or use a different Recovery Service subnet.

See, Register Recovery Service Subnets

A problem occurred while creating the protected database resource

If there is a problem while creating a protected database, then you may encounter an error message that suggests to contact Oracle Support for assistance.

Probable Cause
Protected database creation may fail for unknown reasons.

Solution
You may retry later. If the problem persists, contact Oracle Support.
See, Submit a Service Request.

Getting Help for Recovery Service

You can collect diagnostics to analyze an issue. If you need help to resolve the issue, raise a service request with My Oracle Support and share the diagnostics.

- Collect Diagnostics
  Review this section to learn how you can diagnose backup and restore issues.
- Submit a Service Request
  You can contact Oracle Support for assistance with onboarding your database, backup failures, or restore issues while working with Recovery Service.

Collect Diagnostics

Review this section to learn how you can diagnose backup and restore issues.

Database Service	How to Diagnose Backup and Restore Issues
Oracle Base Database Service	Identify the Cause of Backup Failures
Oracle Exadata Database Service on Dedicated Infrastructure	For backup failures, see: SRDC - Exadata Cloud Required Diagnostic Data Collection for RMAN Backup (Doc ID 2653098.1) For restore issues, see: SRDC - Exadata Cloud Required Diagnostic Data Collection for RMAN Restore and Recover (Doc ID 2653673.1)

Submit a Service Request

You can contact Oracle Support for assistance with onboarding your database, backup failures, or restore issues while working with Recovery Service.

Before you create a service request:

- You must have a Support Identifier which verifies your eligibility for Support services
- You must have an account at My Oracle Support

Use these steps to submit a service request to Oracle Support.

1. Access and log in to My Oracle Support.
2. Select the **Service Requests** tab, and click **Create Technical SR**.

   The Create Service Request wizard is displayed.

3. In the **Problem Summary** field, enter a brief description of the problem.
4. In the **Problem Description** field, enter a detailed information of the problem. Include any diagnostic information or error messages you may have encountered in the OCI Console. See, Collect Diagnostics.

> **Note:**
>
> It is important that you specify that the issue is related to Autonomous Recovery Service, and also indicate whether the problem affects onboarding, backups, or restore operations for your database.

5. Select an appropriate **Severity** value for the issue.
6. Navigate to the **Where is the problem?** section.
7. Select the **Cloud** tab.
8. In the **Service Type** field, do one of the following:
   - For Oracle Base Database Service service, select **Oracle Cloud Infrastructure - Database Service**
   - For Oracle Exadata Database Service on Dedicated Infrastructure, select **Oracle Cloud Infrastructure - Exadata Cloud Service**
9. In the **Problem Type** field, do one of the following:
   - For Oracle Base Database Service, select **OCI VM/BM Database Administration**, and then select one of these options:
     - **Backup** - for onboarding or backup related issues for your database
     - **Restore** - for issues related to restoring backups from Recovery Service
   - For Oracle Exadata Database Service on Dedicated Infrastructure, select **Database Lifecycle > Backup Cloud Services (Backup, Restore, Recovery)**.
10. Provide the **Support Identifier** details.
11. Click **Next** until you have provided all the mandatory information.
12. Click **Submit**.

    Your service request is submitted.

B
Reference

This section provides reference information about Recovery Service.

- Life Cycle States of Recovery Service Resources
  Learn how Recovery Service resources progress through different life cycle states based on specific events.

Life Cycle States of Recovery Service Resources

Learn how Recovery Service resources progress through different life cycle states based on specific events.

Table B-1 Life Cycle States of Protected Databases

Life Cycle State	Description
Creating	A protected database is in the process of being created. You must wait for a protected database to reach the **Active** state before you can modify or delete the resource.
Active	A protected database is created and available for use.
Updating	A protected database is being updated. A protected database usually moves back to the **Active** state after modification.
Failed	A protected database failed during creation or modification.

Table B-1 (Cont.) Life Cycle States of Protected Databases

Life Cycle State	Description
Delete Scheduled	The protected database and its backups are scheduled for deletion due to one of these reasons: • You have terminated the source database • You have disabled automatic backups for the database Before you terminate a database, you can specify whether to retain the protected database backups for a period of 72 hours or until the policy retention period expires. After you terminate the source database: • Recovery Service schedules the deletion of the associated protected database and its backups • The protected database enters the **Delete Scheduled** state • The protected database remains in the **Delete Scheduled** state, either for 72 hours (default delay) or until the policy retention period ends, depending on the option that you have selected while terminating the source database When you disable automatic backups for a database, the protected database enters the **Delete Scheduled** state. Recovery Service schedules the deletion of the associated protected database and its backups after a 72 hour delay. At the end of the scheduled delay, the protected database exits the **Delete Scheduled** state and enters the **Deleting** state. When a protected database is in the **Delete Scheduled** state, the **Health** field does not display the protection status. A protected database may return to the **Active** state if the scheduled deletion is canceled.
Deleting	The protected database and its backups is being deleted, and cannot be modified. A protected database exits the **Delete Scheduled** state and enters the **Deleting** state when the scheduled delay of 72 hours ends or after the backup retention period ends, depending on the option you have selected while terminating the source database.
Deleted	The protected database is deleted and cannot be modified.

Table B-2 Life Cycle States of Recovery Service Subnets

Life Cycle State	Description
Creating	The Recovery Service subnet is being created. At this stage, you cannot modify or delete the resource.
Active	The Recovery Service subnet has been created and is available for use.
Updating	The Recovery Service subnet is being updated and not available for modification.
Failed	The Recovery Service subnet failed during creation or modification.
Deleting	The Recovery Service subnet is being deleted and cannot be modified.
Deleted	The Recovery Service subnet is deleted and cannot be modified.

Table B-3 Life Cycle States of Protection Policies

Life Cycle State	Description
Creating	The protection policy is being created. You cannot modify or delete a policy when it is in this state.
Active	The protection policy is created and available for use.
Updating	The protection policy is being modified.
Failed	The protection policy failed while being created or modified.
Deleting	The protection policy is being deleted, and cannot be modified.
Deleted	The protection policy is deleted.