MARIADB PLC
Support Policy



Release: November 3, 2026
Copyright © 2026 MariaDB PLC
All Rights Reserved

The latest version of this Support Policy may be found at:
https://mariadb.com/support-policy

Introduction **3**
Supported Products **4**
Release Stage Support Levels 4
Types of Support Provided **5**
OEM Support 5
Standard Support 6
Premium Support 6
Product Support **6**
Problem Resolution Support 7
Engineering Support 7
Real-Time Chat Support 7
Telephone Support 8
Issue Severity and Service Level Agreements **8**
Special Support Scenarios **9**
Escalation Requests 9
Extended Support 10
Data Sovereignty 10
Root Cause Analysis 10
Commercially Reasonable Effort Support 11
Additional Information **11**
Addendum A: OEM Support **12**
Addendum B: Cloud Support **14**
Definitions 14
Shared Responsibility Model 14
Excluded Downtime 18
Service Level Matrix 19
Service Credits 19
Addendum C: Bring Your Own Cloud (BYOC) **21**
Definitions 21
Deployment Model and Responsibilities 21
Shared Responsibility Model 23
Additional Excluded Downtime 23
Addendum D: Managed Operations **24**
Service Scope - Managed Operations 24
Connectivity and Access 28
Data Processing and Access 30
Onboarding and Offboarding 30

Introduction

All capitalized terms not defined in this Policy have the meanings set forth in the MariaDB Subscription Agreement published on https://mariadb.com/terms or in the MariaDB Engineering Policy published on https://mariadb.com/engineering-policies (the “Engineering Policy”), which forms part of this Policy as described below.

Customers have access to technical support services, including Problem Resolution Support, Engineering Support and Telephone Support (where included in the Customer’s support tier) for Supported Products via the Customer Support Portal (see table of Support Services below). Customers may also purchase Managed Operations (“MO”) services (previously known as “Remote DBA” or “RDBA”) for additional support options.

This MariaDB Support Policy describes (1) Supported Products, (2) the types of support provided by MariaDB, including Cloud Support and MO, and (3) issue severity designations and service level agreements. The latest version of this policy is available at https://mariadb.com/support-policy.

The Addenda to this Policy apply only to Customers that have purchased the corresponding service: Addendum A (OEM Support), Addendum B (Cloud Support), Addendum C (Bring Your Own Cloud) and Addendum D (Managed Operations). Where an Addendum conflicts with the main body of this Policy, the Addendum prevails for that service.

Each of the Customer’s designated technical contacts will receive a Customer Support Portal login (based on their associated email address) that can be used to report new, monitor ongoing, or review historical support issues. The Customer can find information about changing its technical contacts in the “Welcome Letter” it receives after signing up, or in the “Contact Us” section of the Customer Support Portal. If a technical contact has any difficulty initially logging into the Customer Support Portal, that contact should email success@mariadb.com for further assistance.

MariaDB support is delivered in English. MariaDB will use commercially reasonable efforts to provide technical support in languages other than English using MariaDB’s available personnel via voice calls and in-person meetings, but may not have such resources available in general or at the time of a particular support request. All communication via the Customer Support Portal should be in English. There are no Service Level Agreements for non-English support at this time. Each support request is assigned a separate ticket number and prioritized based on its severity. Support will ask the Customer to open a new ticket for each new support request.

Supported Products

MariaDB provides OEM, Standard, Premium, and Managed Operations Support services, subject to the restrictions in this Policy, for MariaDB Enterprise Server, MariaDB MaxScale, MariaDB Connectors, MariaDB GridGain, and other software, in each case only for the release series, operating systems and platforms listed as supported in the Engineering Policy and until each Product release series' End of Standard Support date or, where the Engineering Policy states none, its End of Life date ("Supported Products"). Between a Product release series' End of Standard Support date and its End of Life date, support is available only as Extended Support, or, without Extended Support, as Reasonable Effort Support. MariaDB Customers use Supported Products on-premises, in the cloud, including MariaDB Cloud, or in hybrid environments.

The Engineering Policy forms part of this Policy. It sets out, for each Supported Product, its release series, General Availability, End of Standard Support and End of Life dates, and the operating systems and platforms on which it is supported. MariaDB regularly updates the Engineering Policy and may amend it at any time in its sole discretion, including by adding, changing or removing products, release series, platforms and dates. Each update to the Engineering Policy is an update to this Policy and takes effect when published, superseding all earlier versions. Support Services are provided in accordance with the Engineering Policy in effect when the relevant Support Services are requested or performed. If this Policy and the Engineering Policy conflict, this Policy prevails. Updates to the Engineering Policy do not entitle the Customer to any refund, credit or termination right.

Release Stage Support Levels

	Limited Preview	Public Preview	General Availability (GA)
Definition	An early build released to a controlled set of Customers to validate direction and gather feedback. Functionality may be incomplete and can change or be withdrawn without notice.	A feature-complete release available to all Customers for real-world testing ahead of General Availability.	The production-ready, fully supported release, backed by SLAs, documentation, and the lifecycle set out in the Engineering Policy.
Audience and access	Invitation or nomination only. Access is gated and enabled by MariaDB.	Open to all Customers. Not gated by tier, entitlement, or approval. Self-service opt-in.	All Customers.
Production use	No production use. This is for development and testing only; no SLA.	No production use. This is for development and testing only; no SLA.	Fully supported, including mission-critical deployments.

	Limited Preview	Public Preview	General Availability (GA)
Support model	No SLA. Direct engagement with Product Management and Engineering through a named channel. Not routed through the Customer Support Portal.	No SLA. Reasonable Effort Support through the Customer Support Portal.	Full support in line with the Customer's contracted SLA.

Types of Support Provided

Through the Customer Support Portal, MariaDB Customers have access to MariaDB's global team of MariaDB Support Engineers who are available to assist with product questions and tasks as they relate to Supported Products.

Support Services	OEM Support	Standard Support	Premium Support
Problem Resolution Support	✓	✓	✓
Engineering Support	✓	✓	✓
Escalation Requests	✓	✓	✓
Extended Support[1]		✓	✓
Real-Time Chat Support			✓
Telephone Support	S1 only	S1 only	✓
Managed Operations[2]		Add-On	

OEM Support

Customers who serve End Users (as defined in Addendum A) can purchase OEM Support for agreed MariaDB products. The terms of OEM Support are set out in Addendum A.

[1] Available for purchase by Customers with Standard or Premium Support for additional fees; not included in the Fees for those Support Services. See Extended Support below.

[2] Real-Time Chat Support and Telephone Support are also included with Managed Operations.

Standard Support

MariaDB Standard Support is a technical support subscription tier designed for environments that require reliable, enterprise-grade stability and access to the MariaDB Engineering team.

Standard Support covers a comprehensive range of lifecycle and problem-resolution activities to keep the Customer's environment running smoothly:

- **Installation and Configuration Help:** Assistance with the initial setup, deployment, upgrades, and optimal configuration of MariaDB products to align with MariaDB best practices.
- **Troubleshooting:** Assistance with identifying and resolving operational failures, performance bottlenecks, replication issues, and system crashes.
- **Bug Fixing:** Alignment with the MariaDB Engineering team to deliver patches, bug fixes, and urgent hotfix builds for software defects.
- **General Guidance:** Provision of administrative guidance, documentation assistance, and authoritative technical advice regarding general usage of MariaDB products.

Premium Support

MariaDB Premium Support is a technical support subscription tier extending Standard Support to include a dedicated support engineer who knows the Customer's environment in depth and acts as the primary contact for all MariaDB product-related matters. Note that Premium Support is not available for MariaDB Cloud.

For critical issues (S1), Premium Support provides a 15-minute Initial Response Time 24 x 7, with management updates for S1 issues every 4 hours 24 x 7. To maintain these SLAs, the Customer must upgrade to the latest or previous maintenance release (N or N-1) of its release series within 6 months of a new maintenance release.

Product Support

Product support encompasses the services provided to Customers to help them use a product effectively, troubleshoot issues, and resolve problems. This can include access to technical assistance, documentation and maintenance, aiming to ensure successful product adoption.

Problem Resolution Support

The focus of Problem Resolution Support is helping to restore service (due to outages caused by crashes, replication failures, table corruption, etc.) and assisting with command syntax, installation, configuration, upgrades, and other general product usage topics.

Support offers troubleshooting guidance and dedicates reasonable effort to resolving performance issues, architectural risks, and security vulnerabilities; direct performance tuning, architecture reviews, and security tuning are distinct services.

Engineering Support

Engineering Support can include bug fixes, patches, hotfixes, and topics that require communication with or escalation to MariaDB's product engineering teams concerning MariaDB Supported Products.

Hotfixes (also known as "custom builds") are provided to address critical failures and may not receive the full Quality Assurance and regression testing performed on regular maintenance releases due to the urgent nature of the situation. Hotfixes are generally built upon the last General Availability (GA) release of a product and are intended for temporary use until a fixed GA release is available.

Custom feature development (Non-Recurring Engineering) is subject to a separate written agreement and is not included in Engineering Support.

Engineering Support is available only for Supported Products, and for Product release series under Extended Support as described below, on platforms for which MariaDB produces supported product binaries as stated in the Engineering Policy. Engineering Support is unavailable for Product release series that have reached their End of Life date. Review the Engineering Policy for more information. For third-party products, please see the respective vendor's website.

Real-Time Chat Support

Real-time chat support is available to Customers with Premium Support or Managed Operations Support services. Customer technical contacts will be invited to join a real-time chat facilitated through a private channel as provided by MariaDB.

Real-time chat allows for better communication between the Customer and MariaDB. However, there is no response SLA or expectation of immediacy for chat requests. Chat is provided first come, first served, as available, and does not replace the Customer Support Portal as the primary way to receive support. All issues, requests, etc. must be ticketed.

Telephone Support

Premium Support and Managed Operations Support services include telephone support, although that support does not replace the need to open tickets.

For Standard and OEM Support, telephone support is reserved for S1 emergency production outages, for which the Customer may request that a MariaDB Support Engineer make contact by voice. Resolving technical issues generally requires analysis of system logs and other data that must be transmitted via file attachments to the support issue or by uploading to MariaDB's upload server rather than by telephone. Including this information when reporting the support issue dramatically hastens the process of resolving the problem and restoring production functionality.

For Managed Operations, telephone support is provided as necessary and available, is prioritized for S1 issues, is subject to engineer availability, and may require scheduling for non-urgent consultations.

Issue Severity and Service Level Agreements

All issues are assigned a severity level (S1-S4) reflecting the impact to production operations. This is set initially by the Customer technical contact when reporting a new issue via the Customer Support Portal, and MariaDB Support (including Managed Operations) will, in its sole discretion, confirm that the issue receives an appropriate rating. Each severity level has a corresponding Service Level Agreement (SLA) that is an Initial Response Time.

The Initial Response Time means the goal for a MariaDB Support Engineer to respond to a Customer issue according to the assigned severity level. The Initial Response Time is measured from the time an issue is created in the MariaDB Customer Support Portal.

Severity	Description	Initial Response Time		
		OEM Support	Standard Support	Premium Support
S1	Critical impact problem that severely affects the ability to conduct business. This means that	30 min 24 x 7	30 min 24 x 7	15 min 24 x 7

Severity	Description	Initial Response Time		
		OEM Support	Standard Support	Premium Support
	production systems are down (completely non-responsive or not functioning) and no known workaround exists.			
	Ongoing S1 issue updates to management	NA	24 hrs	4 hrs
S2	High impact problem in which production operations are disrupted but remain somewhat productive or have an available workaround.	2 hrs 24 x 5	2 hrs 24 x 5	1 hr 24 x 5
S3	Medium impact problem that involves partial loss of non-critical functionality. This may be a minor issue with limited or no loss of functionality or impact to production operations. This includes administrative requests and errors in product documentation.	4 hrs 24 x 5	4 hrs 24 x 5	4 hrs 24 x 5
S4	Low level problem that does not significantly affect system function or operations. This includes new feature requests.	8 hrs 24 x 5	8 hrs 24 x 5	8 hrs 24 x 5

MariaDB Support working hours are Monday to Friday (24 x 5), excluding public holidays. Business-critical incidents (S1 tickets) will be handled 24 x 7. Assessing the business impact is part of MariaDB Standard Operating Procedure.

Special Support Scenarios

Escalation Requests

Customers may request escalation of a ticket by creating a new ticket in the Customer Support Portal that references the ticket to be escalated.

Available escalations include:

- Emergency Callbacks for S1 emergency production outages.
- Higher Severity Handling when an issue has become more serious than reported.
- Engineer in a Different Timezone (unless overridden by the Customer's data sovereignty restriction(s); see the Data Sovereignty section below).
- Escalation to MariaDB Management (ticket review and - when required - corrections).

Extended Support

When a Product release series reaches its End of Standard Support date in the Engineering Policy, a Customer with Standard or Premium Support may purchase Extended Support for additional fees until the End of Life date stated there. Extended Support covers security fixes and highly critical bug fixes only, as described in the Engineering Policy.

Data Sovereignty

Due to security policies or regulations, a Customer may require data sovereignty regarding the location of MariaDB personnel. In such cases, MariaDB personnel must be located in a single region or designated regions, and the Customer will not allow personnel outside of those areas to access its environment. The Customer and MariaDB must agree in writing to any sovereignty requirements placed on the locations of MariaDB Support Engineers.

Full Sovereignty

The Customer and MariaDB may agree on full sovereignty, requiring MariaDB Support Engineers to be located only in a specific region. SLAs will only apply during business hours for the given region. Outside these hours, MariaDB will make commercially reasonable efforts to support the Customer as resources are available.

Partial Sovereignty

The Customer and MariaDB may agree on partial sovereignty, restricting MariaDB Support Engineers outside of a specific region from accessing data (read or write) in the Customer’s environment. This allows for data definition language, replication, and infrastructure-related assistance to continue from other regions while maintaining strict sovereignty over the data itself.

Root Cause Analysis

A Root Cause Analysis (RCA) can only be requested for a production outage. To enable analysis, the Customer must provide relevant logs and configuration information. An RCA request must be made in a support ticket that is separate from other requests for assistance. All RCA tickets are handled at an S4 severity level, without an Initial Response Time. RCAs are provided on a Reasonable Effort Support basis.

Commercially Reasonable Effort Support

Some scenarios, such as help with Product release series that have reached their End of Standard Support date without Extended Support, some third-party products, and operating systems or platforms not listed as supported in the Engineering Policy, may only qualify for commercially reasonable effort support (“Reasonable Effort Support”). This means MariaDB Support will try to help resolve the issue, but will not be able to offer any product modifications such as bug fixes or security patches. MariaDB will usually recommend upgrading to a fully supported version.

Examples include operating systems no longer listed as supported in the Engineering Policy (such as RHEL 7 and Windows Server 2008), and platforms for which MariaDB does not produce supported product binaries (such as FreeBSD).

MariaDB will make commercially reasonable efforts to work with other product and platform vendors to resolve issues affecting MariaDB’s Supported Products.

There are no SLAs for Reasonable Effort Support.

Additional Information

The overall level of support available for a particular product and platform combination may vary from version to version. Support for release series that have reached their End of Life date is outside the scope of this Policy and may be subject to a separate written agreement.

Contact Sales for more information regarding support for a particular product and platform combination or for release series that have reached their End of Life date.

MariaDB may modify this MariaDB Support Policy, including the Engineering Policy, at any time and publish the updated versions at https://mariadb.com/support-policy and https://mariadb.com/engineering-policies. MariaDB plc or any of its affiliates may do so on MariaDB’s behalf. It is the Customer’s obligation to keep up to date on changes to this Policy and the Engineering Policy.

Addendum A: OEM Support

This Addendum A applies only to Customers that have purchased OEM Support.

OEM Support means the Support Services provided by MariaDB to Customers that serve End Users as further defined in this Policy. “End User” means an entity that acquires Customer’s products, software or services for its internal use, and not for resale, lease, loan, or redistribution. In each case, the Customer and MariaDB agree on OEM Support for specific Customer products, software or services that rely on or embed agreed MariaDB products (“Named Application”).

Agreed MariaDB products and the Named Application(s) are specified in an Order Form or in a negotiated agreement between the Customer and MariaDB.

Prior to making agreed MariaDB products embedded in the Named Application available to End Users, the Customer will require End Users to agree to Customer’s then-current end user agreement, which will include terms no less protective of MariaDB and the MariaDB products and services than (i) the terms of the MariaDB Subscription Agreement published on https://mariadb.com/terms and (ii) the terms protecting the Customer and the Customer’s own products, software and services.

Customer will provide L0 - L2 Support for its Named Application. If the cause of the Named Application issue is suspected to be related to an agreed MariaDB product, Customer will make an effort to resolve the issue before involving MariaDB. Issues handed over to MariaDB must be documented in English.

Customer’s support obligations include:

1. Engaging with End Users, inspecting the Support issue, reviewing the End User’s use case, and (re-)configuring software based on documented requirements.
2. Fixing configuration issues and giving guidance for changing unsupported use cases.
3. Attempting to find a workaround for the problem to limit and prevent further damage to the Named Application.
4. For suspected bugs, pinpointing the location of the defect and collecting and properly recording the necessary diagnostic data for further follow-up by MariaDB, preferably with a reproducible test case.

MariaDB will deliver L3 Support to the Customer and not to End Users.

L0 - L3 Support mean technical support and maintenance services divided into the following categories:

- L0 Support covers entitlement verification and End User self-services.
- L1 Support covers basic installation and upgrades, configuration, general usage and best practices, and simple service restoration, typically supplying information contained within product documentation and knowledge bases.
- L2 Support covers issues requiring in-depth analysis such as attempts to reproduce a problem in the absence of existing test cases.
- L3 Support covers issues that require knowledge of the product source code and internals, such as bug fixes for defect resolution, problems caused by complex interactions with third-party software, and explanation or analysis of the internal behavior of a product.

Addendum B: Cloud Support

This Addendum B applies only to Customers using MariaDB Cloud services. It describes the Support Services for MariaDB products used in the MariaDB Cloud services and contains the Service Level Agreement (“Monthly Uptime SLA”) for the availability of MariaDB Cloud services.

Definitions

- **Monthly Uptime Percentage:** The total number of minutes in a billing month, minus the total number of minutes of Downtime suffered in that month, divided by the total number of minutes in that month, expressed as a percentage. The formula for calculation is:

  ((Total Minutes in Month - Minutes of Downtime) / Total Minutes in Month) * 100.

- **Downtime:** The period during which the managed database service is “Unavailable”, excluding the Excluded Downtime, as defined below.
- **Unavailable/Unavailability:** A database instance or cluster shall be considered “Unavailable” if it experiences a continuous period of 5 minutes or more (1 minute or more for the MariaDB Cloud Power Tier and PowerPlus Tier) with a 0% success rate for valid connection attempts or primary read/write operations. A “valid connection attempt” is one that conforms to MariaDB documentation and would normally result in a non-error response.
- **Service Credit:** A credit applied to the Customer’s account, calculated as a percentage of the monthly service fee for the affected database instance or cluster, to compensate for a breach of the Monthly Uptime SLA.

Shared Responsibility Model

MariaDB operates the cloud infrastructure for MariaDB components, database infrastructure and maintenance, while the Customer is responsible for the configuration and administration of the database provisioned by MariaDB. In BYOC the Customer is also responsible for the Customer’s cloud account, including its IAM, billing and account-level infrastructure. The table below summarizes the responsibilities of MariaDB and the Customer.

Customer Responsibility - The Customer is responsible for the setup and/or configuration of the feature. For example:

- Creation of database users and credentials (Self Service or Managed Operations)
- Set up the Allow List for application access to the database

MariaDB Responsibility - MariaDB is responsible for setup and/or execution of the feature. For example:

- Provisioning and maintenance of Cloud infrastructure for MariaDB components
- Patching for vulnerabilities detected in operating system and database software (Enterprise Server, MaxScale)
- Backup management

Shared Responsibility - MariaDB provides the feature set as UI or API controls, and the Customer is responsible for the configuration. For example:

- Root cause analysis for platform incidents in Customer cloud accounts (BYOC)
- PrivateLink setup and configuration

Not Applicable (N/A) - When databases are provisioned in MariaDB managed clouds, some responsibilities that apply to BYOC are not applicable, and are marked as N/A.

Responsibilities for maintaining systems are as follows:

Responsibility Area	MariaDB Cloud	Customer DB in BYOC	Subject to Change Management
Cloud Infrastructure & Account			
Cloud Infrastructure for MariaDB components (provisioning & maintenance)	MariaDB Responsibility	MariaDB Responsibility	No
Cloud Account Ownership	MariaDB Responsibility	Customer Responsibility	Yes
Cloud Account Billing	MariaDB Responsibility	Customer Responsibility	No
Service Quotas, Limit Increases, Org Policies / SCPs	MariaDB Responsibility	Customer Responsibility	Yes
Resource Tagging and Cost Governance	N/A	Customer Responsibility	No
Operating System & Database Software			
Operating System (provisioning, hardening, patching)	MariaDB Responsibility	MariaDB Responsibility	Yes
Database Infrastructure	MariaDB Responsibility	MariaDB Responsibility	Yes
Database Launch and Configuration	Customer Responsibility	Customer Responsibility	No

Responsibility Area	MariaDB Cloud	Customer DB in BYOC	Subject to Change Management
External Replication to/from non-Cloud instances	Customer Responsibility	Customer Responsibility	No
Vulnerabilities and Patching (DB Engine, MaxScale)	MariaDB Responsibility	MariaDB Responsibility	Yes
Maintenance Window Scheduling (proposed by MariaDB)	MariaDB Responsibility	MariaDB Responsibility	Yes
Networking			
VPC / Subnet / Route Table / DNS Design	MariaDB Responsibility	Customer Responsibility	Yes
PrivateLink Setup	Shared Responsibility	Shared Responsibility	Yes
Allow List for Application Access	Customer Responsibility	Customer Responsibility	No
Identity & Access			
IAM and Cloud Account Security	MariaDB Responsibility	Customer Responsibility	No
Cross-Account IAM Role Provisioning for MariaDB Operator Access	N/A	Customer Responsibility	No
Documentation of Required IAM Permissions	MariaDB Responsibility	MariaDB Responsibility	No
Audit / Review of MariaDB Access into Customer Cloud Account	N/A	Customer Responsibility	No
Database User Management	Customer Responsibility	Customer Responsibility	No
Data Protection			
Encryption at Rest	MariaDB Responsibility	MariaDB Responsibility	No
Encryption in Transit & TLS Certificate Management	MariaDB Responsibility	MariaDB Responsibility	No
Backup & Disaster Recovery			
Limited Daily Automatic Backup Scheduling, Execution, Retention	MariaDB Responsibility	MariaDB Responsibility	No

Responsibility Area	MariaDB Cloud	Customer DB in BYOC	Subject to Change Management
Additional Backup Scheduling, Execution	Customer Responsibility	Customer Responsibility	Yes
Backup Storage Bucket Ownership	MariaDB Responsibility	Customer Responsibility	No
Restore Testing	Customer Responsibility	Customer Responsibility	No
Monitoring, Logging & Audit			
Database Audit Log Generation	Customer Responsibility	Customer Responsibility	No
Audit Logging Bucket Ownership and Retention	MariaDB Responsibility	Customer Responsibility	No
SIEM Integration for database logs	Customer Responsibility	Customer Responsibility	No
Application-Level Monitoring	Customer Responsibility	Customer Responsibility	No
Database Operations			
Schema Design, Indexing, Query Tuning	Customer Responsibility	Customer Responsibility	No
Application Connection Pooling & Client Configuration	Customer Responsibility	Customer Responsibility	No
Compliance			
Platform Compliance Certifications (SOC 2, ISO 27001, etc.)	MariaDB Responsibility	MariaDB Responsibility	No
Customer Cloud Account Compliance Posture	N/A	Customer Responsibility	Yes
Support & Incident Response			
Anomaly Detection on Platform	MariaDB Responsibility	MariaDB Responsibility	No
Event Case Creation, Severity Classification, Escalation	MariaDB Responsibility	MariaDB Responsibility	In Arrears
Service Request Creation	Customer Responsibility	Customer Responsibility	No
Root Cause Analysis for Platform Incidents	MariaDB Responsibility	Shared Responsibility	Yes

 All Rights Reserved.

Responsibility Area	MariaDB Cloud	Customer DB in BYOC	Subject to Change Management
Root Cause Analysis for Customer-Account Incidents	N/A	Customer Responsibility	No
Lifecycle			
Data Offboarding at Contract End	Customer Responsibility	Customer Responsibility	Yes
Decommissioning of Cross-Account IAM Role & Cloud Resources	N/A	Customer Responsibility	Yes

Excluded Downtime

The following events or circumstances are excluded from the Downtime and from the Monthly Uptime Percentage calculation:

- **Deployment:** Period for planned provisioning of the Customer's MariaDB Cloud instance. Once the MariaDB Cloud instance access details are provided to the Customer, availability starts.
- **Scheduled Maintenance:** Any period of maintenance for which the Customer is notified at least 7 days in advance. The total duration of Scheduled Maintenance shall not exceed 24 hours per annum.
- **Emergency Maintenance:** Any period of maintenance that MariaDB deems necessary to perform urgently to address a security vulnerability or a condition that could otherwise impact the stability and integrity of the MariaDB Cloud service. MariaDB will use commercially reasonable efforts to provide advance notice to the Customer, and such maintenance is excluded from the Downtime calculation regardless of the notice period.
- **Maintenance Window:** A pre-scheduled period during which MariaDB performs technical updates, security patches, or infrastructure upgrades that may cause temporary service interruptions or performance degradation. Duration: up to 1 hour per month per server.
- **Customer-Induced Issues:** Any downtime resulting from:
    - The Customer's applications, data, code, or custom configurations.
    - The Customer's misuse of the MariaDB Cloud service or use of the service in a manner inconsistent with MariaDB's official documentation, e.g. intentionally reducing or degrading the availability of the service.
    - The Customer exceeding its allocated resource quotas or service limits.

    - Any other actions, errors or omissions of the Customer, its employees, agents, or end users that violate the terms of the applicable agreement.
- **Force Majeure:** Unavailability of communications facilities or energy sources (including blackouts or brownouts), acts of God, acts of government, pandemic, epidemic, fires, earthquakes, quarantine, strikes, delays in transportation, shortages, riots, terrorism, war or other events outside MariaDB's reasonable control.
- **Third-Party Failures:** Issues with networks, services, or hardware outside MariaDB's direct control and demarcation point.
- **Beta or Preview Features:** Any downtime related to services or features explicitly designated by MariaDB as "beta", "preview", "pilot", or otherwise non-production ready.
- **Suspension of Service:** Any downtime that occurs while the service is suspended due to the Customer's failure to pay fees, or its violation of the applicable agreement.

Service Level Matrix

MariaDB commits to the following Monthly Uptime SLA for the respective service tiers:

Tier	Performance Standard
MariaDB Cloud Foundation Tier	Multi-node configurations will deliver a Monthly Uptime Percentage of 99.95%. For example, with this availability target in a 30-day billing month the maximum service downtime is 21 minutes and 36 seconds.
MariaDB Cloud Power Tier	Multi-node configurations will deliver a Monthly Uptime Percentage of 99.995%. For example, with this availability target in a 30-day billing month the maximum service downtime is 2 minutes and 10 seconds.
MariaDB Cloud PowerPlus Tier	Multi-node configuration based on Galera will deliver a Monthly Uptime Percentage of 99.995%. For example, with this availability target in a 30-day billing month the maximum service downtime is 2 minutes and 10 seconds.

Single-node configurations are not covered by a Monthly Uptime SLA.

Service Credits

MariaDB provides Service Credits as specified by MariaDB or agreed with the Customer.

Service Credits are non-transferable and will be credited against future invoices for the affected MariaDB Cloud database instance or cluster. Service Credits will not be applied to fees for any other MariaDB product or service and are not redeemable for cash. Service Credits awarded in

a single billing month shall not exceed 100% of the monthly fee for the affected database instance or cluster.

To be eligible for a Service Credit, the Customer must submit a request in writing to MariaDB within 30 days of the end of the billing month in which the Downtime occurred. The request must include the dates and times of the Downtime for which the credit is being claimed. Otherwise, the Customer forfeits its right to receive a Service Credit.

The Service Credits set forth in this Monthly Uptime SLA shall be MariaDB's sole and exclusive obligation, and Customer's sole and exclusive remedy, for any Downtime or other failure by MariaDB to meet the Monthly Uptime SLA.

Addendum C: Bring Your Own Cloud (BYOC)

This Addendum C applies only to Customers using MariaDB Cloud in a Bring Your Own Cloud (BYOC) deployment. Addendum B applies to BYOC deployments, as supplemented by this Addendum C.

Definitions

- CSP (Cloud Service Provider): The third-party infrastructure provider (such as AWS, Azure, or GCP) hosting the Customer's cloud account in which MariaDB components are deployed and operated.
- Control Plane: The centralized management environment operated by MariaDB to deploy and manage MariaDB Cloud.
- Data Plane: The compute, storage, and networking resources in the Customer's account.

Deployment Model and Responsibilities

BYOC is a deployment model for MariaDB Cloud where the database software runs inside the *Customer's own* cloud account rather than in infrastructure fully controlled by MariaDB. MariaDB manages the database layer remotely, while the underlying cloud account and its resources belong to the Customer. Upon termination or expiration of MariaDB Cloud in BYOC, the Customer will, within 10 business days, remove all MariaDB Cloud components, including license keys, tokens, or other credentials, and certify such removal in writing upon MariaDB's request.

Customer's responsibilities

- Owns the relationships with, and payments to, the CSP and other environment suppliers, including all CSP charges generated by MariaDB-managed database operations within the account (e.g. compute for high-availability replicas, backup and snapshot storage, cross-AZ/region data transfer, and monitoring resources). MariaDB is not liable for any infrastructure costs, fees, or overages incurred in the Data Plane.
- Provisions and maintains the account-level infrastructure: networking, VPC/VNet configuration, subnets, security groups/firewalls.
- Provides, grants and manages the Identity and Access Management (IAM) roles/permissions, networks, and telemetry (including system metrics and logs) required for MariaDB's Control Plane to operate on top of Customer's Data Plane, and restricts MariaDB's access to what is necessary for the provision of the services. The Customer will not revoke, rotate, or materially modify such roles, credentials, network paths, or telemetry without at least 5 business days' prior written notice to, and coordination with,

MariaDB (except where required for the Customer's emergency security response, with notice as soon as practicable).

- Remains responsible for account-level compliance, cost governance, managing cloud account-level permissions and quota increases, and any organizational policies (tagging, resource quotas, region restrictions).
- Ensures connectivity requirements are met (VPC peering, private link, etc.) if applicable and provides MariaDB with timely access, logs, and knowledgeable personnel needed to diagnose and remediate incidents. SLA response targets are suspended while a ticket is pending Customer action.
- Maintains current, restorable backups of the Customer's cloud account data, software, and systems including the Data Plane.
- Complies with industry standards and with MariaDB baseline security and connectivity prerequisites as communicated or published and updated by MariaDB from time to time. The Customer will remediate identified deviations within the period stated in MariaDB's notice; SLAs are suspended for affected instances until remediation. MariaDB may, without liability, decline to deploy or suspend the services if these prerequisites are not met or if the Control Plane loses required connectivity or operational telemetry from the Data Plane.
- Maintains at least 1 trained technical contact reachable 24 x 7 for S1 incidents; reasonable emergency actions taken by MariaDB to protect service integrity when such contact is unreachable shall not give rise to MariaDB liability.
- Does not alter the Customer's cloud account parameters, install software, or take any other action in a manner that could degrade the services or interfere with MariaDB-deployed components on top of the Customer's Data Plane.
- Remains responsible and strictly liable for the security posture, misconfigurations, and unauthorized access to the Data Plane itself (including who else has access and what other resources reside there), except where such misconfigurations or unauthorized access are directly caused by MariaDB's gross negligence or willful misconduct.

MariaDB's responsibilities

- Deploys, configures, and operates the MariaDB components including database software (provisioning, patching, upgrades, database-level backup configuration, monitoring, database-level high availability and failover configuration for HA/DR) on top of the Customer's Data Plane. Except for the database-level backups described in this Policy, MariaDB does not host, back up, or provide disaster recovery for the Data Plane.
- Verifies that the Customer's Data Plane meets the MariaDB baseline security and connectivity prerequisites before deployment and periodically thereafter.
- Monitors MariaDB-deployed components for configuration drift. MariaDB may revert unauthorized changes or treat them as Customer-Induced Issues, with applicable SLA commitments suspended, until remediated.

- Provides the Control Plane and automation used to manage the database layer.
- Provides the database service in accordance with applicable SLAs and support commitments. The Monthly Uptime SLA is strictly conditioned upon the Customer's compliance with its BYOC obligations set out in this Policy and any applicable agreement. Support time spent on issues arising from or relating to the Data Plane may be billed at MariaDB's then-current Professional Services rates.
- Uses commercially reasonable administrative and technical measures for the database-level security configuration (encryption at rest/in transit, access controls to the database itself, vulnerability patching of the database engine).
- Coordinates operational readiness before go-live with the Customer's designated technical contact or engineering team.

Shared Responsibility Model

The division of responsibilities for BYOC deployments is set out in the "Customer DB in BYOC" column of the Shared Responsibility Model table in Addendum B.

Additional Excluded Downtime

In BYOC deployments, the following are also excluded from the Downtime and from the Monthly Uptime Percentage calculation, in addition to the Excluded Downtime set out in Addendum B:

- Customer Action Required for Maintenance: Where maintenance requires Customer action (e.g. IAM approvals, capacity provisioning, or network changes), any delay, downtime, or degradation attributable to the Customer's failure to timely complete such actions.
- Customer-Induced Issues: In addition to the Customer-Induced Issues set out in Addendum B, any downtime resulting from:
    - The unavailability or exhaustion of CSP capacity, service quotas, or instance types in the Customer's cloud account.
    - The Customer's alteration of Customer's cloud account parameters, installation of software that degrades the services, interference with MariaDB-deployed infrastructure, or periods where MariaDB cannot measure availability due to the Customer's failure to maintain required IAM roles, monitoring access, connectivity, or telemetry.
- Third-Party Failures: Downtime or data loss caused by the Customer's CSP.
- Suspension of Service: Any downtime that occurs while the service is suspended due to the Customer's failure to perform its BYOC obligations.

Addendum D: Managed Operations

This Addendum D applies only to Customers that have purchased Managed Operations. Managed Operations (MO, previously known as Remote Database Administrator, Remote DBA, RDBA or Remote Login Support) provides proactive and reactive operational management of Customer MariaDB environments. The MO team monitors, maintains, responds to incidents, and performs advisory and change management tasks directly within the Customer environment via secure remote access. MO supports deployment models including on-premises, hybrid, and cloud environments.

Under MO, Support Engineers log directly into the Customer environment and perform work on the Customer's behalf. Under other Support options, Support Engineers guide Customers through resolution steps via the MariaDB Customer Support Portal.

MO is available as an add-on to Standard Support or Premium Support for MariaDB Enterprise offerings. When a Customer has also contracted Premium Support, heightened Premium SLAs apply to all incident responses.

Service Scope - Managed Operations

MO services are organized into 2 categories and a separate commercially reasonable effort category.

Category 1 - Operational Baseline (Always Included)

The following services are performed by the MO team without requiring a Customer request (unless stated otherwise) and are non-negotiable components required for MO to function correctly.

- Monitoring and alerting setup and maintenance
    - Deployment of MariaDB-approved monitoring tooling.
    - Ongoing maintenance and configuration of alert thresholds for server availability, replication health, and other key indicators.
    - Automatic ticket creation in MariaDB's Customer Support Portal for qualifying alerts.
- Incident response
    - 24 x 7 response for critical incidents within specified SLA times.
    - 24 x 5 (business days) follow-up on other severity cases.
- Backup configuration and status monitoring
    - Configuration of database-level backup settings and monitoring of backup job status and logs. MariaDB's responsibility is limited to database-level configuration and to monitoring the logs and status provided by the database or agreed tools.

    - Except for MariaDB Cloud, Customers are responsible for providing and maintaining the required backup infrastructure.
- Product release series and maintenance release upgrades of contracted MariaDB systems to Supported Products
    - Applies to all upgrades, including major version upgrades (e.g. 10.x to 11.x).
    - Requires collaborative planning, Customer approval, and adherence to agreed maintenance windows.
    - Application compatibility testing for major version upgrades is the Customer's responsibility and is out of MO scope.
- Initial environment and configuration review.
- Quarterly platform configuration recommendations.
- Semi-annual, on Customer request:
    - Architecture reviews.
    - Security and performance audits.
- Annual backup verification via automated restore.
    - Customers must provide and maintain a suitable target environment for the restore process.

Category 2 - Advisory and Project Tasks (Included with Effort Limits)

The following services are included within MO and are subject to commercially reasonable efforts. MO activities that grow into larger, multi-day engagements or require dedicated project resourcing require a separate Statement of Work (SOW). The MO team will notify the Customer when a task is approaching this threshold.

- Replication setup, configuration, and repair
    - Initial replication setup and significant reconfigurations are treated as project-scoped tasks.
    - Break-fix repair of existing replication as part of incident response is covered under "Category 1 (Operational Baseline)".
- Migration hardware provisioning assistance
    - Advisory and coordination guidance for new server or cloud instance deployments.
    - Physical or cloud infrastructure procurement, provisioning, and payment remain the Customer's responsibility.
- Schema adjustment assistance / Change Management
    - Planning, guidance, and execution support for straightforward schema changes and migrations (changes without data transformation).
    - Complex adjustments involving multiple systems or large-scale data transformation require a separate SOW.
- Reactive SQL query optimization
    - Optimization of specific queries identified as bottlenecks through monitoring or incident investigation.

    - Open-ended or application-wide tuning engagements are out of scope.
- Database recovery assistance
    - This service is exclusively for live production databases facing critical data loss or corruption.
    - The environment will be checked before execution.
- Capacity planning recommendations (storage, vCPU, network…)
- High availability configuration guidance
    - Advice based on best practices and available documentation.

Commercially Reasonable Effort - Degraded Coverage

When a Customer is operating a Product release series of a MariaDB product that has reached its End of Standard Support date without Extended Support, or its End of Life date, or an operating system or platform not listed as supported in the Engineering Policy, MO coverage transitions to Reasonable Effort Support. The following conditions apply:

- No SLA guarantees for issues attributable to the unsupported software versions or operating systems.
- Bug fixes, security patches, and hotfixes are not available for those release series, operating systems or platforms.
- The MO team will make commercially reasonable efforts to stabilize and restore service, but an upgrade to a fully supported version will be strongly recommended.
- Customers under Reasonable Effort Support coverage are expected to maintain an active upgrade plan. Continued Reasonable Effort Support coverage is provided at MariaDB's discretion, is not indefinite and may be subject to further restrictions.

Incident Management Exclusions

The following incident types are outside MO scope. MariaDB will assist with recovery within commercially reasonable efforts when practical. No SLAs apply to the following:

- Hardware failures outside MariaDB's direct control.
- Incidents caused by non-MariaDB actions or configuration changes not performed by the MO team.
- Incidents arising from Customer-owned network infrastructure, third-party services, or Customer applications.
- Performance degradation that does not constitute an availability incident (e.g. the cluster is operational but not meeting performance expectations).
- Security incidents or suspected data breaches (e.g. compromised accounts, malware, unauthorized access), which fall under the Customer's information security or incident response program.

- Incidents arising from application-level defects, bad releases, or schema changes owned by the Customer's development team (e.g. bad deployments, incompatible Object-Relational Mapping changes, code bugs).
- Incidents whose root cause is data quality, user error, or business-process issues (e.g. wrong data loaded, incorrect bulk updates, accidental deletes without backups).
- Incidents caused by denial-of-service attacks, upstream provider outages, or broader security events outside the managed environment.

Out of Scope

The following activities are outside the scope of MO and require a separate Statement of Work (SOW):

- New application development or schema design from scratch
- Application compatibility testing
- Data transfer between platforms and/or cloud providers
- Custom scripting, automation, or application development
- Deep, multi-day performance tuning engagements
- Compliance audit support and reporting artifacts (e.g. PCI-DSS, HIPAA)
- Training or knowledge transfer sessions
- Architecture design or re-design of platform topology (e.g. HA/DR patterns, multi-region design, sharding strategy, selection of specific cloud services)
- Cross-engine or cross-technology migrations (e.g. relational to columnar, introduction of the GridGain layer)
- Capacity planning and sizing studies for new workloads or major product launches, including load testing and benchmarking
- Integration work with third-party tools or platforms (e.g. BI tools, ETL/ELT frameworks, CDC pipelines, message queues, analytics platforms)

Managed Operations Scope Summary

The table below provides a consolidated reference of MO activities and their scope category.

Service	Scope
Monitoring and alerting setup and maintenance	Category 1
Automated alert response (availability, replication, etc.)	Category 1
Backup configuration and status monitoring	Category 1
Product release series and maintenance release upgrades	Category 1
Event responses (monitoring tickets)	Category 1
Initial environment and configuration review	Category 1

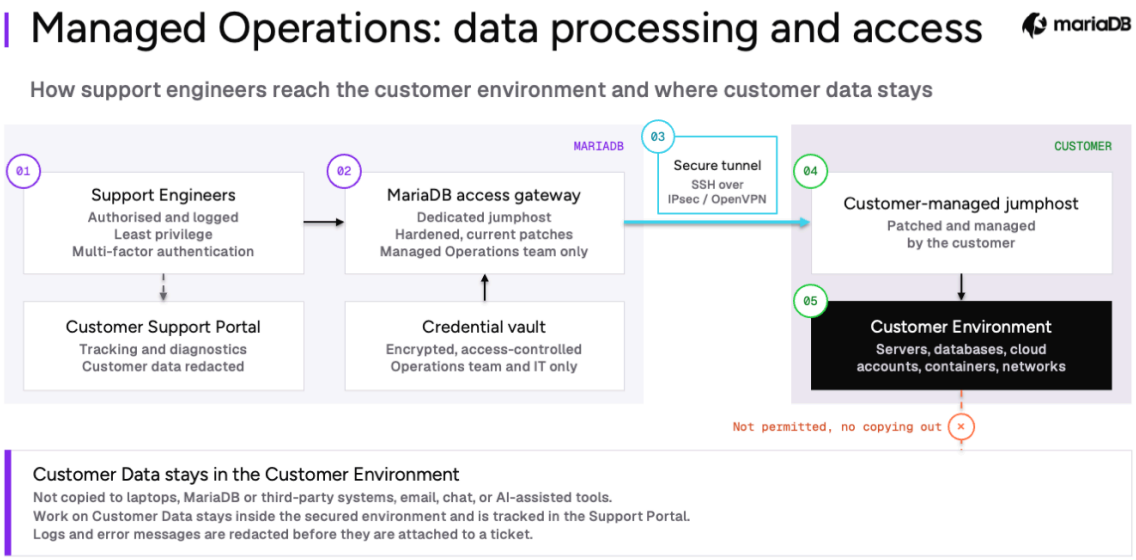
Service	Scope
Quarterly configuration recommendations	Category 1
Semi-annual security and performance audits (on request)	Category 1
Semi-annual architecture review (on request)	Category 1
Annual backup verification via automated restore	Category 1
Replication setup and configuration	Category 2
Migration hardware provisioning assistance	Category 2
Schema adjustment assistance / Change Management	Category 2
Reactive SQL query optimization	Category 2
Database recovery assistance	Category 2
Capacity planning recommendations	Category 2
High availability configuration guidance	Category 2

Connectivity and Access

Support Engineers require secure remote access to Customer environments other than MariaDB Cloud. The following conditions apply:

- The Customer must provide and manage a jumphost system for connectivity and monitoring purposes.
- Access is provided exclusively via SSH through the Customer-managed jumphost over a point-to-point IPsec or OpenVPN tunnel from a MariaDB-managed jumphost.
- Any deviation from the standard connectivity model requires a written exception agreed by both parties and may result in adjusted SLAs or additional fees.

Screen-sharing applications (such as Zoom, Microsoft Teams, or Webex) are not supported as primary access methods for MO delivery.



This diagram is for illustration only. If it conflicts with the text of this Addendum D, the text prevails.

Server and Database Accounts

A single shared vendor account for server, database, and VPN access is strongly preferred. Where security policy, regulation, or compliance requirements (e.g. PCI-DSS or HIPAA) prevent the use of a shared vendor account, individual accounts may be created for each Support Engineer. The following conditions apply:

- The Customer is responsible for timely creation and maintenance of the shared vendor account or, where permitted, the individual Support Engineer accounts.
- No SLA guarantees or 24 x 7 coverage can be provided where individual accounts are required, unless otherwise agreed in writing.
- SSH key-based authentication is strongly recommended in all configurations.

Monitoring Infrastructure

The MO team requires a server within the Customer's infrastructure for the installation of monitoring software and related utilities. A standalone server is recommended; however, the jumphost may serve this purpose where a dedicated server is not available.

Data Processing and Access

As used in this section, “Customer Data” refers to all Customer data and information that Support Engineers are provided access to in order to perform MO.

- Support Engineers comply with the terms of any applicable data processing agreement with the Customer.
- Customer environments are accessed exclusively through a dedicated MariaDB-managed jumphost that is maintained with current security patches and is accessible only to the MO team.
- Credentials are stored in a PCI-compliant, access-controlled password vault accessible only to the MO team and designated MariaDB IT personnel.
- Credentials for Customers with data sovereignty or geographical restrictions are only accessible to MariaDB personnel in approved regions.
- Support Engineers will not remove Customer Data from the Customer environment by storing or copying it to MariaDB or third-party systems, other than diagnostic information permitted below.
- Where Customer Data must be accessed to perform troubleshooting or tuning, work is performed within the secured Customer environment and tracked via the MariaDB Customer Support Portal.
- Error codes, error messages, logs, and similar diagnostic metrics, with Customer Data redacted, may be included in the ticketing system for tracking and performance improvement purposes.

Onboarding and Offboarding

Onboarding

The MO service lifecycle commences on the service start date as specified in the relevant contract. Within one week of the service start date, the MO team schedules an onboarding call to gather information about the Customer’s environment, including architecture, operating systems, product versions, and backup or persistence schedules. The onboarding process includes:

- Deployment of the jumphost and configuration of secure remote access.
- Installation and configuration of monitoring software and alerting.
- Setup of server, database, and cluster accounts, and VPN where required.
- Initial environment and configuration review.
- Formal acceptance of operational accountability once all service components are verified and operational. MO SLAs apply from that acceptance.

Offboarding

Upon the expiration or termination of the relevant contract, the MO team initiates a structured decommissioning process to be completed within 30 days of its start:

- Disconnection of all proprietary monitoring and alerting systems.
- Removal of all MO-specific software and utilities from the Customer's environment.
- Delivery of a documented handoff runbook covering environment configuration, monitoring setup, and operational procedures.
- Revocation of all Support Engineer access credentials.

Where active contract renewal negotiations are in progress at the contract expiration date, MariaDB may suspend service delivery and defer the start of offboarding by up to 30 days after the contract expiration date while negotiations continue.