Oracle® Cloud

Using Oracle Database Autonomous Recovery Service

F47893-48
June 2026

Oracle Cloud Using Oracle Database Autonomous Recovery Service,

F47893-48

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, Rohan Daniel

Contents

B Reference

Preface

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

Audience

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

- Managing backup and restores for Oracle 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.

1

What's New in Recovery Service

Learn about the new features in Recovery Service.

- Automated Cleanup of Recovery Service Subnets Registered by the Service
- Protect on-premises Oracle Databases with Oracle Database Zero Data Loss Cloud Protect
- Recovery Service now supports Oracle Database@AWS
- Create long-term retention backups with Recovery Service
- Multicloud Database Backup Support
- Support for Network Security Groups (NSG)
- Create a Protected Database in a Dry-Run Mode
- Retention Lock for Protected Database Backups
- Delayed Deletion of Protected Database Resources and Database Backups
- Oracle Database Autonomous Recovery Service is Now Available

Automated Cleanup of Recovery Service Subnets Registered by the Service

- **Service**: Oracle Database Autonomous Recovery Service
- **Release Date**: January 21, 2026

Recovery Service automates the maintenance of unused Recovery Service subnets that are automatically registered by the service.

After deleting a protected database, Recovery Service also removes the automatically registered Recovery Service subnet if it is unchanged and has no dependencies with any other protected database.

See Deleting a Recovery Service Subnet for details.

Protect on-premises Oracle Databases with Oracle Database Zero Data Loss Cloud Protect

- **Service**: Oracle Database Autonomous Recovery Service
- **Release Date**: October 09, 2025

Oracle Database Zero Data Loss Cloud Protect is now available.

Protect on-premises Oracle Databases using Oracle Zero Data Loss Autonomous Recovery Service deployed in OCI. This new feature provides real-time transaction protection, logically air-gapped immutable backups, and enables fast, point-in-time recovery to any location.

Related Topics

- Protecting On-premises Databases using Oracle Database Zero Data Loss Cloud Protect
  Oracle Database Zero Data Loss Cloud Protect offers on-premises database protection using Oracle Zero Data Loss Autonomous Recovery Service deployed in OCI. This new feature provides real-time transaction protection, logically air-gapped immutable backups, and enables fast, point-in-time recovery to any location.

Recovery Service now supports Oracle Database@AWS

- **Service**: Oracle Database Autonomous Recovery Service
- **Release Date**: October 08, 2025

Oracle Database Autonomous Recovery Service adds support for Oracle Database@AWS.

Related Topics

- Multicloud Oracle Database Backup Support
  Recovery Service supports Oracle Multicloud Databases, and also provides the flexibility to store backups in the same cloud location where a multicloud database resides.

Create long-term retention backups with Recovery Service

- **Service**: Oracle Database Autonomous Recovery Service
- **Release Date**: January 23, 2025

You can now create a long-term retention (LTR) backup of your database with Autonomous Recovery Service and retain the backup for up to 10 years. LTR backups are stored in the Object Storage Infrequent Access tier. You can restore an LTR backup to create a new database within the retention period.

Related Topics

- Create Long-Term Retention Backups with Recovery Service
  You can create long-term retention backups (LTR) for compliance, regulatory, and other business needs. LTR backups are independent of the automatic backups and stored in the Object Storage Infrequent Access tier. You can restore an LTR backup to create a new database within the retention period.

Multicloud Database Backup Support

- **Service**: Oracle Database Autonomous Recovery Service
- **Release Date**: September 09, 2024

Autonomous Recovery Service now supports Oracle Multicloud Databases such as Oracle Database@Azure and Oracle Database@Google Cloud. Recovery Service also provides the option to store the backups in the same cloud location as the database.

If you enable the **Store backups in the same cloud provider as the database** option for a protection policy and choose this policy for automatic backups to Recovery Service, then the database backups will be stored in the same cloud provider where the database resides. For example, for Oracle Database@Azure, Recovery Service stores the backups in Azure if you have selected the **Store backups in the same cloud provider as the database** option in the chosen protection policy.

Related Topics

- Multicloud Oracle Database Backup Support
  Recovery Service supports Oracle Multicloud Databases, and also provides the flexibility to store backups in the same cloud location where a multicloud database resides.

Support for Network Security Groups (NSG)

- **Service**: Oracle Database Autonomous Recovery Service
- **Release Date**: May 01, 2024

You can now optionally use network security groups (NSGs) to implement the security rules that control the inbound and outbound traffic between your Oracle Database and Recovery Service. In the OCI console, you can use options to add a Recovery Service subnet to the Recovery Service NSGs configured in the database VCN.

Related Topics

- Configuring Network Resources for Recovery Service
  Create or use an existing IPv4-only subnet for Recovery Service operations in the database VCN. Define security rules to control the backup traffic between your database and Recovery Service.

Create a Protected Database in a Dry-Run Mode

- **Service**: Oracle Database Autonomous Recovery Service
- **Release Date**: October 18, 2023

You can perform a dry run of the `CreateProtectedDatabase` API to verify that you meet all the prerequisites before creating a protected database. A dry run request returns error messages identifying the missing requirements and also indicates the recommended action to fulfill each requirement.

Related Topics

- Using the API to Manage Protected Databases
  Review the list of REST API endpoints to manage protected databases.

Retention Lock for Protected Database Backups

- **Service**: Oracle Database Autonomous Recovery Service
- **Release Date**: October 18, 2023

You can now enforce a lock for the backup retention period defined in a protection policy. When a retention lock is in effect, Recovery Service prohibits the modification or deletion of backups during the specified duration. The retention lock feature helps to protect your database backups from accidental or malicious damages such as ransomware.

Related Topics

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

Delayed Deletion of Protected Database Resources and Database Backups

- **Service**: Oracle Database Autonomous Recovery Service
- **Release Date**: October 18, 2023

Protected databases now have a new lifecycle state called **Delete Scheduled**.

A protected database resource enters the **Delete Scheduled** state after you terminate the source database or if you disable its automatic backups. Recovery Service delays the deletion of the protected database resource and the database backups for 72 hours, or until the backup retention period ends. This feature provides you an opportunity to recover data even after you terminate a database.

Related Topics

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

Oracle Database Autonomous Recovery Service is Now Available

- **Service**: Oracle Database Autonomous Recovery Service
- **Release Date**: February 15, 2023

Oracle Database Zero Data Loss Autonomous Recovery Service is a fully managed data protection service for Oracle databases running on Oracle Cloud Infrastructure (OCI). Unique, automated capabilities protect Oracle Database changes in real time, validate backups without production database overhead, and enable fast, predictable recovery to any point in time. Low costs based on the amount of data being protected mean that zero data loss resiliency is available to organizations of any size and virtually any budget.

Related Topics

- About Oracle Database Autonomous Recovery Service
  Understand the core concepts and key features of Recovery Service.

2

Overview of Oracle Database Autonomous Recovery Service

This chapter introduces you to Oracle Database Zero Data Loss Autonomous Recovery Service.

- About Oracle Database Autonomous Recovery Service
  Understand the core concepts and key features of Recovery Service.
- 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 Resources
  You can create and manage Recovery Service resources using the Console, the Recovery Service APIs, or the CLI commands.
- Oracle Database Autonomous Recovery Service Technical Architecture
  This technical architecture diagram illustrates the Autonomous Recovery Service backup and recovery workflow for Oracle Databases in OCI and for Oracle multicloud databases.

About Oracle Database Autonomous Recovery Service

Understand the core concepts and key features of Recovery Service.

Oracle Database Zero Data Loss Autonomous Recovery Service is a fully managed service based on the on-premises Oracle Zero Data Loss Recovery Appliance (ZDLRA) technology. It provides modern cybersecurity protection for Oracle Databases of any size running on Exadata Database Service on Dedicated Infrastructure, Exadata Database Service on Exascale Infrastructure, Oracle Base Database Service, Oracle Database@AWS, Oracle Database@Azure, Oracle Database@Google Cloud, or on-premises environments.

Recovery Service is the recommended solution for protecting Oracle Databases and provides the following unique advantages over Object Storage backups:

- **Zero Data Loss for All Database Backups** - Zero Data Loss Autonomous Recovery Service provides real-time protection of the database, enabling recovery to within less than a second of when an outage or ransomware attack occurs. If a ransomware attack happens, you know you are protected up to the moment before the attack instead of having to go back to the last scheduled backup, which could have been hours ago.
- **Achieve Faster Backups with Less Database Overhead** - Recovery Service elminates the need for weekly full backups using an offloaded incremental-forever backup paradigm, reducing database CPU, memory, and I/O overhead along with the backup window. Your valuable database resources can now be more focused on business needs rather than backup tasks.
- **Be Confident in Reliable Recovery** - All backups are validated for data anomalies that can impact recovery operations. Combined with immutability and enforced encryption, your data is safe, unalterable by anyone in the tenancy, and always ready for recovery in case of a ransomware attack.

- **Get Deeper Insights into your Database Protection** - A centralized data protection dashboard addresses key questions about the state of your database backups. Are my backups healthy? How long has it been since my last backup? How far back can I recover? How much space is my backup using? Are all my databases using the same retention policy?

For Recovery Service backups without Zero Data Loss protection, costs remain the same as Object Storage backups. Zero Data Loss is a premium option enabled by selecting Real-Time Protection.

Select Autonomous Recovery Service as the backup destination for Oracle managed automatic backups, which is the method that Oracle recommends for backing up Oracle Cloud and Oracle Multicloud Databases. See Backing Up Oracle Cloud Databases to Recovery Service for details.

To protect on-premises databases using Recovery Service, you must use Oracle Database Zero Data Loss Cloud Protect.

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.

Oracle Database Zero Data Loss Cloud Protect
Protects on-premises Oracle databases using Oracle Zero Data Loss Autonomous Recovery Service deployed in the OCI or multicloud environment.

Protected Database
An Oracle Database that sends backups to Recovery Service. Recovery Service supports Oracle Cloud Databases, Oracle Multicloud Databases, and on-premises databases.

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 used for 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.
For Oracle Databases deployed in OCI, if the backup subnet meets the recommended subnet size (at least 12 free IP addresses), then Recovery Service automatically registers the Recovery Service subnet.

- For Oracle Exadata Database Service on Dedicated Infrastructure, Recovery Service automatically registers the backup subnet as the Recovery Service subnet.
- For Oracle Base Database Service, Recovery Service automatically registers the database subnet as the Recovery Service subnet.

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 Resources

You can create and manage Recovery Service resources using the Console, the Recovery Service APIs, or the CLI commands.

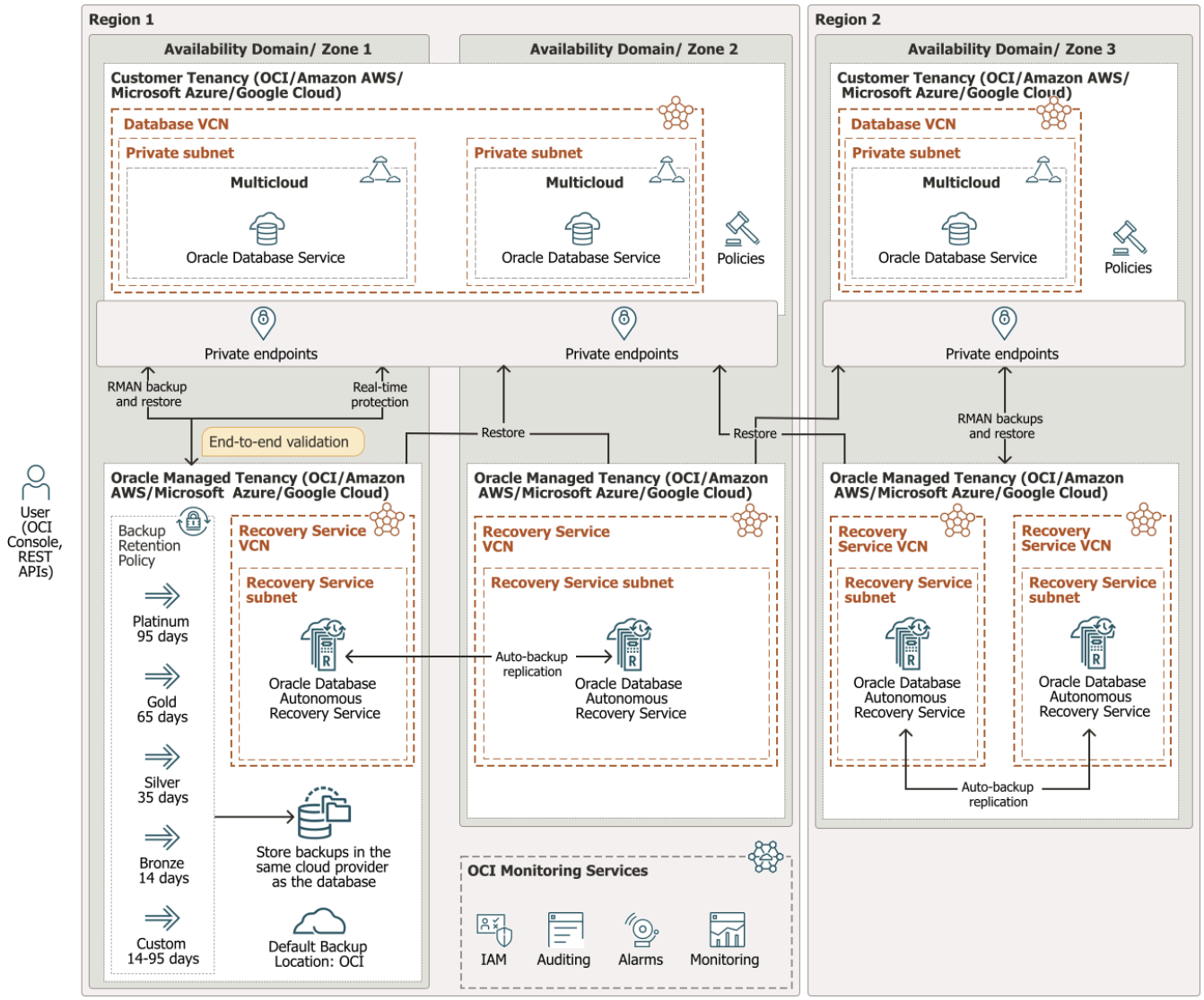
Table 2-1 Recovery Service Resources

Resource	Description	More Information
Protected databases	A protected database resource is created when you enable backups to **Autonomous Recovery Service**. A protected database can be associated with: • An Oracle Cloud Database For example, a DB system database. • An Oracle Multicloud Database For example, an Oracle Database@Azure resource • An externally managed Oracle Database For example, An Oracle Database deployed on-premises	About Protected Databases
Recovery Service subnets	Recovery Service subnets provide the backup network to facilitate Recovery Service operations in the database virtual cloud network (VCN).	About Recovery Service Subnets
Protection policies	A protection policy defines the rules for backup retention, backup immutability, and the preferred backup storage location for Oracle Multicloud Databases.	About Protection Policies

Oracle Database Autonomous Recovery Service Technical Architecture

This technical architecture diagram illustrates the Autonomous Recovery Service backup and recovery workflow for Oracle Databases in OCI and for Oracle multicloud databases.

Figure 2-1 Oracle Database Autonomous Recovery Service Technical Architecture



> **Note**
>
> Explore Oracle Database interactive architecture diagrams on Oracle Help Center.

Oracle Database Autonomous Recovery Service supports backups and data protection for Oracle Databases in OCI, Oracle Multicloud Databases, and on-premises databases.

Recovery Service supports these Oracle Multicloud Databases:

- Oracle AI Database@Azure
- Oracle AI Database@Google Cloud
- Oracle AI Database@AWS

You must use the Cloud Protect Fleet Agent to add an on-premises Oracle Database to Recovery Service for data protection. See Protecting On-premises Databases using Oracle Database Zero Data Loss Cloud Protect for details.

The OCI Console provides a unified interface to define your backup strategy using Recovery Service resources. Recovery Service centralizes backup storage in Oracle Cloud (default cloud backup location for protected databases). 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.

Recovery Service requires a private subnet for backup and recovery operations in each database virtual cloud network (VCN) within your tenancy. Oracle recommends that your database VCN includes at least one private subnet used for backups to Recovery Service. You can then register a Recovery Service subnet to allow Recovery Service to access databases in the VCN.

You can implement access control by assigning Oracle Cloud Infrastructure (OCI) policies. In the Console, use the Policy Builder to select **Autonomous Recovery Service** as the **Policy Use Case**, and then select the predefined policy templates.

Recovery Service retains protected database backups for a minimum period of 14 days and a maximum period of 95 days. You can either select the Oracle-defined policies (Platinum, Gold, Silver, or Bronze) that support common use cases for data retention, or create custom policies to suit your demands for backup retention. You can optionally enforce a retention lock on the backup retention period so that Recovery Service can prevent the modification or deletion of backups until the retention period ends. Retention lock is an optional feature to safeguard your protected database backups from inadvertent changes or malicious damages, such as ransomware attacks.

Recovery Service supports multicloud Oracle Databases and provides the flexibility to store backups either in Oracle Cloud (default backup storage location) or in the same cloud location where the database resides. By default, Recovery Service stores protected databases and related backups in Oracle Cloud. If you enable the **Store backups in the same cloud provider as the database** option for a protection policy, then Recovery Service stores the policy-linked protected database and its backups in the target database cloud location instead of Oracle Cloud. For example, for Oracle AI Database@Azure, Recovery Service stores the associated protected database backups in Azure if you have selected the **Store backups in the same cloud provider as the database** option in the protection policy.

Auto-backup replication is used for backup high-availability within a region. You can restore to any availability domain, zone, or region.

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

You can also use the Oracle Cloud Infrastructure Monitoring service, including Alarms, to monitor database protection status and storage utilization. Recovery Service uses the Oracle Cloud Infrastructure Audit service, which automatically records calls to Recovery Service application programming interface (API) endpoints as log events.

3

Onboarding Oracle Database to Recovery Service

Use checklists to review the mandatory requirements, and plan to onboard your Oracle Database to Recovery Service.

- Mandatory Requirements Checklist for Recovery Service
  Use this checklist to verify the mandatory prerequisites to onboard your Oracle Database to Recovery Service.
- Optional Configuration Checklist for Recovery Service
  You may choose to configure these additional options for Recovery Service.
- Recovery Service Resource Limits
  A service limit is the quota or allowance set on a resource. Autonomous Recovery Service has maximum limits for the number of protected databases and the backup storage space utilization. The limits apply to each region.
- Optional Permissions for Oracle Databases in OCI
  By default, Oracle Databases in OCI are assigned with the permissions to access Recovery Service. The service can also access the network resources within the database VCN. You may choose to assign the additional and optional permissions for OCI Databases, as described in this topic.
- Permissions Required for Oracle Multicloud Databases to Use Recovery Service
  Assign Recovery Service IAM policies that allow Oracle Multicloud Database to send backups to Recovery Service.
- Configuring Network Resources for Recovery Service
  Create or use an existing IPv4-only subnet for Recovery Service operations in the database VCN. Define security rules to control the backup traffic between your database and Recovery Service.
- Registering the Recovery Service Subnet
  Use this procedure to register a Recovery Service subnet.
- 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.

Mandatory Requirements Checklist for Recovery Service

Use this checklist to verify the mandatory prerequisites to onboard your Oracle Database to Recovery Service.

> **Note**
>
> Operational backups to two different backup destinations may create data loss scenarios. Therefore, before you enable automatic backups to Recovery Service, you must disable manual backup scripts and processes to other storage destinations.

Table 3-1 Mandatory Requirements for Onboarding your Database to Recovery Service

Check	Task
Ports used by Recovery Service	You must open these network ports and configure the security rules for Recovery Service. • Port **2484** - Enables SQL*Net connections to the RMAN catalog which is used by Recovery Service. • Port **8005** - Enables backup traffic from the database to Recovery Service.
Security rules for Recovery Service	Use Security Lists or network security groups (NSGs) to configure the security rules. • **Security Rules for Oracle Databases deployed in OCI** For OCI Databases, Oracle recommends that you use security lists to implement the security rules for the Recovery Service subnet in the database VCN. – For **Oracle Exadata Database Service on Dedicated Infrastructure**, the backup subnet is used as the Recovery Service subnet. – For **Oracle Base Database Service**, the database subnet is used as the Recovery Service subnet. See Subnet Size and Security Rules for Recovery Service Subnet for details. • **Security Rules for Oracle Multicloud Databases** For Oracle Multicloud Databases, you must use network security groups (NSGs) to define the security rules and associate the NSGs (maximum five) while registering the Recovery Service subnet.
Supported platform	Linux x86-64
Target database compatibility level	19.0.0 or later Ensure that the target database compatibility level (the `COMPATIBLE` initialization parameter) is set to 19.0.0 or later.

Table 3-1 (Cont.) Mandatory Requirements for Onboarding your Database to Recovery Service

Check	Task
Supported Oracle Database releases	**Oracle Cloud Databases and Oracle Multicloud Databases** You can set **Autonomous Recovery Service** as the backup destination for Oracle Cloud Databases and Oracle Multicloud Databases provisioned with any of these releases: • Oracle AI Database 26ai Release Update 23.4 or later • Oracle Database 21c Release Update 21.7 or later To use the Real-time data protection feature, your database must be provisioned with Oracle Database 21c Release Update 21.8 or later. • Oracle Database 19c Release Update 19.16 or later To use the Real-time data protection feature, your database must be provisioned with Oracle Database 19c Release Update 19.18 or later. **On-Premises Oracle Databases** You can add on-premises Oracle Databases provisioned with any of these releases to Recovery Service. • Oracle AI Database 26ai Release Update 23.4 or later • Oracle Database 19c Release Update 19.18 or later See Add On-Premises Database to Recovery Service Using Cloud Protect for details. **Oracle Database Releases that Support Recovery Service on Government Cloud** • Oracle Database Releases That Support Recovery Service in Oracle US Government Cloud • Oracle Database Releases That Support Recovery Service in Oracle US Defense Cloud • Oracle Database Releases That Support Recovery Service in United Kingdom Government Cloud
Recovery Service resource limits	Ensure that the Recovery Service resource limits are adequate and request for an increase in service limits, if necessary. For Oracle Multicloud Databases, you must review and adjust the limits specific to your multicloud subscription from the **Limits, Quotas and Usage** page in the OCI Console. **⚠ Caution** If you do not select the multicloud subscription, then the increased limits will be applied to OCI resources. See Recovery Service Resource Limits for details.

Table 3-1 (Cont.) Mandatory Requirements for Onboarding your Database to Recovery Service

Check	Task
Recovery Service IAM policies	• **Oracle Databases in OCI** By default, Oracle Databases deployed in OCI are already assigned with the permissions to access Recovery Service for backups. You can assign the optional policies, such as the `tag namespace` policy, or the policy that restricts access to specific users or groups to manage the Recovery Service resources. See Optional Permissions for Oracle Databases in OCI • **Oracle Multicloud Databases** You must assign the permissions required for Oracle Multicloud Database services to use Recovery Service for backups. – Permissions for Oracle AI Database@Azure – Permissions for Oracle AI Database@Google Cloud – Permissions for Oracle AI Database@AWS **Note** For an existing OCI tenancy, you must assign the permissions required for Oracle Database@AWS to use Recovery Service. For a new OCI tenancy, the same permissions are assigned by default. See Permissions Required for Oracle Multicloud Databases to Use Recovery Service for details.

Table 3-1 (Cont.) Mandatory Requirements for Onboarding your Database to Recovery Service

Check	Task
Database encryption	If you are backing up on-premises Oracle Database to Recovery Service, then the TDE wallet must be setup and open irrespective of whether TDE is configured for the database. If pluggable databases (PDBs) use local TDE wallets, then the local TDE wallets must be open. This is required for encrypting backups to Recovery Service. For more information, refer to these sections in the *Transparent Data Encryption Guide*: • Introduction to Transparent Data Encryption • Managing the Keystore and the Master Encryption Key **⚠ Caution** Oracle strongly recommends to use an external key management system, such as Oracle Key Vault. Storing the decryption keys on the same server as the encrypted data allows database server attacks to potentially gain access to the keys and the database. Encrypted backups cannot be recovered if the keys are compromised or stolen. See Protecting On-premises Databases using Oracle Database Zero Data Loss Cloud Protect for detailed steps to add on-premises databases to Recovery Service.
DNS resolution	If you are adding an on-premises Oracle Database to Recovery Service, then a DNS Listener is required to accept DNS requests from the on premises network. The DNS Listener will be used to resolve the Recovery Service backup IP addresses. The FQDN must be registered with the Recovery Service subnet. See Protecting On-premises Databases using Oracle Database Zero Data Loss Cloud Protect for detailed steps to add on-premises databases to Recovery Service.

Table 3-1 (Cont.) Mandatory Requirements for Onboarding your Database to Recovery Service

Check	Task
Recovery Service subnet for Oracle Databases in OCI	For OCI Databases, such as Oracle Exadata Database Service on Dedicated Infrastructure and Oracle Base Database Service, Recovery Service automatically registers the Recovery Service subnet when you enable automatic backups. • For Oracle Exadata Database Service on Dedicated Infrastructure, Recovery Service automatically registers the backup subnet as the Recovery Service subnet. • For Oracle Base Database Service, Recovery Service automatically registers the database subnet as the Recovery Service subnet. Choose one of these options: • Use the Recovery Service subnet that is already registered by the service (recommended). See Getting the Recovery Service Subnet Details of a Protected Database for details. • (Optional) Create your own Recovery Service subnet in the database VCN. Recovery Service requires an IPv4-only subnet in the same virtual cloud network (VCN) where your database resides. First, create your own Recovery Service subnet in the database VCN and then assign the security rules to the Recovery Service subnet that you create. Finally, register the Recovery Service subnet. If you have used network security groups (NSG)s to define the security rules, then you must add the NSGs (maximum five) to the Recovery Service subnet.

Table 3-1 (Cont.) Mandatory Requirements for Onboarding your Database to Recovery Service

Check	Task
Recovery Service subnet for Oracle Multicloud Databases	For an Oracle Multicloud Database, if you have used a network security group (NSG) to the implement security rules for Recovery Service in the database VCN, then you must add the Recovery Service NSG to the Recovery Service subnet. The recommended subnet size is /24. See Register a Recovery Service Subnet for details. Recovery Service supports these Oracle Multicloud Database services: • Oracle AI Database@Azure • Oracle AI Database@Google Cloud • Oracle AI Database@AWS **Note** Network ports **2484** and **8005** enable the network connectivity between Oracle Database@AWS and Recovery Service. In an existing OCI tenancy, ensure to open the network ports **2484** and **8005**. In a new OCI tenancy, the same networks ports are open by default for Oracle Database@AWS. When you onboard an Oracle Database@AWS resource to Recovery Service, the service automatically registers the backup subnet as the Recovery Service subnet. You can either use the Recovery Service subnet that is automatically registered by the service or register your own Recovery Service subnet.
SBT Library for on-premises Oracle Databases	The Cloud Protect Fleet Agent requires the SBT library file `libra.so` to perform database backup and recovery operations with Recovery Service. For Oracle Database 19.27 or later versions and Oracle AI Database 26ai Release Update 23.8 or later versions, the `libra.so` SBT library is available in the `$ORACLE_HOME/lib` directory after you install the database. For Oracle Database 19.26 and earlier versions, ensure to download the `libra.so` SBT library file from My Oracle Support Patch Number 37855779. See Protecting On-premises Databases using Oracle Database Zero Data Loss Cloud Protect for details.

Related Topics

- Autonomous Recovery Service Checklist

Optional Configuration Checklist for Recovery Service

You may choose to configure these additional options for Recovery Service.

Table 3-2 Optional Configuration Checklist for Recovery Service

Check	More Information
Protection policy options	• **Custom Protection Policy** In addition to using Oracle-defined protection policies, you can also create a custom protection policy and define the required retention period (minimum 14 days to maximum 95 days). • **Choose the Backup Storage Location** By default, Recovery Service creates protected databases and related backups in Oracle Cloud. You can optionally override this default behavior for your Oracle Multicloud Databases such as Oracle AI Database@Azure, Oracle AI Database@Google Cloud, and Oracle AI Database@AWS. If you enable the **Store backups in the same cloud provider as the database** option for a custom protection policy, then the policy-linked protected database and backups will be stored in the same cloud provider where the Oracle Database is provisioned. See Multicloud Oracle Database Backup Support for details. • **Enable Retention Lock** Retention locking is an optional feature to safeguard protected database backups. See Using Retention Lock to Protect Backups for details.
IAM users and groups to manage Recovery Service resources	As a tenancy administrator, you can create IAM users and groups to manage Recovery Service related tasks. You can then assign Recovery Service policy statements to the groups. For example, create a group called `recoveryserviceadmin`, and then assign the policy that allows the `recoveryserviceadmin` group to manage protected databases, protection policies, and Recovery Service subnets. • Create a group • Create a user • To add a user to a group

Related Topics

- Autonomous Recovery Service Checklist

Recovery Service Resource Limits

A service limit is the quota or allowance set on a resource. Autonomous Recovery Service has maximum limits for the number of protected databases and the backup storage space utilization. The limits apply to each region.

Table 3-3 Autonomous Recovery Service Resource Limits

Resource	Oracle Universal Credits	Pay As You Go or Trial
Autonomous Recovery Service Protected Database Count	Contact Us	Contact Us
Autonomous Recovery Service Space Used for Recovery Window (GB)	Contact Us	Contact Us

Use the console to review the current service limits and usage information, and request an increase in resource limits, if necessary.

1. In the navigation menu, select **Governance & Administration**, and then select **Tenancy Management**.
2. Select **Limits, Quotas and Usage**.
3. Select **Autonomous Recovery Service** from the **Service** list.

   Review the current limits and usage information.
4. Request a service resource limit increase, if necessary. For Oracle Multicloud Databases, ensure to review and adjust the limits specific to your multicloud subscription from the **Limits, Quotas and Usage** page.

   > ⚠ **Caution**
   >
   > If you do not select the multicloud subscription, then the increased limits will be applied to OCI resources.
5. (Optional) You can also control the resource utilization within compartments. See Quota Policy Quick Start for detailed information.

Related Topics

- Service Limits

Optional Permissions for Oracle Databases in OCI

By default, Oracle Databases in OCI are assigned with the permissions to access Recovery Service. The service can also access the network resources within the database VCN. You

may choose to assign the additional and optional permissions for OCI Databases, as described in this topic.

> **Note**
>
> Recovery Service includes separate IAM policy templates for Oracle AI Database@Azure, Oracle AI Database@Google Cloud, and Oracle AI Database@AWS.
>
> If you are configuring Recovery Service for your Oracle Multicloud Database, then skip this section and proceed to Permissions Required for Oracle Multicloud Databases to Use Recovery Service.

To assign the optional permissions for OCI Databases:

1. In the Policy Builder, select **Autonomous Recovery Service** as the **Policy Use Case**.
2. Select the policy templates or add the policy statements using the manual editor in the Policy Builder. (see Table 3-4, Table 3-5, and Table 3-6)

Table 3-4 Additional Permissions in the Ability to do all things with Autonomous Recovery Service Policy Template

Policy Statement	Create In	Purpose
`Allow service database to manage tagnamespace in tenancy`	Root compartment	Enables the OCI Database Service to access the tag namespace in a tenancy. If you assign this permissions, then a protected database can inherit the tags from the source database.
`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.

Table 3-5 Let users manage protection policies in Autonomous Recovery Service

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
```

The **Let users manage Autonomous Recovery Service subnets** policy template

Table 3-6 Let users manage Autonomous 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.

Permissions Required for Oracle Multicloud Databases to Use Recovery Service

Assign Recovery Service IAM policies that allow Oracle Multicloud Database to send backups to Recovery Service.

In the Policy Builder, select **Autonomous Recovery Service** as the **Policy Use Case**, and then assign one of these policies that is relevant to your Oracle Multicloud Database.

Table 3-7 Recovery Service Policies for Oracle Multicloud Databases

Oracle Multicloud Service	Recovery Service Policy Template and Statements

Oracle AI Database@Azure	**Let Oracle AI Database@Azure use Autonomous Recovery Service for backup**
	
	`Allow service database to manage tagnamespace in tenancy`
	`Allow group admin to manage recovery-service-family in tenancy`
	`Allow service database to use organizations-assigned-subscription in tenancy`
	`where target.subscription.serviceName = 'ORACLEDBATAZURE'`
	
	`ORACLEDBATAZURE` indicates the service name for Oracle AI Database@Azure.

Table 3-7 (Cont.) Recovery Service Policies for Oracle Multicloud Databases

Oracle Multicloud Service	Recovery Service Policy Template and Statements

Oracle AI Database@Google Cloud	**Let Oracle AI Database@Google Cloud use Autonomous Recovery Service for backup**
	
	`Allow service database to manage tagnamespace in tenancy`
	`Allow group admin to manage recovery-service-family in tenancy`
	`Allow service database to use organizations-assigned-subscription in tenancy where target.subscription.serviceName = 'ORACLEDBATGOOGLE'`
	
	`ORACLEDBATGOOGLE` indicates the service name for Oracle AI Database@Google Cloud.

Oracle AI Database@AWS	For an existing OCI tenancy, use the policy builder's manual editor to add these policy statements required for Oracle AI Database@AWS to back up to Recovery Service. For a new OCI tenancy, these permissions are assigned by default.
	
	`Allow service database to manage tagnamespace in tenancy`
	`Allow group admin to manage recovery-service-family in tenancy`
	`Allow service database to use organizations-assigned-subscription in tenancy where target.subscription.serviceName = 'ORACLEDBATAWS'`
	
	`ORACLEDBATAWS` indicates the service name for Oracle AI Database@AWS.

Related Topics

- Multicloud Oracle Database Backup Support
  Recovery Service supports Oracle Multicloud Databases, and also provides the flexibility to store backups in the same cloud location where a multicloud database resides.

Configuring Network Resources for Recovery Service

Create or use an existing IPv4-only subnet for Recovery Service operations in the database VCN. Define security rules to control the backup traffic between your database and Recovery Service.

> **Note**
>
> For Oracle Multicloud Databases, ensure to register the backup subnet as the Recovery Service subnet. The recommended subnet size is **/24**.
>
> Recovery Service supports these Oracle Multicloud Database services:
>
> - Oracle Database@Azure
> - Oracle Database@Google Cloud
> - Oracle Database@AWS
>   Network ports **2484** and **8005** enable the network connectivity between Oracle Database@AWS and Recovery Service. In an existing OCI tenancy, ensure to open the network ports **2484** and **8005**. In a new OCI tenancy, the same network ports are open by default for Oracle Database@AWS.
>
>   When you onboard an Oracle Database@AWS resource to Recovery Service, the service automatically registers the backup subnet as the Recovery Service subnet. You can either use the Recovery Service subnet that is automatically registered by the service or register your own Recovery Service subnet.

- About Using a Private Subnet for Recovery Service Operations
  Recovery Service requires a private subnet in the same virtual cloud network (VCN) where your database resides. The private subnet must include security rules to control the backup network between your database and Recovery Service.
- Review Networking Service Permissions to Configure a Subnet
  Ensure that you have these Networking Service permissions required to create a subnet in the database VCN and to assign security rules for Recovery Service.
- Subnet Size and Security Rules for Recovery Service Subnet
  The security rules are necessary to allow backup traffic between a database and Recovery Service.
- Create a Recovery Service Subnet in the Database VCN
  Use the OCI Console to configure a private subnet for Recovery Service in your database virtual cloud network (VCN).

About Using a Private Subnet for Recovery Service Operations

Recovery Service requires a private subnet in the same virtual cloud network (VCN) where your database resides. The private subnet must include security rules to control the backup network between your database and Recovery Service.

Recommendations for Recovery Service Subnets in the Database VCN

- Your database VCN must have a single private subnet for backups to Recovery Service. The private subnet must reside in the same VCN where the database resides.
- Select an IPv4-only subnet for Recovery Service in your database VCN. Do not select an IPv6-enabled subnet as Recovery Service does not support using an IPv6-enabled subnet. See Creating a Subnet to learn more.
- The recommended subnet size is **/24** (256 IP addresses).
  Recovery Service dynamically assigns the required number of free IP addresses to support the private endpoints. If you have any limitations on the available number of free IP addresses, then use a minimum **/27** subnet size which will allow 32 IP addresses.

You can either create a new private subnet or select any preexisting subnet (of the recommended size) available in the database VCN.

For Oracle Exadata Database Service on Dedicated Infrastructure, by default, the backup subnet is used for Recovery Service operations. For Oracle Base Database Service, the database subnet is also used for backing up to Recovery Service.

- When you enable automatic backups to Autonomous Recovery Service, the service automatically registers the private subnet as a Recovery Service subnet. You can either use the automatically registered Recovery Service subnet or register your own Recovery Service subnet.
  If you have used network security groups (NSGs) to implement the security rules, then you must associate the Recovery Service NSGs to the Recovery Service subnet. See Register a Recovery Service Subnet for details.
- If a Recovery Service subnet contains insufficient number of available IP addresses, then Recovery Service issues an alert message when you try to add a new database. In this scenario, you can add IP addresses by associating multiple subnets to the Recovery Service subnet. See Add or Replace Subnets for a Recovery Service Subnet.
- Your Oracle Cloud database can reside in the same private subnet used by Recovery Service or in a different subnet within the same VCN.

> **Note**
>
> Oracle recommends using a private subnet for backups to Recovery Service. However, it is possible to use a public subnet.

Implementing Security Rules for Recovery Service Subnet

The database VCN requires security rules to allow backup traffic between your database and Recovery Service.

Security rules for the Recovery Service subnet must include stateful ingress rules to allow destination ports 8005 and 2484.

Use these Networking service features to implement security rules:

- Security Lists
  A security list allows you to add security rules at the subnet level.

  In your database VCN, select the security list that is used for the Recovery Service subnet, and add the ingress rules to allow destination ports 8005 and 2484.
- Network Security Groups (NSG)
  Network security groups (NSG) enable granular control over security rules that apply to individual VNICs in a VCN. Recovery Service supports these options to configure security rules using NSGs:
  - Create one NSG for the database VNIC with egress rules to allow ports 2484 and 8005. Add a separate NSG for Recovery Service with ingress rules to allow ports 2484 and 8005. Use this approach if you want to implement network isolation.
  - Create and use a single NSG (with egress and ingress rules) for the database VNIC and Recovery Service.

> **Note**
>
> - If you use network security groups (NSG) to implement security rules or if your database VCN restricts network traffic between subnets, then ensure to add an egress rule for ports 2484 and 8005 from the database NSG or subnet to the Recovery Service NSG or subnet that you create.
> - If you have created NSGs to implement the security rules, then you must associate the Recovery Service NSG to the Recovery Service subnet. See Registering the Recovery Service Subnet for details.
> - If you have configured a security list and an NSG within your database VCN, then the rules defined in the NSGs takes precedence over the rules defined in a security list.

See Comparison of Security Lists and Network Security Groups to learn more.

Related Topics

- Autonomous Recovery Service Checklist

Review Networking Service Permissions to Configure a Subnet

Ensure that you have these Networking Service permissions required to create a subnet in the database VCN and to assign security rules for Recovery Service.

Table 3-8 Networking Service Permissions Required to Create a Private Subnet and Configure Security Rules for Recovery Service

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 3-1 Policy for Network Administrators

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

Subnet Size and Security Rules for Recovery Service Subnet

The security rules are necessary to allow backup traffic between a database and Recovery Service.

> **Note**
>
> - Select an IPv4-only subnet for Recovery Service in your database VCN. Do not select an IPv6-enabled subnet as Recovery Service does not support using an IPv6-enabled subnet. See Creating a Subnet to learn more.
> - You can use network security groups (NSGs) to control the traffic for the Recovery Service subnet. Security rules must include stateful ingress rules to allow destination ports 8005 and 2484.

Table 3-9 Subnet Size and Security Rules for the Recovery Service Subnet

Item	Requirements
Recommended subnet size	/24 (256 IP addresses) If you have any limitations on the available number of free IP addresses, then use a minimum **/27** subnet size which will allow 32 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 you use network security groups (NSG) to implement security rules or if your database VCN restricts network traffic between subnets, then ensure to add an egress rule for ports 2484 and 8005 from the database NSG or subnet to the Recovery Service NSG or subnet that you create.

Create a Recovery Service Subnet in the Database VCN

Use the OCI Console to configure a private subnet for Recovery Service in your database virtual cloud network (VCN).

> **Note**
>
> For Oracle Multicloud Databases, ensure to register the backup subnet as the Recovery Service subnet. The recommended subnet size is **/24**.
>
> Recovery Service supports these Oracle Multicloud Database services:
>
> - Oracle Database@Azure
> - Oracle Database@Google Cloud
> - Oracle Database@AWS
>
> Network ports **2484** and **8005** enable the network connectivity between Oracle Database@AWS and Recovery Service. In an existing OCI tenancy, ensure to open the network ports **2484** and **8005**. In a new OCI tenancy, the same network ports are open by default for Oracle Database@AWS.
>
> When you onboard an Oracle Database@AWS resource to Recovery Service, the service automatically registers the backup subnet as the Recovery Service subnet. You can either use the Recovery Service subnet that is automatically registered by the service or register your own Recovery Service subnet.

1. In the navigation menu, select **Networking**, and then select **Virtual cloud networks** to display the Virtual Cloud Networks list page.
2. Select the VCN in which your database resides.
3. Use these steps to create a Recovery Service subnet with a security list. If you want to use network security groups, then proceed to step 4.
   a. On the details page for the virtual cloud network, select the **Security** tab.
   b. Under **Security Lists**, select the security list that is used for the VCN.
   c. On the details page for the security list, select the **Security rules** tab.

      You must add two ingress rules to allow destination ports **8005** and **2484**.
   d. Select **Add Ingress Rules** and add these details to set up a stateful ingress rule that **allows HTTPS traffic from anywhere**:
      - **Source Type**: `CIDR`
      - **Source CIDR**: Specify the CIDR of the VCN where the database resides.
      - **IP Protocol**: `TCP`
      - **Source Port Range**: `All`
      - **Destination Port Range**: `8005`
      - **Description**: Specify an optional description of the ingress rule to help manage the security rules.
   e. Select **+Another Ingress Rule** and add these details to set up a stateful ingress rule that **allows SQLNet traffic from anywhere**:

- **Source Type**: `CIDR`
- **Source CIDR**: Specify the CIDR of the VCN where the database resides.
- **IP Protocol**: `TCP`.
- **Source Port Range**: `All`
- **Destination Port Range**: `2484`.
- **Description**: Specify an optional description of the ingress rule to help manage the security rules.

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

See: Subnet Size and Security Rules for Recovery Service Subnet for more information.

f. Select **Add Ingress Rules**.

g. On the details page for the virtual cloud network page, select the **Subnets** tab and then select **Create Subnet**.

h. Create a private subnet or select a private subnet that already exists in the database VCN. Oracle recommends a subnet size of /24 (256 IP addresses) for the private subnet.

i. On the details page for the subnet, select the **Security** tab. Under **Security Lists**, add the security list that includes the ingress rules to allow destination ports 8005 and 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.

4. Use these steps to create a Recovery Service subnet with network security groups (NSG).

   a. On the details page for the virtual cloud network, select the **Security** tab and go to the **Network Security Groups** section.

   b. Select **Create Network Security Group**.

   Use one of these supported methods to configure security rules using NSGs:

   - To implement network isolation, create one NSG for the database VNIC (add egress rules to allow ports 2484 and 8005) and a separate NSG for Recovery Service (add ingress rules to allow ports 2484 and 8005).
   - Create and use a single NSG (with egress and ingress rules) for the database VNIC and Recovery Service.

   The Network Security Group page lists the NSGs that you create.

> **Note**
>
> For additional configuration details, refer the relevant OCI Database Service documentation.

> **Note**
>
> - For OCI Databases, Recovery Service automatically registers Recovery Service subnet.
>   You can either use the Recovery Service subnet registered by the service or register your own Recovery Service subnet.
> - If you have implemented security rules using NSGs, then you must register the Recovery Service subnet by adding the Recovery Service NSGs (maximum five).
> - Oracle recommends that you register only a single Recovery Service subnet per VCN.

Registering the Recovery Service Subnet

Use this procedure to register a Recovery Service subnet.

> **Note**
>
> Before you register a Recovery Service subnet:
>
> - Ensure to open these network ports and configure the security rules for Recovery Service.
>   - Port **2484** - Enables SQL*Net connections to the RMAN catalog which is used by Recovery Service.
>   - Port **8005** - Enables backup traffic from the database to Recovery Service.
> - Ensure that you have reviewed and confirmed the mandatory prerequisites described in Mandatory Requirements Checklist for Recovery Service.
> - Ensure that you select an IPv4-only subnet for Recovery Service operations in your database VCN. Do not select an IPv6-enabled subnet as Recovery Service does not support using an IPv6-enabled subnet.
> - For Oracle Databases deployed in OCI, if your backup subnet meets the recommended subnet size (at least 12 free IP addresses), then Recovery Service automatically registers the Recovery Service subnet. If you want to replace the subnet registered by Recovery Service, use the steps described in Add or Replace Subnets for a Recovery Service Subnet.
> - If you have used network security groups (NSG) to implement the security rules for Recovery Service in the database VCN, then you must add the Recovery Service NSGs (maximum five) to the Recovery Service subnet, as described in step 8. The recommended subnet size is **/24**.
>   Recovery Service supports these Oracle Multicloud Database services:
>   - Oracle AI Database@Azure
>   - Oracle AI Database@Google Cloud
>   - Oracle AI Database@AWS
>   Network ports **2484** and **8005** enable the network connectivity between Oracle AI Database@AWS and Recovery Service. In an existing OCI tenancy, ensure to open the network ports **2484** and **8005**. In a new OCI tenancy, the same networks ports are open by default for Oracle AI Database@AWS.
>
>   When you onboard an Oracle AI Database@AWS resource to Recovery Service, the service automatically registers the backup subnet as the Recovery Service subnet. You can either use the Recovery Service subnet that is already registered by the service or use the steps provided in this section to register your own Recovery Service subnet.
> - 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.

1. On the **Recovery Service subnets** list page, select **Register Recovery Service subnet**. See Listing Recovery Service Subnets for detailed steps to access the list page.

2. Enter a name for the Recovery Service subnet. Avoid entering confidential information in the **Name** field.
3. Verify the compartment where you want to create the Recovery Service subnet. Use the **Create in compartment** field to select a different compartment, if necessary.
4. Select the **Compartment** that contains the virtual cloud network (VCN) that you want to use. You can select a VCN from only one compartment at a time.
5. Select the **virtual cloud network**.
6. Under **Subnets**, select these options:
   a. Select the **Compartment** that contains the private subnet that you want to use.
   b. Select the **Subnet** that you have configured for Recovery Service operations in the selected VCN.
7. (Optional) Select **+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.

   See About Using a Private Subnet for Recovery Service Operations for details.
8. Expand **Advanced options** to configure these options:
   - **Network security groups**
     If you have used network security groups (NSG) to implement the security rules for Recovery Service in the database VCN, then you must add the Recovery Service NSGs (maximum five) to the Recovery Service subnet. The Recovery Service NSG can reside in the same compartment or in a different compartment. However, the NSG must belong to the same VCN to which the specified subnet belongs.

     Use these steps to add the Recovery Service NSG to the Recovery Service subnet:
     a. In the **Network security groups** section, select **Use network security groups to control traffic**.
     b. Select the Recovery Service NSG you have created in the database VCN.
     c. Select **+Another network security group** to associate multiple NSGs (maximum five).
   - **Tags**: (Optional) Add one or more tags to the resource. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags. If you are not sure whether to apply tags, skip this option or ask an administrator. You can apply tags later.
9. Select **Register**.

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

You can replace a subnet or add more subnets to support the required number of private endpoints. See Add or Replace Subnets for a Recovery Service Subnet for details.
See Associate NSGs to a Recovery Service Subnet for detailed steps to add NSGs to an existing Recovery Service subnet.

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
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.

4

Key Features of Recovery Service as an Immutable Cloud Service

Recovery Service is an immutable cloud service and an isolated Oracle-managed solution that offers automated backup life cycle management with strict policy-based retention strategy which prevents modification and deletion of backup data. Recovery Service supports Oracle Databases in OCI and multicloud Oracle Databases.

This section provides information about the key features of Recovery Service as an immutable cloud service.

- Security and Availability
  Recovery Service implements the following security best practices to safeguard backup data.
- Immutability and Anomaly Detection
  Recovery Service controls backup retention and performs continuous anomaly detection.

Related Topics

- Enhancing Cloud Cyber Security with Immutable Oracle Zero Data Loss Autonomous Recovery Service

Security and Availability

Recovery Service implements the following security best practices to safeguard backup data.

Tenancy Isolation

The Recovery Service infrastructure is located in an Oracle-managed tenancy which prevents direct access and provides a logical air gap between the backups and the database in your tenancy. The backup automation process leverages a private endpoint which provides an encrypted communication channel that only allows RMAN backup data to be sent and received.

Backup Encryption

Recovery Service enforces backup encryption. Any unencrypted backup data will be rejected by the service. All backups, which include operational backups and long-term retention (LTR) backups, must be encrypted using Transparent Data Encryption (TDE). Backups remain encrypted throughout the backup life cycle and the encryption keys are managed by the database service or the customer. Recovery Service does not have access to the encryption keys.

High-Availability

Recovery Service is built on Oracle Engineered Systems, which provides a fast, scalable, fault-tolerant infrastructure with enhanced security. The infrastructure is deployed in a manner which ensures that backups are located at two physical locations in a region. This ensures that backup and restore operations are highly available.

OCI Identity and Access Management (IAM) Integration with Recovery Service

Identity and Access Management (IAM) enables granular role-based access control. You can configure OCI policies to only allow specific users to access Recovery Service resources.

Observability and Management

Recovery Service is integrated with OCI Observability and Management which allows Metrics Explorer to display historical backup metrics. You can configure alarms to help ensure that the backups are meeting your service level agreements.

Immutability and Anomaly Detection

Recovery Service controls backup retention and performs continuous anomaly detection.

Strict Backup Retention and Immutability

Recovery Service uses protection policies to control backup retention and prevent any modifications to backups. Additionally, a policy can be retention locked to enforce strict backup retention. If the retention lock is in effect, then Recovery Service strictly prohibits the modification or deletion of backups until the retention period expires, and this restriction applies to all users including tenancy administrators. See Retention Lock for details.

Continuous Data Anomaly Detection

Recovery Service performs continuous data anomaly detection of all backups to identify any issues that can compromise data recovery. This helps in case there is malicious user activity or a ransomware attack. Any anomaly issue is immediately reported through alerts in the OCI console and by health status reporting.

Recovery Service performs anomaly detection throughout these different stages of the data protection life cycle:

- At the source database before backups are sent to Recovery Service.
- When backups arrive on Recovery Service.
- When backups are replicated.
- Regularly during the recovery window.

5

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
  Recovery Service stores backups in Oracle Cloud by default.
- 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.

Backup Automation and Storage in Oracle Cloud

Recovery Service stores backups in Oracle Cloud by default.

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

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

When you enable automatic backups for an Oracle Database Service resource, such as an Exadata Cloud Service instance database or an Oracle Base Database DB System, you can set Autonomous Recovery Service as the backup destination. You must assign a Recovery Service protection policy to automate backup retention, cloud storage location, and backup protection.

The database can then transfer backups to Recovery Service for complete and secure data protection.

On-premises Oracle Databases can be onboarded to Recovery Service using the Cloud Protect Fleet Agent. See Protecting On-premises Databases using Oracle Database Zero Data Loss Cloud Protect for details.

You can create an on-demand long-term retention (LTR) backup with Recovery Service and retain the backup for up to **10** years. LTR backups are independent of the automatic backups and stored in the Object Storage Infrequent Access tier. You can restore an LTR backup to create a new database within the retention period.

> **Note**
>
> Recovery Service currently supports long-term retention (LTR) backups only for OCI Databases, Oracle Database@Azure, and Oracle Database@Google Cloud.

Recovery Service enforces a single protection policy for each database. A protection policy defines the number of days to retain database backups for recoverability. A policy also allows you to set a preferred cloud location to store the backups (for multicloud Oracle Databases) and provides the option to set retention locking to safeguard the backups.

> **Note**
>
> For Oracle Multicloud Databases, Recovery Service provides the flexibility to store backups in the same cloud location where the source database resides. See Multicloud Oracle Database Backup Support for more information.

Recovery Service includes a group of Oracle-defined protection policies (**Platinum**, **Gold**, **Silver**, and **Bronze** 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.

> **Note**
>
> 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.

Related Topics

- 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 Oracle Cloud databases in your tenancy.
- About Protection Policies
  Recovery Service uses protection policies to control specific requirements for backup retention, storage location, and backup protection. Use the OCI Console to configure and manage protection policies.
- Create Long-Term Retention Backups with Recovery Service
  You can create long-term retention backups (LTR) for compliance, regulatory, and other business needs. LTR backups are independent of the automatic backups and stored in the Object Storage Infrequent Access tier. You can restore an LTR backup to create a new database within the retention period.

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 used 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 then select **Database Backups** to view and configure these Recovery Service resources:

Protected Databases
The Protected databases page lists the Oracle Databases protected by Recovery Service. Oracle Cloud databases and Oracle Multicloud 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. The Cloud Protect Fleet Agent enables you to add an on-premises Oracle Database to Recovery Service and create the protected database resource.

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. Long-term retention (LTR) backups can be retained for a period ranging from **90** days to **3650** days (10 years).
- 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
  The retention lock option is designed to enforce Recovery Service immutability at the protection policy level. Retention lock is an optional feature to safeguard your protected

database backups from inadvertent changes or malicious damages, such as ransomware attacks.

- Multicloud Oracle Database Backup Support
  Recovery Service supports Oracle Multicloud Databases, and also provides the flexibility to store backups in the same cloud location where a multicloud database resides.

Backup Retention

Recovery Service retains protected database backups for a minimum period of **14** days and a maximum period of **95** days. Long-term retention (LTR) backups can be retained for a period ranging from **90** days to **3650** days (10 years).

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.

You can create a long-term retention (LTR) backup with Recovery Service and define a custom long-term retention period (**90** days to **10** years). See Create Long-Term Retention Backups with Recovery Service for detailed information.

> **Note**
>
> Recovery Service currently supports long-term retention (LTR) backups only for OCI Databases, Oracle Database@Azure, and Oracle Database@Google Cloud.

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

The retention lock option is designed to enforce Recovery Service immutability at the protection policy level. 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.

Multicloud Oracle Database Backup Support

Recovery Service supports Oracle Multicloud Databases, and also provides the flexibility to store backups in the same cloud location where a multicloud database resides.

Recovery Service supports these Oracle Multicloud Database Services:

- Oracle AI Database@Azure
- Oracle AI Database@Google Cloud
- Oracle AI Database@AWS

Review the permissions required for Oracle Multicloud Databases to use Recovery Service for backups.

> **Note**
>
> For an existing OCI tenancy, you must assign the permissions required for Oracle Database@AWS to use Recovery Service. For a new OCI tenancy, the same permissions are assigned by default.

By default, Oracle-managed keys and Recovery Service backups are stored in Oracle Cloud, so that the recovery assets are stored together to support resilient recovery. You can optionally override this default behavior for your Oracle Multicloud Databases.

If you enable the **Store backups in the same cloud provider as the database** option for a protection policy, then the policy-linked protected database and backups will be stored in the same cloud location where the Oracle Database is provisioned. For example, for Oracle AI Database@Azure, Recovery Service stores the associated protected database backups in Azure if you have selected the **Store backups in the same cloud provider as the database** option in the protection policy.

If you do not select the **Store backups in the same cloud provider as the database** for a protection policy, then the policy-linked protected database and backups will be stored in Oracle Cloud even if your Oracle Database is provisioned in a different cloud location.

Related Topics

- About Protection Policies
  Recovery Service uses protection policies to control specific requirements for backup retention, storage location, and backup protection. Use the OCI Console to configure and manage protection policies.

- Creating a Protection Policy
  Create a custom protection policy in Recovery Service.
- 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 Oracle Cloud databases in your tenancy.

Real-time Data Protection

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

After you onboard your Oracle Database to Recovery Service, you can enable the real-time data protection for your database.

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 Databases.

6

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.
- 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 and Deletion Options for Protected Databases
  Recovery Service enables you to recover your database in case of accidental or malicious damages, database termination, or if you disable automatic backups.

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.

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 Oracle Cloud databases in your tenancy.
- Create Long-Term Retention Backups with Recovery Service
  You can create long-term retention backups (LTR) for compliance, regulatory, and other business needs. LTR backups are independent of the automatic backups and stored in the Object Storage Infrequent Access tier. You can restore an LTR backup to create a new database within the retention period.
- Getting the Protection Details of a Database
  A protected database is an Oracle Cloud Database that uses Autonomous Recovery Service as the backup destination.
- Viewing the Backups List for a Protected Database
  View the list of protected database backups using the OCI Console.

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.

> **Note**
>
> Operational backups to two different backup destinations may create data loss scenarios. Therefore, before you enable automatic backups to Recovery Service, you must disable manual backup scripts and processes to other storage destinations.

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 Oracle Cloud databases in your tenancy.

> **Note**
>
> Operational backups to two different backup destinations may create data loss scenarios. Therefore, before you enable automatic backups to Recovery Service, you must disable manual backup scripts and processes to other storage destinations.

Ensure that you have met all the prerequisites as described in Onboarding Oracle Database to Recovery Service.

1. Open the **navigation** menu, select **Oracle Database**, and then select the relevant database service. Navigate to the required database system page.

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

   a. Open the **navigation** menu, select **Oracle Database**, then select **Oracle Exadata Database Service on Dedicated Infrastructure**.

   b. Select **Exadata VM Clusters**.

   c. In the list of VM clusters, find the VM cluster you want to access.

   Follow these steps to access DB systems:

   a. Open the **navigation** menu, select **Oracle Database** and then select **Oracle Base Database Service**.

   b. Select **DB Systems**.

   c. In the list of DB systems, find the DB System you want to access, and then select its name to display details about the system.

2. In the Database information page, from the **Actions** menu, select **Configure automatic backups**.
3. In the **Configure automatic backups** panel, select **Enable automatic backups**.
4. Select these options to configure automatic backups:

   a. **Backup destination** - Select **Autonomous Recovery Service** as the backup destination for the database.

   b. **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.

5. Review the backup **Location** for this database.

   Location indicates the cloud location where the backups will be stored for this database.

- **OCI**: Indicates that Recovery Service will store the database backups in Oracle Cloud.
- **Store backup in the same cloud provider as the database**: Indicates that Recovery Service will store the database backups in the same cloud location where the database is provisioned.

Recovery Service stores backups in Oracle Cloud by default. However, if the database is provisioned in a different cloud location and if you have enabled the **Store backups in the same cloud provider as the database** option in the chosen protection policy, then Recovery Service stores the backups in the same cloud location where the database is provisioned. For example, for Oracle AI Database@Azure, Recovery Service stores the associated protected database backups in Azure if you have selected the **Store backups in the same cloud provider as the database** option in the protection policy. See Multicloud Oracle Database Backup Support for more information.

When the protected database backup is complete, the protected database details page displays the relevant cloud provider **Subscription** details and the exact **Backup location** information. See Getting the Protection Details of a Database for more information.

6. Review whether the chosen protection policy enforces a **Retention lock** to protect the database backups. If the lock is **Enabled**, then Recovery Service prohibits the modification or deletion of backups until the retention period expires.

   See Using Retention Lock to Protect Backups to know more about retention lock and how the retention lock takes effect.

7. **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.

   Refer Oracle Database versions that support using Real-time data protection.

8. **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.

9. Select **Save**.

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

   In the Database information tab, 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 120 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 120 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. Select **Edit Policy** to view the Configure automatic backups pane and change the protection policy.

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

Related Topics

- Managing Protected Databases
  A protected database is an Oracle Database that sends backups to Recovery Service. Recovery Service supports Oracle Databases deployed in Oracle Cloud, Oracle Multicloud, or on-premises. Learn how 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 Databases.

Create Long-Term Retention Backups with Recovery Service

You can create long-term retention backups (LTR) for compliance, regulatory, and other business needs. LTR backups are independent of the automatic backups and stored in the Object Storage Infrequent Access tier. You can restore an LTR backup to create a new database within the retention period.

Recovery Service retains long-term backups for a period ranging from **90** days to **10** years.

> **Note**
>
> Recovery Service currently supports long-term retention (LTR) backups only for OCI Databases, Oracle Database@Azure, and Oracle Database@Google Cloud.

In the OCI Console, create a LTR backup from the Backups tab of the source database's details page. Select **Create Backup** and then select the **Specify long-term backup retention period** option. Specify the long-term retention period in **Days** (90 - 3650) or **Years** (1 - 10) from when the backup was created.

The **Backups** tab of the Database details page lists all the backups, including the **Long-term backup** type that you create.

> **Note**
>
> Refer the relevant OCI Database Service documentation for detailed steps to create LTR backups using the OCI Console.

Recovery Service automatically deletes an LTR backup after the specified retention period ends.

When you terminate a database, Recovery Service retains the LTR backups as per one of these retention options that you have selected while terminating the source database:

- **Delete backups in 72 hours**: Recovery Service retains LTR backups for a maximum period of 72 hours after you terminate the database.
- **Delete based on policy**: Recovery Service retains LTR backups until the specified LTR retention period ends.

Getting the Protection Details of a Database

A protected database is an Oracle Cloud Database that uses Autonomous Recovery Service as the backup destination.

When you enable automatic backups for an Oracle Cloud database and set **Autonomous Recovery Service** as the backup destination, then Recovery Service creates an associated protected database resource.
Use this procedure to review the details of a protected database resource.

Using the Console

1. Perform one of these steps to view the protected database details page:
   - On the **Protected databases** list page, select the protected database that you want to work with. See Listing Protected Databases for detailed steps to access the list page.
   - For databases in OCI and OCI multicloud, open the **navigation** menu, select **Oracle Database**, select the relevant database service, and navigate to the **Database information** page.
     In the **Backups** section, select **Autonomous Recovery Service** in the **Backup destination** field.

     The Protected database details page displays the information about the protected database.
   - Review these details in the **Details** tab.
     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 120 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 120 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.
- **Management type**: Indicates how the source database is deployed and managed. The values are:
  - **Provisioned through Oracle Cloud**: Indicates that the source database is managed in Oracle Cloud or in a Oracle Multicloud environment.
  - **Provisioned through Cloud Protect**: Indicates that the database is deployed on-premises and managed by the Cloud Protect Fleet Agent. See Protecting On-premises Databases using Oracle Database Zero Data Loss Cloud Protect for detailed information.
- **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

- **Recovery window current space used**: The amount of storage space that is currently used to meet the recovery window goal for the protected database.
- **Recovery window projected space used for policy**: The estimated amount of storage space that is required to meet the recovery window goal as per the retention period defined in the protection policy.
- **Long-term retention current space used**: If you have created long-term retention (LTR) backups for the database, then this field displays the amount of storage space that is currently used to store the LTR backups.

> **Note**
>
> Recovery Service currently supports long-term retention (LTR) backups only for OCI Databases, Oracle Database@Azure, and Oracle Database@Google Cloud.

- **Protected database size**: The size of the database that is being protected.

Database backup summary

> **Note**
>
> The **Database backup summary** section is displayed only for Oracle Databases deployed in Oracle Cloud or Oracle Multicloud.

- **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
- **Last backup duration**: The time taken to complete the most recent successful backup

Protected database

- **Database details**: For databases deployed on Oracle Cloud or Oracle Multicloud, this field displays the database name as a hyperlink. Click the link to view the associated Database Details page.
- **DB unique name**: The globally unique name of the database.
- **Database name**: The name used to identify the database. This field is applicable only for on-premises Oracle Databases.
- **Database Identifier**: The unique identifier of the database. This field is applicable only for on-premises Oracle Databases.
- **Database version**: The Oracle Database version.

General information

- **Subscription**: The cloud provider subscription with which the protected database resource is associated. For example, this field displays the Microsoft Azure subscription information for a Oracle AI Database@Azure service resource linked with this protected database.
- **Backup location**: Indicates the backup storage location for the protected database.
  The backup location is controlled by the **Store backups in the same cloud provider as the database** option in the protection policy linked with the protected database. If the option is enabled, then the protected database backups will be stored in the same cloud provider as the database. See Enable Automatic Backups to Recovery Service for details.

  The **Backup location** field displays one of these values:

  * **Oracle Cloud** - Indicates that the protected database backups are stored in OCI (Oracle Cloud), which is the default storage location for protected database backups.
  * **Microsoft Azure** - Indicates that the protected database is associated with a Oracle AI Database@Azure service database and its backups are also stored in Microsoft Azure.
  * **Google Cloud** - Indicates that the protected database is associated with a Oracle AI Database@Google Cloud service database and its backups are also stored in Google Cloud.

    - **Amazon Web Services** - Indicates that the protected database is associated with a Oracle AI Database@AWS service database and its backups are also stored in Amazon Web Services.
  - **OCID**: Select **Copy** to copy the OCID of the protected database. The OCID value is displayed only for Oracle Cloud or Oracle Multicloud Databases.
  - **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

2. Select the **Network details** tab to view the Recovery Service subnets associated with the protected database.
3. Select the **Monitoring** tab to view the default metric charts to monitor the protected database. See, Available Metrics: oci_recovery_service for details.
4. Select the **Work requests** tab to view the work requests associated with the protected database.
5. Select the **Tags** section to view the tags applied to the protected database resource item.

Using the CLI

Use the oci recovery protected-database get

See Autonomous Recovery Service CLI Command Reference for a complete list of parameters and values for CLI commands.

Using the API

Run the GetProtectedDatabase API operations to view the details of a protected database.

Viewing the Backups List for a Protected Database

View the list of protected database backups using the OCI Console.

1. In the **navigation** menu, select **Oracle Database** and then select the relevant database service. Select the source database resource that you want to work with.

   Consider the following examples:

   - **Exadata VM Clusters**: Under **Oracle Exadata Database Service on Dedicated Infrastructure**, select **Exadata VM Clusters**. In the list of VM clusters, select the VM cluster you want to work with.
   - **DB Systems**: Under **Oracle Base Database (VM, BM)**, select **DB Systems**. In the list of Exadata DB systems, select the DB system that you want to work with. Select the **Databases** tab and then select the relevant source database.

   The database details page is displayed.
2. Select the **Backups** tab.
3. The Backups list displays detailed information about each operational backup and long-term retention (LTR) backups that you create.

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 the automatic 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 the automatic backups created by Recovery Service.

> **Note**
>
> The in-place restore options described in this section do not apply to long-term retention (LTR) backups. You can restore an LTR backup to create a new database. See Create a DB System From a Backup Using the Console for detailed information.

1. Open the **navigation** menu, select **Oracle Database** and then select the relevant database service. Navigate to the required database system details page.
2. Select the name of the required database.

   For example, to restore a bare metal or virtual machine DB system database, select **Oracle Database**, **Oracle Base Database (VM, BM)** and then select a DB system and database that you want to restore.
3. On the details page, from the **Actions** menu at the top of the table, select **Restore**.
4. Select one of these 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.
5. Select **Restore** and confirm the action.

Backup Retention and Deletion Options for Protected Databases

Recovery Service enables you to recover your database in case of accidental or malicious damages, database termination, or if you disable automatic backups.

- **Recovery from Accidental or Malicious Damages**
  In case of accidental or malicious damages to a database, Recovery Service supports recovery from backups for a period of 72 hours (3-days).
- **Recovery Upon Database Termination**
  In the OCI Console, you can select one of these options to retain the 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 the protected database backups as per the **Backup retention period** defined in the associated protection policy. Long-term retention (LTR) backups are retained as per the specified LTR backup retention period.
  - **Retain backups for 72 hours, then delete** - Recovery Service will retain all backups, including LTR backups, for a period of 72 hours (3 days) after you terminate a database.

  After you terminate a 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. Recovery Service automatically deletes the protected database resource and the database backups after the scheduled delay ends.
- **Recovery After You Disable Automatic Backups**
  If you disable automatic backups for a database, then Recovery Service continues to retain the database backups as per the backup retention period defined in the protection policy.

  The protected database resource enters the **Delete Scheduled** state and remains in this state for the period defined in the protection policy. Recovery Service automatically deletes the protected database and the associated backups after the backup retention period 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.

7

Protecting On-premises Databases using Oracle Database Zero Data Loss Cloud Protect

Oracle Database Zero Data Loss Cloud Protect offers on-premises database protection using Oracle Zero Data Loss Autonomous Recovery Service deployed in OCI. This new feature provides real-time transaction protection, logically air-gapped immutable backups, and enables fast, point-in-time recovery to any location.

- About Data Protection for On-Premises Databases
  The Cloud Protect Fleet Agent is a SQLcl based tool that enables on-premises Oracle Databases to use Recovery Service for data protection.
- Prerequisites for Cloud Protect Fleet Agent
  There are specific requirements for using the Cloud Protect Fleet Agent.
- Preparing to Use Cloud Protect Fleet Agent with SQLcl
  The Cloud Protect Fleet Agent uses the SQLcl interface for on-premises database interaction with Recovery Service. Learn how to download, install, and set up SQLcl.
- Configuring OCI Authentication for Database Access to Recovery Service
  Oracle recommends that you configure OCI API authentication for on-premises databases to access Recovery Service.
- Add On-Premises Database to Recovery Service Using Cloud Protect
  The Cloud Protect Fleet Agent registers the on-premises database with Recovery Service to create a protected database.
- Viewing On-Premises Database Protection Summary
  View the latest protection summary of an on-premises Oracle Database.
- Restore On-Premises Database Using Backups from Recovery Service
  Use SQLcl to prepare the RMAN environment for restores using backups stored in Recovery Service.
- Using the OCI Console to View Protected Database Details
  After you add an on-premises database to Recovery Service, log in to the OCI Console and follow these steps to view the protected database details.

About Data Protection for On-Premises Databases

The Cloud Protect Fleet Agent is a SQLcl based tool that enables on-premises Oracle Databases to use Recovery Service for data protection.

To use the Cloud Protect Fleet Agent, your database must be deployed on a Linux x86-64 platform. The supported Oracle Database versions are Oracle Database 19.18 or later and Oracle AI Database 26ai Release Update 23.4 or later.

The Cloud Protect Fleet Agent leverages the Oracle SQLcl (SQL Developer Command Line) interface for on-premises database interactions with Recovery Service. You can invoke the Cloud Protect Fleet Agent commands in SQLcl using `rcv`.

The Cloud Protect Fleet Agent can automatically detect all database clients and add the databases to Recovery Service, and help to maintain data protection. You can use a simple SQLcl command to retrieve the latest protection status.

First, review and confirm the specific Prerequisites for Cloud Protect Fleet Agent, and then perform these one-time configuration tasks to add your on-premises database to Recovery Service:

1. Set up Cloud Protect Fleet Agent on the target database server.
2. Configure OCI API authentication to allow on-premises database to securely access Recovery Service.
3. Add database to Recovery Service and enable Real-time data protection (recommended).
4. Perform restore and recovery operations using familiar RMAN commands.

After you add an on-premises database to Recovery Service, use the Oracle Cloud Infrastructure (OCI) Monitoring service (alarms feature) to configure notifications that alert you when metrics meet your specified criteria. See Using Alarms to Monitor Protected Databases for details.

Prerequisites for Cloud Protect Fleet Agent

There are specific requirements for using the Cloud Protect Fleet Agent.

Table 7-1 Prerequisites to Use Cloud Protect Fleet Agent

Requirement	More Information
Mandatory requirements for Recovery Service	Ensure to review and confirm the mandatory requirements to onboard databases to Recovery Service.
Oracle Cloud account, tenancy, and subscription	Get an Oracle Cloud Account
Supported Operating System/platform	Linux x86-64
Supported Oracle Database Releases	Ensure that the target database compatibility level (the `COMPATIBLE` initialization parameter) is set to 19.0.0 or higher. You can use the Cloud Protect Fleet Agent with Oracle Databases provisioned with any of these releases: • Oracle AI Database 26ai Release Update 23.4 or later • Oracle Database 19c Release Update 19.18 or later

Table 7-1 (Cont.) Prerequisites to Use Cloud Protect Fleet Agent

Requirement	More Information
Database encryption	If you are backing up on-premises Oracle Database to Recovery Service, then the TDE wallet must be setup and open irrespective of whether TDE is configured for the database. If pluggable databases (PDBs) use local TDE wallets, then the local TDE wallets must be open. This is required for encrypting backups to Recovery Service. For more information, refer to these sections in the *Transparent Data Encryption Guide*: • Introduction to Transparent Data Encryption • Managing the Keystore and the Master Encryption Key **⚠ Caution** Oracle strongly recommends to use an external key management system, such as Oracle Key Vault. Storing the decryption keys on the same server as the encrypted data allows database server attacks to potentially gain access to the keys and the database. Encrypted backups cannot be recovered if the keys are compromised or stolen.
DNS resolution	If you are adding an on-premises Oracle Database to Recovery Service, then a DNS Listener is required to accept DNS requests from the on premises network. The DNS Listener will be used to resolve the Recovery Service backup IP addresses. The FQDN must be registered with the Recovery Service subnet.

Table 7-1 (Cont.) Prerequisites to Use Cloud Protect Fleet Agent

Requirement	More Information
SBT Library	Cloud Protect Fleet Agent requires the SBT library file `libra.so` to perform backup and recovery operations with Recovery Service. For Oracle Database 19.27 or later versions and Oracle AI Database 26ai Release Update 23.8 or later versions, the `libra.so` SBT library is available in the `$ORACLE_HOME/lib` directory after you install the database. For Oracle Database 19.26 and earlier versions, you must download the `libra.so` SBT library file from My Oracle Support Patch Number 37855779.

Preparing to Use Cloud Protect Fleet Agent with SQLcl

The Cloud Protect Fleet Agent uses the SQLcl interface for on-premises database interaction with Recovery Service. Learn how to download, install, and set up SQLcl.

- Download and Set Up Cloud Protect Fleet Agent (SQLcl)
  Use these steps to download the RPM required to install the Cloud Protect Fleet Agent (SQLcl) on the target database server.
- Cloud Protect Fleet Agent Commands in SQLcl
  Review the Cloud Protect Fleet Agent commands in SQLcl, and their usage.

Download and Set Up Cloud Protect Fleet Agent (SQLcl)

Use these steps to download the RPM required to install the Cloud Protect Fleet Agent (SQLcl) on the target database server.

1. Go to the Oracle yum site and download the latest RPM required to install SQLcl. For example: `sqlcl-25.4.2-1.el8.noarch.rpm`.
   - **Oracle Linux 8**: SQLcl on Oracle Linux 8 (x86-64)
   - **Oracle Linux 9**: SQLcl on Oracle Linux 9 (x86-64)
2. Install the RPM on each compute node, as shown in this example.

```
root@computenode# rpm -ivh /test/sqlcl-linux-25.3.0-1.el8.x86_64.rpm



Verifying...                          ################################
[100%]
Preparing...                          ################################
[100%]
Updating / installing...
1:sqlcl-linux-25.3.0-1.el8         ################################ [100%]
```

3. Enable the scheduler to start on system start up, as shown in this example.

```
root@computenode# systemctl enable sql-scheduler


Synchronizing state of sql-scheduler.service with SysV service script
with /usr/lib/systemd/systemd-sysv-install.
  Executing: /usr/lib/systemd/systemd-sysv-install enable sql-scheduler
  Created symlink /etc/systemd/system/multi-user.target.wants/sql-
scheduler.service → /etc/systemd/system/sql-scheduler.service.
  Created symlink /etc/systemd/system/graphical.target.wants/sql-
scheduler.service → /etc/systemd/system/sql-scheduler.service.
```

4. Start the scheduler.

```
root@computenode# systemctl start sql-scheduler
```

5. Check the status of the scheduler, as shown in this example.

```
[root@nshqaw20adm05 ~]# systemctl status sql-scheduler



   sql-scheduler.service - SQLcl scheduler services
   Loaded: loaded (/etc/systemd/system/sql-scheduler.service; enabled;
vendor preset: disabled)
   Active: active (running) since Mon 2025-10-06 00:25:33 EDT;
```

6. Set the SQLcl binary for the Oracle software owner user (`oracle`).

   Add the SQLcl binary location in the `PATH` environment variable, as shown below.

```
export PATH=/opt/oracle/sqlcl/bin:$PATH
```

Related Topics

- Using a Unix Service to Manage Daemons

Cloud Protect Fleet Agent Commands in SQLcl

Review the Cloud Protect Fleet Agent commands in SQLcl, and their usage.

Use this format to run the Cloud Protect Fleet Agent commands:

```
SQL> rcv <action> <object> [options]
```

- `rcv` - Use `rcv` to invoke the Cloud Protect Fleet Agent commands in SQLcl.
- `action` - Specifies the action you want to perform, such as `backup`, `configure`, or `add`.
- `object` - Specifies the object to perform the action. Example, `database`, `recovery_service_subnet`, or `protection_policy`.
- `options` - Specifies an option to run the command.

Run `help rcv` to preview the list of Cloud Protect Fleet Agent commands.

```
SQL> help rcv
```

> **Note**
>
> Ensure to set the `ORACLE_HOME` environmental variable before you run the `rcv` commands in SQLcl. For example,
>
> ```
> ORACLE_HOME=/u01/app/oracle/product/19.25.0.0/dbhome_3
> ```
>
> In an Oracle RAC environment, set the `ORACLE_HOME` environmental variable on the current node.

Table 7-2 Summary of Cloud Protect Fleet Agent Commands

Action	Purpose
`add` *`object`*	Adds an object such as a database or a protection policy.
`configure` *`object`*	Configures an object such as a Recovery Service subnet or schedule.
`remove` *`object`*	Removes an object such as a protection policy or a database.
`show` *`object`*	Displays the information about an object, such as the protection details of a database.
`backup` *`object`*	Backs up a database.
`run` *`object`*	Runs checks on a database.
`import` *`object`*	Imports an object such as a database.

Table 7-3 add *<object>*

add *<object>*	Requires SYSBACKUP Privileges?
`add database`	No
`add protection_policy`	No
`add recovery_service_subnet`	No
`add realtime_redo`	Yes
`add schedule`	Yes

Table 7-4 configure *<object>*

configure *<object>*	Requires SYSBACKUP Privileges?
`configure database`	Yes
`configure rman`	Yes
`configure rman_env`	Yes
`configure protection_policy`	No

Table 7-4 (Cont.) configure <*object*>

configure <*object*>	Requires SYSBACKUP Privileges?
`configure recovery_service_subnet`	No
`configure schedule`	Yes
`configure authentication`	No

Table 7-5 remove <*object*>

remove <*object*>	Requires SYSBACKUP Privileges?
`remove database`	Yes
`remove protection_policy`	No
`remove realtime_redo`	Yes
`remove schedule`	Yes

Table 7-6 show <*object*>

show <*object*>	Requires SYSBACKUP Privileges?
`show database`	Yes
`show rman`	Yes
`show protection_policy`	No
`show recovery_service_subnet`	No
`show schedule`	Yes
`show authentication`	No
`show restore_range`	Yes

Table 7-7 backup <*object*>

backup <*object*>	Requires SYSBACKUP Privileges?
`backup database`	Yes

Table 7-8 run <*object*>

run <*object*>	Requires SYSBACKUP Privileges?
`run checks`	Yes

Table 7-9 import <*object*>

import <*object*>	Requires SYSBACKUP Privileges?
`import database`	No

Configuring OCI Authentication for Database Access to Recovery Service

Oracle recommends that you configure OCI API authentication for on-premises databases to access Recovery Service.

1. In the OCI Console, add the API signing key and generate the configuration file for the API signing key. See Adding an API Signing Key for details.
2. Store the API keys and the configuration file in a secure directory that is accessible to the `Oracle` user.
3. Start up SQLcl.

   ```
   /opt/oracle/sqlcl/bin/sql /nolog
   ```

4. Run the `rcv CONFIGURE AUTHENTICATION` command and specify the directory location containing API signing key and configuration file, as shown below.

   ```
   SQL> rcv configure authentication -method api_key -oci_config <API
   configuration file location>
   ```

Related Topics

- Working with API Keys
- How to Generate an API Signing Key

Add On-Premises Database to Recovery Service Using Cloud Protect

The Cloud Protect Fleet Agent registers the on-premises database with Recovery Service to create a protected database.

In SQLcl, run the `rcv add database` command to automatically detect the database clients and generate a configuration (JSON) file. The configuration file includes the parameters required to add the database to Recovery Service. Then, run the `rcv add database` command again, along with the configuration file, to register the database with Recovery Service and create the protected database. Oracle recommends that you follow this automated method to add databases to Recovery Service.
Another method is by manually connecting to every database (with `SYSBACKUP` privileges) and then using the `rcv add database` command to add each database individually.

> **Note**
>
> Cloud Protect assigns the Oracle defined **Bronze** protection policy as the default policy for all databases. You can change the default policy in the configuration file before adding the database.

Use these steps to add an on-premises database to Recovery Service.

1. Log in to the database as the Oracle software owner user (`oracle`). Verify that the `ORACLE_HOME` environmental variable is set.

   In this example, the `ORACLE_HOME` environmental variable points to the directory where the Oracle database client is installed.

   ```
   echo $ORACLE_HOME
   /u01/app/oracle/product/19.0.0.0/dbhome_1
   ```

2. Start SQLcl as an `oracle` user.

   In an Oracle RAC environment, start SQLcl only on the first compute node.

   ```
   oracle@host$ /opt/oracle/sqlcl/bin/sql /nolog
   SQL>
   ```

3. Run the `rcv add database` command along with these *options* to automatically detect the databases and generate a configuration file.

   - `-auto_discover`
   - `-generate_config_only`
   - `-compartment_id <COMPARTMENT_OCID>`
   - `-recovery_service_subnets <SUBNET_OCID>`

   ```
   SQL> rcv add database -auto_discover -generate_config_only -compartment_id
   <COMPARTMENT_OCID> -recovery_service_subnets <SUBNET_OCID>
   ```

   In this sample output, the `rcv add database` command generates the `add_database.json` configuration file which contains the compartment ID and Recovery Service subnet ID values required to create protected database. The **Bronze** policy is assigned as the default protection policy.

   ```
   2025-08-15 09:22:16: Created config JSON /u01/app/oracle/rcv/
   add_database.json
   2025-08-15 09:22:16: You can onboard a database by running 'rcv add
   database -config /u01/app/oracle/rcv/add_database.json'
   ```

   Sample contents of the `add_database.json` configuration file.

   ```
   [
       {
           "dbUniqueName": "DB1",
           "displayName": "DB1",
           "compartmentId": "ocid1.compartment.oc1..aaa...",
           "protectionPolicy": "ocid1.recoveryservicepolicy.region1..aaa...",
           "sbtLibrary": "/u01/app/oracle/product/19.24.0.0/dbhome_2/lib/
   libra.so",
           "oracleHome": "/u01/app/oracle/product/19.24.0.0/dbhome_2",
           "oracleSid": "DB1",
           "recoveryServiceSubnets": [
               "ocid1.subnet.oc1.phx.aaa..."
           ]
       },
   ```

```
    {
        "dbUniqueName": "DB2",
        "displayName": "DB2",
        "compartmentId": "ocid1.compartment.oc1..aaaaaa...",
        "protectionPolicy": "ocid1.recoveryservicepolicy.region1..aaa...",
        "sbtLibrary": "/u01/app/oracle/product/19.27.0.0/dbhome_1/lib/
libra.so",
        "oracleHome": "/u01/app/oracle/product/19.27.0.0/dbhome_1",
        "oracleSid": "DB2",
        "recoveryServiceSubnets": [
            "ocid1.subnet.oc1.phx.aaa..."
        ]
    },
    {
        "dbUniqueName": "DB3",
        "displayName": "DB3",
        "compartmentId": "ocid1.compartment.oc1..aaa...",
        "protectionPolicy": "ocid1.recoveryservicepolicy.region1..aaa...",
        "sbtLibrary": "/u01/app/oracle/product/19.26.0.0/dbhome_3/lib/
libra.so",
        "oracleHome": "/u01/app/oracle/product/19.26.0.0/dbhome_3",
        "oracleSid": "DB3",
        "recoveryServiceSubnets": [
            "ocid1.subnet.oc1.phx.aaa..."
        ]
    }
]
SQL>
```

4. (Optional) Edit the configuration file to modify the assigned values, if necessary.

   ```
   edit /u01/app/oracle/rcv/add_database.json
   ```

5. Run the `rcv add database` command again and specify the configuration file.

   ```
   SQL> rcv add database -config <configuration file location>
   ```

   In this example, you specify the path for the `add_database.json` configuration file.

   ```
   SQL> rcv add database -config /u01/app/oracle/rcv/add_database.json
   ```

   The Cloud Protect Fleet Agent performs these steps internally:

   - Verifies the prerequisites for adding the database to Recovery Service.
   - Creates a `SYSBACKUP` user and password, if the `SYSBACKUP` user does not exist.

> **Note**
>
> The `SYSBACKUP` user and password is required for the Cloud Protect Fleet Agent to establish a named connection to the database. Use this command to connect to the database as the `SYSBACKUP` user:
>
> `/opt/oracle/sqlcl/bin/sql -name <DB_UNIQUE_NAME>_rcv_conn`
>
> *DB_UNIQUE_NAME* is the globally unique name of the database.

- Generates a random password for the `VPC` user account. The VPC user credentials are required to authenticate database access to the RMAN recovery catalog.
- Invokes the Recovery Service API to create a protected database resource.
- Invokes the API every 10 minutes until the protected database enters the **Active** life cycle state.
- Extracts the protected database network connection details and updates the configuration file.
- Registers the database in Recovery Appliance of Recovery Service using RMAN
- Configures the protected database with Cloud Protect.
- Cloud Protect maintains data protection.

6. (Recommended) Enable Real-time data protection.
   a. Use SQLcl to log in to the database as a user with the `SYSBACKUP` privileges.

      ```
      oracle@host$ /opt/oracle/sqlcl/bin/sql -name <DB_UNIQUE_NAME>_rcv_conn
      ```

      In this example, you connect to the database `c1db1`.

      ```
      oracle@host$ /opt/oracle/sqlcl/bin/sql -name c1db1_rcv_conn
      ```

   b. Run the `rcv realtime_redo` command.

      ```
      SQL> rcv add realtime_redo
      ```

      Review the sample output for the database `c1db1`.

      ```
      2025-08-15 10:33:48: Log file: /u01/app/oracle/rcv/dbs/c1db1/log/
      add_realtime_redo_c1db1.20250815.103348.log
      SQL>
      ```

   c. Restart the database for the changes to take effect.

Viewing On-Premises Database Protection Summary

View the latest protection summary of an on-premises Oracle Database.

1. Use SQLcl to log in to the database as the `SYSBACKUP` user.

   ```
   /opt/oracle/sqlcl/bin/sql -name <DB_UNIQUE_NAME>_rcv_conn
   ```

   In this example, you log in to the database `c1db1`.

   ```
   /opt/oracle/sqlcl/bin/sql -name c1db1_rcv_conn
   ```

2. Run the `rcv show database` command.

   ```
   SQL> rcv show database
   ```

   Review the sample output. This sample output indicates the **Protected** health status for the `c1db1` database.

   ```
   2025-08-15 10:42:56: DB Unique Name:    c1db1
   2025-08-15 10:42:56: Health:            Protected
   2025-08-15 10:42:56: Health Details:    Protected Database is Healthy.
   Last updated on Fri Aug 15 14:34:28 UTC 2025
   ...
   ```

> **Note**
>
> The protected database **Health** indicates one of these values:
>
> - 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 120 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 120 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.

Restore On-Premises Database Using Backups from Recovery Service

Use SQLcl to prepare the RMAN environment for restores using backups stored in Recovery Service.

1. Use SQLcl to log in to the database as a user with `SYSBACKUP` privileges.

   ```
   /opt/oracle/sqlcl/bin/sql -name <DB_UNIQUE_NAME>_rcv_conn
   ```

In this example, you connect to the database `c1db1`.

```
/opt/oracle/sqlcl/bin/sql -name c1db1_rcv_conn
```

2. Run the `rcv show restore_range` command to view the restore range of the database for backups stored in Recovery Service.

   ```
   SQL> rcv show restore_range
   ```

3. Run the `rcv configure rman_env` command to generate the `rcv_restore_template.rman` script.

   ```
   rcv configure rman_env
   ```

   Review the sample output. In this example, the `rcv configure rman_env` command creates the `rcv_restore_template.rman` script.

   ```
   2025-09-17 23:41:35: Generated template backup script /u01/app/
   oracle/rcv/dbs/c1db1/rman_env/rcv_restore_template.rman
   2025-09-17 23:41:35: Edit script with RMAN commands to execute.
   2025-09-17 23:41:35: To run script: source /u01/app/oracle/rcv/dbs/c1db1/
   rman_env/rman_env.sh
   2025-09-17 23:41:35: rman target / catalog /@c1db1_DBRS cmdfile /u01/app/
   oracle/rcv/dbs/c1db1/rman_env/rcv_restore_template.rman
   2025-09-17 23:41:35: rcv configure rman_env completed successfully
   ```

4. Edit the RMAN script template `rcv_restore_template.rman` to include the required RMAN commands.
5. Source the RMAN environment script and connect RMAN to the target database and the recovery catalog.

   In this example, you source the `rman_env.sh` script and then connect RMAN to the target database `c1db1`.

   ```
   [oracle@host ~] source /u01/app/oracle/rcv/dbs/c1db1/rman_env/rman_env.sh
   [oracle@host ~] rman target / catalog /@c1db1_DBRS cmdfile /u01/app/
   oracle/rcv/dbs/c1db1/rman_env/rcv_restore_template.rman

   Recovery Manager: Release 19.0.0.0.0 - Production
   ...
   connected to target database: C1DB1 (DBID=1111401884)
   ...
   RMAN>
   ```

   You can now use regular RMAN commands to `RESTORE` or `LIST` backups.

   See *Oracle Database Backup and Recovery Reference* to learn about RMAN commands.

Using the OCI Console to View Protected Database Details

After you add an on-premises database to Recovery Service, log in to the OCI Console and follow these steps to view the protected database details.

Using the Console

1. Perform one of these steps to view the protected database details page:
   - On the **Protected databases** list page, select the protected database that you want to work with. See Listing Protected Databases for detailed steps to access the list page.
   - For databases in OCI and OCI multicloud, open the **navigation** menu, select **Oracle Database**, select the relevant database service, and navigate to the **Database information** page.
     In the **Backups** section, select **Autonomous Recovery Service** in the **Backup destination** field.

     The Protected database details page displays the information about the protected database.
   - Review these details in the **Details** tab.
     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 120 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 120 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.
     - **Management type**: Indicates how the source database is deployed and managed. The values are:
       * **Provisioned through Oracle Cloud**: Indicates that the source database is managed in Oracle Cloud or in a Oracle Multicloud environment.
       * **Provisioned through Cloud Protect**: Indicates that the database is deployed on-premises and managed by the Cloud Protect Fleet Agent. See Protecting On-premises Databases using Oracle Database Zero Data Loss Cloud Protect for detailed information.

- **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

- **Recovery window current space used**: The amount of storage space that is currently used to meet the recovery window goal for the protected database.
- **Recovery window projected space used for policy**: The estimated amount of storage space that is required to meet the recovery window goal as per the retention period defined in the protection policy.
- **Long-term retention current space used**: If you have created long-term retention (LTR) backups for the database, then this field displays the amount of storage space that is currently used to store the LTR backups.

> **Note**
>
> Recovery Service currently supports long-term retention (LTR) backups only for OCI Databases, Oracle Database@Azure, and Oracle Database@Google Cloud.

- **Protected database size**: The size of the database that is being protected.

Database backup summary

> **Note**
>
> The **Database backup summary** section is displayed only for Oracle Databases deployed in Oracle Cloud or Oracle Multicloud.

- **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
- **Last backup duration**: The time taken to complete the most recent successful backup

Protected database

- **Database details**: For databases deployed on Oracle Cloud or Oracle Multicloud, this field displays the database name as a hyperlink. Click the link to view the associated Database Details page.
- **DB unique name**: The globally unique name of the database.
- **Database name**: The name used to identify the database. This field is applicable only for on-premises Oracle Databases.

- **Database Identifier**: The unique identifier of the database. This field is applicable only for on-premises Oracle Databases.
- **Database version**: The Oracle Database version.

General information

- **Subscription**: The cloud provider subscription with which the protected database resource is associated. For example, this field displays the Microsoft Azure subscription information for a Oracle AI Database@Azure service resource linked with this protected database.
- **Backup location**: Indicates the backup storage location for the protected database.
  The backup location is controlled by the **Store backups in the same cloud provider as the database** option in the protection policy linked with the protected database. If the option is enabled, then the protected database backups will be stored in the same cloud provider as the database. See Enable Automatic Backups to Recovery Service for details.

  The **Backup location** field displays one of these values:

  * **Oracle Cloud** - Indicates that the protected database backups are stored in OCI (Oracle Cloud), which is the default storage location for protected database backups.
  * **Microsoft Azure** - Indicates that the protected database is associated with a Oracle AI Database@Azure service database and its backups are also stored in Microsoft Azure.
  * **Google Cloud** - Indicates that the protected database is associated with a Oracle AI Database@Google Cloud service database and its backups are also stored in Google Cloud.
  * **Amazon Web Services** - Indicates that the protected database is associated with a Oracle AI Database@AWS service database and its backups are also stored in Amazon Web Services.
- **OCID**: Select **Copy** to copy the OCID of the protected database. The OCID value is displayed only for Oracle Cloud or Oracle Multicloud Databases.
- **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

2. Select the **Network details** tab to view the Recovery Service subnets associated with the protected database.
3. Select the **Monitoring** tab to view the default metric charts to monitor the protected database. See, Available Metrics: oci_recovery_service for details.
4. Select the **Work requests** tab to view the work requests associated with the protected database.
5. Select the **Tags** section to view the tags applied to the protected database resource item.

8

Managing Protected Databases

A protected database is an Oracle Database that sends backups to Recovery Service. Recovery Service supports Oracle Databases deployed in Oracle Cloud, Oracle Multicloud, or on-premises. Learn how to view and monitor the protected databases in your tenancy.

- About Protected Databases
  A protected database is an Oracle Database that sends backups to Recovery Service.
- Listing Protected Databases
  View the protected databases in a specific compartment in Recovery Service.
- Getting Protected Database Details
  View the details of a protected database.
- Getting the Recovery Service Subnet Details of a Protected Database
  View the Recovery Service subnet associated with a protected database.
- Getting the Protection Policy Details of a Protected Database
  View the protection policy that defines the backup retention rules for a protected database.
- 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 Databases.
- Getting Protected Database Network Connection Details
  Download the network service configuration details for a specified protected database.
- Moving a Protected Database
  Move a protected database to a different compartment in your tenancy.
- Scheduled Deletion of a Protected Database
  Recovery Service schedules the deletion of a protected database resource and the associated backups.

About Protected Databases

A protected database is an Oracle Database that sends backups to Recovery Service.

Each protected database uniquely identifies an Oracle Database that uses Recovery Service for data protection. The source database may be provisioned in Oracle Cloud (OCI), in Oracle Multicloud environment, or deployed on-premises.

For Oracle Cloud Databases or Oracle Multicloud Databases, Recovery Service automatically creates the protected database resource when you enable **Autonomous Recovery Service** as the backup destination.

Use the Cloud Protect Fleet Agent to add on-premises Oracle Databases to Recovery Service. See Protecting On-premises Databases using Oracle Database Zero Data Loss Cloud Protect for details.

Use the Protected database list page to view the list of protected databases in your tenancy. You can view the protection summary and monitor the backup performance. You can also view the Recovery Service subnet and Protection policy associated with each protected database.

Applying Tags

Apply tags to resources to help organize them according to your business needs. You can apply tags to a resource when you create it, and you can update a resource later to add, revise, or remove tags. For general information about tags and instructions for applying them, see Resource Tags.

Listing Protected Databases

View the protected databases in a specific compartment in Recovery Service.

Using the Console

1. Open the **navigation** menu, select **Oracle Database**, and then select **Database Backups**. The Protected databases list page displays all the protected databases belonging to the selected compartment.
2. To view the protected databases in a different compartment, use the **Compartment** filter to switch compartments.

> **Note**
>
> You must have permission to work in a compartment to see the resources in it. If you are not sure which compartment to use, contact an administrator. See Understanding Compartments for details.

Filtering List Results
Use filters to limit the resources displayed in the list. Perform one of these actions depending on the options that you see:

- From the **Search and Filter** box above the list table, select one or more filters and specify the values that you want to use to narrow the list. In general, the filters correspond to the columns shown in the list table, although some filters represent attributes that are not shown in the table. The **Compartment** filter is always displayed next to **Applied filters**.
- Select a value for the selected filter such as **Compartment**, **State**, or **Tags**.

Change the order of the items in the list table by using the sort icons next to the column names.

For information about searching for resources and managing the columns in the list table, if those features are available, see Listing Resources.

Actions

In the list table, select the name of a protected database to open its details page, where you can view its status and perform other tasks.

To perform an action on protected database directly from the list table, select any of the following options from the Actions menu in the row corresponding to the required resource:

- **View details**: Displays the protected database details page.
- **Move resource**: Move the protected database to another compartment.
- **Copy OCID**: Copy the `OCID` of the protected database to the clipboard.
- **Manage tags**: Add one or more tags to the protected database resource. See Resource Tags.

Using the CLI

Use the oci recovery protected-database-collection list-protected-databases command and required parameters to list the protected database resources.

See Autonomous Recovery Service CLI Command Reference for a complete list of parameters and values for CLI commands.

Using the API

Run the ListProtectedDatabases API operation to list protected databases.

Getting Protected Database Details

View the details of a protected database.

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

For Oracle Databases deployed in Oracle Cloud or Oracle Multicloud, when you enable the automatic backups feature and set **Autonomous Recovery Service** as the backup destination, Recovery Service automatically registers a protected database resource. For on-premises Oracle Databases, you must use the Cloud Protect Fleet Agent to register protected databases in Recovery Service.

Using the Console

1. Perform one of these steps to view the protected database details page:
   - On the **Protected databases** list page, select the protected database that you want to work with. See Listing Protected Databases for detailed steps to access the list page.
   - For databases in OCI and OCI multicloud, open the **navigation** menu, select **Oracle Database**, select the relevant database service, and navigate to the **Database information** page.
     In the **Backups** section, select **Autonomous Recovery Service** in the **Backup destination** field.

     The Protected database details page displays the information about the protected database.
   - Review these details in the **Details** tab.
     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 120 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 120 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.
- **Management type**: Indicates how the source database is deployed and managed. The values are:
    - **Provisioned through Oracle Cloud**: Indicates that the source database is managed in Oracle Cloud or in a Oracle Multicloud environment.
    - **Provisioned through Cloud Protect**: Indicates that the database is deployed on-premises and managed by the Cloud Protect Fleet Agent. See Protecting On-premises Databases using Oracle Database Zero Data Loss Cloud Protect for detailed information.
- **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

- **Recovery window current space used**: The amount of storage space that is currently used to meet the recovery window goal for the protected database.
- **Recovery window projected space used for policy**: The estimated amount of storage space that is required to meet the recovery window goal as per the retention period defined in the protection policy.
- **Long-term retention current space used**: If you have created long-term retention (LTR) backups for the database, then this field displays the amount of storage space that is currently used to store the LTR backups.

  > **Note**
  >
  > Recovery Service currently supports long-term retention (LTR) backups only for OCI Databases, Oracle Database@Azure, and Oracle Database@Google Cloud.

- **Protected database size**: The size of the database that is being protected.

Database backup summary

> **Note**
>
> The **Database backup summary** section is displayed only for Oracle Databases deployed in Oracle Cloud or Oracle Multicloud.

- **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
- **Last backup duration**: The time taken to complete the most recent successful backup

Protected database

- **Database details**: For databases deployed on Oracle Cloud or Oracle Multicloud, this field displays the database name as a hyperlink. Click the link to view the associated Database Details page.
- **DB unique name**: The globally unique name of the database.
- **Database name**: The name used to identify the database. This field is applicable only for on-premises Oracle Databases.
- **Database Identifier**: The unique identifier of the database. This field is applicable only for on-premises Oracle Databases.
- **Database version**: The Oracle Database version.

General information

- **Subscription**: The cloud provider subscription with which the protected database resource is associated. For example, this field displays the Microsoft Azure subscription information for a Oracle AI Database@Azure service resource linked with this protected database.
- **Backup location**: Indicates the backup storage location for the protected database.
  The backup location is controlled by the **Store backups in the same cloud provider as the database** option in the protection policy linked with the protected database. If the option is enabled, then the protected database backups will be stored in the same cloud provider as the database. See Enable Automatic Backups to Recovery Service for details.

  The **Backup location** field displays one of these values:

  * **Oracle Cloud** - Indicates that the protected database backups are stored in OCI (Oracle Cloud), which is the default storage location for protected database backups.
  * **Microsoft Azure** - Indicates that the protected database is associated with a Oracle AI Database@Azure service database and its backups are also stored in Microsoft Azure.
  * **Google Cloud** - Indicates that the protected database is associated with a Oracle AI Database@Google Cloud service database and its backups are also stored in Google Cloud.
  * **Amazon Web Services** - Indicates that the protected database is associated with a Oracle AI Database@AWS service database and its backups are also stored in Amazon Web Services.
- **OCID**: Select **Copy** to copy the OCID of the protected database. The OCID value is displayed only for Oracle Cloud or Oracle Multicloud Databases.

- **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

2. Select the **Network details** tab to view the Recovery Service subnets associated with the protected database.
3. Select the **Monitoring** tab to view the default metric charts to monitor the protected database. See, Available Metrics: oci_recovery_service for details.
4. Select the **Work requests** tab to view the work requests associated with the protected database.
5. Select the **Tags** section to view the tags applied to the protected database resource item.

Using the CLI

Use the oci recovery protected-database get command and required parameters to get the details of a protected database.

See Autonomous Recovery Service CLI Command Reference for a complete list of parameters and values for CLI commands.

Using the API

Run the GetProtectedDatabase API operation to view the details of a protected database.

Getting the Recovery Service Subnet Details of a Protected Database

View the Recovery Service subnet associated with a protected database.

1. On the Protected databases list page, select the protected database that you want to work with. See Listing Protected Databases for detailed steps to access the list page.
2. In the Protected database details page, select the **Network details** tab.
3. Perform one of these steps:
   - In the **Network details** list, select the name of the Recovery Service subnet to view its details.
   - From the **Actions** menu in the row for the resource, select **View details**.

   The Recovery Service subnet details page is displayed. See About Recovery Service Subnets.

Getting the Protection Policy Details of a Protected Database

View the protection policy that defines the backup retention rules for a protected database.

1. On the Protected databases list page, select the protected database that you want to work with. See Listing Protected Databases for detailed steps to access the list page.
2. In the Protected database information tab, select the name of the **Protection policy** to view its details.

   The Protection policy details page is displayed.

3. See Getting Protection Policy Details for protection policy field descriptions.

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 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 and Oracle multicloud 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
> - Oracle AI Database 26ai Release Update 23.4 or later
>
> To enable Real-time data protection for an on-premises Oracle Database, see Add On-Premises Database to Recovery Service Using Cloud Protect.

1. On the Protected databases list page, select the protected database that you want to work with. See Listing Protected Databases for detailed steps to access the list page.
2. Perform one of these steps in the Protected database details page:
   - The page displays a warning message with instructions to enable real-time data protection. Select **View Source Database** in the warning message.
   - In the **Protected database information** tab, navigate to the **Protected database** section and select the name of the database in the **Database details** field.

   The database details page is displayed.
3. From the **Actions** menu, select **Configure automatic backups**.
4. Enable **Real-time data protection**.
5. Select **Save**.

Getting Protected Database Network Connection Details

Download the network service configuration details for a specified protected database.

Using the Console

1. On the Protected databases list page, select the protected database that you want to work with. See Listing Protected Databases for detailed steps to access the list page.
2. On the details page, select the **Actions** menu from the top of the page, and then select **Download configuration**.
   By default, the file name is `dbrsconfig.zip`. You can rename the zip file with a name of your choice.
3. 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`

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

Using the CLI

Use the oci recovery protected-database fetch-protected-database-configuration and required parameters to download the network connection details of a protected database.

See Autonomous Recovery Service CLI Command Reference for a complete list of parameters and values for CLI commands.

Using the API

Run the FetchProtectedDatabaseConfiguration API operation to download the network configuration details for a protected database.

Moving a Protected Database

Move a protected database to a different compartment in your tenancy.

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.

Using the Console

1. On the Protected databases list page, select the protected database that you want to work with. See Listing Protected Databases for detailed steps to access the list page.
2. From the **Actions** menu in the row for the protected database, select **Move resource**.
3. In the **Move resource** panel, select the destination compartment from the list.
4. Select **Move resource**.

Using the CLI

Use the oci recovery protected-database change-compartment command and required parameters to move a protected database resource to a different compartment.

See Autonomous Recovery Service CLI Command Reference for a complete list of parameters and values for CLI commands.

Using the API

Run the ChangeProtectedDatabaseCompartment API operation to move a protected database to a different compartment.

Scheduled Deletion of a Protected Database

Recovery Service schedules the deletion of a protected database resource and the associated backups.

A protected database resource automatically enters the **Delete Scheduled** state in these scenarios:

- You have terminated the source database
  The 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 retention option that you have selected before terminating the database.
- You have disabled automatic backups for the source database
  The protected database resource enters the **Delete Scheduled** state and remains in this state for the period defined in the protection policy. Recovery Service automatically deletes the protected database and the associated backups after the backup retention period ends.

At the end of the scheduled delay, the protected database exits the **Delete Scheduled** state and enters the **Deleting** state. Finally, the **Deleted** status indicates that the protected database resource is deleted and cannot be modified.

See Life Cycle States of Recovery Service Resources for details.

Automated Cleanup of Recovery Service Subnets Registered by the Service

After deleting a protected database, Recovery Service also removes the Recovery Service subnet if it was registered by the service and if these conditions are true:

- You have not modified or updated the Recovery Service subnet after it was registered by the service
- The Recovery Service subnet is in an **Active** life cycle state and it has no dependencies with any other protected database

Using the Console

On the **Protected databases** list, the **State** column indicates the status **Delete Scheduled**, **Deleting** or **Deleted**. See Listing Protected Databases for details steps to access the list page.

Using the CLI

Use the oci recovery protected-database schedule-protected-database-deletion command and required parameters to schedule the deletion of a protected database resource.

See Autonomous Recovery Service CLI Command Reference for a complete list of parameters and values for CLI commands.

Using the API

Run the ScheduleProtectedDatabaseDeletion API operation to schedule the deletion of a protected database resource.

Related Topics

- Backup Retention and Deletion Options for Protected Databases
  Recovery Service enables you to recover your database in case of accidental or malicious damages, database termination, or if you disable automatic backups.

9

Managing Protection Policies

Protection policies provide automated backup retention management. Learn how to configure and manage protection policies in Recovery Service.

- About Protection Policies
  Recovery Service uses protection policies to control specific requirements for backup retention, storage location, and backup protection. 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.
- Listing Protection Policies
  View the protection policies in a specific compartment in Recovery Service.
- Getting Protection Policy Details
  Use these steps to access information about a protection policy.
- Creating a Protection Policy
  Create a custom protection policy in Recovery Service.
- Updating a User-Defined Protection Policy
  While Oracle-defined protection policies cannot be modified, you can update the configuration of a user-defined custom protection policy.
- Moving a Protection Policy
  Move a protection policy to a different compartment in your tenancy.
- Deleting a Protection Policy
  You can delete only the user-defined protection policies that you no longer use.

About Protection Policies

Recovery Service uses protection policies to control specific requirements for backup retention, storage location, and backup protection. Use the OCI Console to configure and manage protection policies.

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

A protection policy allows you to define these rules for backup retention, protection, and backup storage location (for Oracle Multicloud Databases):

- **Backup retention period** (required)
  Defines the maximum period to retain database backups created by Recovery Service. The allowed range is 14 days to 95 days.
- **Retention lock** (optional)
  Safeguards protected database backups by restricting the modification or deletion of backups until the retention period ends.
- **Preferred cloud location to store backups** (optional)
  Recovery Service supports Oracle Multicloud Databases and provides the flexibility to store backups either in Oracle Cloud (default storage location) or in the same cloud location where the database resides.

By default, Recovery Service stores protected databases and related backups in Oracle Cloud. You can override this default behavior for your Oracle Multicloud Database services.

Recovery Service supports Oracle AI Database@Azure, Oracle AI Database@Google Cloud, and Oracle AI Database@AWS.

If you enable the **Store backups in the same cloud provider as the database** option for a protection policy, then Recovery Service stores the policy-linked protected database and its backups in the target database cloud location instead of Oracle Cloud. For example, for Oracle AI Database@Azure, Recovery Service stores the associated protected database backups in Azure if you have selected the **Store backups in the same cloud provider as the database** in the protection policy.

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 these 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** (95 days): The **Platinum** policy retains backups for **95** days
  - **Gold** (65 days): The **Gold** policy retains backups for **65** days
  - **Silver** (35 days): The **Silver** policy retains backups for **35** days
  - **Bronze** (14 days): 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 policies for all databases in your tenancy.

Applying Tags

Apply tags to resources to help organize them according to your business needs. You can apply tags to a resource when you create it, and you can update a resource later to add, revise, or remove tags. For general information about tags and instructions for applying them, see Resource Tags.

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.

Listing Protection Policies

View the protection policies in a specific compartment in Recovery Service.

Using the Console

1. Open the **navigation** menu, select **Oracle Database**, and then select **Database Backups**.
2. Under **Database Backups**, select **Protection Policies**.
   The Protection policy list page displays all the policies belonging to the selected compartment.
3. To view the protection policies in a different compartment, use the **Compartment** filter to switch compartments.

> **Note**
>
> You must have permission to work in a compartment to see the resources in it. If you are not sure which compartment to use, contact an administrator. See Understanding Compartments for details.

Filtering List Results
Use filters to limit the resources displayed in the list. Perform one of these actions depending on the options that you see:

- From the **Search and Filter** box above the list table, select one or more filters and specify the values that you want to use to narrow the list. In general, the filters correspond to the columns shown in the list table, although some filters represent attributes that are not shown in the table. The **Compartment** filter is always displayed next to **Applied filters**.
- Select a value for the selected filter such as **Compartment**, **State**, or **Tags**.

Change the order of the items in the list table by using the sort icons next to the column names.

For information about searching for resources and managing the columns in the list table, if those features are available, see Listing Resources.

Actions

In the list table, select the name of a protection policy to open its details page, where you can view its status and perform other tasks.

To perform an action on a protection policy directly from the list table, select any of the following options from the **Actions** menu in the row corresponding to the required resource:

- **View details**: Displays the protection policy details page.
- **Copy OCID**: Copy the `OCID` of the protection policy to the clipboard.
- **Edit**: Update the protection policy.
- **Move resource**: Move the protection policy to another compartment.
- **Manage tags**: Add one or more tags to the protection policy resource. See Resource Tags.
- **Delete**: Delete the protection policy.

Using the CLI

Use the oci recovery protection-policy-collection list-protection-policies command and required parameters to list the protection policy resources.

See CLI for Oracle Database Autonomous Recovery Service for a complete list of parameters and values for CLI commands.

Using the API

Run the ListProtectionPolicies API operation to list protection policies.

Getting Protection Policy Details

Use these steps to access information about a protection policy.

Using the Console

1. On the **Protection policies** list page, select the policy that you want to work with. See Listing Protection Policies for details.
   The Protection policy details page displays the following information about the policy. Access the various resources associated with the policy by selecting their links or tabs.
2. Review the information in the **Details** tab.
   - **OCID** - Select **Copy** to copy the OCID of the protection policy
   - **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 location** - Indicates the backup storage location for protected databases using this policy.

  - **OCI**: Indicates that the backups will be stored in Oracle Cloud (default backup location).
  - **Same cloud provider as the database**: Indicates that the backups will be stored in the same cloud provider where the source database is provisioned. For example, if this policy is linked to an Oracle AI Database@Azure service database, then Recovery Service stores the backups in Microsoft Azure.
- **Backup retention period** - The retention period (in days) defined in the policy. The value ranges from **14** days to **95** days.

3. Select the **Protected databases** tab to view the list of all protected database that are using this policy.
4. Select the **Work requests** tab to view the work requests associated with the protection policy.
5. Select the **Tags** section to view the tags applied to the policy.

Using the CLI

Use the oci recovery protection-policy get command and required parameters to get the details of a protection policy.

For a complete list of parameters and values for CLI commands, see Oracle Database Autonomous Recovery Service CLI.

Using the API

Run the GetProtectionPolicy API operation to view the details of a protection policy.

Creating a Protection Policy

Create a custom protection policy in Recovery Service.

Using the Console

1. On the **Protection Policies** list page, select **Create protection policy**. See Listing Protection Policies for detailed steps to access the list page.
2. Enter a descriptive name for the protection policy. Avoid entering confidential information in the **Name** field.
3. Verify the compartment where you want to create the policy. Use the **Create in compartment** field to select a different compartment, if necessary.
4. In the **Backup retention period (in days)** field, specify the maximum number of days to retain backups using this policy.
   You can specify a retention period value ranging from **14** days to a maximum period of **95** days.
5. (Optional) Use these steps to enforce a lock to the backup retention period.
   - Select **Enable retention lock**.
   - 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.

6. (Optional) Select the **Store backups in the same cloud provider as the database** option if the source database is provisioned in a different cloud location and if you want Recovery Service to store the backups in the same cloud location as the database.
Recovery Service creates protected databases and related backups in Oracle Cloud by default. You can optionally override this default behavior for Oracle Multicloud Databases. Recovery Service supports these Oracle Multicloud services:

   - Oracle AI Database@Azure
   - Oracle AI Database@Google Cloud
   - Oracle AI Database@AWS

   If you enable the **Store backups in the same cloud provider as the database** option for a protection policy, then the policy-linked protected database and backups will be stored in the same cloud location where the database is provisioned. For example, for Oracle AI Database@Azure, Recovery Service stores the associated protected database backups in Azure cloud if you have selected the **Store backups in the same cloud provider as the database** option in the protection policy.

   If you do not select the **Store backups in the same cloud provider as the database** for a protection policy, then the policy-linked protected database and backups will be stored in Oracle Cloud even if your Oracle Database is provisioned in a different cloud location.

   > ⚠ **Caution**
   >
   > You cannot undo the selection of the **Store backups in the same cloud provider as the database** option after you create the policy.

7. Expand **Advanced options** and add the following information.
Tags: (Optional) Add one or more tags to the resource. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags. If you are not sure whether to apply tags, skip this option or ask an administrator. You can apply tags later.

8. Select **Create**.
The protection policy is created.

Using the CLI

Use the oci recovery protection-policy create command and required parameters to create a protection policy.

See Autonomous Recovery Service CLI Command Reference for a complete list of parameters and values for CLI commands.

Using the API

Run the CreateProtectionPolicy API operation to create a protection policy.

Related Topics

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

Updating a User-Defined Protection Policy

While Oracle-defined protection policies cannot be modified, you can update the configuration of a user-defined custom protection policy.

When you edit a protection policy, you can also update its tags. For more information about tagging, see Resource Tags.

Using the Console

1. On the Protection policies list, select the protection policy that you want to work with. See Listing Protection Policies for detailed steps to access the list page.
2. From the **Actions** menu for the policy, select **Edit**.
3. Enter a new name for the protection policy, if necessary.
4. In the **Backup retention period (in days)** field, you can update the retention period. You can specify a value ranging from **14** days to **95** days.

> **Note**
>
> 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.

5. 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.
6. Select **Save changes**.

Using the CLI

Use the oci recovery protection-policy update command and the required parameters to update a protection policy.

See Autonomous Recovery Service CLI Command Reference for a complete list of parameters and values for CLI commands.

Using the API

Run the UpdateProtectionPolicy API operation to update a protection policy.

Moving a Protection Policy

Move a protection policy to a different compartment in your tenancy.

Using the Console

1. On the **Protection policies** list page, select the policy that you want to work with. See Listing Protection Policies for detailed steps.
2. From the **Actions** menu in the row for the policy, select **Move resource**.
3. In the **Move resource** panel, select the destination compartment from the list.
4. Select **Move resource**.

Using the CLI

Use the oci recovery protection-policy change-compartment command and the required parameters to move a policy to a different compartment.

See Autonomous Recovery Service CLI Command Reference for a complete list of parameters and values for CLI commands.

Using the API

Run the ChangeProtectionPolicyCompartment API operation to move a policy to a different compartment.

Deleting a Protection Policy

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

Using the Console

1. On the **Protection policies** list, select the policy that you want to work with. See Listing Protection Policies for details.
2. From the **Actions** menu for the user-defined policy, select **Delete**.
3. When prompted, confirm the deletion.

Using the CLI

Use the oci recovery protection-policy delete command and required parameters to delete a protection policy.

See Autonomous Recovery Service CLI Command Reference for a complete list of parameters and values for CLI commands.

Using the API

Run the DeleteProtectionPolicy API operation to delete a protection policy.

10

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 Recovery Service Subnets
  Recovery Service subnets enable network isolation for Recovery Service operations in a VCN.
- Listing Recovery Service Subnets
  View the Recovery Service subnets in a specific compartment.
- Register a Recovery Service Subnet
  Use this procedure to register a Recovery Service subnet.
- Add or Replace Subnets for a Recovery Service Subnet
  You can replace a subnet or add more subnets to support the required number of private endpoints for Recovery Service operations.
- Associate NSGs to a Recovery Service Subnet
  If you have used network security groups (NSG) to implement security rules for Recovery Service in the database VCN, then you must add the Recovery Service NSGs to the Recovery Service subnet.
- Getting Recovery Service Subnet Details
  Access the details of a Recovery Service subnet.
- Rename a Recovery Service Subnet
  Modify the name of an existing Recovery Service subnet.
- Moving a Recovery Service Subnet
  Move a Recovery Service subnet to a different compartment in your tenancy.
- Deleting a Recovery Service Subnet
  Recovery Service performs an automatic clean-up of Recovery Service subnets that are registered by the service but no longer used. Alternatively, use these steps to manually delete a Recovery Service subnet.

About 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 used 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.

Applying Tags

Apply tags to resources to help organize them according to your business needs. You can apply tags to a resource when you create it, and you can update a resource later to add, revise, or remove tags. For general information about tags and instructions for applying them, see Resource Tags.

Related Topics

- Register a Recovery Service Subnet
  Use this procedure to register a Recovery Service subnet.
- About Using a Private Subnet for Recovery Service Operations
  Recovery Service requires a private subnet in the same virtual cloud network (VCN) where your database resides. The private subnet must include security rules to control the backup network between your database and Recovery Service.
- Create a Recovery Service Subnet in the Database VCN
  Use the OCI Console to configure a private subnet for Recovery Service in your database virtual cloud network (VCN).

Listing Recovery Service Subnets

View the Recovery Service subnets in a specific compartment.

Using the Console

1. Open the **navigation** menu and select **Oracle Database**. Under **Oracle Database**, select **Database Backups**.
2. Under **Database Backups**, select **Recovery Service Subnets**.
   The **Recovery Service subnets** list page displays all the Recovery Service subnets belonging to the selected compartment.
3. To view the Recovery Service subnets in a different compartment, use the **Compartment** filter to switch compartments.

> **Note**
>
> You must have permission to work in a compartment to see the resources in it. If you are not sure which compartment to use, contact an administrator. See Understanding Compartments for details.

Filtering List Results

Use filters to limit the resources displayed in the list. Perform one of these actions depending on the options that you see:

- From the **Search and Filter** box above the list table, select one or more filters and specify the values that you want to use to narrow the list. In general, the filters correspond to the columns shown in the list table, although some filters represent attributes that are not shown in the table. The **Compartment** filter is always displayed next to **Applied filters**.
- Select a value for the selected filter such as **Compartment**, **State**, or **Tags**.

Change the order of the items in the list table by using the sort icons next to the column names.

For information about searching for resources and managing the columns in the list table, if those features are available, see Listing Resources.

Actions
In the list table, select the name of a Recovery Service subnet to open its details page, where you can view its status and perform other tasks.

To perform an action on a Recovery Service subnet directly from the list table, select any of the following options from the **Actions** menu in the row corresponding to the required resource:

- **View details**: Displays the Recovery Service subnets details page.
- **Copy OCID**: Copy the OCID of the Recovery Service subnets to the clipboard.
- **Rename**: Modify the name of a Recovery Service subnet.
- **Move resource**: Move the Recovery Service subnet to a different compartment.
- **Manage tags**: Add one or more tags to the Recovery Service subnet resource. See Resource Tags.
- **Delete**: Delete the Recovery Service subnet.

Using the CLI

Use the list-recovery-service-subnets command and the required parameters to list the Recovery Service subnet resources.

See Autonomous Recovery Service CLI Command Reference for a complete list of parameters and values for CLI commands.

Using the API

Run the ListRecoveryServiceSubnets API operation to list Recovery Service subnets.

Register a Recovery Service Subnet

Use this procedure to register a Recovery Service subnet.

> **Note**
>
> Before you register a Recovery Service subnet:
>
> - Ensure to open these network ports and configure the security rules for Recovery Service.
>   - Port **2484** - Enables SQL*Net connections to the RMAN catalog which is used by Recovery Service.
>   - Port **8005** - Enables backup traffic from the database to Recovery Service.
> - Ensure that you have reviewed and confirmed the mandatory prerequisites described in Mandatory Requirements Checklist for Recovery Service.
> - Ensure that you select an IPv4-only subnet for Recovery Service operations in your database VCN. Do not select an IPv6-enabled subnet as Recovery Service does not support using an IPv6-enabled subnet.
> - For Oracle Databases deployed in OCI, if your backup subnet meets the recommended subnet size (at least 12 free IP addresses), then Recovery Service automatically registers the Recovery Service subnet. If you want to replace the subnet registered by Recovery Service, use the steps described in Add or Replace Subnets for a Recovery Service Subnet.
> - If you have used network security groups (NSG) to implement the security rules for Recovery Service in the database VCN, then you must add the Recovery Service NSGs (maximum five) to the Recovery Service subnet, as described in step 8. The recommended subnet size is **/24**.
>   Recovery Service supports these Oracle Multicloud Database services:
>   - Oracle AI Database@Azure
>   - Oracle AI Database@Google Cloud
>   - Oracle AI Database@AWS
>   Network ports **2484** and **8005** enable the network connectivity between Oracle AI Database@AWS and Recovery Service. In an existing OCI tenancy, ensure to open the network ports **2484** and **8005**. In a new OCI tenancy, the same networks ports are open by default for Oracle AI Database@AWS.
>
>   When you onboard an Oracle AI Database@AWS resource to Recovery Service, the service automatically registers the backup subnet as the Recovery Service subnet. You can either use the Recovery Service subnet that is already registered by the service or use the steps provided in this section to register your own Recovery Service subnet.
> - 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.

1. On the **Recovery Service subnets** list page, select **Register Recovery Service subnet**. See Listing Recovery Service Subnets for detailed steps to access the list page.

2. Enter a name for the Recovery Service subnet. Avoid entering confidential information in the **Name** field.
3. Verify the compartment where you want to create the Recovery Service subnet. Use the **Create in compartment** field to select a different compartment, if necessary.
4. Select the **Compartment** that contains the virtual cloud network (VCN) that you want to use. You can select a VCN from only one compartment at a time.
5. Select the **virtual cloud network**.
6. Under **Subnets**, select these options:
   a. Select the **Compartment** that contains the private subnet that you want to use.
   b. Select the **Subnet** that you have configured for Recovery Service operations in the selected VCN.
7. (Optional) Select **+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.

   See About Using a Private Subnet for Recovery Service Operations for details.
8. Expand **Advanced options** to configure these options:
   - **Network security groups**
     If you have used network security groups (NSG) to implement the security rules for Recovery Service in the database VCN, then you must add the Recovery Service NSGs (maximum five) to the Recovery Service subnet. The Recovery Service NSG can reside in the same compartment or in a different compartment. However, the NSG must belong to the same VCN to which the specified subnet belongs.

     Use these steps to add the Recovery Service NSG to the Recovery Service subnet:
     a. In the **Network security groups** section, select **Use network security groups to control traffic**.
     b. Select the Recovery Service NSG you have created in the database VCN.
     c. Select **+Another network security group** to associate multiple NSGs (maximum five).
   - **Tags**: (Optional) Add one or more tags to the resource. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags. If you are not sure whether to apply tags, skip this option or ask an administrator. You can apply tags later.
9. Select **Register**.

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

You can replace a subnet or add more subnets to support the required number of private endpoints. See Add or Replace Subnets for a Recovery Service Subnet for details.
See Associate NSGs to a Recovery Service Subnet for detailed steps to add NSGs to an existing Recovery Service subnet.

Related Topics

- About Recovery Service Subnets
  Recovery Service subnets enable network isolation for Recovery Service operations in a VCN.

Add or Replace Subnets for a Recovery Service Subnet

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

- If a Recovery Service subnet contains insufficient number of available IP addresses, then Recovery Service issues an alert message when you try to add a new database. In this scenario, you can add IP addresses by associating multiple subnets to the Recovery Service subnet.
- If you want to replace the subnet registered by Recovery Service, then you must first add the new subnet before deleting the existing one.

For subnet size recommendations, see About Using a Private Subnet for Recovery Service Operations.

Using the Console

1. On the **Recovery Service subnets** list page, select the Recovery Service subnet that you want to work with. See Listing Recovery Service Subnets for details to access the list page.
2. On the details page, go to the **Subnets** tab.
   - Select **Add subnets**.
   - In the **Add subnets** panel, select the **Compartment** and the **Subnet** you want to add.
   - Select **Add subnets**.
3. On the **Subnets** tab, use these steps to replace an existing subnet. You must ensure to first add the new subnet before deleting the existing one.
   - Select **Add subnet** to add a new subnet.
   - From the **Actions** menu, select **Delete** to delete the subnet that you no longer want to use.

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

Using the CLI

Use the oci recovery recovery-service-subnet update command and required parameters to update a Recovery Service subnet and add subnets.

See Autonomous Recovery Service CLI Command Reference for a complete list of parameters and values for CLI commands.

Using the API

Run the UpdateRecoveryServiceSubnet API operation to update a Recovery Service subnet.

Associate NSGs to a Recovery Service Subnet

If you have used network security groups (NSG) to implement security rules for Recovery Service in the database VCN, then you must add the Recovery Service NSGs to the Recovery Service subnet.

The Recovery Service NSG can reside in the same compartment or in a different compartment. However, the NSG must belong to the same VCN to which the specified subnet belongs.

Using the Console

1. On the **Recovery Service subnets** list page, select the Recovery Service subnet that you want to work with. See Listing Recovery Service Subnets for details to access the list page.
2. On the details page, go to the **Network security groups** tab.
3. Select **Add network security groups**.
4. In the **Add network security groups** panel, select the **Compartment** and the **network security group** you want to add.
5. Select **Add network security group**.

> **Note**
>
> You can add a maximum of five NSGs to a Recovery Service subnet.

6. If you want to replace an existing network security group (NSG), then from the **Actions** menu, select **Remove** and then select **Add network security group** to add a new NSG.

Using the CLI

Use the oci recovery recovery-service-subnet get command and parameters to update the Recovery Service subnet.

See Autonomous Recovery Service CLI Command Reference for a complete list of parameters and values for CLI commands.

Using the API

Run the UpdateRecoveryServiceSubnet API operation to update a Recovery Service subnet.

Getting Recovery Service Subnet Details

Access the details of a Recovery Service subnet.

Using the Console

1. On the **Recovery Service subnets** list, select the Recovery Service subnet that you want to work with. See Listing Recovery Service Subnets for detailed steps to access the list page.
2. Review the information in the **Recovery Service subnet information** tab.
   - **OCID Copy** - Select **Copy** to copy the Recovery Service subnet's OCID.
   - **Compartment**: The compartment to which the Recovery Service subnet belongs.

- **Created** - The date and time when the resource was created.
- **Updated** - The date and time when the resource was last updated.
- **VCN** - The VCN in which the Recovery Service subnet exists. Select the link to view the virtual cloud network (VCN) details page.

3. On the **Subnets** tab, select the **Actions** menu and select **View details** to view the details of a specific subnet. You can also add multiple subnets. See Add or Replace Subnets for a Recovery Service Subnet for details.
4. On the **Network security groups** tab, select the **Actions** menu and select **View details** to view the details of a NSG.
5. Select the **Work requests** tab to view the work requests associated with the Recovery Service subnet.

Using the CLI

Use the oci recovery recovery-service-subnet get command and required parameters to view the details of a Recovery Service subnet.

See Autonomous Recovery Service CLI Command Reference for a complete list of parameters and values for CLI commands.

Using the API

Run the GetRecoveryServiceSubnet API operation to get the details of a Recovery Service subnet.

Rename a Recovery Service Subnet

Modify the name of an existing Recovery Service subnet.

Using the Console

1. On the **Recovery Service subnet** list page, select the Recovery Service subnet that you want to work with. See Listing Recovery Service Subnets for detailed steps to access the list page.
2. From the **Actions** menu for the resource, select **Rename**.
3. In the **Rename Recovery Service subnet** panel, specify a new name.
4. Select **Update**.

Moving a Recovery Service Subnet

Move a Recovery Service subnet to a different compartment in your tenancy.

Using the Console

1. On the **Recovery Service subnets** list page, select the Recovery Service subnet that you want to work with. See Listing Recovery Service Subnets for detailed steps to access the list page.
2. From the **Actions** menu for the resource, select **Move resource**.
3. In the **Move resource** panel, select the destination compartment from the list.
4. Select **Move resource**.

Using the CLI

Use the oci recovery recovery-service-subnet change-compartment command and required parameters to move a Recovery Service subnet to a different compartment in your tenancy.

Using the API

Run the ChangeRecoveryServiceSubnetCompartment API operation to move a Recovery Service subnet to a different compartment in your tenancy.

Deleting a Recovery Service Subnet

Recovery Service performs an automatic clean-up of Recovery Service subnets that are registered by the service but no longer used. Alternatively, use these steps to manually delete a Recovery Service subnet.

Automated Cleanup of Recovery Service Subnets Registered by the Service

After deleting a protected database, Recovery Service also removes the Recovery Service subnet if it was registered by the service and if these conditions are true:

- You have not modified or updated the Recovery Service subnet after it was registered by the service
- The Recovery Service subnet is in an **Active** life cycle state and it has no dependencies with any other protected database

Using the Console to Delete a Recovery Service Subnet

1. On the **Recovery Service subnets** list page, select the Recovery Service subnet that you want to work with. See Listing Recovery Service Subnets for detailed steps to access the list page.
2. From the **Actions** menu for the resource, select **Delete**.
3. Confirm the deletion when prompted.

Using the CLI to Delete a Recovery Service Subnet

Use the oci recovery recovery-service-subnet delete command and required parameters to delete a Recovery Service subnet.

See Autonomous Recovery Service CLI Command Reference for a complete list of parameters and values for CLI commands.

Using the API to Delete a Recovery Service Subnet

Run the DeleteRecoveryServiceSubnet API operation to delete a Recovery Service subnet.

11

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.
- Using the APIs to Manage LTR Backups
  Review the list of REST API endpoints to create and manage long-term retention (LTR) backups of a protected database using Recovery Service.

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 error 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 a Recovery Service Subnet
- Recovery Service does not have permissions to manage the network resources in a chosen compartment.
  Review and assign the required policies. See, Optional Permissions for Oracle Databases in OCI
- 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 a Recovery Service Subnet

Example 11-1 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 Onboarding Oracle Database to 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

Using the APIs to Manage LTR Backups

Review the list of REST API endpoints to create and manage long-term retention (LTR) backups of a protected database using Recovery Service.

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 long-term backups for your Oracle Databases that use Recovery Service as the backup destination.

- **Create a long-term backup of a protected database:** `CreateLongTermBackup`
- **Update a long-term backup of a protected database:** `UpdateLongTermBackup`
- **Retrieve a long-term backup of a protected database:** `GetLongTermBackup`
- **Lists all the long-term backups of a protected database:** `ListLongTermBackups`
- **Delete a long-term backup of a protected database:** `DeleteLongTermBackup`
- **Cancel a long-term backup of a protected database:** `CancelLongTermBackup`

Related Topics

- REST APIs
- Security Credentials
- Software Development Kits and Command Line Interface
- CreateLongTermBackup
- UpdateLongTermBackup
- GetLongTermBackup
- ListLongTermBackups
- DeleteLongTermBackup
- CancelLongTermBackup

12

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

- Optional Permissions for Oracle Databases in OCI
  By default, Oracle Databases in OCI are assigned with the permissions to access Recovery Service. The service can also access the network resources within the database VCN. You may choose to assign the additional and optional permissions for OCI Databases, as described in this topic.

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
long-term-backup
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.
- long-term backup
  Review the list of permissions and API operations for the `long-term backup` 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 12-1 recovery-service-family - *INSPECT*

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 RECOVERY_SERVICE_LONG_TERM_BACKUP_INSPECT	ListProtectedDatabases FetchProtectedDatabaseConfiguration ListProtectionPolicies ListRecoveryServiceSubnets ListWorkRequests ListLongTermBackups	*none*

Table 12-2 recovery-service-family - *READ*

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 RECOVERY_SERVICE_LONG_TERM_BACKUP_READ	GetProtectedDatabase GetProtectionPolicy GetRecoveryServiceSubnet GetWorkRequest GetLongTermBackup	*none*

Table 12-3 recovery-service-family - *UPDATE*

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

Table 12-4 recovery-service-family - *MANAGE*

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 RECOVERY_SERVICE_LONG_TERM_BACKUP_CREATE RECOVERY_SERVICE_LONG_TERM_BACKUP_DELETE RECOVERY_SERVICE_LONG_TERM_BACKUP_CANCEL	CreateProtectedDatabase DeleteProtectedDatabase ChangeProtectedDatabaseCompartment CreateProtectionPolicy DeleteProtectionPolicy ChangeProtectionPolicyCompartment CreateRecoveryServiceSubnet DeleteRecoveryServiceSubnet ChangeRecoveryServiceSubnetCompartment CreateLongTermBackup DeleteLongTermBackup CancelLongTermBackup	*none*

recovery-service-protected-database

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

Table 12-5 recovery-service-protected-database - *INSPECT*

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

Table 12-6 recovery-service-protected-database - *READ*

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

Table 12-7 recovery-service-protected-database - *UPDATE*

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

Table 12-8 recovery-service-protected-database - *MANAGE*

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 12-9 recovery-service-subnet - *INSPECT*

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

Table 12-10 recovery-service-subnet - *READ*

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

Table 12-11 recovery-service-subnet - *UPDATE*

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

Table 12-12 recovery-service-subnet - *MANAGE*

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 12-13 recovery-service-policy - *INSPECT*

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

Table 12-14 recovery-service-policy - *READ*

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

Table 12-15 recovery-service-policy - *UPDATE*

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

Table 12-16 recovery-service-policy - *MANAGE*

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

long-term backup

Review the list of permissions and API operations for the `long-term backup` resource type.

Table 12-17 long-term-backup - *INSPECT*

Permissions	APIs Fully Covered	APIs Partially Covered
RECOVERY_SERVICE_LONG_TERM_BACKUP_INSPECT	ListLongTermBackups	*none*

Table 12-18 long-term-backup - *READ*

Permissions	APIs Fully Covered	APIs Partially Covered
INSPECT+ RECOVERY_SERVICE_LONG_TERM_BACKUP_READ	GetLongTermBackup	*none*

Table 12-19 long-term-backup - *UPDATE*

Permissions	APIs Fully Covered	APIs Partially Covered
READ+ RECOVERY_SERVICE_LONG_TERM_BACKUP_UPDATE	UpdateLongTermBackup	*none*

Table 12-20 long-term-backup - *MANAGE*

Permissions	APIs Fully Covered	APIs Partially Covered
USE+ RECOVERY_SERVICE_LONG_TERM_BACKUP_CREATE RECOVERY_SERVICE_LONG_TERM_BACKUP_CANCEL RECOVERY_SERVICE_LONG_TERM_BACKUP_DELETE	CreateLongTermBackup CancelLongTermBackup DeleteLongTermBackup	*none*

recovery-service-work-request

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

Table 12-21 recovery-service-work-request - *INSPECT*

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

Table 12-22 recovery-service-work-request - *READ*

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 12-23 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 12-23 (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
long-term-backup	RECOVERY_SERVICE_LONG_TERM_BACKUP_INSPECT RECOVERY_SERVICE_LONG_TERM_BACKUP_READ RECOVERY_SERVICE_LONG_TERM_BACKUP_CREATE RECOVERY_SERVICE_LONG_TERM_BACKUP_UPDATE RECOVERY_SERVICE_LONG_TERM_BACKUP_DELETE RECOVERY_SERVICE_LONG_TERM_BACKUP_CANCEL

Table 12-24 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
ChangeProtectedDatabase Compartment	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
ChangeProtectionPolicyC ompartment	RECOVERY_SERVICE_POLICY_MOVE
CreateRecoveryServiceSu bnet	RECOVERY_SERVICE_SUBNET_CREATE

Table 12-24 (Cont.) API Operations and Permissions

API Operation	Permissions Required for the Operation
DeleteRecoveryServiceSubnet	RECOVERY_SERVICE_SUBNET_DELETE
GetRecoveryServiceSubnet	RECOVERY_SERVICE_SUBNET_READ
ListRecoveryServiceSubnets	RECOVERY_SERVICE_SUBNET_INSPECT
UpdateRecoveryServiceSubnet	RECOVERY_SERVICE_SUBNET_UPDATE
ChangeRecoveryServiceSubnetCompartment	RECOVERY_SERVICE_SUBNET_MOVE
ListWorkRequests	RECOVERY_SERVICE_WORK_REQUEST_INSPECT
GetWorkRequest ListWorkRequestErrors ListWorkRequestLogs	RECOVERY_SERVICE_WORK_REQUEST_READ
CreateLongTermBackup	RECOVERY_SERVICE_LONG_TERM_BACKUP_CREATE
DeleteLongTermBackup	RECOVERY_SERVICE_LONG_TERM_BACKUP_DELETE
GetLongTermBackup	RECOVERY_SERVICE_LONG_TERM_BACKUP_READ
UpdateLongTermBackup	RECOVERY_SERVICE_LONG_TERM_BACKUP_UPDATE
CancelLongTermBackup	RECOVERY_SERVICE_LONG_TERM_BACKUP_CANCEL

13

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.
- Viewing Protected Database Metrics
  Use the console to view the various metric charts and monitor the performance of protected database backups.
- 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 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 13-1 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 13-2 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 13-2 (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	Seconds	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

- Viewing Protected Database Metrics
  Use the console to view the various metric charts and monitor the performance of protected database backups.

Viewing Protected Database Metrics

Use the console to view the various metric charts and monitor the performance of protected database backups.

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

1. On the Protected databases list page, select the protected database that you want to work with. See Listing Protected Databases for detailed steps to access the list page.
2. On the details page, select the **Monitoring** tab.:
   The **Metrics** section displays a default set of charts for the protected database.
3. Use the date filter to specify a date and time when the metric period starts and ends. You can also select a predetermined length of time for the metric period.

4. For each metric displayed on the page, you can apply these commands from the **Actions** menu displayed in the upper right corner:
   - **View query in Metrics Explorer**: View the metric in the Monitoring service's Metrics Explorer, see Viewing a Custom Metric Chart.
   - **Copy Chart URL**: Copy the URL for the metric chart.
   - **Copy Query (MQL)**: Copy the predefined service query used in the metric chart in Monitoring Query Language (MQL) format.
   - **Create an alarm on this query**: Copy the query from this metric chart to a new alarm. See Using Alarms to Monitor Protected Databases.
   - **Table view**: Displays the metrics in a tabular format.

To view the default metric chart for multiple protected databases

1. Open the **navigation** menu and select **Observability & Management**.
2. Under **Monitoring**, select **Service Metrics**.
3. Change the **Compartment** to find the protected database that you want to monitor.
4. In the **Metric namespace** field, select **oci_recovery_service**.
5. 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 select **Observability & Management**. Under **Monitoring**, select **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. Select **Update Chart**.
7. The chart shows the results of your new query.
8. Select **Add Query** below the chart to add more queries.
9. Optionally, select **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. On the Protected database list page, select the protected databases that you want to work with. See Listing Protected Databases for details to access the list page.
2. On the details page, select the **Monitoring** tab and go to the **Metrics** section.
3. Select the **Actions** menu in the upper-right corner of the chart and select **Create an alarm on this query**.
   The Oracle Cloud Infrastructure Monitoring service Create Alarm page is displayed.
4. 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 select **Observability & Management**. Under **Monitoring**, select **Alarm Definitions**.
2. Select **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

14

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 14-1 Recovery Service: Protected Database Event Types

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

Table 14-1 (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 14-1 Reference Event for Protected Databases

Here's a reference event for protected databases:

```
{
    "eventType":
"com.oraclecloud.autonomousrecoveryservice.updateprotecteddatabase.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 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 14-2 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 14-2 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 14-3 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`
Protection Policy - Update End	`com.oraclecloud.autonomousrecoveryservice.updateprotectionpolicy.end`

Example 14-3 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 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 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 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, Getting 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 a Recovery Service Subnet

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 and remains in this state for the period defined in the protection policy. Recovery Service retains the protected database backups until the backup retention period ends. 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.