



# PERCONA

## Server for MongoDB Documentation 5.0

5.0.29-25 (September 26, 2024)

*Percona Technical Documentation Team*

*Percona LLC, © 2024*

# Table of contents

1. Percona Server for MongoDB 5.0 Documentation	4
1.1  Installation guides	4
1.2 Get expert help	5
2. Percona Server for MongoDB feature comparison	6
2.1 Profiling Rate Limiting	6
2.2 Get expert help	6
3. Get started	8
3.1 Quickstart guides	8
3.2 1. Installation	10
3.3 Connect to Percona Server for MongoDB	26
3.4 Manipulate data in Percona Server for MongoDB	29
3.5 What's next?	32
4. Features	34
4.1 Storage	34
4.2 Backup	39
4.3 Authentication	46
4.4 Encryption	79
4.5 Auditing	95
4.6 Profiling Rate Limit	101
4.7 Log Redaction	103
4.8 Additional text search algorithm - ngram	104
5. Administration	106
5.1 Percona Server for MongoDB Parameter Tuning Guide	106
5.2 Upgrade	107
5.3 Uninstall Percona Server for MongoDB	113
6. Release notes	116
6.1 Percona Server for MongoDB 5.0 Release Notes	116
6.2 Percona Server for MongoDB 5.0.29-25 (2024-09-26)	117
6.3 Percona Server for MongoDB 5.0.28-24 (2024-08-08)	118
6.4 Percona Server for MongoDB 5.0.27-23 (2024-06-19)	120
6.5 Percona Server for MongoDB 5.0.26-22 (2024-04-09)	121
6.6 Percona Server for MongoDB 5.0.24-21 (2024-02-01)	122
6.7 2023 (versions 5.0.15-13 through 5.0.23-20)	123
6.8 2022 (versions 5.0.6-5 through 5.0.15-13)	132

6.9 2021 (versions 5.0.2-1 through 5.0.5-4)	144
7. FAQ	150
7.1 How to check Percona Server for MongoDB version?	150
7.2 Where is the location of the configuration and data files?	150
7.3 Get expert help	150
8. Reference	151
8.1 Glossary	151
8.2 Telemetry and data collection	152
8.3 Copyright and licensing information	159
8.4 Trademark policy	160

# 1. Percona Server for MongoDB 5.0 Documentation

Percona Server for MongoDB is an enhanced, fully compatible, source available, drop-in replacement for MongoDB 5.0 Community Edition with [enterprise-grade features](#). [To migrate to Percona Server for MongoDB](#) requires no changes to MongoDB applications or code.

## What's new in Percona Server for MongoDB 5.0.29-25

### 1.1 Installation guides

Ready to try out Percona Server for MongoDB? Get started quickly with the step-by-step installation instructions.

#### Quickstart guides →

#### 1.1.1 Control database access

Define who has access to the database and manage their permissions in a single place like LDAP server, ensuring only authorized users have access to resources and operations.

#### Authentication →

#### 1.1.2 Backup and restore

Make enterprise-level backups and restores with guaranteed data consistency using Percona Backup for MongoDB (PBM). Or, create physical backups on a running server using the built-in **hot backup** functionality.

#### Get started with PBM →

#### 1.1.3 Secure access to data

Keep your sensitive data safe, ensuring users only see the data they are authorized to access.

#### Data-at-rest encryption →

**PERCONA**

## 1.2 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 February 28, 2024

 December 8, 2022

## 2. Percona Server for MongoDB feature comparison

Percona Server for MongoDB 5.0 is based on [MongoDB Community Edition 5.0](#) and extends it with the functionality that is otherwise only available in MongoDB Enterprise Edition.

	<b>PSMDB</b>	<b>MongoDB</b>
<b>Storage Engines</b>	- <a href="#">WiredTiger</a> (default) - <a href="#">Percona Memory Engine</a>	- <a href="#">WiredTiger</a> (default) - <a href="#">In-Memory</a> (Enterprise only)
<b>Encryption-at-Rest</b>	- Key servers = <a href="#">Hashicorp Vault</a> , <a href="#">KMIP</a> - Fully open source	- Key server = <a href="#">KMIP</a> - Enterprise only
<b>Hot Backup</b>	<a href="#">YES</a> (replica set)	NO
<b>LDAP Authentication</b>	(legacy) <a href="#">LDAP authentication with SASL</a>	Enterprise only
<b>LDAP Authorization</b>	<a href="#">YES</a>	Enterprise only
<b>Kerberos Authentication</b>	<a href="#">YES</a>	Enterprise only
<b>AWS IAM authentication</b>	<a href="#">YES</a>	MongoDB Atlas
<b>Audit Logging</b>	<a href="#">YES</a>	Enterprise only
<b>Log redaction</b>	<a href="#">YES</a>	Enterprise only
<b>SNMP Monitoring</b>	NO	Enterprise only
<b>Database profiler</b>	<a href="#">YES</a> with the <code>--rateLimit</code> argument	<a href="#">YES</a>

### 2.1 Profiling Rate Limiting

Profiling Rate Limiting was added to *Percona Server for MongoDB* in v3.4 with the `--rateLimit` argument. Since v3.6, MongoDB Community (and Enterprise) Edition includes a similar option [slowOpSampleRate](#). Please see [Profiling Rate Limit](#) for more information.

## PERCONA

### 2.2 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

🕒 February 28, 2024

🕒 December 8, 2022

## 3. Get started

### 3.1 Quickstart guides

Percona Server for MongoDB is an enhanced, fully compatible, source available, drop-in replacement for MongoDB 6.0 Community Edition with [enterprise-grade features](#).

Find the full list of supported platforms for Percona Server for MongoDB on the [Percona Software and Platform Lifecycle](#) page.



### 3.1.1 Install Percona Server for MongoDB

You can use any of the easy-install guides. We recommend to use **the package manager of your operating system** for a convenient and quick way to install the software for production use. **Use Docker** to try the software first.

 Package manager
  Docker
  Kubernetes
  Build from source
  Manual download

Use the package manager of your operating system to install Percona Server for MongoDB:

[on Debian and Ubuntu →](#)

[on RHEL and derivatives →](#)

We gather [Telemetry data](#) in Percona packages.

Get our Docker image and spin up Percona Server for MongoDB for a quick evaluation.

Check the Docker guide for step-by-step guidelines.

[Run in Docker →](#)

We gather [Telemetry data](#) in Docker images.

**Percona Operator for Kubernetes** is a controller introduced to simplify complex deployments that require meticulous and secure database expertise.

Check the Quickstart guides how to deploy and run Percona Server for MongoDB on Kubernetes with Percona Operator for MongoDB.

[Deploy in Kubernetes Quickstart →](#)

Have a full control over the installation by building Percona Server for MongoDB from source code.

Check the guide below for step-by-step instructions.

[Build from source →](#)

If you need to install Percona Server for MongoDB offline or prefer a specific version of it, check out the link below for a step-by-step guide and get access to the downloads directory.

Note that for this scenario you must make sure that all dependencies are satisfied.

[Install from tarballs →](#)

### 3.1.2 Upgrade instructions

If you are currently using MongoDB Community Edition, see [Upgrading from MongoDB](#).

If you are running an earlier version of Percona Server for MongoDB, see [Upgrading from Version 4.4](#).

## PERCONA

### 3.1.3 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 August 8, 2024

 December 8, 2022

## 3.2 1. Installation

### 3.2.1 System requirements

#### x86\_64

Percona Server for MongoDB has the same [system requirements](#) as the MongoDB Community Edition.

Starting in MongoDB 5.0, `mongod`, `mongos`, and the legacy `mongo` shell are supported on x86\_64 platforms that must meet these minimum micro-architecture requirements:

- Only Oracle Linux running the Red Hat Compatible Kernel (RHCK) is supported. MongoDB does not support the Unbreakable Enterprise Kernel (UEK).
- MongoDB 5.0 and above requires use of the AVX instruction set, available on [select Intel and AMD processors](#).

#### ARM64


Percona Server for MongoDB requires the ARMv8.2-A or later microarchitecture.

Currently, only [Docker images](#) are available.

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 February 28, 2024

 February 28, 2024

### 3.2.2 Installing Percona Server for MongoDB on Debian and Ubuntu

This document describes how to install Percona Server for MongoDB from Percona repositories on DEB-based distributions such as Debian and Ubuntu.

We gather [Telemetry data](#) to understand the use of the software and improve our products.

Package contents	
Package	Contains
percona-server-mongodb	The mongo shell, import/export tools, other client utilities, server software, default configuration, and init.d scripts.
percona-server-mongodb-server	The mongod server, default configuration files, and init.d` scripts
percona-server-mongodb-shell	The mongo shell
percona-server-mongodb-mongos	The mongos sharded cluster query router
percona-server-mongodb-tools	Mongo tools for high-performance MongoDB fork from Percona
percona-server-mongodb-dbg	Debug symbols for the server

#### Procedure

Before you start, check the [system requirements](#).

##### CONFIGURE PERCONA REPOSITORY

To install from Percona repositories, first you need to enable the required repository using the [percona-release](#) repository management tool.

1. Fetch **percona-release** packages from Percona web:

```
$ wget https://repo.percona.com/apt/percona-release_latest.$(lsb_release -sc)_all.deb
```

2. Install the downloaded package with **dpkg**:

```
$ sudo dpkg -i percona-release_latest.$(lsb_release -sc)_all.deb
```

After you install this package, you have the access to Percona repositories. You can check the repository setup in the `/etc/apt/sources.list.d/percona-release.list` file.

## 3. Enable the repository:

```
$ sudo percona-release enable psmdb-50 release
```

## 4. Remember to update the local cache:

```
$ sudo apt update
```

## INSTALL PERCONA SERVER FOR MONGODB

 Install the latest version      Install a specific version

Run the following command to install the latest version of Percona Server for MongoDB:

```
$ sudo apt install percona-server-mongodb
```

To install a specific version of Percona Server for MongoDB, do the following:

## 1. List available versions:

```
$ sudo apt-cache madison percona-server-mongodb
```

 **Sample output** 

```
percona-server-mongodb | 5.0.13-11.jammy | http://repo.percona.com/psmdb-50/apt jammy/main amd64 Packages
percona-server-mongodb | 5.0.11-10.jammy | http://repo.percona.com/psmdb-50/apt jammy/main amd64 Packages
percona-server-mongodb | 5.0.10-9.jammy | http://repo.percona.com/psmdb-50/apt jammy/main amd64 Packages
percona-server-mongodb | 5.0.9-8.jammy | http://repo.percona.com/psmdb-50/apt jammy/main amd64 Packages
percona-server-mongodb | 5.0.13-11 | http://repo.percona.com/psmdb-50/apt jammy/main Sources
percona-server-mongodb | 5.0.11-10 | http://repo.percona.com/psmdb-50/apt jammy/main Sources
percona-server-mongodb | 5.0.10-9 | http://repo.percona.com/psmdb-50/apt jammy/main Sources
percona-server-mongodb | 5.0.9-8 | http://repo.percona.com/psmdb-50/apt jammy/main Sources
```

2. Install a specific version packages. You must specify each package with the version number. For example, to install Percona Server for MongoDB 5.0.13-11, run the following command:

```
$ sudo apt install percona-server-mongodb=5.0.13-11.buster \
percona-server-mongodb-mongos=5.0.13-11.buster \
percona-server-mongodb-shell=5.0.13-11.buster \
percona-server-mongodb-server=5.0.13-11.buster \
percona-server-mongodb-tools=5.0.13-11.buster
```

By default, Percona Server for MongoDB stores data files in `/var/lib/mongodb/` and configuration parameters in `/etc/mongod.conf`.

**Run Percona Server for MongoDB****Start the service**

Percona Server for MongoDB is started automatically after installation unless it encounters errors during the installation process.

You can also manually start it using the following command:

```
$ sudo systemctl start mongod
```

### Confirm that the service is running

Check the service status using the following command:

```
$ sudo systemctl status mongod
```

### Stop the service

Stop the service using the following command:

```
$ sudo systemctl stop mongod
```

### Restart the service

Restart the service using the following command:

```
$ sudo systemctl restart mongod
```

Congratulations! Your Percona Server for MongoDB is up and running.

### Next steps

[Connect to MongoDB →](#)

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

[Community Forum](#) [Get a Percona Expert](#)

🕒 February 28, 2024

🕒 December 8, 2022

### 3.2.3 Install Percona Server for MongoDB on Red Hat Enterprise Linux and CentOS

This document describes how to install Percona Server for MongoDB on RPM-based distributions such as Red Hat Enterprise Linux and compatible derivatives.

We gather [Telemetry data](#) to understand the use of the software and improve our products.

Package contents	
Package	Contains
percona-server-mongodb	The <code>mongo</code> shell, import/export tools, other client utilities, server software, default configuration, and <code>init.d</code> scripts.
percona-server-mongodb-server	The <code>mongod</code> server, default configuration files, and <code>init.d`</code> scripts
percona-server-mongodb-shell	The <code>mongo</code> shell
percona-server-mongodb-mongos	The <code>mongos</code> sharded cluster query router
percona-server-mongodb-tools	Mongo tools for high-performance MongoDB fork from Percona
percona-server-mongodb-dbg	Debug symbols for the server

#### Procedure

Before you start, check the [system requirements](#).

#### CONFIGURE PERCONA REPOSITORY

To install from Percona repositories, first you need to enable the required repository using the [percona-release](#) repository management tool.

1. Install **percona-release**:

```
$ sudo yum install https://repo.percona.com/yum/percona-release-latest.noarch.rpm
```

2. Enable the repository:

```
$ sudo percona-release enable psmdb-50 release
```

## INSTALL PERCONA SERVER FOR MONGODB PACKAGES

 Install the latest version      Install a specific version

To install the latest version of *Percona Server for MongoDB*, use the following command:

```
$ sudo yum install percona-server-mongodb
```

To install a specific version of *Percona Server for MongoDB*, do the following:

1. List available versions:

```
$ sudo yum list percona-server-mongodb --showduplicates
```

#### Sample output

```
Available Packages
percona-server-mongodb.x86_64 5.0.2-1.el8 psmdb-50-release-x86_64
percona-server-mongodb.x86_64 5.0.3-2.el8 psmdb-50-release-x86_64
percona-server-mongodb.x86_64 5.0.4-3.el8 psmdb-50-release-x86_64
percona-server-mongodb.x86_64 5.0.5-4.el8 psmdb-50-release-x86_64
percona-server-mongodb.x86_64 5.0.6-5.el8 psmdb-50-release-x86_64
percona-server-mongodb.x86_64 5.0.7-6.el8 psmdb-50-release-x86_64
percona-server-mongodb.x86_64 5.0.8-7.el8 psmdb-50-release-x86_64
percona-server-mongodb.x86_64 5.0.9-8.el8 psmdb-50-release-x86_64
percona-server-mongodb.x86_64 5.0.10-9.el8 psmdb-50-release-x86_64
percona-server-mongodb.x86_64 5.0.11-10.el8 psmdb-50-release-x86_64
percona-server-mongodb.x86_64 5.0.13-11.el8 psmdb-50-release-x86_64
```

2. Install a specific version packages. For example, to install Percona Server for MongoDB 5.0.13-11, run the following command:

```
$ sudo yum install percona-server-mongodb-5.0.13-11.el8
```

By default, Percona Server for MongoDB stores data files in `/var/lib/mongodb/` and configuration parameters in `/etc/mongod.conf`.

### Run Percona Server for MongoDB

#### Note

If you use SELinux in enforcing mode, you must customize your SELinux user policies to allow access to certain `/sys` and `/proc` files for OS-level statistics. Also, you must customize directory and port access policies if you are using non-default locations.

Please refer to [Configure SELinux](#) section of MongoDB Documentation for policy configuration guidelines.

### Start the service

Percona Server for MongoDB is not started automatically after installation. Start it manually using the following command:

```
$ sudo systemctl start mongod
```

### Confirm that service is running

Check the service status using the following command: `service mongod status`

```
$ sudo systemctl status mongod
```

### Stop the service

Stop the service using the following command: `service mongod stop`

```
$ sudo systemctl stop mongod
```

### Restart the service

Restart the service using the following command: `service mongod restart`

```
$ sudo systemctl restart mongod
```

#### RUN AFTER REBOOT

The `mongod` service is not automatically started after you reboot the system.

For RHEL or CentOS versions 5 and 6, you can use the `chkconfig` utility to enable auto-start as follows:

```
$ sudo chkconfig --add mongod
```

For RHEL or CentOS version 7, you can use the `systemctl` utility:

```
$ sudo systemctl enable mongod
```

Congratulations! Your Percona Server for MongoDB is up and running.

#### Next steps

[Connect to MongoDB →](#)

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)



🕒 February 28, 2024

🕒 December 8, 2022

### 3.2.4 Installing Percona Server for MongoDB from binary tarball


You can find links to the binary tarballs under the *Generic Linux* menu item on the [Percona website](#). The list provides a binary tarball for every [supported operating system](#).

#### Tarball types

Type	Name	Description
Full	percona-server-mongodb-5.0.29-25-x86_64.tar.gz	Contains binaries and libraries
Minimal	percona-server-mongodb-5.0.29-25-x86_64-minimal.tar.gz	Contains binaries and libraries without debug symbols
Checksum	percona-server-mongodb-5.0.29-25-x86_64-minimal.tar.gz.sha256sum	Contains the MD5 checksum to verify the integrity of the files after the extraction

#### Preconditions

Install the following dependencies required to install Percona Server for MongoDB from tarballs.

 RHEL and derivatives
  Ubuntu
  Debian

```
$ sudo yum install openldap cyrus-sasl-gssapi curl
$ sudo apt install curl libsasl2-modules-gssapi-mit
$ sudo apt curl libsasl2-modules-gssapi-mit
```

#### Procedure

The following example installs Percona Server for MongoDB from a tarball on Ubuntu 22.04. Replace the link to the tarballs for your desired operating system in the following steps:

1. Fetch the binary tarball:

```
$ wget https://www.percona.com/downloads/percona-server-mongodb-5.0/percona-server-mongodb-5.0.29-25/binary/tarball/percona-server-mongodb-5.0.29-25-x86_64.jammy.tar.gz\
```

2. Extract the tarball

```
$ tar -xf percona-server-mongodb-5.0.29-25-x86_64.jammy.tar.gz
```

3. Add the location of the binaries to the `PATH` variable:

```
$ export PATH=~/.percona-server-mongodb-5.0.29-25/bin/:$PATH
```

4. Create the default data directory:

```
$ mkdir -p /data/db
```

5. Make sure that you have read and write permissions for the data directory and run `mongod`.

#### Next steps

[Connect to MongoDB →](#)

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 August 8, 2024

 December 8, 2022

### 3.2.5 Build from source code

To build Percona Server for MongoDB, you need:

- A modern C++ compiler capable of compiling C++17 like GCC 8.2 or newer
- Amazon AWS Software Development Kit for C++ library
- Python 3.6.x and Pip.
- The set of dependencies for your operating system. The following table lists dependencies for Ubuntu 20.04, CentOS 7 and Red Hat Enterprise 8 and compatible derivatives:

Linux Distribution	Dependencies
Debian/Ubuntu	python3 python3-dev python3-pip scons gcc g++ cmake curl libssl-dev libldap2-dev libkrb5-dev libcurl4-openssl-dev libsasl2-dev liblz4-dev libpcap-dev libbz2-dev libsnpappy-dev zlib1g-dev libzlib-dev libsasl2-dev liblzma-dev libext2fs-dev e2fslibs-dev bear
CentOS / RedHat Enterprise Linux 7	centos-release-scl epel-release python3 python3-devel scons gcc gcc-c++ cmake3 openssl-devel cyrus-sasl-devel snappy-devel zlib-devel bzip2-devel libcurl-devel lz4-devel openldap-devel krb5-devel xz-devel e2fsprogs-devel expat-devel devtoolset-8-gcc devtoolset-8-gcc-c++

Linux Distribution	Dependencies
RedHat Enterprise Linux/CentOS 8	python36 python36-devel gcc-c++ gcc cmake3 wget openssl-devel zlib-devel cyrus-sasl-devel xz-devel bzip2-devel libcurl-devel lz4-devel e2fsprogs-devel krb5-devel openldap-devel expat-devel cmake

## Build steps

### INSTALL PYTHON AND PYTHON MODULES

#### 1. Clone Percona Server for MongoDB repository

```
$ git clone https://github.com/percona/percona-server-mongodb.git
```

#### 2. Install the dependencies for your operating system.

Debian/Ubuntu      RHEL/CentOS

The following command installs the dependencies for Ubuntu 20.04:

```
$ sudo apt install -y python3 python3-dev python3-pip scons gcc g++ cmake curl libssl-dev libldap2-dev libkrb5-dev libcurl4-openssl-dev libsasl2-dev liblz4-dev libpcap-dev libbz2-dev libsnappy-dev zlib1g-dev libzlib-dev libsasl2-dev liblzma-dev libext2fs-dev e2fslibs-dev bear
```

#### a. The following command installs the dependencies for CentOS 7:

```
$ sudo yum -y install centos-release-scl epel-release
$ sudo yum -y install python3 python3-devel scons gcc gcc-c++ cmake3 openssl-devel cyrus-sasl-devel snappy-devel zlib-devel bzip2-devel libcurl-devel lz4-devel openldap-devel krb5-devel xz-devel e2fsprogs-devel expat-devel devtoolset-8-gcc devtoolset-8-gcc-c++
```

#### b. Build a specific `curl` version

- Fetch the package archive

```
$ wget https://curl.se/download/curl-7.66.0.tar.gz
```

- Unzip the package

```
$ tar -xvzf curl-7.66.0.tar.gz && cd curl-7.66.0
```

- Configure and build the package

```
$ ./configure
$ sudo make install
```

#### 3. Switch to the Percona Server for MongoDB branch that you are building and install Python3 modules

```
$ cd percona-server-mongodb && git checkout v5.0
$ pip3 install --user -r etc/pip/dev-requirements.txt
```

#### 4. Define Percona Server for MongoDB version (5.0.2 for the time of writing this document)

```
$ echo '{"version": "5.0.2"}' > version.json
```

#### BUILD THE AWS SOFTWARE DEVELOPMENT KIT FOR C++ LIBRARY

##### 1. Clone the AWS Software Development Kit for C++ repository

```
$ git clone --recurse-submodules https://github.com/aws/aws-sdk-cpp.git
```

##### 2. Create a directory to store the AWS library

```
$ mkdir -p /tmp/lib/aws
```

##### 3. Declare an environment variable `AWS_LIBS` for this directory

```
$ export AWS_LIBS=/tmp/lib/aws
```

##### 4. Percona Server for MongoDB is built with AWS SDK CPP 1.9.379 version. Switch to this version

```
$ cd aws-sdk-cpp && git checkout 1.9.379
```

##### 5. It is recommended to keep build files outside the SDK directory. Create a build directory and navigate to it

```
$ mkdir build && cd build
```

##### 6. Generate build files using `cmake`

```
Debian/Ubuntu      RHEL/CentOS 7      RHEL/CentOS 8

$ cmake .. -DCMAKE_BUILD_TYPE=Release -DBUILD_ONLY="s3;transfer" -
DBUILD_SHARED_LIBS=OFF -DMINIMIZE_SIZE=ON -DCMAKE_INSTALL_PREFIX="${AWS_LIBS}"

$ cmake3 .. -DCMAKE_C_COMPILER=/opt/rh/devtoolset-8/root/usr/bin/gcc -
DCMAKE_CXX_COMPILER=/opt/rh/devtoolset-8/root/usr/bin/g++ -DCMAKE_BUILD_TYPE=Release -
DBUILD_ONLY="s3;transfer" -DBUILD_SHARED_LIBS=OFF -DMINIMIZE_SIZE=ON -
DCMAKE_INSTALL_PREFIX="${AWS_LIBS}"

$ cmake .. -DCMAKE_BUILD_TYPE=Release -DBUILD_ONLY="s3;transfer" -
DBUILD_SHARED_LIBS=OFF -DMINIMIZE_SIZE=ON -DCMAKE_INSTALL_PREFIX="${AWS_LIBS}"
```

##### 7. Install the SDK

```
$ make install
```

#### BUILD PERCONA SERVER FOR MONGODB

##### 1. Change directory to `percona-server-mongodb`

```
$ cd percona-server-mongodb
```

## 2. Build Percona Server for MongoDB from `buildscripts/scons.py`.

```

Debian/Ubuntu      RHEL/CentOS 7      RHEL/CentOS 8
$ buildscripts/scons.py -j$(nproc --all) --jlink=2 --disable-warnings-as-errors --ssl
--opt=on --use-sasl-client --wiredtiger --audit --inmemory --hotbackup CPPATH="$
${AWS_LIBS}/include" LIBPATH="${AWS_LIBS}/lib" install-mongod

$ python3 buildscripts/scons.py CC=/opt/rh/devtoolset-8/root/usr/bin/gcc CXX=/opt/rh/
devtoolset-8/root/usr/bin/g++ -j$(nproc --all) --jlink=2 --install-mode=legacy --
disable-warnings-as-errors --ssl --opt=on --use-sasl-client --wiredtiger --audit --
inmemory --hotbackup CPPATH="${AWS_LIBS}/include" LIBPATH="${AWS_LIBS}/lib" mongod

$ buildscripts/scons.py -j$(nproc --all) --jlink=2 --install-mode=legacy --disable-
warnings-as-errors --ssl --opt=on --use-sasl-client --wiredtiger --audit --inmemory --
hotbackup CPPATH="${AWS_LIBS}/include" LIBPATH="${AWS_LIBS}/lib64" mongod

```

This command builds only the database. Other available targets for the `scons` command are:

- `mongod`
- `mongos`
- `mongo`
- `core` (includes `mongod`, `mongos`, `mongo`)
- `all`

The built binaries are in the `percona-server-mongodb` directory.

### Next steps

[Connect to MongoDB →](#)

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 February 28, 2024

 August 10, 2023

### 3.2.6 Running Percona Server for MongoDB in a Docker Container

Docker images of Percona Server for MongoDB are hosted publicly on [Docker Hub](#).

For more information about using Docker, see the [Docker Docs](#).

#### Note

Make sure that you are using the latest version of Docker. The ones provided via `apt` and `yum` may be outdated and cause errors.

By default, Docker pulls the image from Docker Hub if it is not available locally.

We gather [Telemetry data](#) to understand the use of the software and improve our products.

To run the latest Percona Server for MongoDB 5.0 in a Docker container, run the following command as the root user or via `sudo`:

```
$ docker run -d --name psmdb --restart always \
percona/percona-server-mongodb:<TAG>-multi
```

The command does the following:

- The `docker run` command instructs the `docker` daemon to run a container from an image.
- The `-d` option starts the container in detached mode (that is, in the background).
- The `--name` option assigns a custom name for the container that you can use to reference the container within a Docker network. In this case: `psmdb`.
- The `--restart` option defines the container's restart policy. Setting it to `always` ensures that the Docker daemon will start the container on startup and restart it if the container exits.
- The `<TAG>-multi` is the tag specifying the version you need. For example, `5.0.29-25-multi`. The `multi` part of the tag serves to identify the architecture (x86\_64 or ARM64) and pull the respective image. [See the full list of tags](#).

#### Access container shell

Run the following command to start the bash session and run commands inside the container:

```
$ docker exec -it <container-name>
```

where `<container-name>` is the name of your database container.

For example, to connect to Percona Server for MongoDB, run:

```
$ mongo
```

#### Connect from another Docker container

The Percona Server for MongoDB container exposes standard MongoDB port (27017), which can be used for connection from an application running in another container.

For example, to set up a replica set for testing purposes, you have the following options:

- Interconnect the `mongod` nodes in containers on a default `bridge` network. In this scenario, containers communicate with each other by their IP address.
- Create a [user-defined network](#) and interconnect the `mongod` nodes on it. In this scenario, containers communicate with each other by name.
- Automate the container provisioning and the replica set setup via the [Docker Compose tool](#).

In the following example, `rs101`, `rs102`, `rs103` are the container names for Percona Server for MongoDB and `rs` is the replica set name.



Bridge network    User-defined network    Docker Compose

When you start Docker, a default `bridge` network is created and all containers are automatically attached to it unless otherwise specified.

### 1. Start the containers and expose different ports

```
$ docker run --rm -d --name rs101 -p 27017:27017 percona/percona-server-mongodb:5.0 --port=27017 --replSet rs
$ docker run --rm -d --name rs102 -p 28017:28017 percona/percona-server-mongodb:5.0 --port=28017 --replSet rs
$ docker run --rm -d --name rs103 -p 29017:29017 percona/percona-server-mongodb:5.0 --port=29017 --replSet rs
```

### 2. Check that the containers are started

```
$ docker container ls
```

Output:

CONTAINER ID	IMAGE	COMMAND NAMES	CREATED	STATUS	PORTS
3a4b70cd386b	percona/percona-server-mongodb:5.0	--port=27017 --re...	3 minutes ago	Up	0.0.0.0:27017->27017/tcp rs101
c9b40a00e32b	percona/percona-server-mongodb:5.0	--port=28017 --re...	11 seconds ago	Up	0.0.0.0:28017->28017/tcp rs102
b8aebc00309e	percona/percona-server-mongodb:5.0	--port=29017 --re...	3 seconds ago	Up	0.0.0.0:29017->29017/tcp rs103

### 3. Get the IP addresses of each container

```
$ docker inspect --format='{{range .NetworkSettings.Networks}}{{.IPAddress}}{{end}}' rs101
$ docker inspect --format='{{range .NetworkSettings.Networks}}{{.IPAddress}}{{end}}' rs102
$ docker inspect --format='{{range .NetworkSettings.Networks}}{{.IPAddress}}{{end}}' rs103
```

### 4. Interconnect the containers and initiate the replica set. Replace `rs101SERVER`, `rs102SERVER` and `rs103SERVER` with the IP address of each respective container.

```
$ docker exec -ti rs101 mongo --eval 'config={"_id":"rs","members":[{"_id":0,"host":"rs101SERVER:27017"},{"_id":1,"host":"rs102SERVER:28017"},{"_id":2,"host":"rs103SERVER:29017"}]};rs.initiate(config);'
```

### 5. Check your setup

```
$ docker exec -ti rs101 mongo --eval 'rs.status()'
```

You can isolate desired containers in a user-defined network and provide DNS resolution across them so that they communicate with each other by hostname.

#### 1. Create the network:

```
$ docker network create my-network
```

#### 2. Start the containers and connect them to your network, exposing different ports

```
$ docker run --rm -d --name rs101 --net my-network -p 27017:27017 percona/percona-server-mongodb:5.0 --port=27017 --replSet rs
$ docker run --rm -d --name rs102 --net my-network -p 28017:28017 percona/percona-server-mongodb:5.0 --port=28017 --replSet rs
```

**Connect with the `mongo` shell**

To start another container with the `mongo` shell that connects to your Percona Server for MongoDB container, run the following command:

```
$ docker run -it --rm percona/percona-server-mongodb:5.0 mongo mongodb://
MONGODB_SERVER:PORT/DB_NAME
```

Set `MONGODB_SERVER`, `PORT`, and `DB_NAME` with the IP address of the `psmdb` container, the port of your MongoDB Server (default value is 27017), and the name of the database you want to connect to.

You can get the IP address by running this command:

```
$ docker inspect -f '{{range.NetworkSettings.Networks}}{{.IPAddress}}{{end}}' psmdb
```

**PERCONA**

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 February 28, 2024

 December 8, 2022

### 3.3 Connect to Percona Server for MongoDB

After you have successfully installed and started Percona Server for MongoDB, let's connect to it.

By default, access control is disabled in MongoDB. We recommend enabling it so that users must verify their identity to be able to connect to the database. Percona Server for MongoDB supports several [authentication methods](#). We will use the default one, [SCRAM](#), to configure authentication.

The steps are the following:

1. Connect to Percona Server for MongoDB instance without authentication:

```
$ mongosh
```

```

Sample output
Current Mongosh Log ID: 6598270a3a0c418751550ded
Connecting to:      mongodb://127.0.0.1:27017/?
directConnection=true&serverSelectionTimeoutMS=2000&appName=mongosh+2.0.0
Using MongoDB:     5.0.29-25
Using Mongosh:     2.0.0

For mongosh info see: https://docs.mongodb.com/mongod-shell/

test>

```

## 2. Create the administrative user in the `admin` database:

### a. Switch to the `admin` database

```
> use admin
```

#### Sample output

```
switched to db admin
```

### b. Create the user:

```

> db.createUser(
  {
    user: "admin",
    pwd: passwordPrompt(), // or cleartext password
    roles: [
      { role: "userAdminAnyDatabase", db: "admin" },
      { role: "readWriteAnyDatabase", db: "admin" }
    ]
  }
)

```

## 3. Shutdown the `mongod` instance and exit `mongosh`

```
> db.adminCommand( { shutdown: 1 } )
```

#### 4. Enable authentication

 Command line    Configuration file

Start the server with authentication enabled using the following command:

```
$ mongod --auth --port 27017 --dbpath /var/lib/mongodb --fork --syslog
```

##### a. Edit the configuration file

```
/etc/mongod.conf  
  
security:  
  authorization: enabled
```

##### b. Start the mongod service

```
$ systemctl start mongod
```

#### 5. Connect to Percona Server for MongoDB and authenticate.

```
$ mongosh --port 27017 --authenticationDatabase \\  
"admin" -u "admin" -p
```

### 3.3.1 Next steps

[Run simple queries →](#)

## PERCONA

### 3.3.2 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)    [Get a Percona Expert](#)

 February 28, 2024

 February 28, 2024

## 3.4 Manipulate data in Percona Server for MongoDB

After you connected to Percona Server for MongoDB, let's insert some data and operate with it.

### Note

To secure the data, you may wish to use [data-at-rest encryption](#). Note that you can only enable it on an empty database. Otherwise you must clean up the data directory first.

See the following documentation for data-at-rest encryption:

- [Using HashiCorp Vault server](#)
- [Using KMIP server](#)
- [Using a local keyfile](#)

### 3.4.1 Insert data

1. For example, let's add an item to the `fruits` collection. Use the `insertOne()` command for this purpose:

```
> db.fruits.insertOne(
  {item: "apple", qty: 50}
)
```

If there is no `fruits` collection in the database, it will be created during the command execution.

#### Sample output

```
{
  acknowledged: true,
  insertedId: ObjectId('659c2b846252bfad93fc1578')
}
```

2. Now, let's add more fruits to the `fruits` collection using the `insertMany()` command:

```
> db.fruits.insertMany([
  {item: "banana", weight: "kg", qty: 10 },
  {item: "peach", weight: "kg", qty: 30}
])
```

#### Sample output

```
{
  acknowledged: true,
  insertedIds: {
    '0': ObjectId('659c2bc46252bfad93fc1579'),
    '1': ObjectId('659c2bc46252bfad93fc157a')
  }
}
```

See [Insert documents](#) for more information about data insertion.

### 3.4.2 Query data

Run the following command to query data in MongoDB:

```
> db.fruits.find()
```

#### Sample output

```
[
  { _id: ObjectId('659c2b846252bfad93fc1578'), item: 'apple', qty: 50 },
  {
    _id: ObjectId('659c2bc46252bfad93fc1579'),
    item: 'banana',
    weight: 'kg',
    qty: 10
  },
  {
    _id: ObjectId('659c2bc46252bfad93fc157a'),
    item: 'peach',
    weight: 'kg',
    qty: 30
  }
]
```

Refer to the [Query documents](#) documentation to for more information about reading data.

### 3.4.3 Update data

Let's update the `apples` entry by adding weight to it.

1. Use the `updateOne()` command for that:

```
> db.fruits.updateOne(
  {"item": "apple" },
  {$set: {"weight": "kg"}}
)
```

#### Sample output

```
{
  acknowledged: true,
  insertedId: null,
  matchedCount: 1,
  modifiedCount: 1,
  upsertedCount: 0
}
```

2. Query the collection to check the updated document:

```
> db.fruits.find({item: "apple"})
```

```

Sample output
[
  {
    _id: ObjectId('659c2b846252bfad93fc1578'),
    item: 'apple',
    qty: 50,
    weight: 'kg'
  }
]

```

See [Update methods](#) documentation for other available data update methods

### 3.4.4 Delete data

Run the following command to delete all documents where the quantity is less than 30 kg:

```

> db.fruits.deleteMany(
  {"qty": {$lt: 30}}
)

```

```

Sample output
{ acknowledged: true, deletedCount: 1 }

```

Learn more about deleting data in [Delete methods](#) documentation.

Congratulations! You have used basic create, read, update and delete (CRUD) operations to manipulate data in Percona Server for MongoDB. See [MongoDB CRUD Concepts](#) manual to learn more about CRUD operations.

### 3.4.5 Next steps

[What's next? →](#)

## PERCONA

### 3.4.6 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

[Community Forum](#) [Get a Percona Expert](#)

🕒 May 21, 2024

🕒 February 28, 2024

## 3.5 What's next?

Congratulations on completing your first hands-on experience with Percona Server for MongoDB.

To deepen your knowledge in working with the database, see the MongoDB documentation on [aggregation](#), [indexes](#), [data modelling](#), [transactions](#).

The following sections help you achieve your organization's goals on:

### 3.5.1 High availability

Multiple copies of the data on different servers provide redundancy and high availability. MongoDB [replica sets](#) serve this purpose. Replica sets also increase data availability and provide fault tolerance against the loss of a database instance.

[Replica set deployment](#) →

### 3.5.2 Scalability

Ensure your database handles the load as your data set grows without performance degradation. The [sharding](#) method in MongoDB is the distribution of data across multiple servers where each server handles a subset of data. This is the horizontal scaling mechanism where you can add additional servers if needed for a lower overall cost than upgrading existing hardware. The tradeoff is additional complexity in the infrastructure management.

[Deploy a sharded cluster](#) →

### 3.5.3 Encryption

Protecting your data from unauthorized access is crucial. Introducing data-at-rest encryption helps protect sensitive information when it is stored on storage devices, such as hard drives, solid-state drives, or other types of persistent storage. Percona Server for MongoDB is integrated with several external key managers.

[Data-at-rest encryption](#) →

### 3.5.4 Backup and restore

Protect your database against data loss by implementing a backup strategy. You can either use the built-in [hot backup feature](#) or consider deploying Percona Backup for MongoDB - an open source solution for making consistent backups and restores in sharded clusters and replica sets.

[Percona Backup for MongoDB](#) →



### 3.5.5 Monitoring

Get insights into the database health and performance using Percona Monitoring and Management (PMM) - an open-source database monitoring, management, and observability solution for MySQL, PostgreSQL, and MongoDB. It allows you to observe the health of your database systems, explore new patterns in their behavior, troubleshoot them and perform database management operations

[Get started with PMM →](#)

### 3.5.6 Advanced command line tools

Perform sophisticated database management and administration tasks using Percona Toolkit - a collection of advanced command-line tools developed and tested by Percona as an alternative to private or “one-off” scripts.

[Get Percona Toolkit →](#)

## PERCONA

### 3.5.7 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

[Community Forum](#) [Get a Percona Expert](#)

🕒 February 28, 2024

🕒 February 28, 2024

## 4. Features

### 4.1 Storage

#### 4.1.1 Percona Memory Engine

Percona Memory Engine is a special configuration of [WiredTiger](#) that does not store user data on disk. Data fully resides in the main memory, making processing much faster and smoother. Keep in mind that you need to have enough memory to hold the data set, and ensure that the server does not shut down.

The Percona Memory Engine is available in Percona Server for MongoDB along with the default MongoDB engine [WiredTiger](#).


#### Usage

As of version 3.2, Percona Server for MongoDB runs with [WiredTiger](#) by default. You can select a storage engine using the `--storageEngine` command-line option when you start `mongod`. Alternatively, you can set the `storage.engine` variable in the configuration file (by default, `/etc/mongod.conf`):

```
storage:
  dbPath: <dataDir>
  engine: inMemory
```

#### Configuration

You can configure Percona Memory Engine using either command-line options or corresponding parameters in the `/etc/mongod.conf` file. The following are the configuration examples:

 Configuration file     Command line

The configuration file is formatted in YAML

```
storage:
  engine: inMemory
  inMemory:
    engineConfig:
      inMemorySizeGB: 140
      statisticsLogDelaySecs: 0
```

Setting parameters in the configuration file is the same as starting the `mongod` daemon with the following options:

```
mongod --storageEngine=inMemory \
--inMemorySizeGB=140 \
--inMemoryStatisticsLogDelaySecs=0
```

#### OPTIONS

The following options are available (with corresponding YAML configuration file parameters):

<b>Configuration file</b>	<b><code>storage.inMemory.engineConfig.inMemorySizeGB</code></b>
<b>Command line</b>	<code>inMemorySizeGB()</code>

<b>Configuration file</b>	<code>storage.inMemory.engineConfig.inMemorySizeGB</code>
<b>Default</b>	50% of total memory minus 1024 MB, but not less than 256 MB
<b>Description</b>	Specifies the maximum memory in gigabytes to use for data
<b>Configuration file</b>	<code>storage.inMemory.engineConfig.statisticsLogDelaySecs</code>
<b>Command line</b>	<code>inMemoryStatisticsLogDelaySecs()</code>
<b>Default</b>	0
<b>Description</b>	Specifies the number of seconds between writes to statistics log. A 0 value means statistics are not logged

## Switching storage engines

### CONSIDERATIONS

If you have data files in your database and want to change to Percona Memory Engine, consider the following:

- Data files created by one storage engine are not compatible with other engines, because each one has its own data model.
- When changing the storage engine, the `mongod` node requires an empty `dbPath` data directory when it is restarted. Though Percona Memory Engine stores all data in memory, some metadata files, diagnostics logs and statistics metrics are still written to disk. This is controlled with the `--inMemoryStatisticsLogDelaySecs` option.

Creating a new `dbPath` data directory for a different storage engine is the simplest solution. Yet when you switch between disk-using storage engines (e.g. from `WiredTiger` to Percona Memory Engine), you may have to delete the old data if there is not enough disk space for both. Double-check that your backups are solid and/or the replica set nodes are healthy before you switch to the new storage engine.

### PROCEDURE

To change a storage engine, you have the following options:

#### Temporarily test Percona Memory Engine

Set a different data directory for the `dbPath` variable in the configuration file. Make sure that the user running `mongod` has read and write permissions for the new data directory.

1. Stop `mongod`

```
$ service mongod stop
```

2. Edit the configuration file

```
storage:
  dbPath: <newDataDir>
  engine: inmemory
```

3. Start `mongod`

```
$ service mongod start
```

Permanent switch to Percona Memory Engine without any valuable data in your database

Clean out the `dbPath` data directory (by default, `/var/lib/mongodb`) and edit the configuration file:

1. Stop `mongod`

```
$ service mongod stop
```

2. Clean out the `dbPath` data directory

```
$ sudo rm -rf <dbpathDataDir>
```

3. Edit the configuration file

```
storage:  
  dbPath: <newDataDir>  
  engine: inmemory
```

4. Start `mongod`

```
$ service mongod start
```

Switch to Percona Memory Engine with data migration and compatibility

Standalone instance    Replica set

For a standalone instance or a single-node replica set, use the `mongodump` and `mongorestore` utilities:

1. Export the `dataDir` contents

```
$ mongodump --out <dumpDir>
```

2. Stop `mongod`

```
$ service mongod stop
```

3. Clean out the `dbPath` data directory

```
$ sudo rm -rf <dbpathDataDir>
```

4. Update the configuration file by setting the new value for the `storage.engine` variable. Set the engine-specific settings such as `storage.inMemory.engineConfig.inMemorySizeGB`

5. Start `mongod`

```
$ service mongod start
```

6. Restore the database

```
$ mongorestore <dumpDir>
```

Use the “rolling restart” process.

1. Switch to the Percona Memory Engine on the secondary node. Clean out the `dbPath` data directory and edit the configuration file:

2. Stop `mongod`

```
$ service mongod stop
```

3. Clean out the `dbPath` data directory

```
$ sudo rm -rf <dbpathDataDir>
```

4. Edit the configuration file

```
storage:
  dbPath: <newDataDir>
  engine: inmemory
```

5. Start `mongod`

```
$ service mongod start
```

6. Wait for the node to rejoin with the other nodes and report the `SECONDARY` status.
7. Repeat the procedure to switch the remaining nodes to Percona Memory Engine.

## DATA AT REST ENCRYPTION

Using [Data at Rest Encryption](#) means using the same `storage.*` configuration options as for [WiredTiger](#). To change from normal to [Data at Rest Encryption](#) mode or backward, you must clean up the `dbPath` data directory, just as if you change the storage engine. This is because **mongod** cannot convert the data files to an encrypted format 'in place'. It must get the document data again either via the initial sync from another replica set member, or from imported backup dump.

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 February 28, 2024

 December 8, 2022

## 4.2 Backup

### 4.2.1 Hot backup

Percona Server for MongoDB includes an integrated open source hot backup system for the default [WiredTiger](#) storage engine. It creates a physical data backup on a running server without notable performance and operating degradation.

#### Note

Hot backups are done on `mongod` servers independently, without synchronizing them across replica set members and shards in a cluster. To ensure data consistency during backups and restores, we recommend using [Percona Backup for MongoDB](#).

#### Make a backup

To take a hot backup of the database in your current `dbpath`, do the following:

1. Provide access to the backup directory for the `mongod` user:

```
$ sudo chown mongod:mongod <backupDir>
```

2. Run the `createBackup` command as administrator on the `admin` database and specify the backup directory.

```
> use admin
switched to db admin
> db.runCommand({createBackup: 1, backupDir: "<backup_data_path>"})
{ "ok" : 1 }
```

The backup taken is the snapshot of the `mongod` server's `dataDir` at the moment of the `createBackup` command start.

If the backup was successful, you should receive an `{ "ok" : 1 }` object. If there was an error, you will receive a failing `ok` status with the error message, for example:

```
> db.runCommand({createBackup: 1, backupDir: ""})
{ "ok" : 0, "errmsg" : "Destination path must be absolute" }
```

### Save a backup to a TAR archive

To save a backup as a *tar* archive, use the `archive` field to specify the destination path:

```
> use admin
...
> db.runCommand({createBackup: 1, archive: <path_to_archive>.tar })
```

### Streaming hot backups to a remote destination

Percona Server for MongoDB enables uploading hot backups to an [Amazon S3](#) or a compatible storage service, such as [MinIO](#).

This method requires that you provide the `bucket` field in the `s3` object:

```
> use admin
...
> db.runCommand({createBackup: 1, s3: {bucket: "backup20190510", path:
<some_optional_path>} })
```

In addition to the mandatory `bucket` field, the `s3` object may contain the following fields:

Field	Type	Description
<code>bucket</code>	string	The only mandatory field. Names are subject to restrictions described in the <a href="#">Bucket Restrictions and Limitations section of Amazon S3 documentation</a>
<code>path</code>	string	The virtual path inside the specified bucket where the backup will be created. If the <code>path</code> is not specified, then the backup is created in the root of the bucket. If there are any objects under the specified path, the backup will not be created and an error will be reported.
<code>endpoint</code>	string	The endpoint address and port - mainly for AWS S3 compatible servers such as the <i>MinIO</i> server. For a local MinIO server, this can be "127.0.0.1:9000". For AWS S3 this field can be omitted.
<code>scheme</code>	string	"HTTP" or "HTTPS" (default). For a local MinIO server started with the <i>minio server</i> command this should field should contain <i>HTTP</i> .



Field	Type	Description
useVirtualAddressing	bool	The style of addressing buckets in the URL. By default 'true'. For MinIO servers, set this field to <b>false</b> . For more information, see <a href="#">Virtual Hosting of Buckets</a> in the Amazon S3 documentation.
region	string	The name of an AWS region. The default region is <b>US_EAST_1</b> . For more information see <a href="#">AWS Service Endpoints</a> in the Amazon S3 documentation.
profile	string	The name of a credentials profile in the <i>credentials</i> configuration file. If not specified, the profile named <b>default</b> is used.
accessKeyId	string	The access key id
secretAccessKey	string	The secret access key

#### CREDENTIALS

If the user provides the *access key id* and the *secret access key* parameters, these are used as credentials.

If the *access key id* parameter is not specified then the credentials are loaded from the credentials configuration file. By default, it is `~/.aws/credentials`.

#### Example credentials file

##### ~/.aws/credentials

```
[default]
aws_access_key_id = ABC123XYZ456QQQAAFF
aws_secret_access_key = zuf+secretkey0secretkey1secretkey2
[localminio]
aws_access_key_id = ABCABCABCABC55566678
aws_secret_access_key = secretaccesskey1secretaccesskey2secretaccesskey3
```

#### EXAMPLES

##### Backup in root of bucket on local instance of MinIO server

```
> db.runCommand({createBackup: 1, s3: {bucket: "backup20190901500",
scheme: "HTTP",
endpoint: "127.0.0.1:9000",
useVirtualAddressing: false,
profile: "localminio"}}})
```

##### Backup on MinIO testing server with the default credentials profile

The following command creates a backup under the virtual path "year2019/day42" in the `backup` bucket:

```
> db.runCommand({createBackup: 1, s3: {bucket: "backup",
path: "year2019/day42",
endpoint: "sandbox.min.io:9000",
useVirtualAddressing: false}}})
```

##### Backup on AWS S3 service using default settings

```
> db.runCommand({createBackup: 1, s3: {bucket: "backup", path: "year2019/day42"}}})
```

 **See also**

AWS Documentation: [Providing AWS Credentials](#)

## Restore data from backup

### RESTORE ON A STANDALONE SERVER

To restore your database on a standalone server, stop the `mongod` service, clean out the data directory and copy files from the backup directory to the data directory. The `mongod` user requires access to those files to start the service. Therefore, make the `mongod` user the owner of the data directory and all files and subdirectories under it, and restart the `mongod` service.

 **Note**

If you try to restore the node into the existing replica set and there is more recent data, the restored node detects that it is out of date with the other replica set members, deletes the data and makes an initial sync.

Run the following commands as root or by using the `sudo` command

1. Stop the `mongod` service

```
$ systemctl stop mongod
```

2. Clean out the data directory

```
$ rm -rf /var/lib/mongodb/*
```

3. Copy backup files

```
$ cp -RT <backup_data_path> /var/lib/mongodb/
```

4. Grant permissions to data files for the `mongod` user

```
$ chown -R mongod:mongod /var/lib/mongodb/
```

5. Start the `mongod` service

```
$ systemctl start mongod
```

### RESTORE IN A REPLICASET

The recommended way to restore the replica set from a backup is to restore it into a standalone node and then initiate it as the first member of a new replica set.

 **Note**

If you try to restore the node into the existing replica set and there is more recent data, the restored node detects that it is out of date with the other replica set members, deletes the data and makes an initial sync.

Run the following commands as root or by using the **sudo** command

1. Stop the `mongod` service:

```
$ systemctl stop mongod
```

2. Clean the data directory and then copy the files from the backup directory to your data directory. Assuming that the data directory is `/var/lib/mongodb/`, use the following commands:

```
$ rm -rf /var/lib/mongodb/*  
$ cp -RT <backup_data_path> /var/lib/mongodb/
```

3. Grant permissions to the data files for the `mongod` user

```
$ chown -R mongod:mongod /var/lib/mongodb/
```

4. Make sure the replication is disabled in the config file and start the `mongod` service.

```
$ systemctl start mongod
```

5. Connect to your standalone node via the `mongo` shell and drop the local database

```
> mongo  
> use local  
> db.dropDatabase()
```

6. Restart the node with the replication enabled

- Shut down the node.

```
$ systemctl stop mongod
```

- Edit the configuration file and specify the `replication.replSetName` option
- Start the `mongod` node:

```
$ systemctl start mongod
```

7. Initiate a new replica set

- Start the mongo shell

```
> mongo
```

- Initiate a new replica set

```
> rs.initiate()
```

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 February 28, 2024

 December 8, 2022

## 4.2.2 \$backupCursor and \$backupCursorExtend aggregation stages

`$backupCursor` and `$backupCursorExtend` aggregation stages expose the WiredTiger API which allows making consistent backups. Running these stages allows listing and freezing the files so you can copy them without the files being deleted or necessary parts within them being overwritten.

- `$backupCursor` outputs the list of files and their size to copy.
- `$backupCursorExtend` outputs the list of WiredTiger transaction log files that have been updated or newly added since the `$backupCursor` was first run. Saving these files enables restoring the database to any arbitrary time between the `$backupCursor` and `$backupCursorExtend` execution times.

They are available in Percona Server for MongoDB starting with version 4.4.6-8.

Percona provides [Percona Backup for MongoDB \(PBM\)](#) – a light-weight open source solution for consistent backups and restores across sharded clusters. PBM relies on these aggregation stages for physical backups and restores. However, if you wish to develop your own backup application, this document describes the `$backupCursor` and `$backupCursorExtend` aggregation stages.

### Usage

You can run these stages in any type of MongoDB deployment. If you need to back up a single node in a replica set, first run the `$backupCursor`, then the `$backupCursorExtend` and save the output files to the backup storage.

To make a consistent backup of a sharded cluster, run both aggregation stages on one node from each shard and the config server replica set. It can be either the primary or the secondary node. Note that since the secondary node may lag in syncing the data from the primary one, you will have to wait for the exact same time before running the `$backupCursorExtend`.

Note that for standalone MongoDB node with disabled oplogs, you can only run the `$backupCursor` aggregation stage.

GET A LIST OF ALL FILES TO COPY WITH \$BACKUPCURSOR

```
var bkCsr = db.getSiblingDB("admin").aggregate([{$backupCursor: {}}])
bkCsrMetadata = bkCsr.next().metadata
```

Sample output:

```
{
  "metadata" : {
```

```

"backupId": UUID("35c34101-0107-44cf-bdec-fad285e07534"),
"dbpath": '/var/lib/mongodb',
"oplogStart": { ts: Timestamp({ t: 1666631297, i: 1 }), t: Long("-1") },
"oplogEnd": { ts: Timestamp({ t: 1666631408, i: 1 }), t: Long("1") },
"checkpointTimestamp": Timestamp({ t: 1666631348, i: 1 })
"disableIncrementalBackup" : false,
"incrementalBackup" : false,
"blockSize" : 16
}
}

```

Store the `metadata` document somewhere, because you need to pass the `backupId` parameter from this document as the input parameter for the `$backupCursorExtend` stage. Also you need the `oplogEnd` timestamp. Make sure that the `$backupCursor` is complete on all shards in your cluster.

#### Note

Note that when running `$backupCursor` in a standalone node deployment, `oplogStart`, `oplogEnd`, `checkpointTimestamp` values may be absent. This is because standalone node deployments don't have oplogs.

#### RUN \$BACKUPCOURSEXTEND TO RETRIEVE THE WIREDTIGER TRANSACTION LOGS

Pass the `backupId` from the metadata document as the first parameter. For the `timestamp` parameter, use the maximum (latest) value among the `oplogEnd` timestamps from all shards and config server replica set. This will be the target time to restore.

```

var bkExtCsr = db.aggregate([{$backupCursorExtend: {backupId: bkCsrMetadata.backupId,
timestamp: new Timestamp(1666631418, 1)}}])

```

Sample output:

```

{ "filename" : "/data/plain_rs/n1/data/journal/WiredTigerLog.0000000042" }
{ "filename" : "/data/plain_rs/n1/data/journal/WiredTigerLog.0000000043" }
{ "filename" : "/data/plain_rs/n1/data/journal/WiredTigerLog.0000000044" }

```

#### LOOP THE \$BACKUPCURSOR

Prevent the backup cursor from closing on timeout (default – 10 minutes). This is crucial since it prevents overwriting backup snapshot file blocks with new ones if the files take longer than 10 minutes to copy. Use the `getMore` command for this purpose.

#### COPY THE FILES TO THE STORAGE

Now you can copy the output of both aggregation stages to your backup storage.

After the backup is copied to the storage, terminate the `getMore` command and close the cursor.

#### Note

Save the timestamp that you passed for the `$backupCursorExtend` stage somewhere since you will need it for the restore.

This document is based on the blog post [Experimental Feature: \\$backupCursorExtend in Percona Server for MongoDB](#) by Akira Kurogane

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 January 31, 2023

 December 8, 2022

## 4.3 Authentication

### 4.3.1 Authentication

Authentication is the process of verifying a client's identity. Normally, a client needs to authenticate themselves against the MongoDB server user database before doing any work or reading any data from a `mongod` or `mongos` instance.

By default, Percona Server for MongoDB provides a SCRAM authentication mechanism where clients authenticate themselves by providing their user credentials. In addition, you can integrate Percona Server for MongoDB with a separate service, such as OpenLDAP or Active Directory. This enables users to access the database with the same credentials they use for their emails or workstations.

You can use any of these authentication mechanisms supported in Percona Server for MongoDB:

- [SCRAM\(default\)](#)
- [x.509 certificate authentication](#)
- [LDAP authentication with SASL](#)
- [Kerberos Authentication](#)
- [Authentication and authorization with direct binding to LDAP](#)
- [AWS IAM authentication](#)

### SCRAM

SCRAM is the default authentication mechanism. *Percona Server for MongoDB* verifies the credentials against the user's name, password and the database where the user record is created for a client (authentication database). For how to enable this mechanism, see [Enable authentication](#).

### x.509 certificate authentication

This authentication mechanism enables a client to authenticate in Percona Server for MongoDB by providing an x.509 certificate instead of user credentials. Each certificate contains the `subject` field

defined in the DN format. In Percona Server for MongoDB, each certificate has a corresponding user record in the `$external` database. When a user connects to the database, Percona Server for MongoDB matches the `subject` value against the usernames defined in the `$external` database.

For production use, we recommend using valid CA certificates. For testing purposes, you can generate and use self-signed certificates.

x.509 authentication is compatible with [LDAP authorization](#) to enable you to control user access and operations in Percona Server for MongoDB. For configuration guidelines, refer to [Set up x.509 authentication and LDAP authorization](#).

#### See also

MongoDB Documentation: [x.509](#)

Percona Blog: [Setting up MongoDB with Member x509 auth and SSL + easy-rsa](#)

## LDAP authentication with SASL

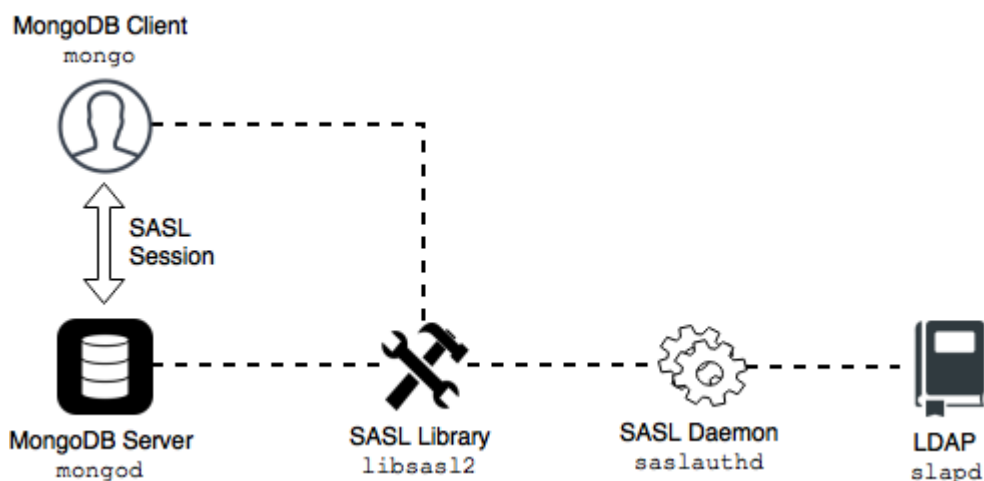
### Overview

LDAP authentication with SASL means that both the client and the server establish a SASL session using the SASL library. Then authentication (bind) requests are sent to the LDAP server through the SASL authentication daemon (`ssslauthd`) that acts as a remote proxy for the `mongod` server.

The following components are necessary for external authentication to work:

- **LDAP Server:** Remotely stores all user credentials (i.e. user name and associated password).
- **SASL Daemon:** Used as a MongoDB server-local proxy for the remote LDAP service.
- **SASL Library:** Used by the MongoDB client and server to create data necessary for the authentication mechanism.

The following image illustrates this architecture:



An authentication session uses the following sequence:

1. A `mongo` client connects to a running `mongod` instance.
2. The client creates a `PLAIN` authentication request using the SASL library.
3. The client then sends this SASL request to the server as a special `mongo` command.

4. The `mongod` server receives this SASL Message, with its authentication request payload.
5. The server then creates a SASL session scoped to this client, using its own reference to the SASL library.
6. Then the server passes the authentication payload to the SASL library, which in turn passes it on to the `saslauthd` daemon.
7. The `saslauthd` daemon passes the payload on to the LDAP service to get a YES or NO authentication response (in other words, does this user exist and is the password correct).
8. The YES/NO response moves back from `saslauthd`, through the SASL library, to `mongod`.
9. The `mongod` server uses this YES/NO response to authenticate the client or reject the request.
10. If successful, the client has authenticated and can proceed.

For configuration instructions, refer to [Setting up LDAP authentication with SASL](#).

### Kerberos authentication

Percona Server for MongoDB supports Kerberos authentication starting from release 4.2.6-6.

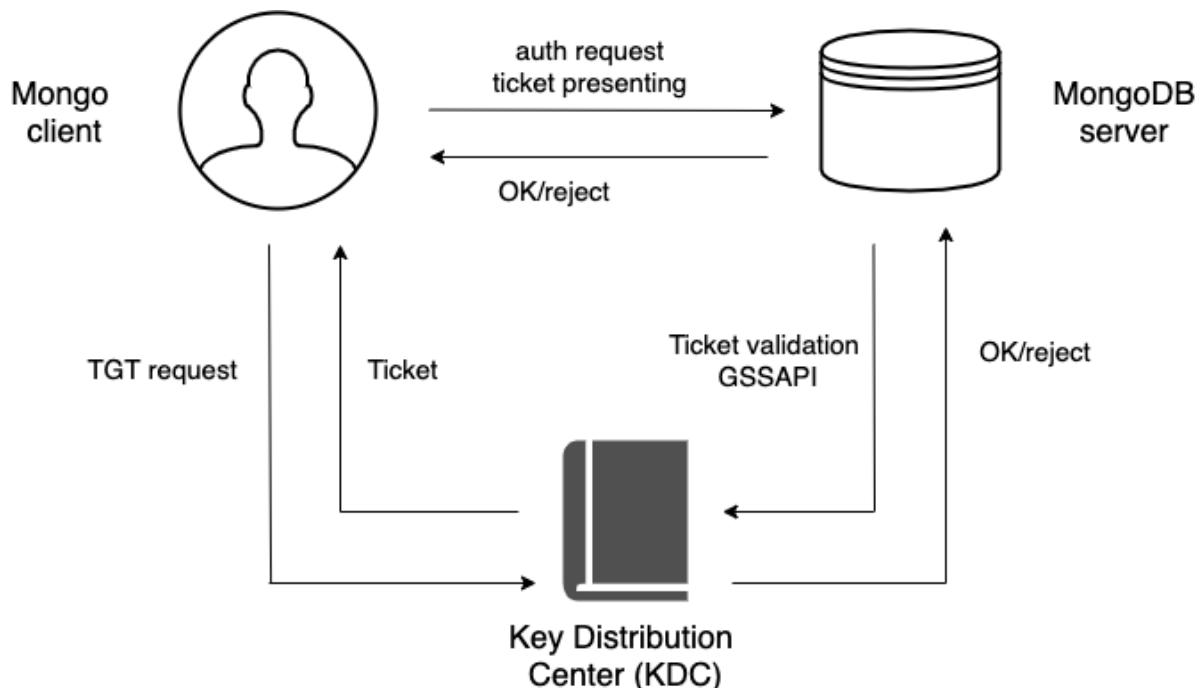
This authentication mechanism involves the use of a Key Distribution Center (KDC) - a symmetric encryption component which operates with tickets. A ticket is a small amount of encrypted data which is used for authentication. It is issued for a user session and has a limited lifetime.

When using Kerberos authentication, you also operate with principals and realms.

A realm is the logical network, similar to a domain, for all Kerberos nodes under the same master KDC.

A principal is a user or a service which is known to Kerberos. A principal name is used for authentication in Kerberos. A service principal represents the service, e.g. `mongodb`. A user principal represents the user. The user principal name corresponds to the username in the `$external` database in *Percona Server for MongoDB*.

The following diagram shows the authentication workflow:



The sequence is the following:



1. A `mongo` client sends the Ticket-Granting Ticket (TGT) request to the Key Distribution Center (KDC)
2. The KDC issues the ticket and sends it to the `mongo` client.
3. The `mongo` client sends the authentication request to the `mongo` server presenting the ticket.
4. The `mongo` server validates the ticket in the KDC.
5. Upon successful ticket validation, the authentication request is approved and the user is authenticated.

Kerberos authentication in *Percona Server for MongoDB* is implemented the same way as in MongoDB Enterprise.

#### See also

MongoDB Documentation: [Kerberos Authentication](#)

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)    [Get a Percona Expert](#)

 February 28, 2024

 December 8, 2022

### 4.3.2 Enable SCRAM authentication

By default, Percona Server for MongoDB does not restrict access to data and configuration.

Enabling authentication enforces users to identify themselves when accessing the database. This document describes how to enable built-in [SCRAM](#) authentication mechanism. *Percona Server for MongoDB* also supports the number of external authentication mechanisms. To learn more, refer to [Authentication](#).

You can enable authentication either automatically or manually.

#### Automatic setup

To enable authentication and automatically set it up, run the `/usr/bin/percona-server-mongodb-enable-auth.sh` script as root or using `sudo`.

This script creates the `dba` user with the `root` role. The password is randomly generated and printed out in the output. Then the script restarts *Percona Server for MongoDB* with access control enabled. The `dba` user

has full superuser privileges on the server. You can add other users with various roles depending on your needs.

For usage information, run the script with the `-h` option.

### Manual setup

To enable access control manually:

1. Add the following lines to the configuration file:

```
security:  
  authorization: enabled
```

2. Run the following command on the `admin` database:

```
> db.createUser({user: 'USER', pwd: 'PASSWORD', roles: ['dbAdmin'] });
```

3. Restart the `mongod` service:

```
$ service mongod restart
```

4. Connect to the database as the newly created user:

```
$ mongo --port 27017 -u 'USER' -p 'PASSWORD' --authenticationDatabase "admin"
```

#### See also


MongoDB Documentation: [Enable Access Control](#)

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)    [Get a Percona Expert](#)

 April 9, 2024

 December 8, 2022

### 4.3.3 Set up LDAP authentication with SASL

This document describes an example configuration suitable only to test out the external authentication functionality in a non-production environment. Use common sense to adapt these guidelines to your production environment.

To learn more about how the authentication works, see [LDAP authentication with SASL](#).

#### Environment setup and configuration

The following components are required:

- `slapd`: OpenLDAP server.
- `libsasl2` version 2.1.25 or later.
- `saslauthd`: Authentication Daemon (distinct from `libsasl2`).

The following steps will help you configure your environment:

#### ASSUMPTIONS

Before we move on to the configuration steps, we assume the following:

1. You have the LDAP server up and running and have configured users on it. The LDAP server is accessible to the server with Percona Server for MongoDB installed. This document focuses on OpenLDAP server. If you use Microsoft Windows Active Directory, see the *Microsoft Windows Active Directory* section for `saslauthd` configuration.
2. You must place these two servers behind a firewall as the communications between them will be in plain text. This is because the SASL mechanism of PLAIN can only be used when authenticating and credentials will be sent in plain text.
3. You have `sudo` privilege to the server with the Percona Server for MongoDB installed.

#### CONFIGURE SASLAUTHD

1. Install the SASL packages. Depending on your OS, use the following command:

Debian and Ubuntu	RHEL and derivatives
<pre>\$ sudo apt install -y sasl2-bin</pre>	<pre>\$ sudo yum install -y cyrus-sasl</pre>

**NOTE:** For Percona Server for MongoDB versions earlier than 4.0.26-21, 4.4.8-9, 4.2.16-17, also install the `cyrus-sasl-plain` package.

2. Configure SASL to use `ldap` as the authentication mechanism.

 **Note**

Back up the original configuration file before making changes.

**Debian and Ubuntu**      **RHEL and derivatives**

Use the following commands to enable the `saslauthd` to auto-run on startup and to set the `ldap` value for the `--MECHANISMS` option:

```
$ sudo sed -i -e s/^MECH=pam/MECH=ldap/g /etc/sysconfig/saslauthd
sudo sed -i -e s/^MECHANISMS="pam"/MECHANISMS="ldap"/g /etc/default/saslauthd
$ sudo sed -i -e s/^START=no/START=yes/g /etc/default/saslauthd
```

Alternatively, you can edit the `/etc/default/sysconfig/saslauthd` configuration file:

```
START=yes
MECHANISMS="ldap"
```

Specify the `ldap` value for the `--MECH` option using the following command:

```
$ sudo sed -i -e s/^MECH=pam/MECH=ldap/g /etc/sysconfig/saslauthd
```

Alternatively, you can edit the `/etc/sysconfig/saslauthd` configuration file:

```
MECH=ldap
```

3. Create the `/etc/saslauthd.conf` configuration file and specify the settings that `saslauthd` requires to connect to a local LDAP service:

OpenLDAP server      Microsoft Windows Active Directory

The following is the example configuration file. Note that the server address **MUST** match the OpenLDAP installation:

```
ldap_servers: ldap://localhost
ldap_mech: PLAIN
ldap_search_base: dc=example,dc=com
ldap_filter: (cn=%u)
ldap_bind_dn: cn=admin,dc=example,dc=com
ldap_password: secret
```

Note the LDAP password (`ldap_password`) and bind domain name (`ldap_bind_dn`). This allows the `saslauthd` service to connect to the LDAP service as `admin`. In production, this would not be the case; users should not store administrative passwords in unencrypted files.

In order for LDAP operations to be performed against a Windows Active Directory server, a user record must be created to perform the lookups.

The following example shows configuration parameters for `saslauthd` to communicate with an Active Directory server:

```
ldap_servers: ldap://localhost
ldap_mech: PLAIN
ldap_search_base: CN=Users,DC=example,DC=com
ldap_filter: (sAMAccountName=%u)
ldap_bind_dn: CN=ldapmgr,CN=Users,DC=<AD Domain>,DC=<AD TLD>
ldap_password: ld@pmgr_Pa55word
```

In order to determine and test the correct search base and filter for your Active Directory installation, the Microsoft [LDP GUI Tool](#) can be used to bind and search the LDAP-compatible directory.

4. Start the `saslauthd` process and set it to run at restart:

```
$ sudo systemctl start saslauthd
$ sudo systemctl enable saslauthd
```

5. Give write permissions to the `/run/saslauthd` folder for the `mongod`. Either change permissions to the `/run/saslauthd` folder:

```
$ sudo chmod 755 /run/saslauthd
```

Or add the `mongod` user to the `sasl` group:

```
$ sudo usermod -a -G sasl mongod
```

#### SANITY CHECK

Verify that the `saslauthd` service can authenticate against the users created in the LDAP service:

```
$ testsaslauthd -u christian -p secret -f /var/run/saslauthd/mux
```

This should return `0:0K "Success"`. If it doesn't, then either the user name and password are not in the LDAP service, or `saslauthd` is not configured properly.

#### CONFIGURE LIBSASL2

The `mongod` also uses the SASL library for communications. To configure the SASL library, create a configuration file.

The configuration file **must** be named `mongod.conf` and placed in a directory where `libsasl2` can find and read it. `libsasl2` is hard-coded to look in certain directories at build time. This location may be different depending on the installation method.

In the configuration file, specify the following:

```
pwcheck_method: saslauthd
saslauthd_path: /var/run/saslauthd/mux
log_level: 5
mech_list: plain
```

The first two entries (`pwcheck_method` and `saslauthd_path`) are required for `mongod` to successfully use the `saslauthd` service. The `log_level` is optional but may help determine configuration errors.

#### See also

[SASL documentation](#)

#### CONFIGURE MONGODB SERVER

The configuration consists of the following steps:

- Creating a user with the **root** privileges. This user is required to log in to Percona Server for MongoDB after the external authentication is enabled.
- Editing the configuration file to enable the external authentication

#### Create a root user

Create a user with the **root** privileges in the `admin` database. If you have already created this user, skip this step. Otherwise, run the following command to create the admin user:

```
> use admin
switched to db admin
> db.createUser({"user": "admin", "pwd": "$3cr3tP4ssw0rd", "roles": ["root"]})
Successfully added user: { "user" : "admin", "roles" : [ "root" ] }
```

#### Enable external authentication

Edit the `etc/mongod.conf` configuration file to enable the external authentication:

```
security:
  authorization: enabled

setParameter:
  authenticationMechanisms: PLAIN,SCRAM-SHA-1
```

Restart the `mongod` service:

```
$ sudo systemctl restart mongod
```

**Add an external user to Percona Server for MongoDB**

User authentication is done by mapping a user object on the LDAP server against a user created in the `$external` database. Thus, at this step, you create the user in the `$external` database and they inherit the roles and privileges. Note that the username must exactly match the name of the user object on the LDAP server.

Connect to Percona Server for MongoDB and authenticate as the root user.

```
$ mongo --host localhost --port 27017 -u admin -p '$3cr3tP4ssw0rd' --authenticationDatabase 'admin'
```

Use the following command to add an external user to Percona Server for MongoDB:

```
> db.getSiblingDB("$external").createUser( {user : "christian", roles: [ {role: "read", db: "test"} ]} );
```

**Authenticate as an external user in Percona Server for MongoDB**

When running the `mongo` client, a user can authenticate against a given database using the following command:

```
> db.getSiblingDB("$external").auth({ mechanism:"PLAIN", user:"christian", pwd:"secret", digestPassword:false})
```

Alternatively, a user can authenticate while connecting to Percona Server for MongoDB:

```
$ mongo --host localhost --port 27017 --authenticationMechanism PLAIN --authenticationDatabase \$external -u christian -p
```

This section is based on the blog post [Percona Server for MongoDB Authentication Using Active Directory](#) by *Doug Duncan*:

**PERCONA**

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 December 8, 2022

 December 8, 2022

#### 4.3.4 Set up x.509 authentication and LDAP authorization

[x.509 certificate authentication](#) is one of the supported authentication mechanisms in Percona Server for MongoDB. It is compatible with [LDAP authorization](#) to enable you to control user access and operations in your database environment.

This document provides the steps on how to configure and use x.509 certificates for authentication in Percona Server for MongoDB and authorize users in the LDAP server.

##### Considerations

1. For testing purposes, in this tutorial we use [OpenSSL](#) to issue self-signed certificates. For production use, we recommend using certificates issued and signed by the CA in Percona Server for MongoDB. Client certificates must meet the [client certificate requirements](#).
2. The setup of the LDAP server and the configuration of the LDAP schema is out of scope of this document. We assume that you have the LDAP server up and running and accessible to Percona Server for MongoDB.

##### Setup procedure

###### ISSUE CERTIFICATES

1. Create a directory to store the certificates. For example, `/var/lib/mongocerts`.

```
$ sudo mkdir -p /var/lib/mongocerts
```

2. Grant access to the `mongod` user to this directory:

```
$ sudo chown mongod:mongod /var/lib/mongocerts
```

###### Generate the root Certificate Authority certificate

The root Certificate Authority certificate will be used to sign the SSL certificates.

Run the following command and in the `-subj` flag, provide the details about your organization:

- C - Country Name (2 letter code);
- ST - State or Province Name (full name);
- L - Locality Name (city);
- O - Organization Name (company);
- CN - Common Name (your name or your server's hostname) .

```
$ cd /var/lib/mongocerts
$ sudo openssl req -nodes -x509 -newkey rsa:4096 -keyout ca.key -out ca.crt -subj "/C=US/ST=California/L=SanFrancisco/O=Percona/OU=root/CN=localhost"
```



## Generate server certificate

1. Create the server certificate request and key. In the `-subj` flag, provide the details about your organization:

- C - Country Name (2 letter code);
- ST - State or Province Name (full name);
- L - Locality Name (city);
- O - Organization Name (company);
- CN - Common Name (your name or your server's hostname) .

```
$ sudo openssl req -nodes -newkey rsa:4096 -keyout server.key -out server.csr -subj "/C=US/ST=California/L=SanFrancisco/O=Percona/OU=server/CN=localhost"
```

2. Sign the server certificate request with the root CA certificate:

```
$ sudo openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt
```

3. Combine the server certificate and key to create a certificate key file. Run this command as the root user:

```
$ cat server.key server.crt > server.pem
```

## Generate client certificates

1. Generate client certificate request and key. In the `-subj` flag, specify the information about clients in the DN format.

```
$ openssl req -nodes -newkey rsa:4096 -keyout client.key -out client.csr -subj "/DC=com/DC=percona/CN=John Doe"
```

2. Sign the client certificate request with the root CA certificate.

```
$ openssl x509 -req -in client.csr -CA ca.crt -CAkey ca.key -set_serial 02 -out client.crt
```

3. Combine the client certificate and key to create a certificate key file.

```
$ cat client.key client.crt > client.pem
```

## SET UP THE LDAP SERVER

The setup of the LDAP server is out of scope of this document. Please work with your LDAP administrators to set up the LDAP server and configure the LDAP schema.

## CONFIGURE THE MONGODB SERVER

The configuration consists of the following steps:

- Creating a role that matches the user group on the LDAP server
- Editing the configuration file to enable the x.509 authentication

**Note**

When you use x.509 authentication with LDAP authorization, you don't need to create users in the `$external` database. User management is done on the LDAP server so when a client connects to the database, they are authenticated and authorized through the LDAP server.

## Create roles

At this step, create the roles in the `admin` database with the names that exactly match the names of the user groups on the LDAP server. These roles are used for user [LDAP authorization](#) in Percona Server for MongoDB.

In our example, we create the role `cn=otherusers,dc=percona,dc=com` that has the corresponding LDAP group.

```
var admin = db.getSiblingDB("admin")
db.createRole(
  {
    role: "cn=otherusers,dc=percona,dc=com",
    privileges: [],
    roles: [
      "userAdminAnyDatabase",
      "clusterMonitor",
      "clusterManager",
      "clusterAdmin"
    ]
  }
)
```

## Output:

```
{
  "role" : "cn=otherusers,dc=percona,dc=com",
  "privileges" : [ ],
  "roles" : [
    "userAdminAnyDatabase",
    "clusterMonitor",
    "clusterManager",
    "clusterAdmin"
  ]
}
```

## Enable x.509 authentication

1. Stop the `mongod` service

```
$ sudo systemctl stop mongod
```

2. Edit the `/etc/mongod.conf` configuration file.

```
net:
  port: 27017
  bindIp: 127.0.0.1
  tls:
    mode: requireTLS
    certificateKeyFile: /var/lib/mongocerts/server.pem
    CAFile: /var/lib/mongocerts/ca.crt
```

```

security:
  authorization: enabled
  ldap:
    servers: "ldap.example.com"
    transportSecurity: none
    authz:
      queryTemplate: "dc=percona,dc=com??sub?(&(objectClass=groupOfNames)
(member={USER}))"

setParameter:
  authenticationMechanisms: PLAIN,MONGODB-X509

```

Replace `ldap.example.com` with the hostname of your LDAP server. In the LDAP query template, replace the domain controllers `percona` and `com` with those relevant to your organization.

### 3. Start the `mongod` service

```
$ sudo systemctl start mongod
```

#### AUTHENTICATE WITH THE X.509 CERTIFICATE

To test the authentication, connect to *Percona Server for MongoDB* using the following command:

```
$ mongo --host localhost --tls --tlsCAFile /var/lib/mongocerts/ca.crt --
tlsCertificateKeyFile <path_to_client_certificate>/client.pem --authenticationMechanism
MONGODB-X509 --authenticationDatabase='$_external'
```

The result should look like the following:

```
> db.runCommand({connectionStatus : 1})
{
  "authInfo" : {
    "authenticatedUsers" : [
      {
        "user" : "CN=John Doe,DC=percona,DC=com",
        "db" : "$external"
      }
    ],
    "authenticatedUserRoles" : [
      {
        "role" : "cn=otherreaders,dc=percona,dc=com",
        "db" : "admin"
      },
      {
        "role" : "clusterAdmin",
        "db" : "admin"
      },
      {
        "role" : "userAdminAnyDatabase",
        "db" : "admin"
      },
      {
        "role" : "clusterManager",
        "db" : "admin"
      },
      {
        "role" : "clusterMonitor",
        "db" : "admin"
      }
    ]
  }
}
```

```


    },
    "ok" : 1
  }

```

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 January 31, 2023

 December 8, 2022

### 4.3.5 Set up Kerberos authentication

This document provides configuration steps for setting up [Kerberos Authentication](#) in Percona Server for MongoDB.

#### Assumptions

The setup of the Kerberos server itself is out of scope of this document. Please refer to the [Kerberos documentation](#) for the installation and configuration steps relevant to your operation system.

We assume that you have successfully completed the following steps:

- Installed and configured the Kerberos server
- Added necessary [realms](#)
- Added service, admin and user [principals](#)
- Configured the `A` and `PTR` DNS records for every host running `mongod` instance to resolve the hostnames onto Kerberos realm.

#### Add user principals to Percona Server for MongoDB

To get authenticated, users must exist both in the Kerberos and Percona Server for MongoDB servers with exactly matching names.

After you defined the user principals in the Kerberos server, add them to the `$external` database in Percona Server for MongoDB and assign required roles:

```

> use $external
> db.createUser({user: "demo@PERCONATEST.COM",roles: [{role: "read", db: "admin"}]})

```

Replace `demo@PERCONATEST.COM` with your username and Kerberos realm.

### Configure Kerberos keytab files

A keytab file stores the authentication keys for a service principal representing a `mongod` instance to access the Kerberos admin server.

After you have added the service principal to the Kerberos admin server, the entry for this principal is added to the `/etc/krb5.keytab` keytab file.

The `mongod` server must have access to the keytab file to authenticate. To keep the keytab file secure, restrict the access to it only for the user running the `mongod` process.

1. Stop the `mongod` service

```
$ sudo systemctl stop mongod
```

2. [Generate the keytab file](#) or get a copy of it if you generated the keytab file on another host. Save the keyfile under a separate path (e.g. `/etc/mongodb.keytab`)

```
$ cp /etc/krb5.keytab /etc/mongodb.keytab
```

3. Change the ownership to the keytab file

```
$ sudo chown mongod:mongod /etc/mongodb.keytab
```

4. Set the `KRB5_KTNAME` variable in the environment file for the `mongod` process.

Debian and Ubuntu      RHEL and derivatives

Edit the environment file at the path `/etc/default/mongod` and specify the `KRB5_KTNAME` variable:

```
KRB5_KTNAME=/etc/mongodb.keytab
```

If you have a different path to the keytab file, specify it accordingly.

Edit the environment file at the path `/etc/sysconfig/mongod` and specify the `KRB5_KTNAME` variable:

```
KRB5_KTNAME=/etc/mongodb.keytab
```

If you have a different path to the keytab file, specify it accordingly.

5. Restart the `mongod` service

```
$ sudo systemctl start mongod
```

### Percona Server for MongoDB configuration

Enable external authentication in Percona Server for MongoDB configuration. Edit the `etc/mongod.conf` configuration file and specify the following configuration:

```
security:
  authorization: "enabled"
```

```
setParameter:
  authenticationMechanisms: GSSAPI
```

Restart the `mongod` service to apply the configuration:

```
$ sudo systemctl start mongod
```

### Test the access to Percona Server for MongoDB

1. Obtain the Kerberos ticket for the user using the `kinit` command and specify the user password:

```
$ kinit demo
Password for demo@PERCONATEST.COM:
```

2. Check the user ticket:

```
$ klist -l
```

Output:

Principal name	Cache name
demo@PERCONATEST.COM	FILE:/tmp/<ticket>

3. Connect to Percona Server for MongoDB:

```
$ mongo --host <hostname> --authenticationMechanism=GSSAPI --
authenticationDatabase='$external' --username demo@PERCONATEST.COM
```

The result should look like the following:

```
> db.runCommand({connectionStatus : 1})
{
  "authInfo" : {
    "authenticatedUsers" : [
      {
        "user" : "demo@PERCONATEST.COM",
        "db" : "$external"
      }
    ],
    "authenticatedUserRoles" : [
      {
        "role" : "read",
        "db" : "admin"
      }
    ]
  },
  "ok" : 1
}
```

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 January 31, 2023

 December 8, 2022

### 4.3.6 AWS IAM authentication

 **Version added: 5.0.15-13**

IAM (Identity Access Management) is the AWS service that allows you to securely control access to AWS resources. Percona Server for MongoDB supports authentication with AWS IAM enabling you to use the same AWS credentials both for it and other components of your infrastructure. This saves your DBAs from managing different sets of secrets and frees their time on other activities.

You can configure AWS IAM for a password-less authentication. Instead of username and password, the user or the application presents the AWS security credentials for authentication, but the secret key is not sent to Percona Server for MongoDB. This significantly increases the security in your infrastructure.

Percona Server for MongoDB supports two authentication types:

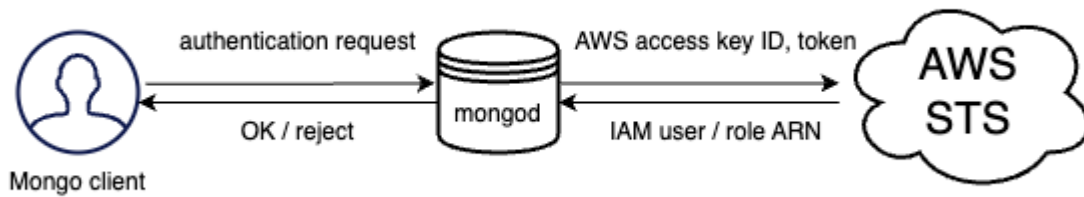
#### User authentication

This authentication type is typically used by human operators. Every user account in AWS has the ARN (Amazon Resource Name), which uniquely identifies this account and the user associated with it. During authentication, the ARN is used to verify the user's identity.

#### Role authentication

This type is typically used for applications / `mongo` clients. For instance, if your application is running on AWS resources like EC2 instance or ECS (Elastic Container Service) which uses the IAM role assigned to it. Another scenario is to allow users to assume the IAM role and in such a way, grant a user the permissions outlined in the IAM role. The ARN of the IAM role is used to authenticate the application in Percona Server for MongoDB.

For either type of AWS IAM authentication, the flow is the following:



1. A `mongo` client (a Mongo shell or an application that talks to Percona Server for MongoDB via a driver) gets AWS credentials from either EC2/ECS instance metadata service, environmental variables or MongoDB URI connection string.
2. The `mongo` client constructs the authentication request which includes the AWS access key ID, token and the signature and sends it to Percona Server for MongoDB

#### Important

The `mongo` client never sends the secret access key to Percona Server for MongoDB.

3. Percona Server for MongoDB sends the received credentials to the AWS STS (Security Token Service) for verification
4. The AWS STS service validates whether the signature is correct and answers with the user / role ARN that created the signature
5. Percona Server for MongoDB looks for the same username as the received ARN in the `$external` database and grants privileges to access Percona Server for MongoDB as defined for the respective user.

Starting with version [5.0.19-16](#), you can [configure the AWS STS endpoint](#) by specifying the `setParameter.awsStsHost` in the configuration file. This allows you to send requests to the AWS resources of your choice to meet security requirements of your organization and ensure successful authentication.

#### See also

- AWS documentation:
  - [AWS Identity and Access Management](#)
  - [Temporary security credentials in IAM](#)
  - [Authenticating Requests \(AWS Signature Version 4\)](#)
  - [Managing AWS STS in an AWS Region](#)
- MongoDB documentation: [Set Up Passwordless Authentication with AWS IAM](#)

## Configuration

For how to configure AWS IAM authentication, see [Setting up AWS IAM authentication](#).



## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 December 21, 2023

 March 16, 2023

### 4.3.7 Setting up AWS IAM authentication

This document provides guidelines how to configure Percona Server for MongoDB to use AWS IAM authentication. The use of this authentication method enables you to natively integrate Percona Server for MongoDB with AWS services, increase security of your infrastructure by setting up password-less authentication and offload your DBAs from managing different sets of secrets. To learn more, see [AWS IAM authentication](#)

To configure AWS IAM authentication means to set up your AWS environment and configure Percona Server for MongoDB. The AWS environment setup is out of scope of this document. Consult the AWS documentation to perform the following setup steps:

1. [Configure the AWS resource to work with IAM.](#)
2. For user authentication:
  - [Create the IAM user](#) and copy its ARN (Amazon Resource Name)

For role authentication:

- [Create the IAM role](#)
- Attach the IAM role to the AWS resource.
- Copy the ARN of the IAM role.

#### Configure Percona Server for MongoDB

The steps are the following:

1. Create users in the `$external` database with the username as the IAM user/role ARN
2. Enable authentication and specify the authentication mechanism as `MONGODB-AWS`.

CREATE USERS IN `$EXTERNAL` DATABASE

During the authentication, Percona Server for MongoDB matches the ARN of the IAM user or role retrieved from AWS STS against the user created in the `$external` database. Thus, the username for this user must include their ARN and have the following format:

User authentication	Role authentication
<code>arn:aws:iam::&lt;ARN&gt;:user/&lt;user_name&gt;</code>	
	<code>arn:aws:iam::&lt;ARN&gt;:role/&lt;role_name&gt;</code>

Create a user and assign the required roles to them. Specify the ARN and names in the following example commands:

User authentication	Role authentication
<pre>&gt; use \$external &gt; db.createUser(   {     user: "arn:aws:iam::000000000000:user/myUser",     roles: [{role: "read", db: "admin"}]   } )</pre>	<pre>&gt; use \$external &gt; db.createUser(   {     user: "arn:aws:iam::111111111111:role/myRole",     roles: [{role: "read", db: "admin"}]   } )</pre>

## ENABLE AUTHENTICATION

Run the following commands as root or via `sudo`

1. Stop the `mongod` service

```
$ sudo systemctl stop mongod
```

2. Edit the `/etc/mongod.conf` configuration file

```
security:
  authorization: enabled

setParameter:
  authenticationMechanisms: MONGODB-AWS
```

3. Start the `mongod` service

```
$ sudo systemctl start mongod
```

## Configure AWS STS endpoint

By default, all authentication requests are sent to the `sts.amazonaws.com` endpoint. If this endpoint is unavailable for some reason, you can override it and send AWS STS requests to the endpoints of your choice to ensure successful authentication. You must [enable the AWS region](#) to use it.

Edit the `/etc/mongod.conf` configuration file and specify the AWS endpoint for the `awsStsHost` parameter.

```
security:
  authorization: enabled

setParameter:
  authenticationMechanisms: MONGODB-AWS
  awsStsHost: <aws-endpoint>
```

See the [list of AWS endpoints](#).

### Authenticate in Percona Server for MongoDB using AWS IAM

To test the authentication, use either of the following methods:

MongoDB connection string      Environment variables      AWS resource metadata

Replace `<aws_access_key_id>`, `<aws_secret_access_key>` and `psmdb.example.com` with actual values in the following command:

```
$ mongo 'mongodb://<aws_access_key_id>:<aws_secret_access_key>@psmdb.example.com/admin?
authSource=$external&authMechanism=MONGODB-AWS'
```

To pass temporary credentials and AWS token, replace `<aws_access_key_id>`, `<aws_secret_access_key>`, `<aws_session_token>` and `psmdb.example.com` in the following command:

```
$ mongo 'mongodb://<aws_access_key_id>:<aws_secret_access_key>@psmdb.example.com/admin?
authSource=$external&authMechanism=MONGODB-
AWS&authMechanismProperties=AWS_SESSION_TOKEN:<aws_session_token>'
```

Set AWS environment variables:

```
export AWS_ACCESS_KEY_ID='<aws_access_key_id>'
export AWS_SECRET_ACCESS_KEY='<aws_secret_access_key>'
export AWS_SESSION_TOKEN='<aws_session_token>'
```

Connect to Percona Server for MongoDB:

```
$ mongo 'mongodb://psmdb.example.com/testdb?authSource=$external&authMechanism=MONGODB-AWS'
```

If your application is running on the AWS resource, it receives the credentials from the resource metadata. To connect to Percona Server for MongoDB, run the command as follows:

```
$ mongo --authenticationMechanism=MONGODB-AWS --authenticationDatabase='$external'
```

Upon successful authentication, the result should look like the following:

```
> db.runCommand( { connectionStatus: 1 } )
{
  authInfo: {
    authenticatedUsers: [
      {
        user: 'arn:aws:iam::000000000000:user/myUser',
        db: '$external'
      }
    ]
  }
}
```

```

    ],
    authenticatedUserRoles: [ { role: 'read', db: 'admin' } ]
  },
  ok: 1
}

```

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)    [Get a Percona Expert](#)

 August 10, 2023

 March 16, 2023

### 4.3.8 LDAP authorization

LDAP authorization allows you to control user access and operations in your database environment using the centralized user management storage – an LDAP server. You create and manage user credentials and permission information in the LDAP server. In addition, you create roles in the `admin` database with the names that exactly match the LDAP group Distinguished Name. These roles define what privileges the users who belong to the corresponding LDAP group.

#### Supported authentication mechanisms

LDAP authorization is compatible with the following authentication mechanisms:

- [x.509 certificate authentication](#)
- [Kerberos Authentication](#)
- [Authentication and authorization with direct binding to LDAP](#)

#### Authentication and authorization with direct binding to LDAP

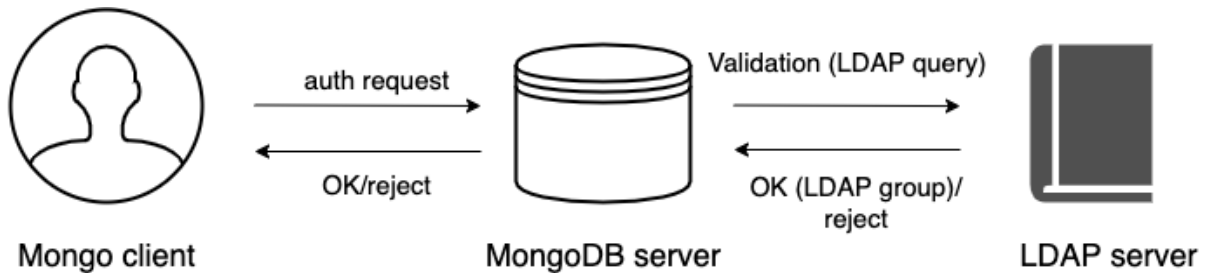
Starting with release 4.2.5-5, you can configure Percona Server for MongoDB to communicate with the LDAP server directly to authenticate and also authorize users.

The advantage of using this mechanism is that it is easy to setup and does not require pre-creating users in the dummy `$external` db. Nevertheless, the `--authenticationDatabase` connection argument will still need to be specified as `$external`.

The following example illustrates the connection to Percona Server for MongoDB from the `mongo` shell:

```
$ mongo -u "CN=alice,CN=Users,DC=engineering,DC=example,DC=com" -p --authenticationDatabase '$external' --authenticationMechanism PLAIN
```

The following diagram illustrates the authentication and authorization flow:



1. A user connects to the db providing their credentials
2. If required, Percona Server for MongoDB [transforms the username](#) to match the user in the LDAP server according to the mapping rules specified for the `--ldapUserToDNMapping` parameter.
3. Percona Server for MongoDB queries the LDAP server for the user identity and /or the LDAP groups this user belongs to.
4. The LDAP server evaluates the query and if a user exists, returns their LDAP groups.
5. Percona Server for MongoDB authorizes the user by mapping the DN of the returned groups against the roles assigned to the user in the `admin` database. If a user belongs to several groups they receive permissions associated with every group.

#### USERNAME TRANSFORMATION

If clients connect to Percona Server for MongoDB with usernames that are not LDAP , these usernames must be converted to the format acceptable by LDAP.

To achieve this, the `--ldapUserToDNMapping` parameter is available in Percona Server for MongoDB configuration.

The `--ldapUserToDNMapping` parameter is a JSON string representing an ordered array of rules expressed as JSON documents. Each document provides a regex pattern (`match` field) to match against a provided username. If that pattern matches, there are two ways to continue:

- If there is the `substitution` value, then the matched pattern becomes the username of the user for further processing.
- If there is the `ldapQuery` value, the matched pattern is sent to the LDAP server and the result of that LDAP query becomes the of the user for further processing.

Both `substitution` and `ldapQuery` should contain placeholders to insert parts of the original username - those placeholders are replaced with regular expression submatches found on the `match` stage.

So having an array of documents, Percona Server for MongoDB tries to match each document against the provided name and if it matches, the name is replaced either with the substitution string or with the result of the LDAP query.

#### LDAP REFERRALS

As of version 4.2.10-11, Percona Server for MongoDB supports LDAP referrals as defined in [RFC 4511 4.1.10](#). For security reasons, referrals are disabled by default. Double-check that using referrals is safe before enabling them.

To enable LDAP referrals, set the `ldapFollowReferrals` server parameter to `true` using the `setParameter` command or by editing the configuration file.

```
setParameter:
  ldapFollowReferrals: true
```

#### CONNECTION POOL

As of version 4.2.10-11, Percona Server for MongoDB always uses a connection pool to LDAP server to process bind requests. The connection pool is enabled by default. The default connection pool size is 2 connections.

You can change the connection pool size either at the server startup or dynamically by specifying the value for the `ldapConnectionPoolSizePerHost` server parameter.

For example, to set the number of connections in the pool to 5, use the `setParameter` command:

Command line	Configuration file
<pre>&gt;db.adminCommand( { setParameter: 1, ldapConnectionPoolSizePerHost: 5 } )</pre>	
	<pre>setParameter:   ldapConnectionPoolSizePerHost: 5</pre>

#### SUPPORT FOR MULTIPLE LDAP SERVERS

As of version 4.2.12-13, you can specify multiple LDAP servers for failover. Percona Server for MongoDB sends bind requests to the first server defined in the list. When this server is down or unavailable, it sends requests to the next server and so on. Note that Percona Server for MongoDB keeps sending requests to this server even after the unavailable server recovers.

Specify the LDAP servers as a comma-separated list in the format `<host>:<port>` for the `-ldapServers` option.

You can define the option value at the server startup by editing the configuration file.

```
security:
  authorization: "enabled"
  ldap:
    servers: "ldap1.example.net,ldap2.example.net"
```

You can change `ldapServers` dynamically at runtime using the `setParameter`.

```
> db.adminCommand( { setParameter: 1,
ldapServers:"localhost,ldap1.example.net,ldap2.example.net"} )
{ "was" : "ldap1.example.net,ldap2.example.net", "ok" : 1 }
```

#### See also

MongoDB Documentation:

- [Authenticate and Authorize Users Using Active Directory via Native LDAP](#)
- [LDAP referrals](#)

## Configuration

For how to configure LDAP authorization with the native LDAP authentication, see [Setting up LDAP authentication and authorization using NativeLDAP](#).

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 December 8, 2022

 December 8, 2022

### 4.3.9 Set up LDAP authentication and authorization using NativeLDAP

This document describes an example configuration of LDAP authentication and authorization using direct binding to an LDAP server (Native LDAP). We recommend testing this setup in a non-production environment first, before applying it in production.

#### Assumptions

1. The setup of an LDAP server is out of scope of this document. We assume that you are familiar with the LDAP server schema.
2. You have the LDAP server up and running and it is accessible to the servers with Percona Server for MongoDB installed.
3. This document primarily focuses on OpenLDAP used as the LDAP server and the examples are given based on the OpenLDAP format. If you are using Active Directory, refer to the [Active Directory configuration](#) section.
4. You have the `sudo` privilege to the server with the Percona Server for MongoDB installed.

#### Prerequisites

- In this setup we use anonymous binds to the LDAP server. If your LDAP server disallows anonymous binds, create the user that Percona Server for MongoDB will use to connect to and query the LDAP server. Define this user's credentials for the `security.ldap.bind.queryUser` and `security.ldap.bind.queryPassword` parameters in the `mongod.conf` configuration file.
- In this setup, we use the following OpenLDAP groups:

```
dn: cn=testusers,dc=percona,dc=com
objectClass: groupOfNames
```

```

cn: testusers
member: cn=alice,dc=percona,dc=com

dn: cn=otherusers,dc=percona,dc=com
objectClass: groupOfNames
cn: otherusers
member: cn=bob,dc=percona,dc=com

```

## Setup procedure

### CONFIGURE TLS/SSL CONNECTION FOR PERCONA SERVER FOR MONGODB

By default, Percona Server for MongoDB establishes the TLS connection when binding to the LDAP server and thus, it requires access to the LDAP certificates. To make Percona Server for MongoDB aware of the certificates, do the following:

1. Place the certificate in the `certs` directory. The path to the `certs` directory is:
  - On Debian / Ubuntu: `/etc/ssl/certs/`
  - On RHEL / CentOS: `/etc/openldap/certs/`
2. Specify the path to the certificates in the `ldap.conf` file:

```

Debian / Ubuntu      RHEL and derivatives
tee -a /etc/openldap/ldap.conf <<EOF
TLS_CACERT /etc/ssl/certs/my_CA.crt
EOF

tee -a /etc/openldap/ldap.conf <<EOF
TLS_CACERT /etc/openldap/certs/my_CA.crt
EOF

```

### CREATE ROLES FOR LDAP GROUPS IN PERCONA SERVER FOR MONGODB

Percona Server for MongoDB authorizes users based on LDAP group membership. For every group, you must create the role in the `admin` database with the name that exactly matches the DN of the LDAP group.

Percona Server for MongoDB maps the user's LDAP group to the roles and determines what role is assigned to the user. Percona Server for MongoDB then grants privileges defined by this role.

To create the roles, use the following command:

```

var admin = db.getSiblingDB("admin")
db.createRole(
  {
    role: "cn=testusers,dc=percona,dc=com",
    privileges: [],
    roles: [ "readWrite" ]
  }
)

db.createRole(
  {
    role: "cn=otherusers,dc=percona,dc=com",
    privileges: [],
    roles: [ "read" ]
  }
)

```



## PERCONA SERVER FOR MONGODB CONFIGURATION

## Access without username transformation

This section assumes that users connect to Percona Server for MongoDB by providing their LDAP DN as the username.

1. Edit the Percona Server for MongoDB configuration file (by default, `/etc/mongod.conf`) and specify the following configuration:

```
security:
  authorization: "enabled"
  ldap:
    servers: "ldap.example.com"
    transportSecurity: tls
    authz:
      queryTemplate: "dc=percona,dc=com??sub?(&(objectClass=groupOfNames)
(member={PROVIDED_USER}))"

setParameter:
  authenticationMechanisms: "PLAIN"
```

The `{PROVIDED_USER}` variable substitutes the provided username before authentication or username transformation takes place.

Replace `ldap.example.com` with the hostname of your LDAP server. In the LDAP query template, replace the domain controllers `percona` and `com` with those relevant to your organization.

2. Restart the `mongod` service:

```
$ sudo systemctl restart mongod
```

3. Test the access to Percona Server for MongoDB:

```
$ mongo -u "cn=alice,dc=percona,dc=com" -p "secretpwd" --authenticationDatabase
'$external' --authenticationMechanism 'PLAIN'
```

## Access with username transformation

If users connect to Percona Server for MongoDB with usernames that are not LDAP DN, you need to transform these usernames to be accepted by the LDAP server.

Using the `--ldapUserToDNMapping` configuration parameter allows you to do this. You specify the match pattern as a regexp to capture a username. Next, specify how to transform it - either to use a substitution value or to query the LDAP server for a username.

If you don't know what the substitution or LDAP query string should be, please consult with the LDAP administrators to figure this out.

Note that you can use only the `query` or the `substitution` stage, the combination of two is not allowed.

## Substitution LDAP query

1. Edit the Percona Server for MongoDB configuration file (by default, `/etc/mongod.conf`) and specify the `userToDNMapping` parameter:

```
security:
  authorization: "enabled"
  ldap:
    servers: "ldap.example.com"
    transportSecurity: tls
    authz:
      queryTemplate: "dc=percona,dc=com??sub?(&(objectClass=groupOfNames)
(member={USER}))"
      userToDNMapping: >-
        [
          {
            match: "([^\@]+)@percona\\.com",
            substitution: "CN={0},DC=percona,DC=com"
          }
        ]

setParameter:
  authenticationMechanisms: "PLAIN"
```

The `{USER}` variable substitutes the username transformed during the `userToDNMapping` stage.

Modify the given example configuration to match your deployment.

2. Restart the `mongod` service:

```
$ sudo systemctl restart mongod
```

3. Test the access to Percona Server for MongoDB:

```
$ mongo -u "alice@percona.com" -p "secretpwd" --authenticationDatabase '$external' --
authenticationMechanism 'PLAIN'
```

1. Edit the Percona Server for MongoDB configuration file (by default, `/etc/mongod.conf`) and specify the `userToDNMapping` parameter:

```
security:
  authorization: "enabled"
  ldap:
    servers: "ldap.example.com"
    transportSecurity: tls
    authz:
      queryTemplate: "dc=percona,dc=com??sub?(&(objectClass=groupOfNames)
(member={USER}))"
      userToDNMapping: >-
        [
          {
            match: "([^\@]+)@percona\\.com",
            ldapQuery: "dc=percona,dc=com??sub?(&(objectClass=organizationalPerson)
(cn={0}))"
          }
        ]

setParameter:
  authenticationMechanisms: "PLAIN"
```

The `{USER}` variable substitutes the username transformed during the `userToDNMapping` stage.

Modify the given example configuration to match your deployment. For example, replace

`ldap.example.com` with the hostname of your LDAP server. Replace the domain controllers (DC) `percona`

and `com` with those relevant to your organization. Depending on your LDAP schema, further

modifications of the LDAP query may be required.

## ACTIVE DIRECTORY CONFIGURATION

Microsoft Active Directory uses a different schema for user and group definition. To illustrate Percona Server for MongoDB configuration, we will use the following AD users:

```
dn:CN=alice,CN=Users,DC=testusers,DC=percona,DC=com
userPrincipalName: alice@testusers.percona.com
memberOf: CN=testusers,CN=Users,DC=percona,DC=com

dn:CN=bob,CN=Users,DC=otherusers,DC=percona,DC=com
userPrincipalName: bob@otherusers.percona.com
memberOf: CN=otherusers,CN=Users,DC=percona,DC=com
```

The following are respective groups:

```
dn:CN=testusers,CN=Users,DC=percona,DC=com
member:CN=alice,CN=Users,DC=testusers,DC=example,DC=com

dn:CN=otherusers,CN=Users,DC=percona,DC=com
member:CN=bob,CN=Users,DC=otherusers,DC=example,DC=com
```

Use one of the given Percona Server for MongoDB configurations for user authentication and authorization in Active Directory:

No username transformation    Username substitution    LDAP query

1. Edit the `/etc/mongod.conf` configuration file:

```
ldap:
  servers: "ldap.example.com"
  authz:
    queryTemplate: "DC=percona,DC=com??sub?(&(objectClass=group)(member:
1.2.840.113556.1.4.1941:={PROVIDED_USER}))"

  setParameter:
    authenticationMechanisms: "PLAIN"
```

2. Restart the `mongod` service:

```
$ sudo systemctl restart mongod
```

3. Test the access to Percona Server for MongoDB:

```
$ mongo -u "CN=alice,CN=Users,DC=testusers,DC=percona,DC=com" -p "secretpwd" --
authenticationDatabase '$external' --authenticationMechanism 'PLAIN'
```

1. Edit the `/etc/mongod.conf` configuration file:

```
ldap:
  servers: "ldap.example.com"
  authz:
    queryTemplate: "DC=percona,DC=com??sub?(&(objectClass=group)(member:
1.2.840.113556.1.4.1941:={USER}))"
    userToDNMapping: >-
      [
        {
          match: "([^@+)]+@([^\.\.]+)\.percona\.com",
          substitution: "CN={0},CN=Users,DC={1},DC=percona,DC=com"
        }
      ]

  setParameter:
    authenticationMechanisms: "PLAIN"
```

2. Restart the `mongod` service:

```
$ sudo systemctl restart mongod
```

3. Test the access to Percona Server for MongoDB:

```
$ mongo -u "alice@percona.com" -p "secretpwd" --authenticationDatabase '$external' --
authenticationMechanism 'PLAIN'
```

1. Edit the `/etc/mongod.conf` configuration file:

```
ldap:
  servers: "ldap.example.com"
  authz:
    queryTemplate: "DC=percona,DC=com??sub?(&(objectClass=group)(member:
1.2.840.113556.1.4.1941:={USER}))"
    userToDNMapping: >-
      [
        {
          match: "(.+)",
          ldapQuery: "dc=example,dc=com??sub?(&(objectClass=organizationalPerson)
(userPrincipalName={0}))"
```

Modify one of this example configuration to match your deployment.

This document is based on the following posts from Percona Database Performance Blog:

- [Percona Server for MongoDB LDAP Enhancements: User-to-DN Mapping](#) by Igor Solodovnikov
- [Authenticate Percona Server for MongoDB Users via Native LDAP](#) by Ivan Groenewold

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 December 8, 2022

 December 8, 2022

## 4.4 Encryption

### 4.4.1 Data at Rest Encryption

Data at rest encryption for the WiredTiger storage engine in MongoDB was introduced in MongoDB Enterprise version 3.2 to ensure that encrypted data files can be decrypted and read by parties with the decryption key.

#### Differences from upstream

The data encryption at rest in Percona Server for MongoDB is introduced in version 3.6 to be compatible with data encryption at rest interface in MongoDB. In the current release of Percona Server for MongoDB, the data encryption at rest does not include support for Amazon AWS key management service. Instead, Percona Server for MongoDB is [integrated with HashiCorp Vault](#).

Starting with release 5.0.7-6, Percona Server for MongoDB supports the secure transfer of keys using [Key Management Interoperability Protocol \(KMIP\)](#). This allows users to store encryption keys in their favorite KMIP-compatible key manager when they set up encryption at rest.

## Workflow

### Important

You can only enable data at rest encryption and provide all encryption settings on an empty database, when you start the mongod instance for the first time. You cannot enable or disable encryption while the Percona Server for MongoDB server is already running and / or has some data. Nor can you change the effective encryption mode by simply restarting the server. Every time you restart the server, the encryption settings must be the same.

Each node of Percona Server for MongoDB generates a random, individual key for every database. It encrypts every database with an individual key and puts those keys into the special, so-called key database. Then each node of Percona Server for MongoDB randomly generates a unique master encryption key and encrypts the key database with this key.

Thus, two types of keys are used for data at rest encryption:

- Database keys to encrypt data. They are stored internally, near the data that they encrypt.
- The master key to encrypt database keys. It is kept separately from the data and database keys and requires external management.

To manage the master encryption key, use one of the supported key management options:

- Integration with an external key server (recommended). Percona Server for MongoDB is [integrated with HashiCorp Vault](#) for this purpose and supports the secure transfer of keys using [Key Management Interoperability Protocol \(KMIP\)](#).
- [Local key management using a keyfile.](#)

Note that you can use only one of the key management options at a time. However, you can switch from one management option to another (e.g. from a keyfile to HashiCorp Vault). Refer to [Migrating from Key File Encryption to HashiCorp Vault Encryption](#) section for details.

### Important configuration options

Percona Server for MongoDB supports the `encryptionCipherMode` option where you choose one of the following cipher modes:

- AES256-CBC
- AES256-GCM

By default, the `AES256-CBC` cipher mode is applied. The following example demonstrates how to apply the `AES256-GCM` cipher mode when starting the `mongod` service:

```
$ mongod ... --encryptionCipherMode AES256-GCM
```

### See also

MongoDB Documentation: [encryptionCipherMode Option](#)



### Encryption of rollback files

Starting from version 3.6, Percona Server for MongoDB also encrypts rollback files when data at rest encryption is enabled. To inspect the contents of these files, use **perconadecrypt**. This is a tool that you run from the command line as follows:

```
$ perconadecrypt --encryptionKeyFile FILE --inputPath FILE --outputPath FILE [--
encryptionCipherMode MODE]
```

When decrypting, the cipher mode must match the cipher mode which was used for the encryption. By default, the `--encryptionCipherMode` option uses the `AES256-CBC` mode.

#### PARAMETERS OF PERCONADECRYPT

Option	Purpose
<code>--encryptionKeyFile</code>	The path to the encryption key file
<code>--encryptionCipherMode</code>	The cipher mode for decryption. The supported values are <code>AES256-CBC</code> or <code>AES256-GCM</code>
<code>--inputPath</code>	The path to the encrypted rollback file
<code>--outputPath</code>	The path to save the decrypted rollback file

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 August 8, 2024

 December 8, 2022

### 4.4.2 HashiCorp Vault integration

Percona Server for MongoDB is integrated with HashiCorp Vault. HashiCorp Vault supports different secrets engines. Percona Server for MongoDB only supports the HashiCorp Vault back end with KV Secrets Engine - Version 2 (API) with versioning enabled.

#### See also

Percona Blog: [Using Vault to Store the Master Key for Data at Rest Encryption on Percona Server for MongoDB](#)

HashiCorp Vault Documentation: [How to configure the KV Engine](#)

## Version changes

The following table lists the changes in the implementation of HashiCorp Vault integration with Percona Server for MongoDB and the versions that introduced those changes:

Version	Description
5.0.15-13	Key rotation in replica sets
5.0.29-25	Master key loss prevention

## HashiCorp Vault parameters

Command line	Configuration file	Type	Description
vaultServerName	security.vault.serverName	string	The IP address of the Vault server
vaultPort	security.vault.port	int	The port on the Vault server
vaultTokenFile	security.vault.tokenFile	string	The path to the vault token file. The token file is used by MongoDB to access HashiCorp Vault. The vault token file consists of the raw vault token and does not include any additional strings or parameters.  Example of a vault token file:  <code>s.uTrHtzsZnEE7KyHeA797CkWA</code>
vaultSecret	security.vault.secret	string	The path to the Vault secret. The Vault secret path format must be <code>&lt;secrets_engine_mount_path&gt;/data/&lt;custom_path&gt;</code>  where: - <code>&lt;secrets_engine_mount_path&gt;</code> is the path to the Key/Value Secrets Engine v2; - <code>data</code> is the mandatory path prefix required by Version 2 API; - <code>&lt;custom_path&gt;</code> is the path to the specific secret.  Example: <code>secret_v2/data/psmdb-test/rs1-27017</code>  Starting with version 5.0.15-13, a distinct Vault secret path for every replica set member is no longer mandatory. In earlier versions, it is recommended to use different secret paths for every

Command line	Configuration file	Type	Description
<code>vaultSecretVersion</code>	<code>security.vault.secretVersion</code>	unsigned long	database node in the entire deployment to avoid issues during the master key rotation.  (Optional) The version of the Vault secret to use
<code>vaultRotateMasterKey</code>	<code>security.vault.rotateMasterKey</code>	switch	When enabled, rotates the master key and exits
<code>vaultServerCAFile</code>	<code>security.vault.serverCAFile</code>	string	The path to the TLS certificate file
<code>vaultDisableTLSForTesting</code>	<code>security.vault.disableTLSForTesting</code>	switch	Disables secure connection to Vault using SSL/TLS client certificates
<code>vaultCheckMaxVersions</code>	<code>security.vault.checkMaxVersions</code>	boolean	Verifies that the current number of secret versions has not reached the maximum, defined by the <code>max_versions</code> parameter for the secret or the secrets engine on the Vault server. If the number of versions has reached the maximum, the server logs an error and exits. Enabled by default. Available starting with version 5.0.29-25.

## CONFIG FILE EXAMPLE

```
security:
  enableEncryption: true
  vault:
    serverName: 127.0.0.1
    port: 8200
    tokenFile: /home/user/path/token
    secret: secret/data/hello
```

## Vault access policy configuration

Starting with 5.0.29-25, Percona Server for MongoDB checks the number of the secrets on the Vault server before adding a new one thus [preventing the loss of the old master key](#). For these checks, Percona Server for MongoDB requires read permissions for the secret's metadata and the secrets engine configuration. You configure these permissions within the access policy on the Vault server.

Find the sample policy configuration below:

```
path "secret/data/*" {
  capabilities = ["create", "read", "update", "delete"]
}
path "secret/metadata/*" {
  capabilities = ["read"]
}
path "secret/config" {
  capabilities = ["read"]
}
```

During the first run of the Percona Server for MongoDB, the process generates a secure key and writes the key to the vault.

During the subsequent start, the server tries to read the master key from the vault. If the configured secret does not exist, vault responds with HTTP 404 error.

## Namespaces

Namespaces are isolated environments in Vault that allow for separate secret key and policy management.

You can use Vault namespaces with Percona Server for MongoDB. Specify the namespace(s) for the `security.vault.secret` option value as follows:

```
<namespace>/secret/data/<secret_path>
```

For example, the path to secret keys for namespace `test` on the secrets engine `secret` will be `test/secret/<my_secret_path>`.

### TARGETING A NAMESPACE IN VAULT CONFIGURATION

You have the following options of how to target a particular namespace when configuring Vault:

1. Set the `VAULT_NAMESPACE` environment variable so that all subsequent commands are executed against that namespace. Use the following command to set the environment variable for the namespace `test`:

```
$ export VAULT_NAMESPACE=test
```

2. Provide the namespace with the `--namespace` flag in commands

#### See also

HashiCorp Vault Documentation:

- [Namespaces](#)
- [Secure Multi-Tenancy with Namespaces](#)

## Key rotation

Key rotation is replacing the old master key with a new one. This process helps to comply with regulatory requirements.

To rotate the keys for a single `mongod` instance, do the following:

1. Stop the `mongod` process
2. Add `--vaultRotateMasterKey` option via the command line or `security.vault.rotateMasterKey` to the config file.
3. Run the `mongod` process with the selected option, the process will perform the key rotation and exit.
4. Remove the selected option from the startup command or the config file.
5. Start `mongod` again.

Rotating the master key process also re-encrypts the keystore using the new master key. The new master key is stored in the vault. The entire dataset is not re-encrypted.

#### KEY ROTATION IN REPLICA SETS

Starting with version [5.0.15-13](#), you can store the master key at the same path on every replica set member in your entire deployment. Vault assigns different versions to the master keys stored at the same path. The path and the version serve as the unique identifier of a master key. The `mongod` server stores that identifier and uses it to retrieve the correct master key from the Vault server during the restart.

In versions 5.0.14-12 and earlier, every `mongod` node in a replica set in your entire deployment must have a distinct path to the master keys on a Vault server.

The key rotation steps are the following:

1. Rotate the master key for the secondary nodes one by one.
2. Step down the primary and wait for another primary to be elected.
3. Rotate the master key for the previous primary node.

#### MASTER KEY LOSS PREVENTION

Starting with version 5.0.29-25, Percona Server for MongoDB checks if the number of secret versions has reached the maximum (10 by default) before adding a new master key to the Vault server as a versioned secret. You configure this number using the `max_versions` parameter on the Vault server.

If the number of secrets reaches the maximum, Percona Server for MongoDB logs an error and exits. This prevents the Vault server from dropping the oldest secret version and the encryption key it stores.

To continue, increase the maximum versions for the secret or the entire secrets engine on the Vault server, then restart Percona Server for MongoDB. To check the number of secrets on the Vault server, ensure Percona Server for MongoDB has [read permissions for the secret's metadata and the secrets engine configuration](#).

#### Upgrade considerations

After upgrading to Percona Server for MongoDB 5.0.29-25, configure the read permissions for it within the access policy on the Vault server. These permissions are required to check for the number of secrets versions to prevent the master key loss.

See [the policy configuration example](#).

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 October 2, 2024

 December 8, 2022

### 4.4.3 Using the Key Management Interoperability Protocol (KMIP)

 **Version added: 5.0.7-6**

Percona Server for MongoDB adds support for secure transfer of keys using the [OASIS Key Management Interoperability Protocol \(KMIP\)](#). The KMIP implementation was tested with the [PyKMIP server](#) and the [HashiCorp Vault Enterprise KMIP Secrets Engine](#).

KMIP enables the communication between key management systems and the database server. KMIP provides the following benefits:

- Streamlines encryption key management
- Eliminates redundant key management processes
- Reduces the mean time to resolve (MTTR) compromised encryption key incidents via [key state polling](#)

#### Version changes

The following table lists the changes in the KMIP implementation in Percona Server for MongoDB and the versions that introduced those changes:

Version	Description
<a href="#">5.0.8-7</a>	<a href="#">Master key rotation.</a>
<a href="#">5.0.9-8</a>	<a href="#">Support for multiple KMIP servers for failover.</a>
<a href="#">5.0.11-10</a>	<a href="#">Changed handling of <code>kmipKeyIdentifier</code> option.</a>
<a href="#">5.0.28-24</a>	<a href="#">Key state polling.</a>

#### Support for multiple KMIP servers

Starting with version 5.0.9-8, you can specify multiple KMIP servers for failover. On startup, Percona Server for MongoDB connects to the servers in the order listed and selects the one with which the connection is successful.

#### Optional key identifier

Starting with version 5.0.11-10, the `kmipKeyIdentifier` option is no longer mandatory. When left blank, the database server creates a key on the KMIP server and uses that for encryption. When you specify the identifier, the key with such an ID must exist on the key storage.

 **Note**

Starting with version 5.0.17-14, the master key is stored in a raw-byte format. If you set up Percona Server for MongoDB 5.0.17-14 with data-at-rest encryption using KMIP and wish to downgrade to some previous version, this downgrade is not possible via binary replacement. Consider using the [logical backup and restore via Percona Backup for MongoDB](#) for this purpose.

#### Key rotation

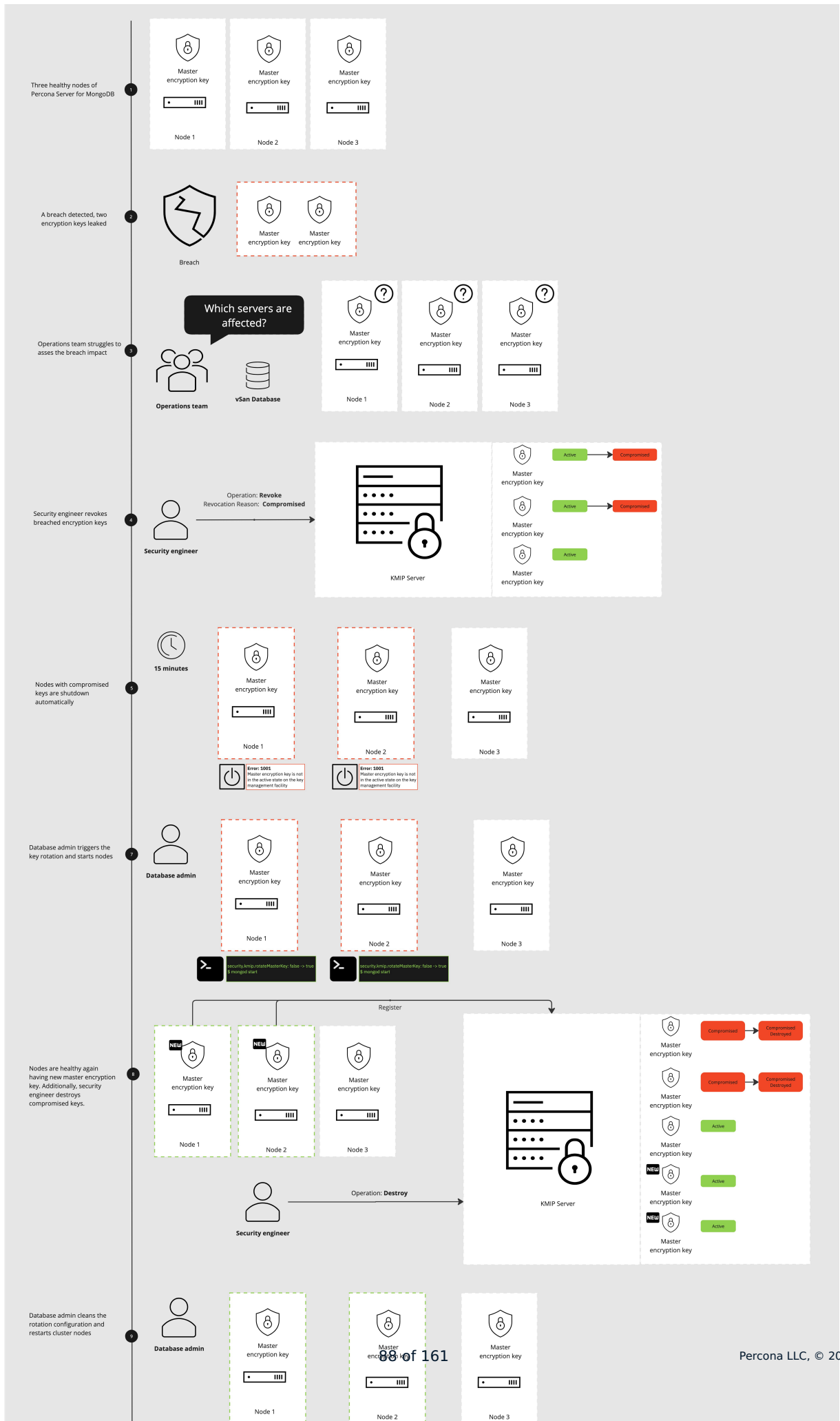
Starting with version 5.0.8-7, the support for [master key rotation](#) is added. This enables users to comply with data security regulations when using KMIP.

**Key state polling**

When a Percona Server for MongoDB node generates a new master encryption key, it registers the key on the KMIP server with the `Pre-Active` state. Starting with version 5.0.28-24, Percona Server for MongoDB automatically activates the master encryption key and periodically checks (polls) its state. If a master encryption key for a node is not in the `Active` state, the node reports an error and shuts down. This process helps security engineers identify the nodes that require out-of-schedule master key rotation.

Key state polling is enabled by default and is regulated by these configuration file options: `kmip.activateKeys` and `kmip.keyStatePollingSeconds`.

The following diagram illustrates the master key lifecycle with key state polling:





The master key state polling functionality is particularly useful in cluster deployments with hundreds of nodes. If some master keys are compromised, security engineers change their state from `Active` so that the nodes encrypted with these keys identify themselves. This approach allows the security engineers to rotate master keys only on the affected nodes instead of the entire cluster, thus reducing the mean time to resolve (MTTR) compromised encryption key incidents.

#### See also

Percona Blog: [Improve the Security of a Percona Server for MongoDB Deployment with KMIP Key State Polling](#) by Konstantin Trushin.

### KMIP parameters

<b>Configuration file</b>	<a href="#">security.kmip.serverName</a>
<b>Command line</b>	<code>kmipServerName</code>
<b>Type</b>	string
<b>Description</b>	The hostname or IP address of the KMIP server. As of version 4.2.21-21, multiple KMIP servers are supported as the comma-separated list, e.g. <code>kmip1.example.com, kmip2.example.com</code>
<b>Configuration file</b>	<a href="#">security.kmip.port</a>
<b>Command line</b>	<code>kmipPort</code>
<b>Type</b>	number
<b>Description</b>	The port used to communicate with the KMIP server. When undefined, the default port <code>5696</code> is used
<b>Configuration file</b>	<a href="#">security.kmip.serverCAFile</a>
<b>Command line</b>	<code>kmipServerCAFile</code>
<b>Type</b>	string
<b>Description</b>	The path to the certificate of the root authority that issued the certificate for the KMIP server. Required only if the root certificate is not trusted by default on the machine the database server works on.
<b>Configuration file</b>	<a href="#">security.kmip.clientCertificateFile</a>
<b>Command line</b>	<code>kmipClientCertificateFile</code>
<b>Type</b>	string
<b>Description</b>	The path to the PEM file with the KMIP client private key and the certificate chain. The database server uses this PEM file to authenticate the KMIP server
<b>Configuration file</b>	<a href="#">security.kmip.keyIdentifier</a>
<b>Command line</b>	<code>kmipKeyIdentifier</code>

<b>Configuration file</b>	<b><code>security.kmip.keyIdentifier</code></b>
<b>Type</b>	string
<b>Description</b>	Optional starting with version 5.0.11-10. The identifier of the KMIP key. If not specified, the database server creates a key on the KMIP server and saves its identifier internally for future use. When you specify the identifier, the key with such an ID must exist on the key storage. You can only use this setting for the first time you enable encryption.
<b>Configuration file</b>	<b><code>security.kmip.rotateMasterKey</code></b>
<b>Command line</b>	<code>kmipRotateMasterKey</code>
<b>Type</b>	boolean
<b>Description</b>	Controls master keys rotation. When enabled, generates the new master key version and re-encrypts the keystore. Available as of version 5.0.8-7.
<b>Configuration file</b>	<b><code>security.kmip.clientCertificatePassword</code></b>
<b>Command line</b>	<code>kmipClientCertificatePassword</code>
<b>Type</b>	string
<b>Description</b>	The password for the KMIP client private key or certificate. Use this parameter only if the KMIP client private key or certificate is encrypted. Available starting with version 5.0.9-8.
<b>Configuration file</b>	<b><code>security.kmip.connectRetries</code></b>
<b>Command line</b>	<code>kmipConnectRetries</code>
<b>Type</b>	int
<b>Description</b>	<p>Defines how many times to retry the initial connection to the KMIP server. The max number of connection attempts equals to <code>connectRetries + 1</code>. Default: 0. The option accepts values greater than zero.</p> <p>Use it together with the <code>connectTimeoutMS</code> parameter to control how long <code>mongod</code> waits for the response before making the next retry.</p>
<b>Configuration file</b>	<b><code>security.kmip.connectTimeoutMS</code></b>
<b>Command line</b>	<code>kmipConnectTimeoutMS</code>
<b>Type</b>	int
<b>Description</b>	<p>The time to wait for the response from the KMIP server. Min value: 1000. Default: 5000.</p> <p>If the <code>connectRetries</code> setting is specified, the <code>mongod</code> waits up to the value specified with <code>connectTimeoutMS</code> for each retry.</p>

<b>Configuration file</b>	<b><code>security.kmip.activateKeys</code></b>
<b>Command line</b>	<code>kmipActivateKeys</code>
<b>Type</b>	boolean
<b>Description</b>	When enabled, Percona Server for MongoDB activates a newly created master encryption key or verifies that the existing master key is in the Active state at startup. It also initiates the key state polling. Enabled by default. Available starting with version 5.0.28-24.
<b>Configuration file</b>	<b><code>security.kmip.keyStatePollingSeconds</code></b>
<b>Command line</b>	<code>kmipKeyStatePollingSeconds</code>
<b>Type</b>	int
<b>Description</b>	The period in seconds to check the state of the master encryption key. Default: 900. If the master encryption key is not in the Active state, the node logs the error and shuts down. Available starting with version 5.0.28-24.

## Configuration

### CONSIDERATIONS

Make sure you have obtained the root certificate, and the keypair for the KMIP server and the `mongod` client. For testing purposes you can use the [OpenSSL](#) to issue self-signed certificates. For production use we recommend you use the valid certificates issued by the key management appliance.

### PROCEDURE

To enable data-at-rest encryption in Percona Server for MongoDB using KMIP, edit the `/etc/mongod.conf` configuration file as follows:

```
security:
  enableEncryption: true
  kmip:
    serverName: <kmip_server_name>
    port: <kmip_port>
    clientCertificateFile: </path/client_certificate.pem>
    clientKeyFile: </path/client_key.pem>
    serverCAFile: </path/ca.pem>
    keyIdentifier: <key_name>
```

Alternatively, you can start Percona Server for MongoDB using the command line as follows:

```
$ mongod --enableEncryption \
  --kmipServerName <kmip_servername> \
  --kmipPort <kmip_port> \
  --kmipServerCAFile <path_to_ca_file> \
  --kmipClientCertificateFile <path_to_client_certificate> \
  --kmipClientKeyFile <path_to_client_private_key> \
  --kmipKeyIdentifier <kmip_identifier>
```

## Upgrade considerations

### TO VERSION 5.0.11-10 AND HIGHER

With the `kmipKeyIdentifier` option becoming optional in version 5.0.11-10, the standard upgrade procedure doesn't work if you are upgrading from version 5.0.10-9 and earlier.

For Percona Server for MongoDB 5.0.13-11 and higher, follow the standard [upgrade procedure](#)

This section provides upgrade instructions from Percona Server for MongoDB 5.0.10-9 or lower to Percona Server for MongoDB version 5.0.11-10 and higher.

For a single-node deployment, use the `mongodump` / `mongorestore` tools to make a backup before the update and to restore from it after binaries are updated.

For replica sets, data must be re-encrypted with the **new** key during the upgrade. Go through the [encrypting existing data steps](#) but perform the [minor upgrade](#) between steps 1 and 2 to replace the `mongod` binary.

### TO VERSION 5.0.28-24 AND HIGHER

Percona Server for MongoDB 5.0.28 and subsequent versions tolerate already existing `Pre-Active` master keys as follows: if at startup Percona Server for MongoDB detects that the data directory is encrypted with an existing master key in the `Pre-Active` state, it logs a warning and continues to operate as usual. In that case, Percona Server for MongoDB does not do periodic key state polling regardless the value specified for the `kmipKeyStatePollingSeconds` option. [Read more about key state polling.](#)

We recommend to either rotate a master encryption key or manually change the existing key to the Active state. You can also explicitly set the `security.kmip.activateKeys` configuration file option to ensure that only the active keys are used. This one-time operation smooths the major upgrade flow.

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 August 12, 2024

 December 8, 2022

### 4.4.4 Local key management using a keyfile

The key file must contain a 32 character string encoded in base64. You can generate a random key and save it to a file by using the `openssl` command:

```
$ openssl rand -base64 32 > mongodb-keyfile
```

Then, as the owner of the `mongod` process, update the file permissions: only the owner should be able to read and modify this file. The effective permissions specified with the `chmod` command can be:

- **600** - only the owner may read and modify the file
- **400** - only the owner may read the file.

```
$ chmod 600 mongodb-keyfile
```

Enable the data encryption at rest in Percona Server for MongoDB by setting these options:

- `--enableEncryption` to enable data at rest encryption
- `--encryptionKeyFile` to specify the path to a file that contains the encryption key

```
$ mongod ... --enableEncryption --encryptionKeyFile <fileName>
```

By default, Percona Server for MongoDB uses the `AES256-CBC` cipher mode. If you want to use the `AES256-GCM` cipher mode, then use the `--encryptionCipherMode` parameter to change it.

If `mongod` is started with the `--relaxPermChecks` option and the key file is owned by `root`, then `mongod` can read the file based on the group bit set accordingly. The effective key file permissions in this case are:

- **440** - both the owner and the group can only read the file, or
- **640** - only the owner can read and the change the file, the group can only read the file.

All these options can be specified in the configuration file:

```
security:
  enableEncryption: <boolean>
  encryptionCipherMode: <string>
  encryptionKeyFile: <string>
  relaxPermChecks: <boolean>
```

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 December 8, 2022

 December 8, 2022

## 4.4.5 Migrating from key file encryption to HashiCorp Vault encryption

The steps below describe how to migrate from the key file encryption to using HashiCorp Vault.

### Note

This is a simple guideline and it should be used for testing purposes only. We recommend to use Percona Consulting Services to assist you with migration in production environment.

#### ASSUMPTIONS

We assume that you have installed and configured the vault server and enabled the KV Secrets Engine as the secrets storage for it.

1. Stop `mongod`.

```
$ sudo systemctl stop mongod
```

2. Insert the key from keyfile into the HashiCorp Vault server to the desired secret path.

- Retrieve the key value from the keyfile

```
$ sudo cat /data/key/mongodb.key
d0JTFcePmvR0yLXwCbAH8fmiP/ZRm0nYbeJDMGaI7Zw=
```

- Insert the key into vault

```
$ vault kv put secret/dc/psmongodb1 value=d0JTFcePmvR0yLXwCbAH8fmiP/ZRm0nYbeJDMGaI7Zw=
```

### Note

Vault KV Secrets Engine uses different read and write secrets paths. To insert data to vault, specify the secret path without the `data/` prefix.

3. Edit the configuration file to provision the HashiCorp Vault configuration options instead of the key file encryption options.

```
security:
  enableEncryption: true
  vault:
    serverName: 10.0.2.15
    port: 8200
    secret: secret/data/dc/psmongodb1
    tokenFile: /etc/mongodb/token
    serverCAFile: /etc/mongodb/vault.crt
```

4. Start the `mongod` service

```
$ sudo systemctl start mongod
```

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 December 8, 2022

 December 8, 2022

## 4.5 Auditing

Auditing allows administrators to track and log user activity on a MongoDB server. With auditing enabled, the server will generate an audit log file. This file contains information about different user events including authentication, authorization failures, and so on.

To enable audit logging, specify where to send audit events using the `--auditDestination` option on the command line or the `auditLog.destination` variable in the configuration file.

If you want to output events to a file, also specify the format of the file using the `--auditFormat` option or the `auditLog.format` variable, and the path to the file using the `--auditPath` option or the `auditLog.path` variable.

To filter recorded events, use the `--auditFilter` option or the `auditLog.filter` variable.

For example, to log only events from a user named **tim** and write them to a JSON file `/var/log/psmdb/audit.json`, start the server with the following parameters:

```
$ mongod \
--dbpath data/db
--auditDestination file \
--auditFormat JSON \
--auditPath /var/log/psmdb/audit.json \
--auditFilter '{ "users.user" : "tim" }'
```

The options in the previous example can be used as variables in the MongoDB configuration file:

```
storage:
  dbPath: data/db
auditLog:
  destination: file
  format: JSON
  path: /var/log/psmdb/audit.json
  filter: '{ "users.user" : "tim" }'
```

This example shows how to send audit events to the `syslog`. Specify the following parameters:

```
mongod \
--dbpath data/db
--auditDestination syslog \
```

Alternatively, you can edit the MongoDB configuration file:

```
storage:
  dbPath: data/db
auditLog:
  destination: syslog
```

#### Note

If you start the server with auditing enabled, you cannot disable auditing dynamically during runtime.

## 4.5.1 Audit options

The following options control audit logging:

Command line	Configuration file	Type	Description
<code>--auditDestination()</code>	<code>auditLog.destination</code>	string	<p>Enables auditing and specifies where to send audit events:</p> <ul style="list-style-type: none"> <li>- <code>console</code>: Output audit events to <code>stdout</code>.</li> <li>- <code>file</code>: Output audit events to a file specified by the <code>--auditPath</code> option in a format specified by the <code>--auditFormat</code> option.</li> <li>- <code>syslog</code>: Output audit events to <code>syslog</code>.</li> </ul>
<code>--auditFilter()</code>	<code>auditLog.filter</code>	string	<p>Specifies a filter to apply to incoming audit events, enabling the administrator to only capture a subset of them. The value must be interpreted as a query object with the following syntax:</p> <pre>{ &lt;field1&gt;: &lt;expression1&gt;, ... }</pre> <p>Audit log events that match this query will be logged. Events that do not match this query will be ignored. For more information, see <a href="#">Audit filter examples</a></p>
<code>--auditFormat()</code>	<code>auditLog.format</code>	string	<p>Specifies the format of the audit log file, if you set the <code>--auditDestination</code> option to <code>file</code>. The default value is <code>JSON</code>.</p>



Command line	Configuration file	Type	Description
<code>--auditPath()</code>	<code>auditLog.path</code>	string	<p>Alternatively, you can set it to BSON</p> <p>Specifies the fully qualified path to the file where audit log events are written, if you set the <code>--auditDestination</code> option to <code>file</code>. If this option is not specified, then the <code>auditLog.json</code> file is created in the server's configured log path. If log path is not configured on the server, then the <code>auditLog.json</code> file is created in the current directory (from which <code>mongod</code> was started).</p> <p><b>NOTE:</b> This file will rotate in the same manner as the system log path, either on server reboot or using the <code>logRotate</code> command. The time of rotation will be added to the old file's name.</p>

## 4.5.2 Audit message syntax

Audit logging writes messages in JSON format with the following syntax:

```
{
  atype: <String>,
  ts : { "$date": <timestamp> },
  local: { ip: <String>, port: <int> },
  remote: { ip: <String>, port: <int> },
  users : [ { user: <String>, db: <String> }, ... ],
  roles: [ { role: <String>, db: <String> }, ... ],
  param: <document>,
  result: <int>
}
```

Parameter	Description
<code>atype</code>	Event type
<code>ts</code>	Date and UTC time of the event
<code>local</code>	Local IP address and port number of the instance
<code>remote</code>	Remote IP address and port number of the incoming connection associated with the event
<code>users</code>	Users associated with the event
<code>roles</code>	Roles granted to the user
<code>param</code>	Details of the event associated with the specific type
<code>result</code>	Exit code ( 0 for success)

### 4.5.3 Audit filter examples

The following examples show the flexibility of audit log filters.

```
auditLog:
  destination: file
  filter: '{atype: {$in: [
    "authenticate", "authCheck",
    "renameCollection", "dropCollection", "dropDatabase",
    "createUser", "dropUser", "dropAllUsersFromDatabase", "updateUser",
    "grantRolesToUser", "revokeRolesFromUser", "createRole", "updateRole",
    "dropRole", "dropAllRolesFromDatabase", "grantRolesToRole", "revokeRolesFromRole",
    "grantPrivilegesToRole", "revokePrivilegesFromRole",
    "replSetReconfig",
    "enableSharding", "shardCollection", "addShard", "removeShard",
    "shutdown",
    "applicationMessage"
  ]}}'
```

#### Standard query selectors

You can use query selectors, such as `$eq`, `$in`, `$gt`, `$lt`, `$ne`, and others to log multiple event types.

For example, to log only the `dropCollection` and `dropDatabase` events:

Command line      Config file

```
--auditDestination file --auditFilter '{ atype: { $in: [ "dropCollection",
"dropDatabase" ] } }'
```

```
auditLog:
  destination: file
  filter: '{ atype: { $in: [ "dropCollection", "dropDatabase" ] } }'
```

#### Regular expressions

Another way to specify multiple event types is using regular expressions.

For example, to filter all `drop` operations:

Command line      Config file

```
--auditDestination file --auditFilter '{ "atype" : /^drop.*/ }'
```

```
auditLog:
  destination: file
  filter: '{ "atype" : /^drop.*/ }'
```

#### Read and write operations

By default, operations with successful authorization are not logged, so for this filter to work, enable `auditAuthorizationSuccess` parameter, as described in [Enabling auditing of authorization success](#).

For example, to filter read and write operations on all the collections in the `test` database:

 **Note**

The dot (.) after the database name in the regular expression must be escaped with two backslashes (\\\\).

Command line      Config file

```
--setParameter auditAuthorizationSuccess=true --auditDestination file --auditFilter
'{"atype": "authCheck", "param.command": { "$in": [ "find", "insert", "delete", "update",
"findandmodify" ] }, "param.ns": /^test\\.\/ } }'
```

```
auditLog:
  destination: file
  filter: '{"atype": "authCheck", "param.command": { "$in": [ "find", "insert", "delete",
"update", "findandmodify" ] }, "param.ns": /^test\\.\/ } }'
```

```
setParameter: { auditAuthorizationSuccess: true }
```

#### 4.5.4 Enabling auditing of authorization success

By default, the audit system logs only authorization failures for the `authCheck` action. The `authCheck` action refers to the operations a user is or is not authorized to perform on the server according to the privileges outlined in the roles assigned to the user.

To enable logging of authorization successes, set the `auditAuthorizationSuccess` parameter to `true`. Audit events will then be triggered by every command that requires authorization, including CRUD ones.

 **Warning**

Enabling the `auditAuthorizationSuccess` parameter heavily impacts the performance compared to logging only authorization failures.

You can enable it on a running server using the following command:

```
db.adminCommand( { setParameter: 1, auditAuthorizationSuccess: true } )
```

To enable it on the command line, use the following option when running `mongod` or `mongos` process:

```
--setParameter auditAuthorizationSuccess=true
```

You can also add it to the configuration file as follows:

```
setParameter:
  auditAuthorizationSuccess: true
```

### Example of the audit message

```
{
  "atype": "authCheck",
  "ts": {
    "$date": "2024-03-13T06:28:04.631-04:00"
  },
  "local": {
    "ip": "172.17.0.2",
    "port": 20040
  },
  "remote": {
    "ip": "127.0.0.1",
    "port": 52128
  },
  "users": [
    {
      "user": "admin",
      "db": "admin"
    }
  ],
  "roles": [
    {
      "role": "clusterAdmin",
      "db": "admin"
    },
    {
      "role": "readWriteAnyDatabase",
      "db": "admin"
    },
    {
      "role": "userAdminAnyDatabase",
      "db": "admin"
    }
  ],
  "param": {
    "command": "insert",
    "ns": "audit_authz_insert.foo",
    "args": {
      "insert": "foo",
      "ordered": true,
      "lsid": {
        "id": {
          "$binary": "nfnnHQo0RD0tI6722F1P5w==",
          "$type": "04"
        }
      }
    },
    "$db": "audit_authz_insert"
  },
  "result": 0
}
```

## PERCONA

### 4.5.5 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

🕒 May 30, 2024

🕒 December 8, 2022

## 4.6 Profiling Rate Limit

Percona Server for MongoDB can limit the number of queries collected by the database profiler to decrease its impact on performance. Rate limit is an integer between 1 and 1000 and represents the fraction of queries to be profiled. For example, if you set it to 20, then every 20<sup>th</sup> query will be logged. For compatibility reasons, rate limit of 0 is the same as setting it to 1, and will effectively disable the feature meaning that every query will be profiled.

The MongoDB database profiler can operate in one of three modes:

- 0: Profiling is disabled. This is the default setting.
- 1: The profiler collects data only for *slow* queries. By default, queries that take more than 100 milliseconds to execute are considered *slow*.
- 2: Collects profiling data for all database operations.

Mode 1 ignores all *fast* queries, which may be the cause of problems that you are trying to find. Mode 2 provides a comprehensive picture of database performance, but may introduce unnecessary overhead.

With rate limiting you can collect profiling data for all database operations and reduce overhead by sampling queries. Slow queries ignore rate limiting and are always collected by the profiler.

### 4.6.1 Comparing to the `sampleRate` option

The `sampleRate` option (= `slowOpSampleRate` config file option) is a similar concept to `rateLimit`. But it works at different profile level, completely ignores operations faster than `slowOpsThresholdMs` (a.k.a. `slowMs`), and affects the log file printing, too.

	<code>sampleRate</code>	<code>rateLimit</code>
Affects profiling level 1	yes	no
Affects profiling level 2	no	yes
Discards/filters slow ops	yes	no
Discards/filters fast ops	no	yes
Affects log file	yes	no
Example value of option	0.02	50

`rateLimit` is a better way to have continuous profiling for monitoring or live analysis purposes. `sampleRate` requires setting `slowOpsThresholdMs` to zero if you want to sample all types of operations. `sampleRate` has an effect on the log file which may either decrease or increase the log volume.

## 4.6.2 Enabling the rate limit

To enable rate limiting, set the profiler mode to `2` and specify the value of the rate limit. Optionally, you can also change the default threshold for slow queries, which will not be sampled by rate limiting.

For example, to set the rate limit to `100` (profile every 100<sup>th</sup> *fast* query) and the slow query threshold to `200` (profile all queries slower than 200 milliseconds), run the `mongod` instance as follows:

```
$ mongod --profile 2 --slowms 200 --rateLimit 100
```

To do the same at runtime, use the `profile` command. It returns the *previous* settings and `"ok" : 1` indicates that the operation was successful:

```
> db.runCommand( { profile: 2, slowms: 200, ratelimit: 100 } );
{ "was" : 0, "slowms" : 100, "ratelimit" : 1, "ok" : 1 }
```

To check the current settings, run `profile: -1`:

```
> db.runCommand( { profile: -1 } );
{ "was" : 2, "slowms" : 200, "ratelimit" : 100, "ok" : 1 }
```

If you want to set or get just the rate limit value, use the `profilingRateLimit` parameter on the `admin` database:

```
> db.getSiblingDB('admin').runCommand( { setParameter: 1, "profilingRateLimit": 100 } );
{ "was" : 1, "ok" : 1 }
> db.getSiblingDB('admin').runCommand( { getParameter: 1, "profilingRateLimit": 1 } );
{ "profilingRateLimit" : 100, "ok" : 1 }
```

If you want rate limiting to persist when you restart `mongod`, set the corresponding variables in the MongoDB configuration file (by default, `/etc/mongod.conf`):

```
operationProfiling:
  mode: all
  slowOpThresholdMs: 200
  rateLimit: 100
```

### Note

The value of the `operationProfiling.mode` variable is a string, which you can set to either `off`, `slowOp`, or `all`, corresponding to profiling modes `0`, `1`, and `2`.

## 4.6.3 Profiler collection extension

Each document in the `system.profile` collection includes an additional `rateLimit` field. This field always has the value of `1` for *slow* queries and the current rate limit value for *fast* queries.

## 4.6.4 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 December 8, 2022

 December 8, 2022

## 4.7 Log Redaction

Percona Server for MongoDB can prevent writing sensitive data to the diagnostic log by redacting messages of events before they are logged. To enable log redaction, run `mongod` with the `--redactClientLogData` option.

### Note

Metadata such as error or operation codes, line numbers, and source file names remain visible in the logs.

Log redaction is important for complying with security requirements, but it can make troubleshooting and diagnostics more difficult due to the lack of data related to the log event. For this reason, debug messages are not redacted even when log redaction is enabled. Keep this in mind when switching between log levels.

You can permanently enable log redaction by adding the following to the configuration file:

```
security:
  redactClientLogData: true
```

To enable log redaction at runtime, use the `setParameter` command as follows:

```
db.adminCommand(
  { setParameter: 1, redactClientLogData : true }
)
```

## PERCONA

### 4.7.1 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

🕒 December 8, 2022

🕒 December 8, 2022

## 4.8 Additional text search algorithm - ngram

The *ngram* text search algorithm is useful for searching text for a specific string of characters in a field of a collection. This feature can be used to find exact sub-string matches, which provides an alternative to parsing text from languages other than the list of European languages already supported by MongoDB Community's full text search engine. It may also turn out to be more convenient when working with the text where symbols like dash('-'), underscore('\_'), or slash("/") are not token delimiters.

Unlike MongoDB full text search engine, *ngram* search algorithm uses only the following token delimiter characters that do not count as word characters in human languages:

- Horizontal tab
- Vertical tab
- Line feed
- Carriage return
- Space

The *ngram* text search is slower than MongoDB full text search.

### 4.8.1 Usage

To use *ngram*, create a text index on a collection setting the `default_language` parameter to **ngram**:

```
> db.collection.createIndex({name:"text"}, {default_language: "ngram"})
```

*ngram* search algorithm treats special characters like individual terms. Therefore, you don't have to enclose the search string in escaped double quotes (\\") to query the text index. For example, to search for documents that contain the date 2021-02-12, specify the following:

```
> db.collection.find({ $text: { $search: "2021-02-12" } })
```

However, both *ngram* and MongoDB full text search engine treat words with the hyphen-minus - sign in front of them as negated (e.g. "-coffee") and exclude such words from the search results.

## PERCONA

### 4.8.2 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)




 December 8, 2022

 December 8, 2022

## 5. Administration

### 5.1 Percona Server for MongoDB Parameter Tuning Guide

Percona Server for MongoDB includes several parameters that can be changed in one of the following ways:

===  Configuration file”

Use the `setParameter` admonitions in the configuration file for persistent changes in production:

```
```yaml
setParameter:
  <parameter>: <value>
```
```

 Command line  The `setParameter` command

Use the `--setParameter` command line option arguments when running the `mongod` process for development or testing purposes:

```
$ mongod \
  --setParameter <parameter>=<value>
```

Use the `setParameter` command on the `admin` database to make changes at runtime:

```
> db = db.getSiblingDB('admin')
> db.runCommand( { setParameter: 1, <parameter>: <value> } )
```


#### 5.1.1 Parameters

See what parameters you can define in the [parameters list](#).

## PERCONA

### 5.1.2 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

🕒 February 28, 2024

🕒 December 8, 2022

## 5.2 Upgrade

### 5.2.1 Upgrading from Percona Server for MongoDB 4.4 to 5.0

#### Considerations


1. To upgrade Percona Server for MongoDB to version 5.0, you must be running version 4.4. Upgrades from earlier versions are not supported.
2. Before upgrading your production Percona Server for MongoDB deployments, test all your applications in a testing environment to make sure they are compatible with the new version. For more information, see [Compatibility Changes in MongoDB 5.0](#)
3. If you are using data-at-rest-encryption with KMIP server, check the [upgrade considerations](#)

We recommend to upgrade Percona Server for MongoDB from official Percona repositories using [percona-release repository management tool](#) and the corresponding package manager for your system.

This document describes this method for the in-place upgrade (where your existing data and configuration files are preserved).

**Warning**

Perform a full backup of your data and configuration files before upgrading.

 On Debian and Ubuntu

 On Red Hat Enterprise Linux and derivatives

1. Stop the `mongod` service:

```
$ sudo systemctl stop mongod
```

2. Enable Percona repository for Percona Server for MongoDB 5.0:

```
$ sudo percona-release enable psmdb-50
```

3. Update the local cache:

```
$ sudo apt update
```

4. Install Percona Server for MongoDB 5.0 packages:

```
$ sudo apt install percona-server-mongodb
```

5. Start the `mongod` instance:

```
$ sudo systemctl start mongod
```

For more information, see [Installing Percona Server for MongoDB on Debian and Ubuntu](#).

1. Stop the `mongod` service:

```
$ sudo systemctl stop mongod
```

2. Enable Percona repository for Percona Server for MongoDB 5.0:

```
$ sudo percona-release enable psmdb-50
```

3. Install Percona Server for MongoDB 5.0 packages:

```
$ sudo yum install percona-server-mongodb
```

4. Start the `mongod` instance:

```
$ sudo systemctl start mongod
```

After the upgrade, Percona Server for MongoDB is started with the feature set of 4.4 version. Assuming that your applications are compatible with the new version, enable 5.0 version features. Run the following command against the `admin` database:

```
db.adminCommand( { setFeatureCompatibilityVersion: "5.0" } )
```

#### See also

MongoDB Documentation:


- [Upgrade a Standalone](#)
- [Upgrade a Replica Set](#)
- [Upgrade a Sharded Cluster](#)

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)    [Get a Percona Expert](#)

 August 8, 2024

 December 8, 2022

### 5.2.2 Upgrade from MongoDB Community Edition to Percona Server for MongoDB

This document provides instructions for an in-place upgrade from MongoDB Community Edition to Percona Server for MongoDB.

An in-place upgrade is done by keeping the existing data in the server and replacing the MongoDB binaries. Afterwards, you restart the `mongod` service with the same `dbpath` data directory.

An in-place upgrade is suitable for most environments except the ones that use ephemeral storage and/or host addresses.

#### Procedure

#### Note

MongoDB creates a user that belongs to two groups, which is a potential security risk. This is fixed in Percona Server for MongoDB: the user is included only in the `mongod` group. To avoid problems with current MongoDB setups, existing user group membership is not changed when you migrate to Percona Server for MongoDB. Instead, a new `mongod` user is created during installation, and it belongs to the `mongod` group.

This procedure describes an in-place upgrade of a `mongod` instance. If you are using data at rest encryption, refer to the [Upgrading to Percona Server for MongoDB with data at rest encryption enabled](#) section.

 **Important**

Before starting the upgrade, we recommend to perform a full backup of your data.



### 1. Save the current configuration file as the backup:

```
$ sudo mv /etc/mongod.conf /etc/mongod.conf.bkp
```

### 2. Stop the `mongod` service:

```
$ sudo systemctl stop mongod
```

### 3. Check for installed packages:

```
$ sudo dpkg -l | grep mongod
```

??? example "Sample output"

```
```{.text .no-copy}
ii mongodb-org          5.0.2    amd64    MongoDB open source document-oriented
database system (metapackage)
ii mongodb-org-database 5.0.2    amd64    MongoDB open source document-oriented
database system (metapackage)
ii mongodb-org-database-tools-extra 5.0.2    amd64    Extra MongoDB database tools
ii mongodb-org-mongos   5.0.2    amd64    MongoDB sharded cluster query router
ii mongodb-org-server   5.0.2    amd64    MongoDB database server
ii mongodb-org-shell    5.0.2    amd64    MongoDB shell client
ii mongodb-org-tools    5.0.2    amd64    MongoDB tools
```
```

### 4. Remove the installed packages:

```
$ sudo apt remove \
mongodb-org \
mongodb-org-mongos \
mongodb-org-server \
mongodb-org-shell \
mongodb-org-tools
```

### 5. Install Percona Server for MongoDB

#### 6. Verify that the configuration file includes correct options:

- Copy the required configuration options like custom `dbPath`/system log path, additional security/replication or sharding options from the backup configuration file (`/etc/mongod.conf.bkp`) to the current one `/etc/mongod.conf`.
- Make sure that the `mongod` user has access to your custom paths. If not, provide it as follows:

```
$ sudo chown -R mongod:mongod <custom-dbPath>
$ sudo chown -R mongod:mongod <custom-systemLog.path>
```

- Make sure the configuration file includes the following configuration:

```
processManagement:
  fork: true
  pidFilePath: /var/run/mongod.pid
```

**Troubleshooting tip:** The `pidFilePath` setting in `mongod.conf` must match the `PIDFile` option in the `systemd mongod` service unit. Otherwise, the service will kill the `mongod` process after a timeout.

#### 7. Restart the `mongod` service:

```
$ sudo systemctl restart mongod
```

To upgrade a replica set or a sharded cluster, use the [rolling restart](#) method. It allows you to perform the upgrade with minimum downtime. You upgrade the nodes one by one, while the whole cluster / replica set remains operational.

#### See also

MongoDB Documentation:

- [Upgrade a Replica Set](#)
- [Upgrade a Sharded Cluster](#)

### Upgrading to Percona Server for MongoDB with data at rest encryption enabled

Steps to upgrade from MongoDB 5.0 Community Edition with data encryption enabled to Percona Server for MongoDB are different. `mongod` requires an empty `dbPath` data directory because it cannot encrypt data files in place. It must receive data from other replica set members during the initial sync. Please refer to the [Switching storage engines](#) for more information on migration of encrypted data. [Contact us](#) for working at the detailed migration steps, if further assistance is needed.

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)    [Get a Percona Expert](#)

 February 28, 2024

 December 8, 2022

### 5.2.3 Minor upgrade of Percona Server for MongoDB

If you are using data-at-rest-encryption, check the upgrade considerations for [the KMIP server](#) and for the [Vault server](#)

To upgrade Percona Server for MongoDB to the latest version, follow these steps:

1. Stop the `mongod` service:

```
$ sudo systemctl stop mongod
```

2. [Install the latest version packages](#). Use the command relevant to your operating system.
3. Start the `mongod` service:



```
$ sudo systemctl start mongod
```

To upgrade a replica set or a sharded cluster, use the [rolling restart](#) method. It allows you to perform the upgrade with minimum downtime. You upgrade the nodes one by one, while the whole cluster / replica set remains operational.


## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)    [Get a Percona Expert](#)

 October 2, 2024

 October 24, 2023

## 5.3 Uninstall Percona Server for MongoDB

To completely remove Percona Server for MongoDB you need to remove all the installed packages, data and configuration files. If you need the data, consider making a backup before uninstalling Percona Server for MongoDB.

Follow the instructions, relevant to your operating system:

 On Debian and Ubuntu       On Red Hat Enterprise Linux and derivatives

You can remove Percona Server for MongoDB packages with one of the following commands:

- `apt remove` will only remove the packages and leave the configuration and data files.
- `apt purge` will remove all the packages with configuration files and data.

Choose which command better suits you depending on your needs.

1. Stop the `mongod` server:

```
$ sudo systemctl stop mongod
```

2. Remove the packages. There are two options.

 Keep the configuration and data files       Delete configuration and data files

```
$ sudo apt remove percona-server-mongodb*
```

```
$ sudo apt purge percona-server-mongodb*
```

1. Stop the `mongod` service:

```
$ sudo systemctl stop mongod
```

2. Remove the packages:

```
$ sudo yum remove percona-server-mongodb*
```

3. Remove the data and configuration files:

```
$ sudo rm -rf /var/lib/mongodb
$ sudo rm -f /etc/mongod.conf
```

#### **Warning**

This will remove all the packages and delete all the data files (databases, tables, logs, etc.). You might want to back up your data before doing this in case you need the data later.

**PERCONA**

### 5.3.1 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 February 28, 2024

 December 8, 2022

## 6. Release notes

### 6.1 Percona Server for MongoDB 5.0 Release Notes

- [Percona Server for MongoDB 5.0.29-25 \(2024-09-26\)](#)
- [Percona Server for MongoDB 5.0.28-24 \(2024-08-08\)](#)
- [Percona Server for MongoDB 5.0.27-23 \(2024-06-19\)](#)
- [Percona Server for MongoDB 5.0.26-22 \(2024-04-09\)](#)
- [Percona Server for MongoDB 5.0.24-21 \(2024-02-01\)](#)
- [Percona Server for MongoDB 5.0.23-20 \(2023-12-21\)](#)
- [Percona Server for MongoDB 5.0.22-19 \(2023-11-09\)](#)
- [Percona Server for MongoDB 5.0.21-18 \(2023-10-12\)](#)
- [Percona Server for MongoDB 5.0.20-17 \(2023-09-07\)](#)
- [Percona Server for MongoDB 5.0.19-16 \(2023-08-10\)](#)
- [Percona Server for MongoDB 5.0.18-15 \(2023-06-01\)](#)
- [Percona Server for MongoDB 5.0.17-14 \(2023-05-04\)](#)
- [Percona Server for MongoDB 5.0.15-13 \(2023-03-16\)](#)
- [Percona Server for MongoDB 5.0.14-12 \(2022-12-08\)](#)
- [Percona Server for MongoDB 5.0.13-11 \(2022-10-12\)](#)
- [Percona Server for MongoDB 5.0.11-10 \(2022-09-01\)](#)
- [Percona Server for MongoDB 5.0.10-9 \(2022-08-09\)](#)
- [Percona Server for MongoDB 5.0.9-8 \(2022-06-20\)](#)
- [Percona Server for MongoDB 5.0.8-7 \(2022-05-10\)](#)
- [Percona Server for MongoDB 5.0.7-6 \(2022-04-20\)](#)
- [Percona Server for MongoDB 5.0.6-5 \(2022-02-10\)](#)
- [Percona Server for MongoDB 5.0.5-4 \(2021-12-28\)](#)
- [Percona Server for MongoDB 5.0.4-3 \(2021-12-08\)](#)
- [Percona Server for MongoDB 5.0.3-2 \(2021-10-14\)](#)
- [Percona Server for MongoDB 5.0.2-1 \(2021-08-16\)](#)

## PERCONA

### 6.1.1 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

🕒 September 26, 2024

🕒 December 8, 2022

## 6.2 Percona Server for MongoDB 5.0.29-25 (2024-09-26)

### Installation

Percona Server for MongoDB 5.0.29-25 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for MongoDB 5.0.x Community Edition.

Percona Server for MongoDB 5.0.29-25 includes improvements and bug fixes of [MongoDB 5.0.29 Community Edition](#) and supports its protocols and drivers.

### 6.2.1 Release Highlights

This release of Percona Server for MongoDB includes the following features and improvements:

#### Prevent master encryption key loss on the Vault server

Before Percona Server for MongoDB puts a new master encryption key to the Vault server as the versioned secret, it now checks if the secret's version reached the defined maximum (10 by default). This prevents the loss of the old secret and the master encryption key it stores on the Vault server.

Make sure Percona Server for MongoDB has read permissions for the secret's metadata and the secrets engine configuration. To learn more, refer to the [documentation](#).

#### Upstream Improvements

The bug fixes, provided by MongoDB and included in Percona Server for MongoDB, are the following:

- [SERVER-59831](#) - Improved inserting unique index keys behavior by preventing an oplog application to check for duplicates on unique indexes except for when building an index and inserting into the `_id` index.
- [SERVER-76777](#) - Fixed the deadlock between external abort and internal abort on index build.
- [SERVER-88750](#) - Provided a way for external tools to insert/update/upsert documents without triggering the "replace Timestamp(0,0) with current time" behavior by adding the "bypassEmptyTsReplacement" parameter to those operations.
- [WT-8771](#) - Avoid marking the page dirty for empty pages to prevent unnecessary page reconciliation.

Find the full list of changes in the [MongoDB 5.0.29 Community Edition release notes](#).

### 6.2.2 Packaging Changes

- Percona Server for MongoDB 6.0.17 is no longer supported for Debian 10 and Red Hat Enterprise 7 and derivatives as these operating systems reached End-Of-Life.

## 6.2.3 Changelog

### Improvements

- [PSMDB-1441](#) - Fixed the issue with master encryption keys getting lost when the number of created secrets exceeds the threshold by preventing a new secret creation and alerting users about it.

### Fixed Bugs

- [PSMDB-1527](#) - Improve the `activateKeys` option handling by changing its type to boolean.

## PERCONA

### 6.2.4 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 September 26, 2024

 September 26, 2024

## 6.3 Percona Server for MongoDB 5.0.28-24 (2024-08-08)

### Installation

Percona Server for MongoDB 5.0.28-24 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for MongoDB 5.0.x Community Edition.

Percona Server for MongoDB 5.0.28-24 includes improvements and bug fixes of [MongoDB 5.0.28 Community Edition](#) and supports its protocols and drivers.

### 6.3.1 Release Highlights

This release of Percona Server for MongoDB includes the following features and improvements:

#### Enhanced Telemetry for better product usage reporting

The enhanced telemetry feature provides comprehensive information about how it works, its components and metrics as well as updated methods how to disable telemetry. Read more in [Telemetry on Percona Server for MongoDB](#)

### Reduce mean time to resolve (MTTR) compromised encryption key incidents in KMIP

Starting with this release, Percona Server for MongoDB automatically activates all new master encryption keys at startup and periodically checks (polls) their status in a KMIP server. If a master encryption key for a node transitions to the state other than Active, the node reports an error and shuts down. This method allows security engineers to quickly identify which nodes require out-of-schedule master key rotation, such as in the case of compromised keys, without needing to rotate keys for the entire cluster.

Learn more about key state polling from [the documentation](#)

### Easier dependency management with thinner tarballs

Tarballs are now available for each supported operating system individually and no longer include built-in libraries. This change reduces the tarball download size and increases their security by simplifying updates for required dependencies.

## 6.3.2 Upstream Improvements

The bug fixes, provided by MongoDB and included in Percona Server for MongoDB, are the following:

- [SERVER-63198](#) - Prevented shutdown command from hanging
- [SERVER-90747](#) - Improve handling of queries with \$elemMatch with empty path in plan enumerator in case an index is used on another predicate of the query
- [SERVER-91362](#) - Fixed performance issues by not copying a JavaScript “scope” object if a cached JsExecution object already exists in a query thread
- [SERVER-91562](#) - Fixed the issue with incorrect handling of ‘unique’ and ‘sparse’ parameters in index signature when comparing indexes.

Find the full list of changes in the [MongoDB 5.0.28 Community Edition release notes](#).

## 6.3.3 Changelog

### Improvements

- [PSMDB-1283](#) - Add the ability to activate master encryption keys in KMIP server and check their state.


## 6.3.4 Packaging Changes

- Percona Server for MongoDB 5.0.28-24 is available on Ubuntu 24.04 (Noble Numbat)

## PERCONA

### 6.3.5 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

🕒 August 8, 2024

🕒 August 8, 2024

## 6.4 Percona Server for MongoDB 5.0.27-23 (2024-06-19)

### Installation

Percona Server for MongoDB 5.0.27-23 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for MongoDB 5.0.x Community Edition.

Percona Server for MongoDB 5.0.27-23 includes improvements and bug fixes of [MongoDB 5.0.27 Community Edition](#) and supports its protocols and drivers.

### 6.4.1 Release Highlights

- [SERVER-78556](#) - Changed default value of `internalInsertMaxBatchSize` to 64 to avoid replication lag if the insert operations are slow
- [SERVER-79637](#) - Fixed the issue with the aggregation pipeline in MongoDB when using the `$lookup` stage with a time series foreign collection using a correlated predicate
- [SERVER-80363](#) - Explicitly stated that the missing `w` field from write concern object will be filled with default write concern value
- [SERVER-86474](#) - Fixed the bug with the replaying oplog updates during mongosync by preserving the zero-valued timestamps.
- [SERVER-86648](#) - Fixed the issue with resumable index build sorter files not to be synced on shutdown

Find the full list of changes in the [MongoDB 5.0.27 Community Edition release notes](#).

### 6.4.2 Bugs Fixed

- [PSMDB-1418](#) - Fixed the issue with the server crash when using LDAP authentication by ensuring that LDAP connections borrowed by a client thread are not disposed.

## PERCONA

### 6.4.3 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)



🕒 June 19, 2024

🕒 June 19, 2024

## 6.5 Percona Server for MongoDB 5.0.26-22 (2024-04-09)

### Installation

Percona Server for MongoDB 5.0.26-22 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for MongoDB 5.0.x Community Edition. Percona Server for MongoDB 5.0.26-22 includes both improvements and bug fixes of [MongoDB 5.0.25 Community Edition](#) and [MongoDB 5.0.26 Community Edition](#).

It supports protocols and drivers of both MongoDB 5.0.25 and MongoDB 5.0.26.

#### ⚠️ Warning

Due to [CVE-2024-1351](#), in all MongoDB versions prior to 4.4.29, the `mongod` server allows incoming connections to skip peer certificate validation which results in untrusted connections to succeed. This issue occurs when the `mongod` is started with TLS enabled (`net.tls.mode` set to `allowTLS`, `preferTLS`, or `requireTLS`) and without a `net.tls.CAFile` configured. For details, see [SERVER-72839](#).

The issue is fixed upstream in versions 4.4.29, 5.0.25, 6.0.14 and 7.0.6 and in Percona Server for MongoDB 4.4.29-28, 5.0.26-22, 6.0.14-11 and 7.0.7-4. Now, configuring MongoDB to use TLS requires specifying the value for the `--tlsCAFile` flag, the `net.tls.CAFile` configuration option, or the `tlsUseSystemCA` parameter.

### 6.5.1 Release Highlights

The bug fixes, provided by MongoDB and included in Percona Server for MongoDB, are the following:

- [SERVER-68128](#) - Fixed the issue with the exceptions thrown while generating command response leading to network error by avoiding closing the connections during the command processing.
- [SERVER-72703](#) - Changed the requirement to use exclusive write lock to intent exclusive write lock that doesn't prevent reading from a collection during the `$out` stage when running the rename collection command.
- [SERVER-83602](#) - Fixed the issue with the match expression optimization for the `$or` to an `$in` rewrite by avoiding creating directly nested `$or`.
- [SERVER-86717](#) - Fixed the issue with the resharding command failing to persist chunk metadata by adding a validation that the user provided zone range doesn't include `$`-prefixed fields.
- [SERVER-72839](#) - Fixed the issue with missing peer certificate validation if neither CAFile nor clusterCAFile is provided.
- [SERVER-83091](#) - Extended the `collMod` command to check and fix invalid boolean index options.
- [SERVER-82353](#) - Fixed the issue with multi-document transactions missing documents when the `movePrimary` operation runs concurrently by detecting placement conflicts in multi-document transactions.
- [SERVER-83564](#) - Add an index on the process field for the `config.locks` collection to ensure update operations on it are completed even in heavy loaded deployments.
- [WT-10017](#) - Removed the unstable historical versions at the end of rollback to stable.

Find the full list of changes in the [MongoDB 5.0.25 Community Edition release notes](#) and [MongoDB 5.0.26 Community Edition release notes](#).

## 6.5.2 Bugs Fixed

- [PSMDB-1434](#) - Fixed the auditing behavior by removing excessive logging for CRUD operations


## PERCONA

### 6.5.3 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 April 9, 2024

 April 9, 2024

## 6.6 Percona Server for MongoDB 5.0.24-21 (2024-02-01)

### Installation

Percona Server for MongoDB 5.0.24-21 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for [MongoDB 5.0.24 Community Edition](#).

It supports MongoDB 5.0.24 protocols and drivers.

### 6.6.1 Release Highlights

The bug fixes, provided by MongoDB and included in Percona Server for MongoDB, are the following:

- [SERVER-50792](#) - Improved shard key index error messages by adding detailed information about an invalid index.
- [SERVER-77506](#) - Fixed the issue with data and ShardVersion mismatch on sharded multi-document transactions by exposing the maxValidAfter timestamp alongside the shardVersion
- [SERVER-83091](#) - Fixed the issue with infinite loop during plan enumeration triggered by the `$or` queries

Find the full list of changes in the [MongoDB 5.0.24 Community Edition release notes](#).

### 6.6.2 Packaging changes

Percona Server for MongoDB 5.0.24-21 is no longer available on Ubuntu 18.04 (Bionic Beaver).

## PERCONA

### 6.6.3 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 February 5, 2024

 February 1, 2024

## 6.7 2023 (versions 5.0.15-13 through 5.0.23-20)

### 6.7.1 Percona Server for MongoDB 5.0.23-20 (2023-12-21)

#### Installation

Percona Server for MongoDB 5.0.23-20 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for [MongoDB 5.0.23 Community Edition](#).

It supports MongoDB 5.0.23 protocols and drivers.

#### Release Highlights

- [AWS IAM authentication](#) is now generally available, enabling you to use this functionality in production environments.

The bug fixes, provided by MongoDB and included in Percona Server for MongoDB, are the following:

- [SERVER-78108](#) - Improved the Primary Only Service interface to expose the primary state upon lookup
- [SERVER-78115](#) - Ensured that shard primaries commit a majority write before using new routing information from the config server.
- [WT-11564](#) - Fixed the rollback-to-stable behavior to read the newest transaction value only when it exists in the checkpoint.
- [WT-11602](#) - Hid expected eviction failures from the application and don't rollback in case of errors

Find the full list of changes in the [MongoDB 5.0.23 Community Edition release notes](#).

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 December 21, 2023

 December 21, 2023

## 6.7.2 Percona Server for MongoDB 5.0.22-19 (2023-11-09)

### Installation

Percona Server for MongoDB 5.0.22-19 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for [MongoDB 5.0.22 Community Edition](#).

It supports MongoDB 5.0.22 protocols and drivers.

#### Release Highlights

- You can now configure the retry behavior for Percona Server for MongoDB to connect to the KMIP server when using [data-at-rest encryption](#).

The bug fixes, provided by MongoDB and included in Percona Server for MongoDB, are the following:

- [SERVER-68548](#) - Fixed the behavior of the `quiet` global server parameter for logging.
- [SERVER-80021](#) - Fixed the conversion from string to `doubleValue` to not lose precision and be able to roundtrip and retrieve the same value back.
- [SERVER-80703](#) - Improved chunk migration logic by avoiding traversing routing table in the migration destination manager.
- [SERVER-81106](#) - Improved the recipient shard behavior during the chunk migration to wait for changes to catalog cache to be persisted before the cloning phase.

Find the full list of changes in the [MongoDB 5.0.22 Community Edition release notes](#).


#### New Features

- [PSMDB-1241](#) - Implement the `connectRetries` and the `connectTimeoutMS` configuration file options

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 November 9, 2023

 November 9, 2023

### 6.7.3 Percona Server for MongoDB 5.0.21-18 (2023-10-12)

#### Installation

Percona Server for MongoDB 5.0.21-18 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for [MongoDB 5.0.21 Community Edition](#).

It supports MongoDB 5.0.21 protocols and drivers.

#### Release Highlights

The bug fixes, provided by MongoDB and included in Percona Server for MongoDB, are the following:

- [SERVER-60466](#) - Fixed the flow for converting a replica set into a sharded cluster by adding support for the drivers to communicate the signed \$clusterTimes to shardsvr replica set before and after the addShard command is run
- [SERVER-71627](#) - Improved performance of updating the routing table and prevented blocking client requests during refresh for clusters with 1 million of chunks
- [SERVER-78813](#) - Fix commit point propagation for exhaust oplog cursors during node sync
- [WT-10759](#) - During reconciliation do not retry to forcibly evict the page.

Find the full list of changes in the [MongoDB 5.0.21 Community Edition release notes](#).

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 October 12, 2023

 October 12, 2023

## 6.7.4 Percona Server for MongoDB 5.0.20-17 (2023-09-07)

### Installation

Percona Server for MongoDB 5.0.20-17 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for [MongoDB 5.0.20 Community Edition](#).

It supports MongoDB 5.0.20 protocols and drivers.

### Release Highlights

- Percona Server for MongoDB 5.0.20-17 features a Docker image for ARM64 architectures.

The bug fixes, provided by MongoDB and included in Percona Server for MongoDB, are the following:

- [SERVER-74954](#) - Fixed the issue with the incorrect output for the query where the `$or` operator rewrites the `$elemMatch` extra condition.
- [SERVER-78813](#) - Fixed commit point propagation for exhaust oplog cursors.
- [SERVER-79136](#) - Blocked the `$group` min/max rewrite in timestamp if there is a non-meta filter.
- [WT-10449](#) - Improved the reconciliation time and slow eviction for pages with lots of updates by avoiding saving the update chain when there are no updates to be written to the history store
- [WT-11031](#) - Fixed the Rollback to Stable behavior to skip tables with no time window information in the checkpoint.

Find the full list of changes in the [MongoDB 5.0.20 Community Edition release notes](#).

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 September 7, 2023

 September 7, 2023

## 6.7.5 Percona Server for MongoDB 5.0.19-16 (2023-08-10)

|                     |   |
|---------------------|---|
| <b>Release date</b> | <b>August 10, 2023</b>                                |
| <b>Installation</b> | <a href="#">Installing Percona Server for MongoDB</a> |

Percona Server for MongoDB 5.0.19-16 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for [MongoDB 5.0.19 Community Edition](#).

It supports MongoDB 5.0.19 protocols and drivers.

### Release Highlights

- The ability to [configure AWS STS endpoint](#) improves authentication and connectivity with AWS services.

The bug fixes, provided by MongoDB and included in Percona Server for MongoDB, are the following:

- [SERVER-71985](#) - Automatically retry time series insert on DuplicateKey error.
- [SERVER-74551](#) - Prevented unnecessary logging of `WriteConflictExceptions` during the execution of a `findAndModify` command.
- [SERVER-77018](#) - Changed the index build behavior so that in-progress index builds are no longer accounted for `indexFreeStorageSize` when running `dbStats`.
- [SERVER-78126](#) - Fixed performance issues of the aggregation framework by improving the `Value::hash_combine()` function operation on big-endian platforms
- [WT-10253](#) - Run session dhandle sweep and session cursor sweep more often

Find the full list of changes in the [MongoDB 5.0.19 Community Edition release notes](#).

### New Features

- [PSMDB-1291](#) - Add the ability to specify the AWS Security Token Service (STS) endpoint for authentication

### Bugs Fixed

- [PSMDB-1280](#) - Improve PSMDB behavior on client disconnect when the `$backupCursorExtend` is opened
- [PSMDB-1289](#) - Fixed the issue with the server crash during LDAP authentication by retrying sending requests to the LDAP server and gracefully report errors.

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 August 10, 2023

 August 10, 2023

## 6.7.6 Percona Server for MongoDB 5.0.18-15 (2023-06-01)

|                     |   |
|---------------------|---|
| <b>Release date</b> | <b>June 1, 2023</b>                                   |
| <b>Installation</b> | <a href="#">Installing Percona Server for MongoDB</a> |

---

Percona Server for MongoDB 5.0.18-15 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for [MongoDB 5.0.18 Community Edition](#).

It supports MongoDB 5.0.18 protocols and drivers.

### Release Highlights

The bug fixes, provided by MongoDB and included in Percona Server for MongoDB, are the following:

- [WT-10551](#) - Fixed the bug with WiredTiger failing to load the incremental backup change bitmap for a file. The issue affects MongoDB versions 4.4.8 through 4.4.21, 5.0.2 through 5.0.17, and 6.0.0 through 6.0.5 causing the server to crash with the checksum error if the affected incremental backup was restored and the affected data is accessed.

If you are using incremental backups, upgrade to the fixed upstream version 5.0.18 / Percona Server for MongoDB 5.0.18-15 as soon as possible. Follow closely the upstream recommendations to remediate the negative impact.

- [SERVER-48196](#) - Updated the built-in timezone files the latest version by upgrading the timezone library
- [SERVER-54150](#) - Improved the oplog application behavior to finish without issues during a recovery from a stable checkpoint
- [SERVER-57056](#) - Fixed the syslog severity level for INFO messages
- [SERVER-72686](#) - Added support for `$collStats` aggregation stage on timeseries collections

Find the full list of changes in the [MongoDB 5.0.18 Community Edition release notes](#).

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)    [Get a Percona Expert](#)

 June 1, 2023

 June 1, 2023



## 6.7.7 Percona Server for MongoDB 5.0.17-14 (2023-05-04)

|                     |   |
|---------------------|---|
| <b>Release date</b> | <b>May 4, 2023</b>                                    |
| <b>Installation</b> | <a href="#">Installing Percona Server for MongoDB</a> |

---

Percona Server for MongoDB 5.0.17-14 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for [MongoDB 5.0.16 Community Edition](#) and [MongoDB 5.0.17 Community Edition](#).

It supports protocols and drivers of both MongoDB 5.0.16 and 5.0.17.

This release of Percona Server for MongoDB includes the improvements and bug fixes of MongoDB Community Edition 5.0.16 and 5.0.17.

### Release Highlights

The bug fixes, provided by MongoDB and included in Percona Server for MongoDB, are the following:

- [SERVER-61909](#) - Fixed a hang when inserting or deleting a document with large number of index entries
- [SERVER-73822](#) - Fixed the failing `$group` min-max rewrite logic for time-series collections when there is a non-constant expression
- [SERVER-74501](#) - Fixed MigrationBatchFetcher/Inserter completion reliance to not spawn an extra cleanup thread
- [SERVER-75205](#) - Fixed deadlock between `stepdown` and `restoring` locks after yielding when all read tickets exhausted
- [SERVER-73229](#) - Fixed the issue with early kills of the cursor during the logical session cache refresh by properly handling write errors.
- [SERVER-75261](#) - Added accounting for array element overhead for `listCollections`, `listIndexes`, `_shardsvrCheckMetadataConsistencyParticipant` commands
- [SERVER-75431](#) - Improved the rename path behavior for a collection in sharded clusters by fixing the check for the databases to reside on the same primary shard
- [SERVER-76098](#) - Allowed queries with search and non-simple collations

Find the full list of changes in the [MongoDB 5.0.16 Community Edition](#) and [MongoDB 5.0.17 Community Edition release notes](#).

### Bugs Fixed


- [PSMDB-1211](#): Improved the master key rotation handling in case of failure
- [PSMDB-1231](#): Register a master key for data-at-rest encryption encryption on the KMIP server in the raw-bytes form
- [PSMDB-1239](#): Fixed the issue with PSMDB failing to restart when wrong data-at-rest encryption options were used during the previous start


**PERCONA**

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 May 4, 2023

 May 4, 2023

## 6.7.8 Percona Server for MongoDB 5.0.15-13 (2023-03-16)

|                     |   |
|---------------------|---|
| <b>Release date</b> | <b>March 16, 2023</b>                                 |
| <b>Installation</b> | <a href="#">Installing Percona Server for MongoDB</a> |

Percona Server for MongoDB 5.0.15-13 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for [MongoDB 5.0.15 Community Edition](#).

It supports MongoDB 5.0.15 protocols and drivers

### **Warning**

Due to critical issues identified in previous releases that may affect data integrity and performance, we recommend upgrading all production environments to the latest version - currently MongoDB 5.0.15. Find details about those issues in [MongoDB 5.0 Community Edition release notes](#).

### Release Highlights

- The support for authentication using [AWS IAM](#) enables you to natively integrate Percona Server for MongoDB with AWS services, increase security of your infrastructure by setting up password-less authentication and offload your DBAs from managing different sets of secrets. This is the [technical preview feature](#)
- Improved master key rotation for data at rest encrypted with HashiCorp Vault enables you to use the same secret key path on every server in your entire deployment thus significantly simplifying the secrets management and key rotation process.

The bug fixes, provided by MongoDB and included in Percona Server for MongoDB, are the following:

- [SERVER-54900](#) - Fixed the issue with blocked networking calls preventing the oplog fetching process to re-establish the connection to an unresponsive sync-source node
- [SERVER-72416](#) - Fixed the issue with incorrect projection parsing when a collection level collation is specified
- [SERVER-71759](#) - Changed the yielding policy of dataSize command to YIELD\_AUTO for both when the command is called with estimate:true or false
- [SERVER-72535](#) - Disallow creating the 'admin', 'local', and 'config' databases with alternative cases in names on sharded clusters
- [SERVER-72222](#) - Fixed the incorrect behavior of the `mapReduce` command with single reduce optimization in sharded clusters
- [WT-9926](#) - Fixed a crash during startup from backup can lose metadata by not deleting checkpoints during recovery from backup
- [WT-9751](#) - Fixed a memory leak in reconciliation after aborted eviction
- [SERVER-72222](#) - Fixed mapReduce with single reduce optimization from failing in sharded clusters
- [SERVER-71399](#) - Fixed the issue with not removing the jumbo flag upon successful split of the chunk
- [SERVER-71191](#) - Fixed the deadlock between index build setup, prepared transaction and stepdown by unlocking and relocking Replication State Transition Lock (RSTL) during index build setup

Find the full list of changes in the [MongoDB 5.0.15 Community Edition release notes](#).

#### New Features

- [PSMDB-1033](#): Add authentication with AWS IAM

#### Improvements

- [PSMDB-1148](#): Improve the master key rotation when using a single master key for data-at-rest encryption with Vault in the entire deployment

#### Bugs Fixed

- [PSMDB-1201](#): Improved the error message if the attempt to save an encryption key to a KMIP server failed
- [PSMDB-1203](#): Gracefully terminate mongod if the master encryption key can't be saved to a KMIP server
- [PSMDB-1204](#): Fixed the handling of attributes list for LDAP authentication with OpenLDAP during the user to DN mapping stage

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

🕒 March 17, 2023

🕒 March 16, 2023

## 6.8 2022 (versions 5.0.6-5 through 5.0.15-13)

### 6.8.1 Percona Server for MongoDB 5.0.14-12 (2022-12-08)

|                     |   |
|---------------------|---|
| <b>Release date</b> | <b>December 8, 2022</b>                               |
| <b>Installation</b> | <a href="#">Installing Percona Server for MongoDB</a> |

Percona Server for MongoDB 5.0.14-12 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for [MongoDB 5.0.14 Community Edition](#).

It supports MongoDB 5.0.14 protocols and drivers

#### Release Highlights

With this release, [\\$backupCursor](#) and [\\$backupCursorExtend](#) aggregation stages is now generally available, enabling you to use it for building custom backup solutions.

The bug fixes, provided by MongoDB and included in Percona Server for MongoDB, are the following:

- [SERVER-68477](#) - Fixed the bug where an unexpected behavior could negatively impact existing TTL indexes with improper configuration and could cause the sudden expiration of TTL-indexed documents in a collection. This sudden expiration could cause data to be aged out prior than planned and could negatively impact write performance.

This bug involves TTL indexes with the `expireAfterSeconds` value of NaN (not-a-number). The TTL indexes are treated as 0 instead of NaN and that resulted in the sudden expiration of TTL-indexed documents in a collection. The bug affects MongoDB 5.0.0 through 5.0.13 and MongoDB 6.0.0 through 6.0.1.

It could be hit on MongoDB 4.4/4.2 when initially syncing from a 5.0.0-5.0.13 or 6.0.0-6.0.1 node and on MongoDB 5.0.0-5.0.13 when restoring from a `mongodump` of 4.2 / 4.4 collection or initially syncing from a 4.2/4.4 node that has a TTL configured with `expireAfterSeconds: NaN`.

The issue is fixed upstream in version 5.0.14 and 6.0.2. As the general recommendation, avoid using `expireAfterSeconds: NaN` as a configuration and correct this config anywhere it exists.

Follow closely the upstream recommendations to detect affected indexes and modify them using the `collMod` command.

- [SERVER-70879](#) - Corrected a potential race condition where multiple writing threads can update collection metadata in a way where overwrites could possibly happen. This could cause data/documents to be either unavailable or lost.
- [SERVER-66289](#) - Fixed the issue with how the server handles batches of writes when running `$out` with secondary read preference by updating write size estimation logic in `DocumentSourceWriter`
- [SERVER-61185](#) - Improved the performance of inserts into unique indexes
- [SERVER-68115](#) - Prevented dropping empty path component from `elemMatch` path during index selection

Find the full list of changes in the [MongoDB 5.0.14 Community Edition release notes](#).

## Improvements

- [PSMDB-1181](#): Add backup cursor parameters to cursor's metadata

## Bugs Fixed

- [PSMDB-1175](#): Fixed Percona Server for MongoDB behavior when calling `$backupCursor` with `disableIncrementalBackup` option

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)    [Get a Percona Expert](#)

 March 16, 2023

 December 8, 2022

## 6.8.2 Percona Server for MongoDB 5.0.13-11 (2022-10-12)

|                     |   |
|---------------------|---|
| <b>Release date</b> | <b>October 12, 2022</b>                               |
| <b>Installation</b> | <a href="#">Installing Percona Server for MongoDB</a> |

Percona Server for MongoDB 5.0.13-12 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for [MongoDB 5.0.13](#) and [MongoDB 5.0.13 Community Edition](#).

It supports protocols and drivers of both MongoDB 5.0.12 and 5.0.13.

This release of Percona Server for MongoDB includes the improvements and bug fixes of MongoDB Community Edition 5.0.12 and 5.0.13.

## Release Highlights

- [Data at rest encryption using the KMIP protocol](#) is now generally available, enabling you to use this functionality in production environments.
- [Percona Server for MongoDB Docker container](#) now includes the `mongodb-tools` utility set to align with the upstream container. This enables users to manage backup/restore operations of Percona Server for MongoDB.
- Updated exit code and status message during the master key rotation improves the user experience while using data-at-rest encryption with KMIP.

- Fixed security vulnerability [CVE-2022-3602](#) for Percona Server for MongoDB version 5.0.9-8 and higher installed from tarballs on Ubuntu 22.04.

The bug fixes, provided by MongoDB and included in Percona Server for MongoDB, are the following:

- [SERVER-68925](#) - Detect and resolve table logging inconsistencies for WiredTiger tables at startup
- [SERVER-60958](#) - Prevent the server from hanging in chunk migration when a step-down occurs.
- [SERVER-65382](#) - Fixed the issue with incorrect chunk size comparison during split by preventing the `AutoSplitVector` from using the `clientReadable`.
- [SERVER-63843](#) - Fixed the logger deadlock by adding a check against recursive logging
- [WT-9870](#) - Fixed the global time window state before performing the rollback to stable operation by updating the pinned timestamp as part of the transaction setup.
- [SERVER-69220](#) - Fixed the issue that could lead to data inconsistency by introducing the additional validation of field types for shard key patterns. Users should not modify the type (hashed or range) for the existing shard key fields
- [SERVER-67650](#) - Fixed the issue with failing resharding operation by introducing the start and end time metrics for resharding recipient
- [SERVER-68094](#) - Fixed the projection error during the resharding operation by using the `$replaceRoot` stage instead of the `$project` one

Find the full list of changes in the [MongoDB 5.0.12 Community Edition](#) and [MongoDB 5.0.13 Community Edition release notes](#).

#### New Features

- [PSMDB-776](#): Align Docker container with upstream by adding missing `mongodb-tools` utilities (Thanks to Denys Holius for reporting this issue)

#### Improvements

- [PSMDB-1116](#): Use proper exit code and logging severity for successful master key rotation

#### Bugs Fixed

- [PSMDB-1172](#): Fixed CVE-2022-3602 by updating the `libssl` for Ubuntu 22.04 tarballs
- [PSMDB-1134](#): Prevent the server crash by ensuring the backup cursor is closed before the server shutdown
- [PSMDB-1130](#): Improve handling of the missing encryption key during KMIP key rotation
- [PSMDB-1129](#): Prevent Percona Server for MongoDB from starting if the configured encryption key doesn't match the one used for data encryption
- [PSMDB-1082](#): Improve error handling for PSMDB when the wrong encryption key is used

**PERCONA**

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 December 8, 2022

 December 8, 2022

### 6.8.3 Percona Server for MongoDB 5.0.11-10 (2022-09-01)

|                     |   |
|---------------------|---|
| <b>Release date</b> | <b>September 01, 2022</b>                             |
| <b>Installation</b> | <a href="#">Installing Percona Server for MongoDB</a> |

Percona Server for MongoDB 5.0.11-10 is an enhanced, source available, and highly-scalable database that is a fully-compatible, drop-in replacement for MongoDB 5.0.11 Community Edition. It supports MongoDB 5.0.11 protocols and drivers.

#### Release Highlights

- [SERVER-68511](#) - Fixed the issue that caused inconsistency in sharding metadata when running the `movePrimary` command on the database that has the Feature Compatibility Version (FCV) set to 4.4 or earlier. Affects MongoDB versions 5.0.0 through 5.0.10 and MongoDB 6.0.0. Upgrade to the the fixed version of MongoDB 5.0.11 / Percona Server for MongoDB 5.0.11-10 as soon as possible.
- [SERVER-61321](#), [SERVER-60607](#) - Improved handling of large/NaN (Not a Number) values for text index and geo index version.
- [SERVER-68628](#) - Prevented potential server crash or lost writes when a resharding retry happens after the primary node failover. This is fixed by refreshing the routing information on the primary node during resharding.
- [WT-9500](#) - Prevent rollback to stable operation to generate wrong updates/tombstones by always reading the cell time window information to decide the history store update visibility.
- [WT-9004](#) - Fixed memory leak in update restore eviction.
- [SERVER-67492](#) - Failed chunk migrations can lead to recipient shard having different config.transactions records between primaries and secondaries - inconsistent data.
- [SERVER-68495](#) - Fixed the issue when resharding a collection with a very large number of zones configured may have stalled on config server primary indefinitely.
- [SERVER-68628](#) - Fixed the issue when retrying a failed resharding operation after a primary failover could lead to server crash or lost writes.
- [SERVER-68193](#) - Prevented sharding DDL coordinator to lock itself out in distlock retry loop.

Find the full list of changes in the [MongoDB 5.0.11 Community Edition release notes](#).

#### Improvements

- [PSMDB-1046](#): Make the `kmipKeyIdentifier` option not mandatory

**Bugs Fixed**

- [PSMDB-1119](#): Fixed the issue with backup cursor not opening if data-at-rest encryption is enabled

**PERCONA**

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 December 8, 2022


 December 8, 2022

**6.8.4 Percona Server for MongoDB 5.0.10-9 (2022-08-09)**

|                     |   |
|---------------------|---|
| <b>Release date</b> | <b>August 09, 2022</b>                                |
| <b>Installation</b> | <a href="#">Installing Percona Server for MongoDB</a> |

Percona Server for MongoDB 5.0.10-9 is an enhanced, source available, and highly-scalable database that is a fully-compatible, drop-in replacement for MongoDB 5.0.10 Community Edition.

It is rebased on [MongoDB 5.0.10 Community Edition](#) and supports MongoDB 5.0.10 protocols and drivers.

** Warning**

We don't recommend this version for the production use due to the critical issue with sharding metadata inconsistency: [SERVER-68511](#). The metadata inconsistency is observed when running the `movePrimary` command on the database that has the Feature Compatibility Version (FCV) set to 4.4 or earlier. Affects MongoDB versions 5.0.0 through 5.0.10 and MongoDB 6.0.0. Upgrade to the fixed version of MongoDB 5.0.11 / Percona Server for MongoDB 5.0.11-10 as soon as possible.

Please follow closely the upstream recommendations outlined in [SERVER-68511](#) to work around this issue and for the remediation steps, if your cluster is affected.



## Release Highlights

This release includes bug fixes and improvements provided by MongoDB and included in Percona Server for MongoDB. It specifically includes multiple fixes relate to sharding and the resharding operation. Bugs of note are the following:

- [SERVER-66418](#) - Fixed the issue with bad projection created during dependency analysis due to string order assumption. It resulted in the `PathCollision` error. The issue is fixed by improving dependency analysis for projections by folding dependencies into ancestor dependencies where possible.
- [SERVER-65821](#) - Fixed the deadlock situation in cross shard transactions that could occur when the FCV (Feature Compatibility Version) was set after the “prepared” state of the transactions. That ended up with both the `setFCV` thread and the `TransactionCoordinator` hung.
- [SERVER-65131](#) - This is a v6.0 backport fix to v5.0 that disables opportunistic read targeting (except for specified hedged reads) in order to prevent possible performance problems associated with uneven read distribution across the secondaries.
- [SERVER-66433](#) - Backported the check for user errors in case deadline on the migration destination manager is hit while waiting for a range to be cleared up. This prevents the balancer from getting blocked.
- [SERVER-67457](#) - Fixed the situation where the shards may skip certain steps in the resharding process but respond to the resharding coordinator as if they had. This can cause the resharding coordinator to continue to wait for updated states in the `config.reshardingOperations` document on the primary config server and stall indefinitely.
- [SERVER-66866](#) - Fixed the potential for the range deleter to wait unnecessarily during concurrent migrations between batches.
- [SERVER-66727](#) Fixed the issue where 2 very different measurements (one in the past and one in future) could be incorrectly included in the same buckettime-series bucket.
- [SERVER-64433](#) - Resolved potential problem when adding or removing shards and incorrectly gossiping a new topology time without it being majorly committed.

Find the full list of changes in the [MongoDB 5.0.10 Community Edition release notes](#).

## Packaging Notes

Debian 9 (“Stretch”) is no longer supported.

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

🕒 December 8, 2022

🕒 December 8, 2022

## 6.8.5 Percona Server for MongoDB 5.0.9-8 (2022-06-20)

|                     |   |
|---------------------|---|
| <b>Release date</b> | <b>June 20, 2022</b>                                  |
| <b>Installation</b> | <a href="#">Installing Percona Server for MongoDB</a> |

Percona Server for MongoDB 5.0.9-8 is an enhanced, source available, and highly-scalable database that is a fully-compatible, drop-in replacement for MongoDB 5.0.9 Community Edition. It supports MongoDB 5.0.9 protocols and drivers.

### Warning

We don't recommend this version for the production use due to the critical issue with sharding metadata inconsistency: [SERVER-68511](#). The metadata inconsistency is observed when running the `movePrimary` command on the database that has the Feature Compatibility Version (FCV) set to 4.4 or earlier. Affects MongoDB versions 5.0.0 through 5.0.10 and MongoDB 6.0.0. Upgrade to the fixed version of MongoDB 5.0.11 / Percona Server for MongoDB 5.0.11-10 as soon as possible.

Please follow closely the upstream recommendations outlined in [SERVER-68511](#) to work around this issue and for the remediation steps, if your cluster is affected.

### Release Highlights

- Support of [multiple KMIP servers](#) adds failover to your data-at-rest encryption setup.
- Allow users to set KMIP client certificate password through a flag to simplify the migration from MongoDB Enterprise to Percona Server for MongoDB.
- Percona Server for MongoDB is now available on Ubuntu 22.04 (Jammy Jellyfish).
- Improvements to initial syncs from a secondary sync source.

The bug fixes, provided by MongoDB and included in Percona Server for MongoDB, are the following:

- [SERVER-65137](#) - Detect namespace changes when refreshing Collection after yielding to maintain data consistency and avoid stale catalogs.
- [SERVER-64822](#) - Fixed the issue with releasing the critical state too early when sharding an empty collection. This could result in unwanted writes to that collection.
- [WT-9096](#) - Fixed the wrong key/value returning during search near when the key doesn't exist
- [SERVER-66041](#) - Prevented shard imbalances due to chunk cloner disregarding oversized chunks that contain only 1 oversized document

Find the full list of changes in the [MongoDB 5.0.9 Community Edition release notes](#).

### Improvements

- [PSMDB-1045](#): Add support for several KMIP servers

- [PSMDB-1043](#): Remove the `kmipClientKeyFile` option and include both the client private key and public certificate in the file specified by the `kmipClientCertificateFile` option.
- [PSMDB-1044](#): Make the `kmipPort` option not mandatory and assign the default value
- [PSMDB-1054](#): Add the ability to specify the password for the KMIP client keys and certificates to simplify migration from MongoDB Enterprise.

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 December 8, 2022

 December 8, 2022

### 6.8.6 Percona Server for MongoDB 5.0.8-7 (2022-05-10)

|                     |   |
|---------------------|---|
| <b>Release date</b> | <b>May 10, 2022</b>                                   |
| <b>Installation</b> | <a href="#">Installing Percona Server for MongoDB</a> |

Percona Server for MongoDB 5.0.8-7 is an enhanced, source available, and highly-scalable database that is a fully-compatible, drop-in replacement for MongoDB 5.0.8 Community Edition. It supports MongoDB 5.0.8 protocols and drivers.

#### **Warning**

We don't recommend this version for the production use due to the critical issue with sharding metadata inconsistency: [SERVER-68511](#). The metadata inconsistency is observed when running the `movePrimary` command on the database that has the Feature Compatibility Version (FCV) set to 4.4 or earlier. Affects MongoDB versions 5.0.0 through 5.0.10 and MongoDB 6.0.0. Upgrade to the fixed version of MongoDB 5.0.11 / Percona Server for MongoDB 5.0.11-10 as soon as possible.

Please follow closely the upstream recommendations outlined in [SERVER-68511](#) to work around this issue and for the remediation steps, if your cluster is affected.

#### Release Highlights

Percona Server for MongoDB now supports master key rotation for data encrypted using the [Keys Management Interoperability Protocol \(KMIP\)](#) protocol (tech preview feature). This improvement allows users to comply with regulatory standards for data security.

Other improvements and bug fixes introduced by MongoDB and included in Percona Server for MongoDB are the following:

- [WT-8924](#) - Fixed a bug that causes replication to stall on secondary replica set members in a sharded cluster handling cross-shard transactions. It is caused by WiredTiger to erroneously return a write conflict when deciding if an update to a record is allowed. If MongoDB decides to retry the operation that caused the conflict in WiredTiger, it will enter an indefinite retry loop, and oplog application will stall on secondary nodes.

If this bug is hit, the secondary nodes will experience indefinite growth in replication lag. Restart the secondary nodes to resume replication.

This bug affects MongoDB 4.4.10 through 4.4.13 and 5.0.4 to 5.0.7.

Update to the latest version to avoid the secondary replication stall and lag issues.

- [SERVER-63531](#) - Fixed the issue with a `commitQuorum` incorrectly allowing non-voting `buildIndexes:false` nodes to be included in the `commitQuorum` count. It also fixed an error message relating to data-bearing nodes and quorum regarding to non-voting nodes.
- [SERVER-63387](#) - Fixed the order of backup blocks returned to the user to match the order retrieved from WiredTiger.
- [SERVER-65261](#) - Fixed the issue reporting an incorrect number of documents deleted from a capped collection when utilizing a collection scan to perform the delete action.

Find the full list of changes in the [MongoDB 5.0.8 Community Edition release notes](#).

### Improvements

- [PSMDB-1011](#): Add KMIP master key rotation

### Bugs Fixed

- [PSMDB-1030](#): Fix descriptions and mutual dependencies of KMIP related options for `mongod` and `perconadecrypt`

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)    [Get a Percona Expert](#)

 December 8, 2022

 December 8, 2022

## 6.8.7 Percona Server for MongoDB 5.0.7-6 (2022-04-20)

|                     |   |
|---------------------|---|
| <b>Release date</b> | <b>April 20, 2022</b>                                 |
| <b>Installation</b> | <a href="#">Installing Percona Server for MongoDB</a> |

Percona Server for MongoDB 5.0.7-6 is an enhanced, source-available and highly-scalable database that is a fully-compatible, drop-in replacement for MongoDB 5.0.7 Community Edition. It supports MongoDB 5.0.7 protocols and drivers.

### Warning

We don't recommend this version for the production use due to the critical issue with sharding metadata inconsistency: [SERVER-68511](#). The metadata inconsistency is observed when running the `movePrimary` command on the database that has the Feature Compatibility Version (FCV) set to 4.4 or earlier. Affects MongoDB versions 5.0.0 through 5.0.10 and MongoDB 6.0.0. Upgrade to the fixed version of MongoDB 5.0.11 / Percona Server for MongoDB 5.0.11-10 as soon as possible.

Please follow closely the upstream recommendations outlined in [SERVER-68511](#) to work around this issue and for the remediation steps, if your cluster is affected.

### Release Highlights

Percona Server for MongoDB now supports [Keys Management Interoperability Protocol \(KMIP\)](#) so that users can store encryption keys in their favorite KMIP-compatible key manager to set up encryption at rest. This is a tech preview feature.

The list of bug fixes introduced by MongoDB and included in Percona Server for MongoDB is the following:

- [SERVER-63203](#) - Fixed the issue where having a large number of split points causes the chunk splitter to not function correctly and huge chunks would not be split without manual intervention. This can be caused when having small shard key ranges and a very high number of documents and where more than 8192 split points would be needed.
- [SERVER-64517](#) - Recover the `RecoverableCriticalSection` service after the `initialSync` and `startupRecovery` stages have completed. This prevents a started up shard to miss an in-memory critical section of a resharded collection.
- [SERVER-64403](#) - Fixed an issue that occurred during the attempt to perform the collation-encoding of a document with a missing sort attribute. In this case an invariant is violated and `mongod` crashes.
- [SERVER-63722](#) - Fixed an issue when the rename collection (sharding step) participants can get stuck.
- [SERVER-61769](#) - Fixed an issue with idle cursors remaining open when the client attempts to run an aggregation with `$out` or `$merge` in a transaction on a sharded cluster.
- [SERVER-60412](#) - Check if the host has cgroups v2 enabled and read the memory limits according to that.
- [WT-7922](#) - Report an error when the WiredTiger version file is empty or missing during a startup.

Find the full list of changes in the [MongoDB 5.0.7 Community Edition Release notes](#).

### New Features

- [PSMDB-971](#): Added support for KMIP encryption. Now users can store encryption keys in their favorite KMIP-compatible key manager to set up encryption at rest.

**Bugs Fixed**

- [PSMDB-1010](#): Fixed the parameters order in the `LOGV2_DEBUG` statement for LDAP logging.
- [PSMDB-957](#): Fixed server crash caused by LDAP misconfiguration. Now the server logs an error message and exits.

**PERCONA**

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 December 8, 2022

 December 8, 2022

## 6.8.8 Percona Server for MongoDB 5.0.6-5 (2022-02-10)

|                     |   |
|---------------------|---|
| <b>Release date</b> | <b>February 10, 2022</b>                              |
| <b>Installation</b> | <a href="#">Installing Percona Server for MongoDB</a> |

Percona Server for MongoDB 5.0.6-5 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for MongoDB 5.0.6 Community Edition. It supports MongoDB 5.0.6 protocols and drivers.

**Warning**

Inconsistent data is observed after the upgrade from MongoDB 4.4.3 and 4.4.4 to versions 4.4.8+ and 5.0.2+. This issue is fixed upstream in versions 4.4.11 and 5.0.6. Percona Server for MongoDB also includes the fix in versions 4.4.12-12 and 5.0.6-5

See the upgrade recommendations below:

- Clusters on versions 4.4.0 and 4.4.1 are safe to upgrade to 4.4.8+ or 5.0.2+ but should upgrade to recommended versions 4.4.11+ or 5.0.5+
- Clusters on versions 4.4.2, 4.4.3, or 4.4.4 should **downgrade** to 4.4.1 and then upgrade to versions 4.4.11+ or 5.0.5+.
- Clusters running versions 4.4.5 - 4.4.7 can and should upgrade to versions 4.4.11+ or 5.0.5+.

Note that clusters running versions 4.4.2 - 4.4.8 are affected by the bug [WT-7995](#). See [WT-7995](#) for specific explanation and instructions on running the `validate` command to check for data inconsistencies. These data inconsistencies can lead to data loss if not identified and repaired at this point between versions 4.4.8 and 4.4.9.

If the `validate` command output reports any failures, resync the impacted node from an unaffected node. **The validate command must be run against all collections in the database. This process can be resource intensive and can negatively impact performance.**

Another critical issue that affects the production use of this version is [SERVER-68511](#). It causes inconsistency in sharding metadata when running the `movePrimary` command on the database that has the Feature Compatibility Version (FCV) set to 4.4 or earlier. Affects MongoDB versions 5.0.0 through 5.0.10 and MongoDB 6.0.0. Upgrade to the fixed version of MongoDB 5.0.11 / Percona Server for MongoDB 5.0.11-10 as soon as possible.

Follow the upstream recommendations in [SERVER-68511](#) to check your clusters and remediate any negative impact if the clusters are affected with this issue.

**Release Highlights**

- [WT-8395](#) - Fixed an issue with inconsistent data observed during the direct upgrade from from 4.4.3 and 4.4.4 to 4.4.8+ and 5.0.2+. Data inconsistency was caused by the incorrect checkpoint metadata to sometimes be recorded by MongoDB versions 4.4.3 and 4.4.4. WiredTiger used this metadata during node startup that could lead to data corruption and could cause the DuplicateKey error. The fix requires the upgrade to versions 4.4.11+ or 5.0.5+.
- [SERVER-62245](#) - Fixed an issue unavailability of a shard in sharded clusters. Affects MongoDB versions 5.0.0 - 5.0.5. Requires the following steps:
  - Restarting the shards as replica sets
  - Checking that range deletion tasks are consistent with migration coordinators
  - Majority-deleting all migration coordinators with a definitive decision
  - Restarting the nodes as shards.
- [SERVER-61194](#) - Fixed time-series bucket OID collisions by adding the difference between the actual timestamp and the rounded timestamp to the instance portion of the OID.
- [SERVER-62147](#) - Fixed broken OP\_QUERY exhaust cursor implementation.

**Bugs Fixed**

- [PSMDB-950](#): Fixed LDAP authentication using mongo CLI for Percona Server for MongoDB installed from a tarball.

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 December 8, 2022

 December 8, 2022

## 6.9 2021 (versions 5.0.2-1 through 5.0.5-4)

### 6.9.1 Percona Server for MongoDB 5.0.5-4 (2021-12-28)

|                     |   |
|---------------------|---|
| <b>Release date</b> | <b>December 28, 2021</b>                              |
| <b>Installation</b> | <a href="#">Installing Percona Server for MongoDB</a> |

#### **Warning**

We don't recommend this version for the production use due to the critical issue with sharding metadata inconsistency: [SERVER-68511](#). The metadata inconsistency is observed when running the `movePrimary` command on the database that has the Feature Compatibility Version (FCV) set to 4.4 or earlier. Affects MongoDB versions 5.0.0 through 5.0.10 and MongoDB 6.0.0. Upgrade to the fixed version of MongoDB 5.0.11 / Percona Server for MongoDB 5.0.11-10 as soon as possible.

Please follow closely the upstream recommendations outlined in [SERVER-68511](#) to work around this issue and for the remediation steps, if your cluster is affected.

Percona Server for MongoDB 5.0.5-4 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for MongoDB 5.0.5 Community Edition. It supports MongoDB 5.0.5 protocols and drivers.



## Release Highlights

The bug fixes and improvements, provided by MongoDB and included in Percona Server for MongoDB, are the following:

- [SERVER-59858](#) - Added histograms to track latency for tasks scheduled on the reactor thread.
- [SERVER-61483](#) - Fixed an issue when resharding a collection that could cause data inconsistency (lost writes) due to incorrect actions by the ReshardingCoordinator and attempts to commit anyway. Also could cause `assert()` to config server primary.
- [SERVER-61482](#) - Fixed an issue with stalls on the config server. Updates to config server during resharding may wait too long for oplog slot thus stalling replication on config server indefinitely.
- [SERVER-61633](#) Fixed a resharding issue relating to RecipientStateMachine that caused the server to crash

Find the full list of changes in the [MongoDB 5.0.5 Community Edition release notes](#).

## Bugs Fixed

- [PSMDB-756](#): Fixed an issue with unmet dependencies for installing MongoDB on Debian (Thanks to Stefan Schlesi for reporting this issue)

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)    [Get a Percona Expert](#)

 December 8, 2022

 December 8, 2022

## 6.9.2 Percona Server for MongoDB 5.0.4-3 (Release Candidate) (2021-12-08)

|                     |   |
|---------------------|---|
| <b>Release date</b> | <b>December 8, 2021</b>                               |
| <b>Installation</b> | <a href="#">Installing Percona Server for MongoDB</a> |

Percona Server for MongoDB 5.0.4-3 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for MongoDB 5.0.4 Community Edition.

It is rebased on [MongoDB 5.0.4 Community Edition](#) and supports MongoDB 5.0.4 protocols and drivers.

 **Note**

Due to many core changes to WiredTiger and the core server introduced to facilitate new features such as resharding, time series collections, and API versioning, MongoDB 5.0.x is still unstable. We do not recommend using this release candidate for production environments.

 **Warning**

We don't recommend this version for the production use due to the critical issue with sharding metadata inconsistency: [SERVER-68511](#). The metadata inconsistency is observed when running the `movePrimary` command on the database that has the Feature Compatibility Version (FCV) set to 4.4 or earlier. Affects MongoDB versions 5.0.0 through 5.0.10 and MongoDB 6.0.0. Upgrade to the fixed version of MongoDB 5.0.11 / Percona Server for MongoDB 5.0.11-10 as soon as possible.

Please follow closely the upstream recommendations outlined in [SERVER-68511](#) to work around this issue and for the remediation steps, if your cluster is affected.

**Release Highlights**

The bug fixes, provided by MongoDB and included in Percona Server for MongoDB, are the following:

- Fixed delays in establishing egress connections on `mongos` due to delayed responses from `libcrypto.so`
- Allowed replication state changes to interrupt lock acquisition. This interruption fixes deadlocks that may occur when a primary node steps down with profiling enabled.

Find the full list of changes in the [MongoDB 5.0.4 Community Edition release notes](#).

**PERCONA**

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 December 8, 2022

 December 8, 2022

## 6.9.3 Percona Server for MongoDB 5.0.3-2 (Release Candidate) (2021-10-14)

|                     |   |
|---------------------|---|
| <b>Release date</b> | <b>October 14, 2021</b>                               |
| <b>Installation</b> | <a href="#">Installing Percona Server for MongoDB</a> |

Percona Server for MongoDB 5.0.3-2 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for MongoDB 5.0.3 Community Edition. It supports MongoDB 5.0.3 protocols and drivers.

#### Note

Due to many core changes to WiredTiger and the core server introduced to facilitate new features such as resharding, time series collections, and API versioning, MongoDB 5.0.x is still unstable. We do not recommend using this release candidate for production environments.

#### Warning

Beginning with MongoDB 5.0.1, several data impacting or corrupting bugs were introduced. Details are listed below.

These bugs are fixed in MongoDB 5.0.3. Percona Server for MongoDB 5.0.3-2 includes the upstream fixes of these bugs.

Unless you are already running a version of MongoDB 5.0.x in your production environments, consider waiting a while longer for any other issues to be worked through.

If you are running any version of MongoDB 5.0.x already, please upgrade to MongoDB 5.0.3 or Percona Server for MongoDB 5.0.3-2 as soon as possible. Please follow closely all MongoDB Inc upstream recommendations regarding avoiding unclean shutdowns, check collections with the [validate](#) command (watch for performance impacts), and make sure and resync any impacted nodes from unaffected nodes as recommended in [WT-7995](#).

Another critical issue that affects the production use of this version is [SERVER-68511](#). It causes inconsistency in sharding metadata when running the `movePrimary` command on the database that has the Feature Compatibility Version (FCV) set to 4.4 or earlier. Affects MongoDB versions 5.0.0 through 5.0.10 and MongoDB 6.0.0. Upgrade to the fixed version of MongoDB 5.0.11 / Percona Server for MongoDB 5.0.11-10 as soon as possible.

Follow the upstream recommendations in [SERVER-68511](#) to check your clusters and remediate any negative impact if the clusters are affected with this issue.

## Release Highlights

The bug fixes, provided by MongoDB and included in Percona Server for MongoDB, are the following:

- [WT-7995](#) - Checkpoint thread can read and persist inconsistent version of data to disk. Can cause Duplicate Key error on startup and prevent the node from starting. Unclean shutdowns can cause data inconsistency within documents, deleted documents to still exist, incomplete query results due to lost or inaccurate index entries, and/or missing documents. Affects MongoDB versions 5.0.0 through 5.0.2. Upgrade to fixed version of MongoDB 5.0.3 / Percona Server for MongoDB 5.0.3-2 as soon as possible.
- [WT-7984](#) - Bug that could cause Checkpoint thread to omit a page of data. If the server experiences an unclean shutdown, an inconsistent checkpoint is used for recovery and causes data corruption. Fixed in version 5.0.3.

Requires the [validate](#) command to be run and possible data remediation via complete initial sync.

Find the full list of changes in the [MongoDB 5.0.3 Community Edition release notes](#).

## Improvements

- [PSMDB-918](#): Disable the deletion of the `mongod` user in RPM packages - This preserves the permissions to the MongoDB data directory for the `mongod` user since its user ID and group ID remain unchanged.

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 December 8, 2022

 December 8, 2022

### 6.9.4 Percona Server for MongoDB 5.0.2-1 (Release Candidate) (2021-08-16)

|                     |   |
|---------------------|---|
| <b>Release date</b> | <b>August 16, 2021</b>                                |
| <b>Installation</b> | <a href="#">Installing Percona Server for MongoDB</a> |

#### Note

With a lot of new features and modifications introduced, we recommend using this release candidate in testing environments only.

#### Warning

Percona Server for MongoDB 5.0.2-1 is not recommended for production use due to the following critical issues: [WT-7984](#) and [WT-7995](#). These issues are fixed in MongoDB 5.0.3 Community Edition and [Percona Server for MongoDB 5.0.3-2 \(Release Candidate\)](#).

Another critical issue that affects the production use of this version is [SERVER-68511](#). It causes inconsistency in sharding metadata when running the `movePrimary` command on the database that has the Feature Compatibility Version (FCV) set to 4.4 or earlier. Affects MongoDB versions 5.0.0 through 5.0.10 and MongoDB 6.0.0. Upgrade to the fixed version of MongoDB 5.0.11 / Percona Server for MongoDB 5.0.11-10 as soon as possible.

We recommend you to upgrade to Percona Server for MongoDB 5.0.11-10 and run the `validate` command on every collection on every replica set node.

Read more about the post-upgrade steps in [WT-7984](#) and [WT-7995](#).

Learn how to check if your cluster is affected with sharding metadata inconsistency and remediate from this impact in [SERVER-68511](#).

We are pleased to announce the release candidate of Percona Server for MongoDB 5.0.2-1. It is available for [download from Percona website](#) and for installation from [Percona Software Repositories](#).

Percona Server for MongoDB 5.0.2-1 is an enhanced, source-available, and highly-scalable database that is a fully-compatible, drop-in replacement for MongoDB 5.0.2 Community Edition. It includes [all features of MongoDB 5.0.2 Community Edition](#). The most notable among these are the following:

- [Resharding](#) allows you to select a new shard key for a collection and then works in the background to correct any data distribution problems caused by bad shard keys and improve performance.
- [Time Series Collections](#) are aimed at storing sequences of measurements over a period of time. These specialized collections will store data in a highly optimized way that will improve query efficiency, allow data analysis in real-time, and optimize disk usage.
- [Resumable Index Builds](#) means that the index build for a collection continues if a primary node in a replica set is switched to another server or when a server restarts. The build process is saved to disk and resumes from the saved position. This allows DBAs to perform maintenance and not worry about losing the index build in the process.
- [Window operators](#) allow operations on a specified span of documents known as window. `$setWindowFields` is a new pipeline stage to operate with these documents.
- [Versioned API](#) allows specifying which API version your application communicating with MongoDB runs against. Versioned API detaches the application's lifecycle from that of the database. As a result, you modify the application only to introduce new features instead of having to maintain compatibility with the new version of MongoDB.

In addition, [new aggregation operators](#) such as `$count`, `$dateAdd`, `$dateDiff`, `$dateSubtract`, `$sampleRate` and `$rand` are available with this release.

Percona Server for MongoDB 5.0.2-1 extends this feature set by providing [enterprise-level enhancements](#) for free.

Percona Server for MongoDB 5.0.2-1 fully supports MongoDB 5.0.2 Community Edition protocols and drivers and requires no changes to MongoDB applications or code.

## PERCONA

Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)    [Get a Percona Expert](#)

 January 2, 2023

 December 8, 2022

## 7. FAQ

### 7.1 How to check Percona Server for MongoDB version?

To see which version of Percona Server for MongoDB you are using, check the value of the `psmdbVersion` key in the output of the `buildInfo` database command. If this key does not exist, Percona Server for MongoDB is not installed on the server.

### 7.2 Where is the location of the configuration and data files?

By default, Percona Server for MongoDB stores data files in `/var/lib/mongodb/` and configuration parameters in `/etc/mongod.conf`.

## PERCONA

### 7.3 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.



[Community Forum](#)



[Get a Percona Expert](#)

February 28, 2024

February 28, 2024

## 8. Reference

### 8.1 Glossary

#### 8.1.1 ACID

Set of properties that guarantee database transactions are processed reliably. Stands for [Atomicity](#), [Consistency](#), [Isolation](#), [Durability](#).

#### 8.1.2 Atomicity

Atomicity means that database operations are applied following a “all or nothing” rule. A transaction is either fully applied or not at all.

#### 8.1.3 Consistency

Consistency means that each transaction that modifies the database takes it from one consistent state to another.

#### 8.1.4 Durability

Once a transaction is committed, it will remain so.

#### 8.1.5 Foreign Key

A referential constraint between two tables. Example: A purchase order in the `purchase_orders` table must have been made by a customer that exists in the `customers` table.

#### 8.1.6 Isolation

The Isolation requirement means that no transaction can interfere with another.

#### 8.1.7 Jenkins

[Jenkins](#) is a continuous integration system that we use to help ensure the continued quality of the software we produce. It helps us achieve the aims of:

- no failed tests in trunk on any platform,
- aid developers in ensuring merge requests build and test on all platforms,
- no known performance regressions (without a damn good explanation).

#### 8.1.8 Kerberos

Kerberos is an authentication protocol for client/server authentication without sending the passwords over an insecure network. Kerberos uses symmetric encryption in the form of tickets - small pieces of encrypted data used for authentication. A ticket is issued for the client and validated by the server.

### 8.1.9 Rolling restart

A rolling restart (rolling upgrade) is shutting down and upgrading nodes one by one. The whole cluster remains operational. There is no interruption to clients assuming the elections are short and all writes directed to the old primary use the `retryWrite` mechanism.

### 8.1.10 Technical preview feature

Technical preview features are not yet ready for enterprise use and are not included in support via SLA. They are included in this release so that users can provide feedback prior to the full release of the feature in a future GA release (or removal of the feature if it is deemed not useful). This functionality can change (APIs, CLIs, etc.) from tech preview to GA.

## PERCONA

### 8.1.11 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)    [Get a Percona Expert](#)

 March 16, 2023

 December 8, 2022

## 8.2 Telemetry and data collection

Percona collects usage data to improve its software. The telemetry feature helps us identify popular features, detect problems, and plan future improvements.

Currently, telemetry is added only to the Percona packages for both basic and Pro builds and to Docker images.

### 8.2.1 What information is collected

Telemetry collects the following information:

- The information about the installation environment when you install the software.
- The information about the operating system such as OS name, the architecture, the list of Percona packages. See more in the [Telemetry Agent section](#).
- The metrics from the database instance. See more in the [Telemetry Subsystem section](#).



## 8.2.2 What is NOT collected

Percona protects your privacy and doesn't collect any personal information about you like database names, user names or credentials or any user-entered values.

All collected data is anonymous, meaning it can't be traced back to any individual user. To learn more about how Percona handles your data, read the [Percona Privacy statement](#).

You control whether to share this information. Participation in this program is completely voluntary. If don't want to share anonymous data, you can [disable telemetry](#).

## 8.2.3 Why telemetry matters

Benefits for Percona:

| Advantages                       | Description  |
|----------------------------------|--|
| See how people use your software | Telemetry collects anonymous data on how users interact with our software. This tells developers which features are popular, which ones are confusing, and if anything is causing crashes. |
| Identify issues early            | Telemetry can catch bugs or performance problems before they become widespread.  |

Benefits for users in the long run:

| Advantages               | Description  |
|--------------------------|--|
| Faster bug fixes         | With telemetry data, developers can pinpoint issues affecting specific users and prioritize fixing them quickly.   |
| Improved features        | Telemetry helps developers understand user needs and preferences. This allows them to focus on features that will be genuinely useful and improve your overall experience. |
| Improved user experience | By identifying and resolving issues early, telemetry helps create a more stable and reliable software experience for everyone.   |

## 8.2.4 Telemetry components

Percona collects information using the following components:

- Telemetry script that sends the information about the software and the environment where it is installed. This information is collected only once during the installation.
- The Telemetry Subsystem collects the necessary metrics directly from the database and stores them in a Metrics File.
- The Metrics File stores the metrics and is a standalone file located on the database host's file system.
- The Telemetry Agent is an independent process running on your database host's operating system and carries out the following tasks:
  - Collects OS-level metrics
  - Reads the Metrics File, adds the OS-level metrics
  - Sends the full set of metrics to the Percona Platform
  - Collects the list of installed Percona packages using the local package manager

The telemetry also uses the Percona Platform with the following components:

- Telemetry Service - offers an API endpoint for sending telemetry. The service handles incoming requests. This service saves the data into Telemetry Storage.
- Telemetry Storage - stores all telemetry data for the long term.

### Telemetry Subsystem

The Telemetry Subsystem extends the functionality of the database. It is built-in in Percona Server for MongoDB and is implemented separately for `mongod` and `mongos` instances. The Telemetry Subsystem is enabled by default during the initial database deployment.

The Telemetry Subsystem collects metrics from the database instance daily to the Metrics File. It creates a new Metrics File for each collection. Before generating a new file, the Telemetry Subsystem deletes the Metrics Files that are older than seven days. This process ensures that only the most recent week's data is maintained.

The Telemetry Subsystem creates a file in the local file system using a timestamp as the name with a `.json` extension.

### Metrics File

The Metrics File is a JSON file with the metrics collected by the Telemetry Subsystem.

#### LOCATIONS

Percona stores the Metrics File in one of the following directories on the local file system. The location depends on the product.

- Telemetry root path - `/usr/local/percona/telemetry`
- Percona Server for MongoDB has two root paths since the telemetry Subsystem is enabled both for the `mongod` and `mongos` instances. The paths are the following:
  - `mongod` root path - `${telemetry root path}/psmdb/`
  - `mongos` root path - `${telemetry root path}/psmdb/`
- PS root path - `${telemetry root path}/ps/`
- PXC root path - `${telemetry root path}/pxc/`
- PG root path - `${telemetry root path}/pg/`

Percona archives the telemetry history in `${telemetry root path}/history/`.

## METRICS FILE FORMAT

The Metrics File uses the Javascript Object Notation (JSON) format. Percona reserves the right to extend the current set of JSON structure attributes in the future.

`mongod` Metrics File      `mongos` Metrics File

The following is an example of the collected data generated by the `mongod` instance of the config server replica set of the sharded cluster:

```
{
  "source": "mongod",
  "pillar_version": "5.0.0",
  "pro_features": [],
  "db_instance_id": "65e9977d58deb2f66faa591c",
  "db_internal_id": "65e9977d58deb2f66faa591c",
  "db_cluster_id": "65e997cb58deb2f66faa5954",
  "shard_svr": "true",
  "config_svr": "true",
  "uptime": "102",
  "storage_engine": "wiredTiger",
  "db_replication_id": "65e997cb58deb2f66faa5944",
  "replication_state": "PRIMARY"
}
```

The following is an example of the collected data generated by the `mongos` instance.

```
{
  "source": "mongos",
  "pillar_version": "5.0.0",
  "pro_features": [],
  "db_instance_id": "6690fea9066216c6d9d77044",
  "uptime": "4",
  "db_cluster_id": "6690fea65d86eb061c0bd728"
}
```

### Telemetry Agent

The Percona Telemetry Agent runs as a dedicated OS daemon process `percona-telemetry-agent`. It creates, reads, writes, and deletes JSON files in the `${telemetry root path}`. You can find the agent's log file at `/var/log/percona/telemetry-agent.log`.

The agent does not send anything if there are no Percona-specific files in the target directory.

The following is an example of a Telemetry Agent payload:

```
{
  "reports": [
    {
      "id": "B5BDC47B-B717-4EF5-AEDF-41A17C9C18BB",
      "createTime": "2024-07-01T10:56:49Z",
      "instanceId": "B5BDC47B-B717-4EF5-AEDF-41A17C9C18BA",
      "productFamily": "PRODUCT_FAMILY",
      "metrics": [
        {
          "key": "OS",
          "value": "Ubuntu"
        }
      ]
    }
  ]
}
```

```

    "key": "pillar_version",
    "value": "5.0.0"
  }
]
}
]
}

```

The agent sends information about the database and metrics.

| Key             | Description  |
|-----------------|--|
| "id"            | A generated Universally Unique Identifier (UUID) version 4   |
| "createTime"    | UNIX timestamp   |
| "instanceId"    | The DB Host ID. The value can be taken from the <code>instanceId</code> , the <code>/usr/local/percona/telemetry_uuid</code> or generated as a UUID version 4 if the file is absent. |
| "productFamily" | The value from the file path   |
| "metrics"       | An array of key:value pairs collected from the Metrics File.   |

The following operating system-level metrics are sent with each check:

| Key                  | Description  |
|----------------------|--|
| "OS"                 | The name of the operating system   |
| "hardware_arch"      | The type of process used in the environment  |
| "deployment"         | How the application was deployed.<br>The possible values could be "PACKAGE" or "DOCKER". |
| "installed_packages" | A list of the installed Percona packages.  |

The information includes the following:

- Package name
- Package version - the same format as Red Hat Enterprise Linux or Debian
- Package repository - if possible

The package names must fit the following pattern:

- `percona-*`
- `Percona-*`
- `proxysql*`
- `pmm`
- `etcd*`
- `haproxy`
- `patroni`
- `pg*`
- `postgis`
- `wal2json`

## 8.2.5 Disable telemetry

Telemetry is enabled by default when you install the software. It is also included in the software packages (Telemetry Subsystem and Telemetry Agent) and enabled by default.

If you don't want to send the telemetry data, here's how:

### Disable the telemetry collected during the installation

If you decide not to send usage data to Percona when you install the software, you can set the `PERCONA_TELEMETRY_DISABLE=1` environment variable for either the root user or in the operating system prior to the installation process.

Debian-derived distribution    Red Hat-derived distribution    Docker

Add the environment variable before the installation process.

```
$ sudo PERCONA_TELEMETRY_DISABLE=1 apt install percona-server-mongodb
```

Add the environment variable before the installation process.

```
$ sudo PERCONA_TELEMETRY_DISABLE=1 yum install percona-server-mongodb
```

Add the environment variable when running a command in a new container.

```
$ docker run -d --name psmdb --restart always \
-e PERCONA_TELEMETRY_DISABLE=1 \
percona/percona-server-mongodb:<TAG>
```

The command does the following:

- `docker run` - This is the command to run a Docker container.
- `-d` - This flag specifies that the container should run in detached mode (in the background).
- `--name psmdb` - Assigns the name "psmdb" to the container.
- `--restart always` - Configures the container to restart automatically if it stops or crashes.
- `-e PERCONA_TELEMETRY_DISABLE=1` - Sets an environment variable within the container. In this case, it disables telemetry for Percona Server for MongoDB.
- `percona/percona-server-mongodb:<TAG>-multi` - Specifies the image to use for the container. For example, `5.0.29-25-multi`. The `multi` part of the tag serves to identify the architecture (x86\_64 or ARM64) and use the respective image.

## 8.2.6 Disable telemetry for the installed software

Percona software you installed includes the telemetry feature that collects information about how you use this software. It is enabled by default. To turn off telemetry, you need to disable both the Telemetry Agent and the Telemetry Subsystem.

### Disable Telemetry Agent

In the first 24 hours, no information is collected or sent.

You can either disable the Telemetry Agent temporarily or permanently.

[Disable temporarily](#)    [Disable permanently](#)

Turn off Telemetry Agent temporarily until the next server restart with this command:

```
$ systemctl stop percona-telemetry-agent
```

Turn off Telemetry Agent permanently with this command:

```
$ systemctl disable percona-telemetry-agent
```

Even after stopping the Telemetry Agent service, a different part of the software (Telemetry Subsystem) continues to create the Metrics File related to telemetry every day and saves that file for seven days.

### Telemetry Agent dependencies and removal considerations

If you decide to remove the Telemetry Agent, this also removes the database. That's because the Telemetry Agent is a mandatory dependency for Percona Server for MongoDB.

On YUM-based systems, the system removes the Telemetry Agent package when you remove the last dependency package.

On APT-based systems, you must use the `'-autoremove'` option to remove all dependencies, as the system doesn't automatically remove the Telemetry Agent when you remove the database package.

The `'-autoremove'` option only removes unnecessary dependencies. It doesn't remove dependencies required by other packages or guarantee the removal of all package-associated dependencies.

### Disable the Telemetry Subsystem

To disable the Telemetry Subsystem, set the `perconaTelemetry` server parameter to `false`. You can do this in one of the following ways:

 Configuration file     Command line     `setParameter` command

Use the `setParameter.perconaTelemetry` parameter in the configuration file for persistent changes:

```
setParameter:
  perconaTelemetry: false
```

Use the `--setParameter` command line option arguments for both `mongod` and `mongos` processes. The server starts with the telemetry Subsystem disabled:

```
$ mongod \
  --setParameter perconaTelemetry=false
$ mongos \
  --setParameter perconaTelemetry=false
```

Use the `setParameter` command on the `admin` database to make changes at runtime. The changes apply until the server restart.

```
> db.adminCommand({setParameter: 1, "perconaTelemetry": false})
```

 **Tip**


If you wish to re-enable the Telemetry Subsystem, set the `perconaTelemetry` to `true` for the `setParameter` command.

## PERCONA

### 8.2.7 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 August 8, 2024

 November 9, 2023

## 8.3 Copyright and licensing information

### 8.3.1 Documentation licensing

Percona Server for MongoDB documentation is (C)2016-2023 Percona LLC and/or its affiliates and is distributed under the [Creative Commons Attribution 4.0 International License](#).

### 8.3.2 Software license

Percona Server for MongoDB is [source-available software](#).

## PERCONA

### 8.3.3 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

🕒 June 27, 2023

🕒 December 8, 2022

## 8.4 Trademark policy

This [Trademark Policy](#) is to ensure that users of Percona-branded products or services know that what they receive has really been developed, approved, tested and maintained by Percona. Trademarks help to prevent confusion in the marketplace, by distinguishing one company's or person's products and services from another's.

Percona owns a number of marks, including but not limited to Percona, XtraDB, Percona XtraDB, XtraBackup, Percona XtraBackup, Percona Server, and Percona Live, plus the distinctive visual icons and logos associated with these marks. Both the unregistered and registered marks of Percona are protected.

Use of any Percona trademark in the name, URL, or other identifying characteristic of any product, service, website, or other use is not permitted without Percona's written permission with the following three limited exceptions.

*First*, you may use the appropriate Percona mark when making a nominative fair use reference to a bona fide Percona product.

*Second*, when Percona has released a product under a version of the GNU General Public License ("GPL"), you may use the appropriate Percona mark when distributing a verbatim copy of that product in accordance with the terms and conditions of the GPL.

*Third*, you may use the appropriate Percona mark to refer to a distribution of GPL-released Percona software that has been modified with minor changes for the sole purpose of allowing the software to operate on an operating system or hardware platform for which Percona has not yet released the software, provided that those third party changes do not affect the behavior, functionality, features, design or performance of the software. Users who acquire this Percona-branded software receive substantially exact implementations of the Percona software.

Percona reserves the right to revoke this authorization at any time in its sole discretion. For example, if Percona believes that your modification is beyond the scope of the limited license granted in this Policy or that your use of the Percona mark is detrimental to Percona, Percona will revoke this authorization. Upon revocation, you must immediately cease using the applicable Percona mark. If you do not immediately cease using the Percona mark upon revocation, Percona may take action to protect its rights and interests in the Percona mark. Percona does not grant any license to use any Percona mark for any other modified versions of Percona software; such use will require our prior written permission.

Neither trademark law nor any of the exceptions set forth in this Trademark Policy permit you to truncate, modify or otherwise use any Percona mark as part of your own brand. For example, if XYZ creates a modified version of the Percona Server, XYZ may not brand that modification as "XYZ Percona Server" or "Percona XYZ Server", even if that modification otherwise complies with the third exception noted above.

In all cases, you must comply with applicable law, the underlying license, and this Trademark Policy, as amended from time to time. For instance, any mention of Percona trademarks should include the full trademarked name, with proper spelling and capitalization, along with attribution of ownership to Percona Inc. For example, the full proper name for XtraBackup is Percona XtraBackup. However, it is acceptable to omit the word "Percona" for brevity on the second and subsequent uses, where such omission does not cause confusion.

In the event of doubt as to any of the conditions or exceptions outlined in this Trademark Policy, please contact [trademarks@percona.com](mailto:trademarks@percona.com) for assistance and we will do our very best to be helpful.



## PERCONA

### 8.4.1 Get expert help

If you need assistance, visit the community forum for comprehensive and free database knowledge, or contact our Percona Database Experts for professional support and services.

 [Community Forum](#)  [Get a Percona Expert](#)

 June 27, 2023

 September 14, 2015