# **Influx DB 1.8.10 installation**

For Ubuntu/Debian users, add the InfluxData repository with the following commands:

*# influxdb.key GPG Fingerprint: 05CE15085FC09D18E99EFB22684A14CF2582E0C5*

wget -q https://repos.influxdata.com/influxdb.key

echo '23a1c8836f0afc5ed24e0486339d7cc8f6790b83886c4c96995b88a061c5bb5d influxdb.key' | sha256sum -c && cat influxdb.key | gpg --dearmor | sudo tee /etc/apt/trusted.gpg.d/influxdb.gpg > /dev/null

echo 'deb [signed-by=/etc/apt/trusted.gpg.d/influxdb.gpg] https://repos.influxdata.com/debian stable main' | sudo tee /etc/apt/sources.list.d/influxdata.list

Then, install and start the InfluxDB service:

sudo apt-get update && sudo apt-get install influxdb

sudo service influxdb start

Or if your operating system is using systemd (Ubuntu 15.04+, Debian 8+):

sudo apt-get update && sudo apt-get install influxdb

sudo systemctl unmask influxdb.service

sudo systemctl start influxdb

### [**Verify the authenticity of downloaded binary (optional)**](https://docs.influxdata.com/influxdb/v1.8/introduction/install/#verify-the-authenticity-of-downloaded-binary-optional)

For added security, follow these steps to verify the signature of your InfluxDB download with gpg.

(Most operating systems include the gpg command by default. If gpg is not available, see the [GnuPG homepage](https://gnupg.org/download/) for installation instructions.)

1. Download and import InfluxData’s public key:
2. curl -s https://repos.influxdata.com/influxdb.key | gpg --import
3. Download the signature file for the release by adding .asc to the download URL. For example:
4. wget https://dl.influxdata.com/influxdb/releases/influxdb-1.8.10\_linux\_amd64.tar.gz.asc
5. Verify the signature with gpg --verify:
6. gpg --verify influxdb-1.8.10\_linux\_amd64.tar.gz.asc influxdb-1.8.10\_linux\_amd64.tar.gz

The output from this command should include the following:

gpg: Good signature from "InfluxDB Packaging Service <support@influxdb.com>" [unknown]

## [**Configuring InfluxDB OSS**](https://docs.influxdata.com/influxdb/v1.8/introduction/install/#configuring-influxdb-oss)

The system has internal defaults for every configuration file setting. View the default configuration settings with the influxd config command.

**Note:** If InfluxDB is being deployed on a publicly accessible endpoint, we strongly recommend authentication be enabled. Otherwise the data will be publicly available to any unauthenticated user. The default settings do **NOT** enable authentication and authorization. Further, authentication and authorization should not be solely relied upon to prevent access and protect data from malicious actors. If additional security or compliance features are desired, InfluxDB should be run behind a third-party service. Review the [authentication and authorization](https://docs.influxdata.com/influxdb/v1.8/administration/authentication_and_authorization/) settings.

Most of the settings in the local configuration file (/etc/influxdb/influxdb.conf) are commented out; all commented-out settings will be determined by the internal defaults. Any uncommented settings in the local configuration file override the internal defaults. Note that the local configuration file does not need to include every configuration setting.

There are two ways to launch InfluxDB with your configuration file:

* Point the process to the correct configuration file by using the -config option:
* influxd -config /etc/influxdb/influxdb.conf
* Set the environment variable INFLUXDB\_CONFIG\_PATH to the path of your configuration file and start the process. For example:
* echo $INFLUXDB\_CONFIG\_PATH
* /etc/influxdb/influxdb.conf
* influxd

InfluxDB first checks for the -config option and then for the environment variable.

See the [Configuration](https://docs.influxdata.com/influxdb/v1.8/administration/config/) documentation for more information.

### [**Data and WAL directory permissions**](https://docs.influxdata.com/influxdb/v1.8/introduction/install/#data-and-wal-directory-permissions)

Make sure the directories in which data and the [write ahead log](https://docs.influxdata.com/influxdb/v1.8/concepts/glossary#wal-write-ahead-log) (WAL) are stored are writable for the user running the influxd service.

**Note:** If the data and WAL directories are not writable, the influxd service will not start.

The user running the influxd process should have the following permissions for directories in the [InfluxDB file system](https://docs.influxdata.com/influxdb/v1.8/concepts/file-system-layout/):

| **Directory path** | **Permission** |
| --- | --- |
| influxdb/ | 755 |
| influxdb/data/ | 755 |
| influxdb/meta/ | 755 |
| influxdb/wal/ | 700 |

Information about data and wal directory paths is available in the [Data settings](https://docs.influxdata.com/influxdb/v1.8/administration/config/#data-settings) section of the [Configuring InfluxDB](https://docs.influxdata.com/influxdb/v1.8/administration/config/) documentation.

## [**Hosting InfluxDB OSS on AWS**](https://docs.influxdata.com/influxdb/v1.8/introduction/install/#hosting-influxdb-oss-on-aws)

### [**Hardware requirements for InfluxDB**](https://docs.influxdata.com/influxdb/v1.8/introduction/install/#hardware-requirements-for-influxdb)

We recommend using two SSD volumes, using one for the influxdb/wal and the other for the influxdb/data. Depending on your load, each volume should have around 1k-3k provisioned IOPS. The influxdb/data volume should have more disk space with lower IOPS and the influxdb/wal volume should have less disk space with higher IOPS.

Each machine should have a minimum of 8GB RAM.

We’ve seen the best performance with the R4 class of machines, as they provide more memory than either of the C3/C4 class and the M4 class.

### [**Configuring InfluxDB OSS instances**](https://docs.influxdata.com/influxdb/v1.8/introduction/install/#configuring-influxdb-oss-instances)

This example assumes that you are using two SSD volumes and that you have mounted them appropriately. This example also assumes that each of those volumes is mounted at /mnt/influx and /mnt/db. For more information on how to do that see the Amazon documentation on how to [Add a Volume to Your Instance](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-attaching-volume.html).

### [**Configuration file**](https://docs.influxdata.com/influxdb/v1.8/introduction/install/#configuration-file)

You’ll have to update the configuration file appropriately for each InfluxDB instance you have.

...

[meta]

dir = "/mnt/db/meta"

...

...

[data]

dir = "/mnt/db/data"

...

wal-dir = "/mnt/influx/wal"

...

...

[hinted-handoff]

...

dir = "/mnt/db/hh"

...

### [**Authentication and Authorization**](https://docs.influxdata.com/influxdb/v1.8/introduction/install/#authentication-and-authorization)

For all AWS deployments, we strongly recommend authentication be enabled. Without this, it is possible that your InfluxDB instance may be publicly available to any unauthenticated user. The default settings do **NOT** enable authentication and authorization. Further, authentication and authorization should not be solely relied upon to prevent access and protect data from malicious actors. If additional security or compliance features are desired, InfluxDB should be run behind additional services offered by AWS. Review the [authentication and authorization](https://docs.influxdata.com/influxdb/v1.8/administration/authentication_and_authorization/) settings.

### [**InfluxDB OSS permissions**](https://docs.influxdata.com/influxdb/v1.8/introduction/install/#influxdb-oss-permissions)

When using non-standard directories for InfluxDB data and configurations, also be sure to set filesystem permissions correctly:

chown influxdb:influxdb /mnt/influx

chown influxdb:influxdb /mnt/db

For InfluxDB 1.7.6 or later, you must give owner permissions to the init.sh file. To do this, run the following script in your influxdb directory:

**if** [ ! -f "$STDOUT" ]; **then**

mkdir -p **$(**dirname $STDOUT**)**

chown $USER:$GROUP **$(**dirname $STDOUT**)**

**fi**

**if** [ ! -f "$STDERR" ]; **then**

mkdir -p **$(**dirname $STDERR**)**

chown $USER:$GROUP **$(**dirname $STDERR**)**

**fi**

*# Override init script variables with DEFAULT values*